Addis Ababa University

College of Natural Sciences

Modeling Smart Mobile Money Wallet and Offline Payment

Tadegew Bogale Mole

A Thesis Submitted to the Department of Computer Science in Partial Fulfillment for the Degree of Master of Science in Computer Science

Addis Ababa, Ethiopia

February 2016

Addis Ababa University

College of Natural Sciences

Tadegew Bogale Mole

Advisor: *Solomon Atnafu (PHD)*

This is to certify that the thesis prepared by *Tadegew Bogale*, titled: *Modeling Smart Mobile Money Wallet and Offline Payment* and submitted in partial fulfillment of the requirements for the Degree of Master of Science in Computer Science complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the Examining Committee:

Name	Signature	Date
Advisor: Solomon Atnafu (PhD),	_____	_____
Examiner: Dida Midekso (PhD),	_____	_____
Examiner: Yaregal Assabie (PhD),	_____	_____

Abstract

Nowadays advanced technologies like smart phones are growing rapidly and digital world is created so that the real world objects can be digitized and accessed more efficiently than the physical world. As a result, smart phones are expected to be at the heart of the new digital economy. With the high and continuous proliferation of smart phones with their ubiquity features and improvement of their hardware and software capacities, it is necessary and useful to design a new form of digital money considering the features of real world money since money is vital for all humankind. This enables citizens of the world to use digital money so that the paper money in the physical world can be eliminated and replaced by digital money in the digital world.

We proposed a model for a Smart Mobile Money Wallet and Offline Payment that can realize a smart money. The smart money we designed exactly reflects the most important features of the real world material money such as serial number, economic value, icon, and signature, which is not currently available in today's digital money platform. The proposed model enables to withdraw, deposit, pay, and receive smart money anywhere at any time. Based on a proposed model, Smart Birr wallet and Smart Bank that shows all the features of the model are developed considering the Ethiopian currency, Birr. Elliptic curve cryptography technology, advanced encryption standard, and biometric based authentication are used to achieve security requirements for open-air communication.

Finally, experiments are conducted in order to test the feasibility of the proposed approach. The processing time experiment result showed that 5.62, 17.8, 606.02, 566.5, and 1471.6 milliseconds processing time is required in order to generate, detect, withdraw, deposit, and pay particular Smart Birr respectively which is affordable by the current computing devices and considerably low CPU and memory utilization is required. In the usability experiment, 97% of participants have agreed that Smart Birr wallet has higher usability than cash.

Keywords: Smart Mobile Money Wallet, Mobile Money Security, Offline Payment, Smart Money Model, Smart Birr

Dedicated To

My Beloved Family and Yalemzewd Mulugeta.

Acknowledgments

I would like to thank almighty God and offer special acknowledgement and heartfelt regards for his remedies for my sickness and his responses for my prayer in each and every bit of my troubles throughout my life and accomplishment of this thesis.

I also would like to offer my special appreciation and thanks to my advisor Dr Solomon Atnafu for his especial and generous commitment, and great contribution throughout this research. He has played a great role and encouraged me to develop independent thinking, be creative and have tremendous research skills. I never forget his patience, generous personality, inspiring guidance, constructive comments and fatherly advices in a numbers of issues throughout my study.

The role of my family for my achievement throughout my life cannot be expressed in words. They are printed in my heart throughout my life and may God listen to my prayer to protect and bless them.

I would like to express my deep love from the bottom of my heart throughout my life for Yalemzewd Mulugeta and I would like to appreciate her treatment and her family prayer for the achievement of this work.

I would like to provide my special thanks for Zewiditu Sisay and her sister Fetle for their unforgettable contribution for this work.

I would like to thank my beloved brothers Erimias Bogale, Desalegn Atnafu, Birhanu Abebe, Fasil Gidaf, H/Mariam, Melaku Fessie, and Jemal Hassen for their contribution and involvement in one or another way for the success of this research work.

Last but not the least, I would like to thank all especially my beloved teachers who have paid a lot of sacrifices and played a great role in order to change my attitude throughout my education life.

Table of Contents

List of Figures ..... **iii**

List of Tables ..... **iv**

List of Algorithms ..... **iv**

1 Introduction **1**

1.1 Background 1
1.2 Motivation 4
1.3 Statement of the Problem 5
1.4 Objective 6
1.5 Methodology 7
1.6 Scope and Limitations of the Study 7
1.7 Application of Results 8
1.8 Thesis Outline 9

2 Literature Review **10**

2.1 What is Money? 10
2.1.1 Material money 11
2.1.2 Electronic Money 13
2.1.3 Mobile Money 13
2.1.4 Virtual Money 16
2.2 Digital Payment 17
2.2.1 Electronic Fund Transfer (EFT) 18
2.2.2 Smart Card based Payment 18
2.2.3 Mobile Based Payment 19
2.3 Security in Digital Money 21
2.3.1 Digital Payment Security Requirements 21
2.3.2 Trends of Mobile Payment Authentication 22
2.4 Tools and Technologies 23
2.4.1 Communication Technology for Online Mobile Payment 23
2.4.2 Communication Technology for Offline Mobile Payment 23
2.4.3 Cryptography Technology 23
2.5 Summary 26

3 Related Work **27**

3.1 Mobile Money Business Model 27
3.1.1 Bank Centric Model 27
3.1.2 MNO Centric Model 28
3.1.3 Hybrid Model (MNO/Bank Model) 29
3.2 Mobile based Payment Architectures 29
3.2.1 EMV Mobile Payment Architecture 30
3.2.2 UICC based Mobile Payment Architecture 31
3.2.3 Embedded-SE based Mobile Payment Architecture 32

3.2.4 Cloud based Mobile Payment Architecture 33
3.3 Reviews of Related Work 34
3.4 Summary 40
4 Modeling Mobile Money Wallet and Offline Payment 41
4.1 The Conceptual Design 41
4.2 The Model for the Smart Mobile Money Wallet and Offline Payment 42
4.2.1 User Interface Component 45
4.2.2 Client-Side Security Subsystem 45
4.2.3 The Smart Mobile Wallet Subsystem 50
4.2.4 Smart Money Transaction Engine 60
4.2.5 Smart Money Object Generator 61
4.2.6 Server-Side Security Subsystem 63
4.3 Database Design 64
4.3.1 Wallet Database Design 64
4.3.2 Server Database Design 66
4.4 Summary 68
5 Experiment 70
5.1 Tools and Technologies used for Development 70
5.2 Proposed Model Components, Implementation Details and Demonstration 75
5.2.1 Smart Birr wallet Security Guard Engine 75
5.2.2 Smart Birr wallet Registration Engine 76
5.2.3 Smart Birr wallet Withdrawal Engine 78
5.2.4 Smart Birr Wallet Payment Engine 79
5.2.5 Smart Birr Wallet Deposit Engine 81
5.3 Proposed Model prototype Performance Evaluation 83
5.4 The Prototype Usability Testing 88
5.5 Summary 91
6 Conclusions and Future Works 92
6.1 Conclusion 92
6.2 Contributions 93
6.3 Future Works 93
Reference 95
Annexes 103
Annex A: Questionnaires 103
Annex B: Java Code Used to Create Smart Birr 104
Annex C: Sequence Diagram to Process Smart Birr Withdrawal 106
Annex D: Sequence Diagram to Process Smart Birr Deposit 107
Annex E: Sequence Diagram to Process Smart Birr Payment 108

List of Figures

Figure 2.1: Evolution of Money 11
Figure 2.2 : Features of Ethiopian money bills of 100 ETB 12
Figure 3.1: EMV Mobile Payment Architecture 30
Figure 3.2: Overall Architecture of UICC based Contactless Payment 31
Figure 3.3: Overall Architecture of Embedded-SE based Contactless Payment 32
Figure 3.4: Overall Architecture of Cloud based Contactless Payment 33
Figure 3.5: Overall Architecture of Mobile Wallet 37
Figure 3.6: Mobile Client and Mobile Banking Platform Architecture Components 38
Figure 4.1: High Level Conceptual Design of the Smart Mobile Money System 42
Figure 4.2: The Model for Smart Mobile Money Wallet and Offline Payment 44
Figure 4.3: The Structure of the Withdrawal Transaction Request Message 53
Figure 4.4: The Structure of the Message for Smart Money Deposit Request 58
Figure 4.5: Smart Mobile Money Wallet Entity Relationship Diagram 65
Figure 4.6: Wallet Database Model 66
Figure 4.7: Server Side Entity Relationship Diagram 67
Figure 4.8: Server Side Database Model 68
Figure 5.1 Smart Birr Wallet Icon 75
Figure 5.2: Smart Birr wallet Welcome User Interface 75
Figure 5.3: User Authentication User Interface 76
Figure 5.4: User Registration User Interface 77
Figure 5.5: Smart Birr Wallet Services User Interface 77
Figure 5.6: Smart Birr Withdrawal Service User Interface 79
Figure 5.7: Smart Birr Wallet Payment Service User Interface 80
Figure 5.8: Smart Birr Wallet Deposit Service User Interface 81
Figure 5.9: Smart Birr Wallet Transaction Flow 82
Figure 5.10 : Evaluation of Processing Time for Generating Smart Birr 85
Figure 5.11: Evaluation of Processing Time for Validating Smart Birr 85
Figure 5.12 : Evaluation of Processing Time for Processing Smart Birr Withdrawal 86
Figure 5.13: Evaluation of Processing Time for Processing Smart Birr Deposit 87
Figure 5.14: Evaluation of Processing Timefor Processing Smart Birr Payment 88
Figure 5.15: Usability Testing Experiment Result 90

List of Tables

Table 2.1 : Some Examples of Mobile Money Applications in Emerging Economies 15
Table 2.2: Comparison between Electronic Money and Virtual Money 17
Table 2.3: Performance Comparison between RSA and ECDSA 25
Table 5.1: Client Side Testing Environment Requirements 84
Table 5.2: Server Side Testing Environment Requirements 84
Table 5.3: Demographic Statistics of Participants for Usability Testing 90
Table 6.1: Demographic Survey Questionnaire 103
Table 6.2: Usability Survey Questionnaire 104

List of Algorithms

Algorithm 4.1: Algorithm to Authenticate Smart Mobile Money Wallet User 47
Algorithm 4.2: Algorithm for Detecting Smart Money 48
Algorithm 4.3: Algorithm to Encrypt Plain Message 50
Algorithm 4.4: Algorithm to Decrypt the Message 50
Algorithm 4.5: Algorithm to Register a User 52
Algorithm 4.6: Algorithm for Smart Money Withdrawal Process 55
Algorithm 4.7: Algorithm for Smart Money Offline Payment Process 57
Algorithm 4.8: Algorithm for Smart Money Deposit Process 60
Algorithm 4.9: Algorithm to Generate Smart Money Object 62
Algorithm 4.10: Algorithm to Authenticate Request Message Sent from Users 64

Abbreviations

ACH	Automatic Clearing House
AES	Advanced Encryption Standard
API	Application Program Interface
ATM	Automatic Teller Machine
CA	Certification Authority
CSC	Common Short Code
DES	Data Encryption Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Standard
EFT	Electronic Fund Transfer
EMV	Europa, Mastercard and Visa
ESB	Enterprise Service Bus
FATF	Financial Action Task Force
MMS	Multimedia Messaging Service
MNO	Mobile Network Operators
MPA	Mobile Payment Application
NFC	Near Field Communication
OOD	Object Oriented Design
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point Of Sale
RFID	Radio Frequency Identification
SAFE	Secured Application for Financial Environment
SE	Secured Element
SIM	Subscriber Identity Module
SMS	Short Message Service
SP	Service Provider
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSM	Trusted Service Manger
TSP	Token Service Provider
UICC	Universal Integrated Circuit Card
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol

Chapter 1

Introduction

This chapter presents background of the research, the statement of problem, as well as the research objectives that the researchers should achieve. It also presents and highlights the research methods, scope and limitation, and finally the organization of the thesis.

1.1 Background

As pointed out in [1], mobile phone is expected to be at the heart of the new digital economy and has already involved in many aspects of daily life by creating a range of new business opportunities and services. As a result, mobile phones are becoming the most required and widely used devices in history of humankind. Mobile phones can play a great role in financial transaction such as mobile banking and mobile payment, which includes sensitive information. Due to the proliferation of mobile phones, more applications such as Short Message Service (SMS), Mobile Internet, Multimedia Messaging Service (MMS), mobile commerce, and mobile banking are becoming commonplace [2]. As stated in [3], around 55% of all mobile phones sold in the second quarter of 2013 were smart phones and there were around 1.5 billion smart phones in use by the end of 2013. It is estimated that the number of smart phone connections in Africa will rise from about 79 million at end of 2012 to 412 million by 2018 [4]. As pointed in [5], there are several options for mobile payment but there is no dominating method. The same authors [5] state that mobile payment methods are sure to be the next standard form of payment, and it will be a practical, convenient, easy-to-use alternative to cash in the near future. As a result, mobile phones can facilitate the best opportunities like mobile money service to economically disadvantaged or isolated communities and some of the world's poorest countries in Africa.

According to the study by Santi [6], the world is getting closer fast and competition is increasing. As a result, some traditional business models in the world will not survive anymore and others, currently unimaginable, will emerge. Nowadays, the user is global and mobile, and the marketplace is larger in the virtual world than it is in the physical. Looking at the trend, one can

anticipate that it may only take few years to see mobile money service as the norm rather than a technological extravaganza. However, the realization of mobile money service for broader set of population requires intensive research and innovations to create user friendly, convenient, and secure approaches of mobile money services so that humankind including the less educated can carry digital money in their mobile phone and be able to perform payment anytime, anywhere for any available services.

Money is a driving engine for our life. The way we access, manage, and use it in the daily transaction can increase or decrease our productivity. Commonly, people should carry cash during long and expensive trips with the risk that the cash can be lost or stolen; physical currency may be exposed to forgery; it is easily damaged; its printing cost is expensive; it is a means to bacteria transmission; it serves for short period of time; and so on. For example, as stated by Mesfin Woldemariam et al. [7], people in remote rural area use jars, envelopes, or boxes to maintain money physically. Due to this fact, physical money becomes dirty and damaged so that it loses its features like economic value, images/icons, and security symbols. As a result, during financial transaction, individuals reject/refuse to accept payments of old paper money. Digitizing money reduces such constraint in a way that everybody can easily access, use, and manage money digitally in every day transaction. This helps to improve the transaction to be more secure, easy, and convenient for users.

Understanding of the barriers and the drivers influencing the adoption of electronic banking and commerce in developing countries are critical [8]. Africa is lagging behind in the adoption of electronic commerce as indicated in different research statistics [9-14]. As Gardachew Worku et al. [15] briefly state it; Ethiopian financial transaction is one of the most underdeveloped compared to the rest of the world. In Ethiopia, cash is still the most dominant medium of exchange and electronic payment systems are in their early developmental stage. The modern electronic banking methods like Automated Teller Machine (ATMs), debit cards, credit cards, Internet banking, mobile banking and others are not yet well matured enough in the Ethiopian banking sector. However, from the public and the economy there is a strong need for strengthening linkages among banks in order to allow healthy flow of financial resources among financial institutions and increase the contributions of the entire financial system to the development processes as a whole. The other important critical issue is that services such as online shopping and electronic offline payments are not yet introduced. This is particularly due

to the very slow adoption of technologies in electronic payment systems , the non-integration of local banks with both domestic and international banks, and lack of regulations. Ethiopian commercial banks are not accessible and available to the majority of the population living in remote rural areas. Even the proportion of banks and their accessibility and availability to the people living in the big cities is not yet satisfactory.

According to [15,16], low level of Internet penetration and poorly developed telecommunication infrastructure, lack of suitable legal and regulatory framework for electronic commerce and payment, high rates of illiteracy, high cost of Internet, absence of financial networks that links different banks, lack of reliable power supply, largely cash-based economy, problems of money laundering, and cyber security issues are the major challenges for the development of electronic banking and development of digital money as whole, in most of the African countries including Ethiopia. Hence, the researchers recommend that addressing these issues and introducing convenient digital money structure is necessary to bring significant solutions to reduce the major problems for usage of digital money.

The definition of mobile money services vary across the banking industry as it covers a wide scope of overlapping applications [17]. In general, mobile money is a term describing electronic financial services performed via a mobile phone. It can be used to assist the billions of people who have little or no access to traditional financial services. Mobile money service can enable users to pay bills, make bank transactions, transfer funds, and purchase goods and services. It can have a great role to bring financial services into rural villages and in everyday retail stores, thus alleviating the lack of banking infrastructure and fill huge gaps in developing countries. It can also avoid high transaction costs faced by banks to set up branches or ATM machines in areas with low infrastructure levels. According to the study in [17], mobile money services can be made highly accessible to all segments of society for three reasons: they are faster, more convenient, and cheaper than formal financial services in addition to their ubiquity features. However, all the current mobile money services require improvement in their usability, security, nature of money representation and payment methods.

As a result, with high continuous proliferation of smart phones and improvement of their hardware and software components, it is very necessary and useful to design inclusive mobile

money wallet and payment scheme that enables the broader set of people to use digital money instead of paper money in their daily life.

1.2 Motivation

Nowadays, technology is becoming advanced and improving rapidly so that the digital world is created and the real world objects can be digitized and accessed more efficiently than the physical world. For instance, smart phones, with increasing software and hardware capabilities, have achieved the task of everywhere computing and are playing a great role to bring different important tasks in our daily life into one device. For example, they can provide many capabilities to the user in order to access financial information and make transaction, accept calls and surf the web, notify appointments, provide direction and maps. Moreover, smart phones enable users to process and manage digital multimedia information such as texts, photos, and videos with satisfactory storage capacity and computing power.

However, the old form of money that is used by the broader citizens throughout the world cannot be fully digitized and replaced by a new form of digital money completely so far. It is clear that this old form of money such as Ethiopian Birr and American Dollar is a paper-based form of money used by broader citizens that are not completely removed from the market even though different forms of electronic representations such as electronic cards are introduced and used in order to represent the old form of money electronically. However, such kinds of electronic money available currently, highly demands expensive infrastructure for the widely adoptions worldwide and are not easy as old form of money to be used by broader citizens. Because the old money is not properly digitized and created in the digital world encapsulating their abstract features such as color, serial number, and economic value.

As a result, the main motivation of the research is to digitize the old form of money being used in the physical world by creating a new form of smart money in the digital world and develop smart mobile money wallet that can be used to withdraw, deposit, and pay smart money.

1.3 Statement of the Problem

According to the study in [18], digital payment systems had not received broader attention as a research topic over the past decade given the relative stability and well-defined roles that exist in the industry. Recently, they have attracted growing attention, and research on the use of mobile money services and their easier access to financial services is required [17]. As the use of mobile phones for money transfer is relatively recent, there are no comprehensive studies on the subject apart from the analysis focusing on specific countries, sectors, and case studies. For example, mobile money systems, like M-PESA [19] in Kenya, Easy Paisa [20] in Pakistan, MTN [21] and WIZZIT [22] in South Africa, EKO [23] in India, and Orange Money [24] in Côte d'Ivoire clearly indicate the rates and uses of mobile money even if all of the current mobile money have their own shortcoming and need robust research. All the current mobile money linked with paper money and cannot completely digitize and avoid the paper money. As a result, paper money is still the dominant means of money representation and commodity exchanging.

The paper money used worldwide nowadays is expensive to print, distribute, collect, and keep in the store. It is exposed for damage and forgery. It serves for short period of time. It is also one of the means of bacterial transmission that may harm human life. As a result, in the twenty first century where digital world is replacing the physical world and technology is becoming advanced, the paper money should be digitized and created in the digital world in understandable way that can totally eliminate the paper money in the physical world.

As it is briefly presented by Mesfin Woldemariam et al. in [7], existing digital money is represented in floating number only and does not incorporate metadata/features of paper money into the structure of digital money. The authors argue that the absence of features of paper money in the digital money affects its usability and acceptability by the broader citizens. Due to this, broader citizens especially in developing countries face a huge challenge to use mobile money solutions. The current mobile money solutions have not considered paper money bill's metadata like icons or images, color, security means, and serial numbers, etc. Such absence of metadata made money bill identification and transactions difficult for less educated users since they validate and develop trust on money bills through the images/icons inscribed on them and through color of money bills. As a result, the structures of current mobile money are not easy to understand by less educated users [25] but the broader set of people including the illiterates can use paper money in the real world that indicates the digital money should be structured keeping

the structures of paper money. In addition, Gardachew Worku et al. [15] argue that low literacy rate is a serious impediment for the adoption of Electronic banking (E-banking) in Ethiopia as it hinders the accessibility of banking services which is similar to most Africa countries. For citizens to fully enjoy the benefits of digital money, they should not be required to know how to read and write but also have basic computer literacy. As a result, lack of digital money structure is major and potential problem identified to be solved by digitizing the paper money with its basic features such as serial number, icon, and economic value.

Therefore, the main purpose of the research is to create smart money by digitizing paper money with its basic features so that paper money can be totally eliminated in the physical world and replaced by smart money in the digital world. As a result, legalized and authorized virtual smart bank is created in order to manage smart money.

1.4 Objective

General objective

The general objective of this research is to design a model for smart mobile money wallet and offline payment that can facilitate the use of digital money to the broader citizens in an economy in a more secured and reliable manner.

Specific objective

In order to achieve and reach the ultimate purpose of this general objective successfully, the following specific objectives will be accomplished.

- Review literature and related works to identify the current practices and technologies.
- Identify the existing available digital money models focusing on mobile money.
- Identify components of the model and specify their functionalities
- Develop the necessary algorithms that can be used in the implementation of the designed model.
- Identify appropriate tools and technologies to employ security techniques
- Develop a smart mobile money wallet and offline payment system based on the designed model incorporating the appropriate technologies and tools for the implementation.

- Design a user-friendly interface that can be easily learned and used by broader set of citizens.
- Evaluate the usability of the prototype

1.5 Methodology

This section briefly presents the methodologies and tools that are used to design, implement, and evaluate the proposed system.

Review Literatures

Review literatures and related works will be used to understand all the significant scientific concepts and current findings in the field to find gaps and identify problems. Accordingly, limitations of those studies and the approaches they have used will be reviewed. From the recent and relevant literatures and related works, useful concepts and design requirements will be identified to design the model of the proposed work. Furthermore, appropriate tool and technologies that can be used for the design of the model will be identified.

Design and Development Approach

Object Oriented Design (OOD) with component model, class model, object model, and sequence diagram will be used in order to design and develop the proposed model prototype. An interactive object oriented programming paradigm using java will be used to develop and implement all the system design components accurately.

Evaluation Approach

Performance of the proposed system will be evaluated in terms of processing time and memory space required to complete the main operation of the proposed system. Moreover, purposive sampling will be used to evaluate the usability of system prototype.

1.6 Scope and Limitations of the Study

The main concern of the research is to design and develop a generic smart mobile money wallet and offline payment system for smart phone's supporting android platform.

The research mainly focuses on building strong security techniques, model smart mobile money, wallet, and design transaction protocol in order to provide the following functionalities:

- Withdraw cash
- Deposit cash
- Pay offline for goods and services
- Verify the digital money for validity

However, as a limitation, the research does not consider online shopping and transaction. Though the model is generic, the implemented prototype is specifically for Android smart phones. Interoperability of various hardware and software platforms are not considered.

1.7 Application of Results

This work plays a valuable role in mobile money ecosystem. It proposes a system that serves like the physical wallet. The smart mobile money wallet can be installed in any Android smart phone in order to manage digital cash and make offline payment to a system that uses the same application. The server side application acts as a bank, while the smart phone serves as a wallet in users pocket in order to withdraw, deposit cash and pay offline in a secured status.

This work will create a mobile money transaction by creating secured and effective money transfer to contribute to both local and global development. It eliminates the time that users need to go to bank to withdraw or deposit money. It permits users to carry their money in their smart phones to make any payment anywhere to a person or organization that uses the same system. This shows the possibility created by the system for a full essence of digital money. The system is also designed for use by a broader citizens irrespective of their education background as the easy-to-use user interface shows the images of the material money bills as the transaction is being made.

In general, the result of this work will have tangible and practical application for business processing to create a cashless society and promote a wide adoption of mobile money transaction.

In order to first change the physical paper money to smart money, the legal body authorizes the service provider so that the service provider exchanges the users' paper money by smart money. Assume that National Bank of Ethiopian (NBE) authorizes the Smart Bank as a service provider

so that the Smart Bank can then get authority to exchange the paper money by smart money. As presented in Chapter 5, the prototype is developed for Ethiopian currency notes by creating digitized Smart Birr for each currency notes such as 100 birr, 50 birr, 10 birr, 5 birr, 1 birr, 50 cent, 25 cent, 10 cent, 5 cent, and 1 cent currency notes. As a result, users can request the Smart Bank in order to change their paper money by Smart Birr.

1.8 Thesis Outline

The remaining part of the thesis is organized as follows.

In Chapter 2, reviews of recent literatures that are relevant for the research are presented. This chapter discusses the important concepts about forms and evolution of money, payment schemes, security techniques, and tools and technologies that are introduced so far. Moreover, gaps and findings related to these concepts are briefly discussed.

In Chapter 3, more related and recent works for the research are explained. This chapter presents more related and scientific works with their gaps in detail. The chapter explains mobile money business models namely bank centric, MNO centric and hybrid model with their risks and problems. Very recent mobile-based payment architectures are also discussed in this chapter.

In Chapter 4, a novel model for smart mobile money wallet and offline payment system is designed and presented in detail. It also illustrates and explains the roles and functions of each components of the model with their interaction and the algorithms that show how they can be implemented.

In Chapter 5, implementation of the designed model as system prototype for the Ethiopian currency is presented. This system, which implements a Smart Birr wallet, demonstrates the different features of the model for a practical mobile money transaction. The tools and techniques that have been used for the implementation are stated and descriptions are given. In this chapter, the evaluation and experimental results of the proposed model prototype performance from different perspectives are also presented. Usability testing is also presented in this chapter. In addition, the requirements of testing environment and testing procedures are illustrated.

Lastly, conclusion, contributions, and future works are presented in Chapter 6.

Chapter 2

Literature Review

This chapter presents the summary of very relevant literatures concerning main concepts on the existing forms of money, payment systems, security techniques, and technologies used in digital money systems in order to provide insight into trends of the current digital money ecosystem. Section 2.1 elaborates the definition and evolution of money, the current forms of money with their detail drawbacks. Section 2.2 presents the details of digital payment schemes especially in mobile payments. Section 2.3 discusses and analyses the security requirements and the security holes in the digital money ecosystem especially in mobile money. Finally, Section 2.4 presents technologies and tools used in the current digital money ecosystem especially in mobile money, and proven technologies available for further improvement and advancement of digital money are presented in detail.

2.1 What is Money?

The definition of the term "money" in particular concerning its form is still a hotly discussed economic subject. Apart from the general concepts, different researchers introduce new definitions and ideas of money. Money has three criteria and a number of purposes in society [27, 28]; first, money must serve as a medium of exchange. Second, money must serve as a store of value: it is a way to store value for convenient future use. Finally, money must serve as a unit of account, which you need in order to measure and compare prices.

The words money[1] and currency are most commonly used interchangeably and often synonymously, but they have different meanings. Money is simply a means of communicating value, while currency is the physical manifestation of money.

Money has taken many different forms throughout history. Early, societies used natural money just like salt for exchanging goods. Later, societies turned to precious metals like gold and silver for use as money. As Figure 2.1 depicts, the paper money used nowadays almost in all societies was introduced in 1700 AC. Without discarding the paper money, symbolic system money, that

[1] http://web.archive.org/web/20010410032230/http://www.goldmoney.com/futuremoney.html#intro

is representation of paper money electronically, uses as a means of payment in electronic commerce in the present. For the future, as stated in [29], it is expected that the digital cash will completely replace the paper money. However, the vital question is that how we can realize the digital cash that is understandable and easy to use for all humankind especially for the illiterates and the less educated society. This is because it is a serious problem for less educated users to use the current digital money systems in their everyday money practices since formats of the current digital money and their accessing techniques are changing and becoming complex in the digital ecosystem. Figure 2.1 [29] shows a possible classification of money evolution process.

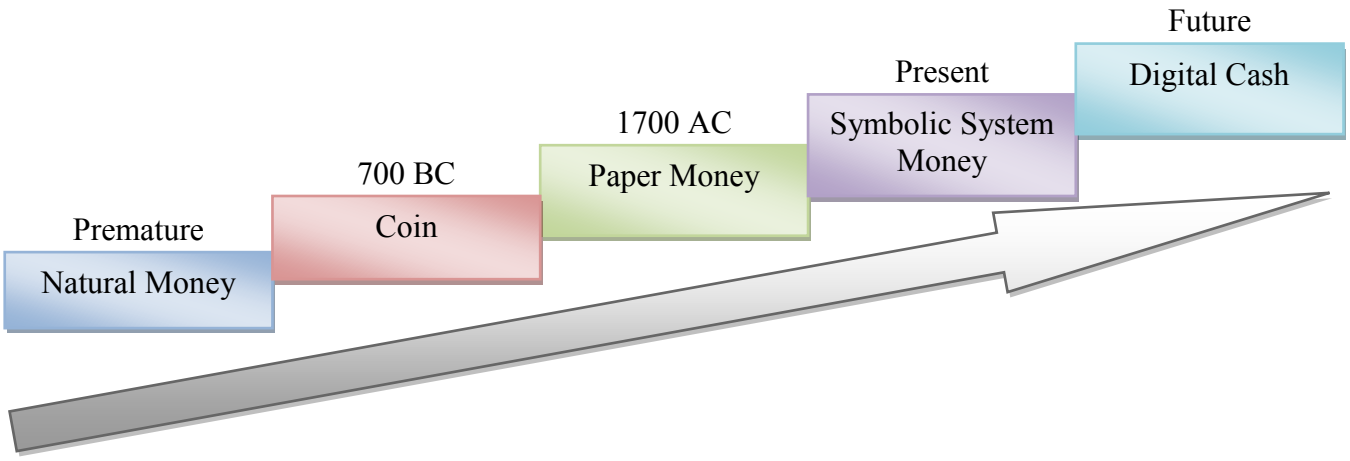


Figure 2.1: Evolution of Money

For further discussion and interpretation of different forms of money from different perspectives such as their existence, forms, usability and accessibility, we classify money into four main types as material money, electronic money, mobile money, and virtual money.

2.1.1 Material money

Material money is physical money used to represent the value of money in the real world, that is, the physical materials such as paper and metal represent the value of money. It has appearance and shape depending on the value of money it represents. This kind of money is well known and matured all over the world to the present. For example, existing currencies, such as Ethiopian Birr and US Dollar are used by the mass. The material money perfectly meets the three criteria of money mentioned in Section 2.1.

Different researchers [7, 9, 39] used different terms for material money like material money, cash, paper currency, paper money, physical currency, and physical money interchangeably. The term material money is used in this research for the sake of consistency.

Mesfin Woldemariam et al. [7] argue that material money objects have their own features that describe and distinguish them from other objects; and they argue that these features must exist and appear in digital money for easy understanding and usability to enable the mass including illiterate users to identify money bills. The main features are color, size, images and icons, security tools, national identifier, serial number, and numbers indicating economic value, and monetary governing body. Figure 2.2 shows the metadata of Ethiopian material money for one hundred Birr. These features, in Ethiopia, enable less educated users to distinguish between different money bills. For example, illiterate individuals know the sum of 10 Ethiopia Birr (ETB) and 5 ETB will give 15 ETB but they do not know how to write these numbers. When they are also asked to pickup money bills of say 100 birr from list of money bills with different denominations, they easily identify these through color and size. As a result, features of material money have main role and are easy to identify that should be considered in designing digital money.

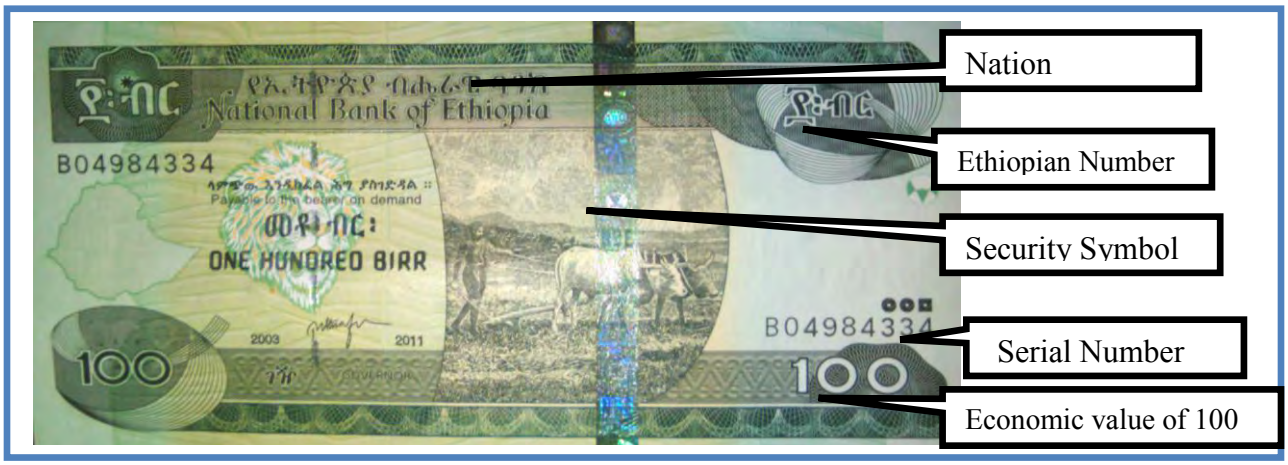


Figure 2.2 : Features of Ethiopian money bills of 100 ETB

Problems Associated with Material Money

Material money requests huge investment for printing, keeping on the shelf, moving from place to place, and protecting from illegal use and robbery. It is exposed to easy damage. Because of this, it loses its actual features used to identify material money. When the bills get old, security

features usually fade away and may not be visible, which makes differentiating forgery from valid money bills difficult [7]. As a result, users do not accept it and users refuse the payment. Users are also exposed for bacterial contamination. In general, the material money is expensive to print, distribute, manage, and protect it against forgery.

2.1.2 Electronic Money

Electronic money can be defined broadly as monetary value stored electronically, on a card, or in a computer for use over a computer network such as the Internet. Electronic money is described as a broader concept that refers to payments made using contactless cards, credit cards, prepaid cards, debit cards, automated teller machines (ATM), as well as mobile phones. It is a digital alternative to cash and it is not unique money, that is, the electronic money does not exist alone without the existence of material money or it is denominated with the material money. As it is briefly discussed in [30], Electronic Fund Transfer (EFT), payment cards, credit cards, debit cards, and smart cards are means of electronically representing money and use it for electronic transaction. The forms of all the current electronic money are represented digitally in terms of floating number only. Unlike material money, electronic money has no size, shape, and appearance. Instead, it is represented in number in the digital devices. This creates challenging problems especially for illiterate users who cannot read and write.

2.1.3 Mobile Money

Mobile money, subset of electronic money, is a term describing the services that allow electronic money transactions over a mobile phone and it is a money that can be accessed and used via mobile phone [31, 35]. It is also referred to as mobile financial services, mobile wallet, and mobile payment.

According to the works in [31, 32, 33], mobile money services can be broadly categorized into three groups as mobile banking, mobile money transfer, and mobile payment. Mobile banking is use of a mobile phone remotely to access a bank account for using financial services, primarily for account balance checkup and bill payment services. Mobile money transfer typically refers to services whereby customers can use their mobile devices to send and receive money or to transfer money electronically from one person to another using a mobile phone and real-time online communication with the server. Mobile payment (commerce) is a use of a mobile phone

to perform financial transactions for purchases or sales, either remotely or on site, retrieve promotion information or coupons, or deliver gift items.

A. Access Channels of Mobile Money Platform

As it is discussed and elaborated in [33,34], the main access channels currently employed for mobile money platforms are Short Message Service (SMS), SIM ToolKit (STK), Unstructured Supplementary Service Data (USSD), and Wireless Application Protocol (WAP).

The default data format for SMS messages is plain text. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. The encryption algorithm used for SMS is A5[2], which has proven to be vulnerable. SMS is not the ideal platform for making payments because of security issues, as messages travel and are stored on the mobile device in plain text without encryption [34]. SMS is the most commonly used application in mobile money transfers in developing countries for low-value payments. However, for developing countries in rural areas where the literacy rate may not be high, the application should be simple, to enable people to understand how to use it.

In case of STK, pass code or PIN is needed to access the application, which is stored on the SIM card. Besides SMS, STK can also use USSD as a data carrier, but it is dependent on the STK implementation on the particular handset.

USSD, unlike SMS, is more responsive in the sense that data are delivered and responses obtained in real-time. USSD is also session-oriented, which has the advantage that it will inform the user whether a message has reached the recipient or not. However, the message is still sent in plain text as in SMS and exposed for attack.

WAP-based implementations, however, can provide better security, as data are encrypted between the customer and the merchant/bank. WAP implementations are more common with banks adding mobile as another channel for users to access their accounts. Encryption in SMS and USSD communications is not necessarily end-to-end, creating vulnerabilities at various points where data can be intercepted, read and acted on by third parties.

[2] https://en.wikipedia.org/wiki/A5

In general, all access channels rely on the use of a Personal Identification Number (PIN) for transaction authentication. As a result, the risk of security in mobile payments may require new authentication technologies such as digital signature, voice recognition, and fingerprinting to verify identification, particularly at vulnerable points of a transaction when cash withdrawals may be conducted.

B. Examples of Mobile Money Platform

In the present, different mobile money applications are available in different countries. Table 2.1 [33] shows some examples of well-known mobile money application with their main features and technologies used.

Table 2.1 : Some Examples of Mobile Money Applications in Emerging Economies

Mobile money application	Countries implemented	Main features	Technology
M-PESA[3]	Kenya, Tanzania, South Africa and Afghanistan	P2P transfers, pay school fees, pay electricity bills, pay for goods and services	STK, USSD
Airtel Money[4]	Indian and 14 Africa countries including Uganda, Tanzania, and Kenya	Make P2P transfers, pay for goods and services, and make bill payments	USSD
MTN Mobile Money[5]	In many Africa countries including Uganda, Ghana, Cameroon, Ivory Cost, Rwanda and Benin	P2P transfers, buy air time, check balances, and pay utility bills	USSD and STK
Easy paisa[6]	Pakistan, South Africa	P2P transfers, pay utility bills, save money, increase air time credits, and pay for goods and services	P2P transfers

[3] www.vodacom.co.za/vodacom/services/financial-solutions/m-pesa
[4] www.airtel.in/money
[5] https://www.mtn.com
[6] www.easypaisa.com.pk/en/money-transfer

2.1.4 Virtual Money

According to [36], virtual money is a type of unregulated digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. This type of digital money is not denominated in any national currency and is not as anonymous as cash. Since such types of virtual money also do not mimic the formats of material money and requires high level of literacy, they are difficult for wide adoptions especially for illiterate societies. As it is stated in [28], the current virtual money such as Bitcoin does not satisfy the three main criteria of money discussed in Section 2.1. It is very volatile and therefore unreliable as a store of value.

In various research papers [36, 38, 39], different terms such as digital cash, electronic cash, virtual currency, digital currency, crypto currency, and virtual money are used interchangeably with the same logic and definition. In this thesis, in order to avoid confusion and inconsistency, we use the term virtual money.

According to [27, 31, 36], virtual money is ideally expected to satisfy properties like security, privacy, transferability, offline payment, divisibility, anonymity, and independency. As pointed out in [37], virtual money is an interesting concept in the security community even if it has not taken off until nowadays. In contrast to material money, virtual money does not have all of the attributes of material money and does not have legal tender status in any jurisdiction. As a result, virtual currency does not meet the criteria to be considered money [39].

A. Comparisons among Electronic Money and Virtual Money

In electronic money schemes, the link between electronic money and fiat currency against which it is issued remains intact, that is, it is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. Electronic money is a digital transfer mechanism for fiat currency, that is, it electronically transfers value that has legal tender status. In virtual money schemes, by contrast, the unit of account has no physical fiat currency counterpart [36]. Table 2.2 [36] shows the comparisons among electronic money and virtual money.

Table 2.2: Comparison between Electronic Money and Virtual Money

Criteria	Electronic Money	Virtual Money
Format	Digital	Digital
Units of account	Fiat currencies (USD, ETB, EUR)	Invented currency (Bitcoins[7], LiteCoin[8], FairCoin[9],etc.) without legal tender status
Means of production	Digitally issued against fiat currency of central authority	Mined/mathematically generated
Issuer	Legally established electronic issuer (which may be financial institution)	Community of people/miners
Legal status	Regulated	Unregulated
Supply of money	Fixed	Not fixed (depends on issuer's decisions)
Types(s) of risk	Mainly operational	Legal credit liquidity and operational

2.2 Digital Payment

A payment at its most basic level is the transfer of money or wealth or value from one person or entity to another. Banks provide payment options and services for their customers. Customers have always been able to use different bank branches to make their payments through bank tellers, ATMs, online banking, and mobile banking [40]. An example of using branches includes the option of making payments through cheques. Apart from previously mentioned, use of ATMs is also very popular in the world today. The introduction of this form of payment was aimed at helping individuals make large payments through the bank to avoid moving around with large chunks of money. However, in recent years, evolutionary changes have taken place where

[7] https://bitcoin.org/
[8] https://litecoin.org/
[9] https://fair-coin.org/

introduction of other forms of payments have emerged. This section reviews the major payment forms and types evolved so far.

2.2.1 Electronic Fund Transfer (EFT)

Electronic funds transfer [30] is one of the oldest electronic payment systems. EFT is the groundwork of the cash-less and check-less payment scheme where paper bills, checks, envelopes, and stamps are eliminated. EFT is used for transferring money from one bank account directly to another without any paper money changing hands. The most popular application of EFT is that instead of getting a paycheck and putting it into a bank account, the money is deposited to an account electronically.

2.2.2 Smart Card based Payment

A smart card is used to process payment using electronic card, made up of a plastic with an embedded microprocessor chip that holds important financial and personal information. Since 2005 contactless payment technologies [41] have been emerging, including ExpressPay[10], Visa payWave[11] and MasterCard PayPass[12]. These technologies mainly use NFC as a new communication means to the already available credit card network, and are online payment applications. Credit and debit cards are one of the smart cards frequently used for payment nowadays.

Smart cards are broadly classified into two categories as contact and contactless smart cards.

Contact smart cards must be inserted into a special card reader to be read and updated. A contact smart card contains a microprocessor chip that makes contact with electrical connectors to transfer the data. In contrast, contactless smart cards can be read from a short distance through radio frequency. A contact-less smart card also contains a microprocessor chip and an antenna that allows data to be transmitted to a special card reader without any physical contact.

One of main problems of smart card based payment is that they do not support transfer of money between cardholders. The main reasons for this are security concerns and the fact that card readers must be involved. Moreover, they are also exposed to theft and lose.

[10] https://expresspaygh.com/howItWorks.php
[11] www.visapaywave.com.au/
[12] www.mastercard.com/contactless/

2.2.3 Mobile Based Payment

Recently, mobile payments have emerged as a new method of transaction and have led to new payment systems, leveraging the explosive growth of mobile phones [42]. Mobile payment is defined as payment for products or services between two parties for which mobile phone plays a key role in the realization of the payment. Mobile payment is divided into two types namely, proximity or remote mobile payment. Proximity mobile payment is termed contactless payment in which payment information is stored on the mobile phone [42, 43]. Remote mobile payment occurs when mobile device used to make purchase does not interact with the merchant's POS [44, 45].

A. Mobile Proximity Payment

Proximity payment occurs while the customer is on site in a physical retail environment, which can be either an attended POS station or an unattended location such as a kiosk or vending machine. Types of mobile proximity payments include Near Field communications (NFC), barcode payment, and numeric-code payments [45].

Unlike smart cards, all of the hardware and data required to make payments reside on the customer's smart phone in case of NFC based payment. The user begins payment by entering a PIN and choosing a payment account, and then holds the device within a few inches of the retailer's contactless POS terminal.

In case of barcode-based payment, the customer begins by registering for an account and the information can be stored on the retailer's own server or can be stored on a third party server. Then the retailer scans a 2-D transaction bar code provided by the customer in order to match the transactions on the server, and the payment is processed. In barcode-based payment, mobile/POS software integration requirements can result in the customer having to download different apps for use with different POS systems, thus inhibiting the adoption of barcode payment. Additionally, even with an educated user, the system is subject to any connectivity, software, and hardware problems that might slow down transactions and creates complexity.

In case of numeric code payment, a code is delivered via SMS that authorizes a payment initiated by the customer. During registration, the customer receives a Common Short Code (CSC) specific to the customer's account. Then when the customer decides to make a purchase at the store, he/she sends a message to the CSC number, which returns a message containing a

purchase authorization code. The customer then gives the authorization code to the cashier, who enters it into the POS system as a mobile purchase request. Consequently, POS system validates the authorization code. As a major drawback, this payment scheme requires real time mobile network and exposed to security breaches.

Major limitations of mobile proximity payments are [42]:

- Currently, there are no technologies that support the use of a proximity payment device to receive cash and store in the device for later payment than payment information.
- In order for payment beneficiaries to spend the funds available via the proximity payment device, merchants and/or vendors must have matching POS devices.

B. Remote Payment

Mobile remote payments are payments to a retailer that take place remotely online while the customer is not present in a physical store environment. Types of mobile remote payment include message-based payments, browser based payment, and application based payments [45].

Message-based payment is done through SMS or Multimedia Messaging Service (MMS). The customer initiates the purchase with a message. Then the merchant sends a return text with billing information. The customer sends confirmation message back to the merchant to accept billing amount and the transaction is complete. As chief advantage, this payment method can work on any text-enabled device, which is virtually any mobile phone. As chief disadvantage, transaction cost, communication time, inconvenience, and security breaches are critical problems [45].

With browser-based remote payment, customers make an online payment using their mobile phone just as they can make it using desktop computer through web browsers. The customer uses browsers and selects the payment method to enter payment information. This information is then sent securely to the payment processor via Secure Socket Layer (SSL) protocols. Accordingly, a confirmation page appears to let the customer know the transaction has been successfully completed. In contrast to SMS based payment, this payment method has stronger security through SSL protocol. As a drawback, web browsers may be unreliable, and may not work on any kind of smart phones [45].

Application-based remote payment allows the customer to make a payment via a retailer's proprietary smart phone applications, which the customer is required to download. Accordingly, payment is processed using the application installed in the customers' smart phone. As a drawback, this payment method requires high communication cost and infrastructure [45].

Major limitations of mobile remote payment are [42]:

- Cash Access: Currently, there are no technologies that support the use of a remote payment device to receive cash without converting the digital payment to physical cash through an agent.
- Infrastructure**:** Network coverage is required for payment beneficiaries to execute transactions using a mobile device.
- Network Interoperability: Many providers of mobile remote payments services operate alone within a single MNO network. As a result, payment beneficiaries will have difficulty receiving or using funds in areas where multiple providers exist.

2.3 Security in Digital Money

Security is one of the major concerns in the adoption of mobile payment since the adoption and wide spread application of mobile payment depends on the strength of security. This section presents requirements of security and trends of mobile payment authentication.

2.3.1 Digital Payment Security Requirements

In order to keep a digital payment system secure, seven security requirements that any security service should be able to accomplish are outlined in [46, 47]. These are:

- Confidentiality: The confidentiality of sensitive information needs to be protected. Unauthorized people should not be able to gain access to confidential material.
- Integrity: Mobile service providers need to protect the integrity of data transmitted over wireless networks from the point of transmission to the point of delivery. The system should be able to check that the data is the same at the points of origin and destination.
- Availability: This is about ensuring that services are available on demand. This is related to security because a security breach causes denial of available services, for example denial of service attacks.

- Non-repudiation: Non-repudiation ensures transactions are legally binding.
- Authorization: Authorization ensures that transactions are authorized by the parties involved.
- Authentication: Authentication is the process of identifying the user to be whom they claim to be.
- Privacy: Privacy is a prominent issue in mobile money that must meet the legal requirements.

With the above security requirements, authentication is a basic building block of security, that is, once the authenticated communication channels are established, other security services such as confidentiality, privacy, authorization, integrity and non-repudiation can be realized [48]. As a result, the compromise of the authentication service breaks down the whole security system on which the provision of other services cannot proceed. Especially, security over the mobile platform is more critical due to the open nature of wireless networks [49]. Therefore, designing a strong security solution for mobile platform is highly required.

2.3.2 Trends of Mobile Payment Authentication

Today in all kinds of mobile money, consumers are given an opportunity to define a 4-character PIN to authorize different transactions so that there is no protection when a consumer loses his/her mobile phone to fraudsters who are able to figure out their PIN [34]. The traditional technologies used to achieve digital payment authentication are knowledge-based methods (e.g., PINs and passwords) and token-based methods (e.g., keys and cards) [26, 50]. Most users set their passwords based on words or digits that they can easily remember such as names and birthdays of family members, and dictionary words. Such passwords are easy to crack by guessing or by a simple brute force dictionary attack[13]. Although it is recommended to use different passwords for different applications and change them frequently, most users use the same password across different applications without changing for long time. As a result, if a single password is compromised, it may result in security breaches in many applications.

[13] https://en.wikipedia.org/wiki/Dictionary_attack

2.4 Tools and Technologies

2.4.1 Communication Technology for Online Mobile Payment

Recent researches like [35] suggest that technological change in the form of less expensive phones and expanded network coverage made mobile money feasible. The most basic technology, as discussed in Section 2.1.3, used for long-distance fund transfer are SMS, USSD, STK, and WAP .

2.4.2 Communication Technology for Offline Mobile Payment

There are various proximity communication technologies to exchange data. However, Bluetooth RFID, and NFC [51, 52, 53] are the common technologies that are selected to be discussed in this section.

NFC is a standard short-range bidirectional wireless communication technology that allows data to be exchanged between devices located a few centimeters apart [51]. Any NFC enabled device can communicate with other NFC devices and with any existing Radio Frequency IDentification (RFID)[14] infrastructure. Compared to RFID and Bluetooth technologies that have a much larger range, NFC has a higher degree of security [52]. Bluetooth is extremely dangerous and can open up vulnerabilities for simple uses that do not require such large distances for transmission, like mobile payments. It is readable at large distances. As a result, a shorter transmission range with stronger security makes NFC a more appealing choice [53].

Bluetooth is a popular short-range communication technology that enables mobile devices to communicate with each other at the distance of up to 80 meters that is to long as compared with 5 cm distance of NFC [54].

2.4.3 Cryptography Technology

Cryptography is a key enabling technology that enables the design of most modern security protocols. The fundamental objective of cryptography is to enable two parties to communicate over an insecure channel while ensuring that a third party cannot understand what is being sent or transferred so that unintended audiences cannot read, understand, or alter the message [55].

[14] http://www.technovelgy.com/ct/technology-article.asp

A cryptography technology helps to provide and achieve almost all security requirement, listed in Section 2.3.1. Symmetric-key cryptography and public key cryptography are the two main categories of cryptography [56].

A symmetric-key cryptography works on the basis that the same key is shared between the sender and the receiver. The two primary types of symmetric-key cryptography are stream ciphers and block ciphers. A block cipher transforms a block of plaintext with a fixed size into a block of cipher text with equal length whereas stream cipher operates on data stream and encrypts a digital data stream one bit or one byte at a time [57]. Data Encryption Standard (DES), double DES, triple DES, and Advanced Encryption Standard (AES) are examples of block cipher algorithms [58]. AES provides a greater security than its symmetric key predecessor does and at key lengths of 128, 192, and 256. AES makes elliptic curve cryptography systems even more secured and attractive [59]. The main problem with symmetric-key cryptography is that the sender and receiver have to share the same secret key. If they are in separate physical locations, it is difficult to establish secured transmission medium to protect the secret key. Anyone who overhears or intercepts the secret key in transition can read, modify, or falsify messages encrypted with that key.

In a public key cryptography, each party gets a pair of keys; one of them is referred to as the public key and the other as the private key [60, 61]. Each party's public key is published while the private key remains secret. All communications involve only public keys and no private key is ever transmitted. Then anyone who wishes to send a message to the holder of the associated private key will take the public key, encrypt a message under it, and send it to the owner of the corresponding private key. The receiver's public key ensures message confidentiality, and the sender's private key signs the message that ensures non-repudiation.

The digital signature is one application of public key cryptography that is used to sign the message to be sent and verify it using private and public key respectively. A digital signature includes three process steps: a key generation process, a signature signing process, and a signature verifying process. There are numerous digital signatures algorithms characterized by their high level of security and their speed to encrypt and decrypt data, their efficiency to generate signatures and verify the data integrity with reduced key sizes [59]. RSA [62] and ECDSA [63] are some examples of well-known and proven digital signature algorithms. RSA

and ECDSA as digital signature algorithms have proven their efficiency against cyber-attacks, they are characterized by their speed to encrypt and decrypt data, in addition to their competence at checking the data integrity [61]. For example, an elliptic curve over a 163-bit field currently gives the same level of security as a 1024-bit RSA [59].

In general, as it is stated and shown in Table 2.3 [61, 64], ECDSA offered the following remarkable advantages over other cryptographic system.

- It provides greater security with smaller key sizes.
- It provides effective and compact implementations for cryptographic operations requiring smaller chips.
- Due to smaller chips less heat generation and less power consumption.
- It is mostly suitable for machines having low bandwidth, low computing power, less memory and it has easier hardware implementations.

Table 2.3: Performance Comparison between RSA and ECDSA

Algorithm	**Security**	**Complexity**	**Domain**	**Key generation**	**Key Size**	**Computational cost**	**Performance**
RSA	High	Integer factorization	PC, laptop, super computers	Very slow	Larger	High	Slow
ECDSA	High	Discrete logarithm	Light-weight devices	Very Fast	Smaller	Low	High

2.5 Summary

This chapter reviewed varies relevant and related issues and concepts concerning the fundamental and general definitions and forms of money, digital payment methods, security requirements, tools and technologies in digital money ecosystem.

The reviews of literatures in this chapter show that all existing digital money, unlike real world material money, are represented in plain numbers or digits, which implies that the form of money in the current digital money ecosystem should be structured and designed in the computer system based on the real world money features.

In the digital payment schemes, electronic fund transfer, smart card based payment, and mobile-based payments are identified as well known payment schemes and the review shows that mobile payment is the promising and convenient payment approaches which needs to be improved and adopted since mobile proliferation is now increasing throughout the world.

This chapter also presented basic requirements of security in the digital money ecosystem such as authentication, confidentiality, non-repudiation, privacy, availability, and integrity. Among these security requirements, authentication is identified as a prerequisite and needs to be achieved properly in order to achieve other security requirements. It is also identified that PIN and token based authentications are the common methods of today's authentication techniques.

Finally, tools and technologies used to process digital payment are identified and discussed. As a result, NFC is identified as one of the novel appealing choice in the proximity mobile payments. The ECDSA cryptography technology is also identified as a proven, powerful, secure, and cheaper digital signature algorithm than others for lightweight devices for exchanging data over insecure communication channels. Moreover, it is identified that AES makes elliptic curve cryptography systems more secured and attractive than other encryption systems. These enabling technologies can be used to realize a secure mobile money transaction over an open air that is not realized in the mobile money ecosystem so far.

Chapter 3
Related Work

This chapter briefly discusses major relevant works related to our proposed work to provide insight into mobile money business models and mobile payment systems investigated and proposed in the last decade up to the present.

3.1 Mobile Money Business Model

More than 120 mobile financial services providers now offer mobile money services of various kinds [65]. Unfortunately, recent deployments of mobile money has led to a very few success worldwide. It implies that dealing with some financial products through mobile phones still require a basic level of financial literacy from poor low income and illiterate end-users. As a result, the current business models of mobile money should be analyzed and investigated to search for their gaps in order to propose appropriate solutions.

This section presents the current business models for mobile money systems namely bank centric model, mobile network operator (MNO) centric model, and hybrid model that are more related to this study. In addition, the problems or the risks of this current business models are also presented in detail to provide insight into challenging risks that must be solved for a wide adoption of mobile money.

3.1.1 Bank Centric Model

In a bank centric model, the bank or other formal financial institution is a role player and controller of the mobile money services. Each client is required to have an established account with the bank [42]. This model provides mobile access to normal banking services, such as balance inquiry, transfer between accounts, and payments. Access to financial service is through MNO based system where MNO provides a menu based communications services such as SMS in partnership with the bank, but is not involved in any underlying financial transactions [67]. An underlining gap in this model is that all cash in and cash out transactions require access to a bank

branch or ATM. This demands an expensive infrastructure to expand the service to a vast amount of customers especially in developing countries where access to formal institutions is limited.

In this model, three main integral components called the agent, bank, and end users participate and collaborate in the mobile money ecosystem during the transaction process. There is always a connection with a central system to complete a single transaction. In other words, the model does not support offline transaction.

3.1.2 MNO Centric Model

A MNO centric business model eliminates the involvement of the financial institution in the payment delivery, clearing, and settlement instead these are done through MNO's established agent network [67]. In emerging markets, mobile network operators are dominating the mobile money transfer market, creating the customer relationship and providing the service distribution channel, with clearing and settlement functions independent of financial institutions or central banks. Individual payment transactions occur entirely within the MNO and do not require the service user to have a bank account. This model expands in developing markets because of its ability to reach large number of unbanked people in physically remote locations beyond the presence of traditional banks infrastructures. The geographic reach of this model may be extended through bilateral and multilateral agreements with other wireless carriers, which allow them to expand their remittance services beyond their own geographic borders and regulatory jurisdictions. For example, Safaricom's M-PESA [69] represents successful model where the mobile operator controls and manages the payment system.

Like bank model, the MNO centric system typically relies on SMS based low value payments. Due to this fact, this model is exposed to security vulnerabilities [70] since it uses weak encryption algorithm and poor end-to-end security protocol. Another underlining gap in this model, like bank-centric model, is that all cash in and cash out transactions require access to agents which cause a serious security breaches and inconvenience.

In this MNO centric business model ecosystem, agent, MNO, and end users are the three components participating in the mobile money system. Like bank centric model, it is always connection based system for each single transaction.

3.1.3 Hybrid Model (MNO/Bank Model)

This model is a combination of bank and MNO models that offer communications and financial transaction services and combine characteristics of both the pure bank and pure MNO models [42, 67]. It is to mean that MNO based payment services handle payments internally with cash in/out through the MNO's agent network, yet link to formal banking services such as savings, loans and insurance in partnership with a regulated financial institution by enabling communications with the bank and transfers between the user's cell phone payment account and accounts at the bank.

In this model, the components participating for completion of each transaction are MNO, agents, bank, and end users. Unlike MNO and bank model, the transaction time in this model is slower and communication cost is expensive. Like other models, each transaction is carried out online.

As pointed out in [66, 67, 68], common challenging problems of these three business models of mobile money system are: too expensive service charges; risk of identity theft; agent charges customer unauthorized fees; customer cannot access cash from mobile money account due to lack of agent availability and lack of agent liquidity; lack of network interoperability; difficulty of using mobile money system by less educated customers; counterfeit cash; security is compromise; and no offline payment services.

In general, in these three models, service providers depend on agents for customer acquisition and for managing liquidity. It implies that agents access customer sensitive information such as the user name, mobile number and other credentials that are used for identification and authentication purpose. These agents are not well equipped to preserve customer sensitive information and can easily lead to information leakage. Any loss of control over protected or sensitive information by service providers is a serious threat to business operations as well as, potentially, customer security.

3.2 Mobile based Payment Architectures

In this section, the overall mobile payment and security architectures closely related to this study are discussed and presented in detail.

3.2.1 EMV Mobile Payment Architecture

Europa, Mastercard and Visa (EMV) mobile payment system architecture consist of customer's mobile device, issuer, acquirer and merchant's POS as major components. Figure 3.1 shows generic mobile payment system architecture as proposed by Temitope et al [70].

The authorization process helps to monitor mobile payment transactions to detect fraudulent use of mobile phone and PO terminal; and makes the decision regarding whether to approve or decline the transaction by validating the dynamic cryptogram. Clearing is the process of transferring payment transaction data between acquirer and issuer. The issuer will provide and deliver EMV compliant payment application to Secured Element (SE) of the mobile device during an over the air provisioning process. Mobile device personalization stage involves customizing payment application with customer payment information. Mobile device is used as payment token and it contains EMV compliant-payment application and cryptographic keys stored on tamper-resistant component of the mobile device called secure element. The secure element in the mobile device provides a tamper-proof environment for storing payment data, performing cryptographic functions, and achieving transaction security. The connection and data transmission between POS and mobile device is facilitated through NFC.

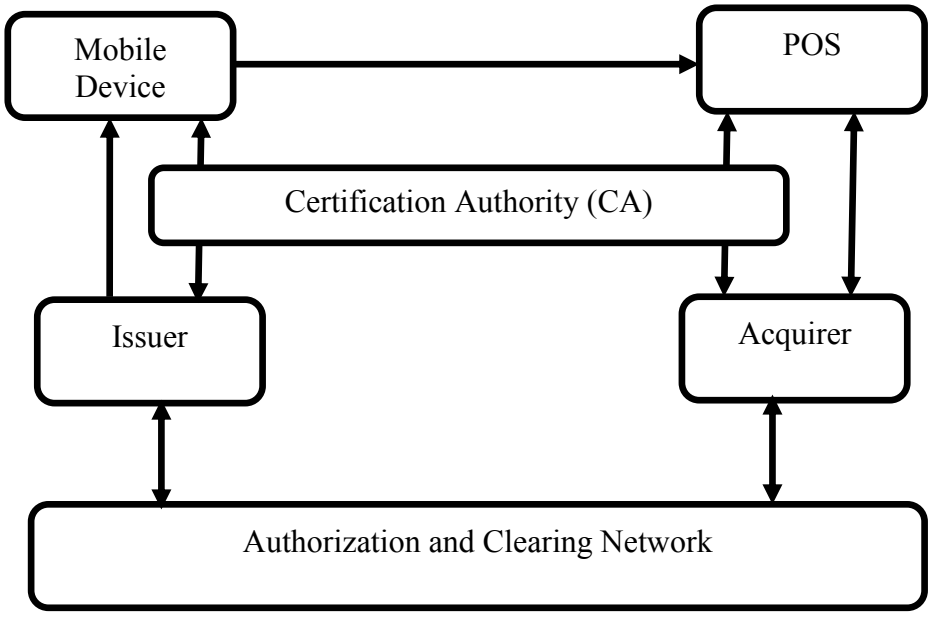


Figure 3.1: EMV Mobile Payment Architecture

Certification Authority (CA) is trusted entity that issues digital certificates to users. Both issuer and acquirer have their individual public key pairs. The CA authenticates the public keys

of both the issuer and acquirer. The POS terminal retrieves its stored copy of the CA public key and uses it to verify the issuer's public key certificate.

3.2.2 UICC based Mobile Payment Architecture

In Universal Integrated Circuit Card (UICC) based model, the payment card is emulated and the mobile payment application is hosted on UICC chip under MNO control. Figure 3.2 [71] shows overall architecture of UICC based mobile payment architecture. This model requires strong collaboration between different types of actors of the ecosystem at technical, commercial and branding levels such as MNOs as Trusted Service Manger (TSM) providers, issuers as card issuer and Service Provider (SP), payment schemes between issuer and acquirer for clearing and settlement.

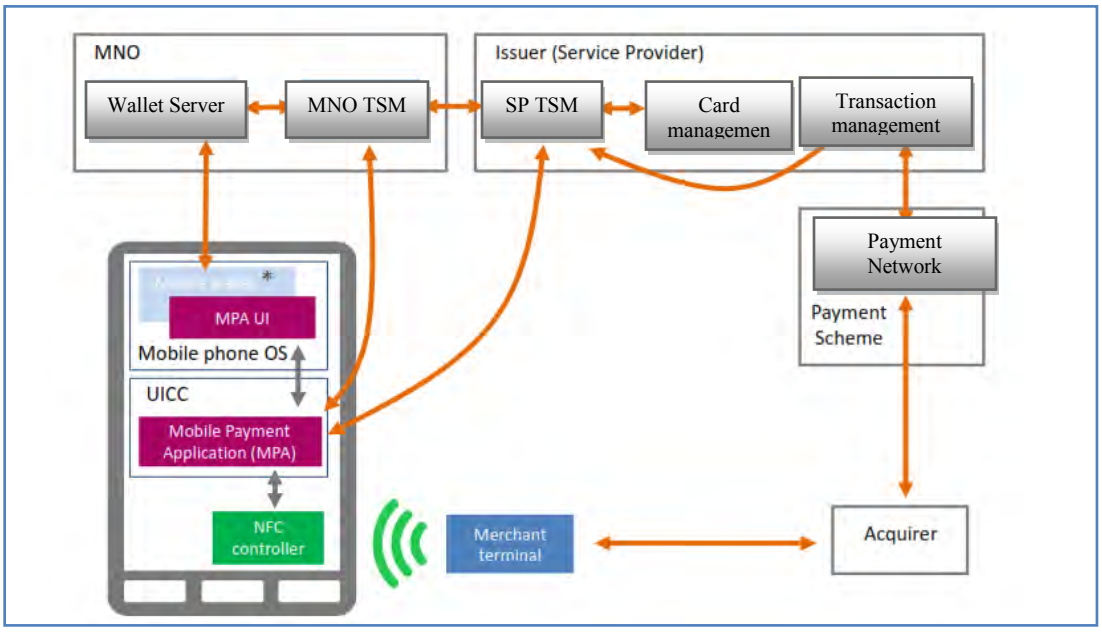


Figure 3.2: Overall Architecture of UICC based Contactless Payment

For the issuer, deploying UICC-based contactless payment services require commercial agreements for the use of the UICC with each MNO. The collaboration of different parties such as MNO, TSM, SP, and banks in the UICC-based ecosystem is required to complete a single transaction. This makes the system much complicated. In addition, as a major drawback, this architecture depends on system hardware called UICC for securing transaction that is expensive and vulnerable as well as it is less portable and interoperable.

3.2.3 Embedded-SE based Mobile Payment Architecture

This architecture allows owners of the phone to get a digitized card into their mobile device for performing contactless payments at participating merchants.

For instance, users can enroll by themselves to the Apple Pay service by adding one or more credit/debit cards into Passbook, Apple's wallet application [71]. The user can either select the credit/debit cards already in his/her mobile devices or add another credit/debit card by taking a picture of the card or manually entering his/her cardholder account data. This selected card must be an eligible card issued by a bank that contracted to Apple Pay services such as American Express, MasterCard, and Visa.

As Figure 3.3 depicts [71], this architecture relies upon an embedded SE-based architecture associated with the Payment Tokenization framework. The Mobile Payment Application (MPA) is hosted on an embedded Secured Element (eSE) and Secured Element Infrastructure (SEI).

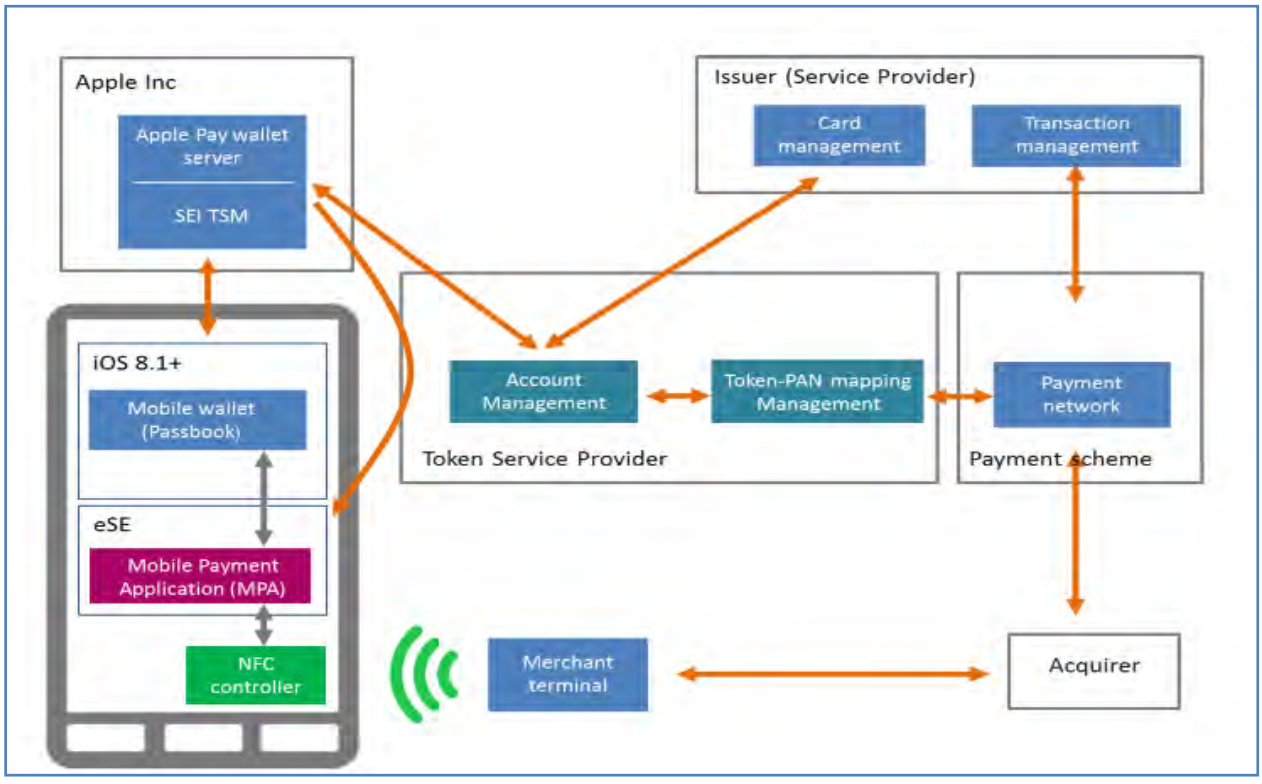


Figure 3.3: Overall Architecture of Embedded-SE based Contactless Payment

TSM allows the provisioning of the MPA into the eSE. The Account Management platform interfaces the different issuers with the Apple Pay platform and enables the card digitalization

process. As a major shortcoming of this architecture, the service is currently supported on iPhone 6 and iPhone6 Plus Smartphone's only [71]. Like UICC based model, this architecture depends on system hardware called SE for securing transaction that is expensive and vulnerable. It is also less portable and interoperable.

3.2.4 Cloud based Mobile Payment Architecture

This newly emerging architecture, as shown in Figure 3.4 [71], removed the dependencies that were created in the SE-based model. The payment credentials used to perform transactions are provided by a remote server (in the cloud) to the mobile application and are dynamically provisioned into the MPA before each transaction (or set of transactions).

Payment Tokenization allows replacement of the cardholder's Primary Account Number (PAN) by payment token, which is used in place of the PAN in payment transactions.

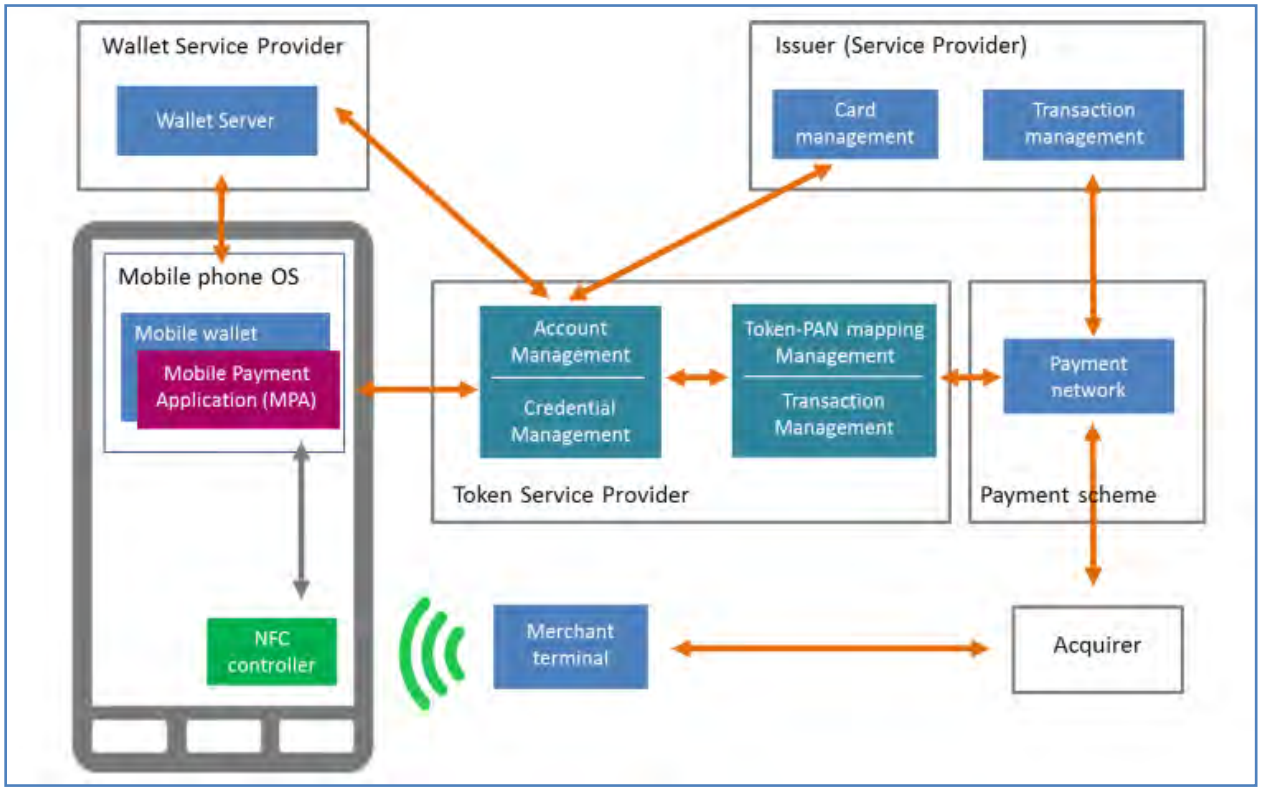


Figure 3.4: Overall Architecture of Cloud based Contactless Payment

In this architecture, the Wallet Service Provider in association with the Token Service Provider (TSP) and the issuer usually perform card digitization. The digitized card data (i.e. cardholder

account data, payment token, cryptographic keys) are provisioned into the credential management system of the TSP and the non-critical elements are downloaded into the MPA. Token-based transactions require a new actor, the Token Service Provider (TSP), to manage Token-PAN mapping, account, credentials, and transaction.

It is important to note that offline authorizations are not supported in this architecture, as the cloud-based payment model requires a systematic check of the Token Cryptogram by the TSP at each payment transaction [71]. Therefore, payment transaction is always authorized online. It means that offline payment and authorizations are not supported. As another shortcoming, cloud based architecture is unreliable than UICC and eSE based architecture since financial data and private data are stored somewhere in the cloud which is unreliable.

3.3 Reviews of Related Work

Mobile Money being a new research area, there is not that much empirical study on this topic [65]. As a result, relevant topics and research works that are closely related to this study are identified and discussed deeply in this section.

Gauthier V. et al in [72] proposed offline payment system based on digital vouchers using Near Field Communication (NFC) technology in mobile phones. The researchers used SE element to store customer's sensitive data and Public Key Infrastructure (PKI) for validating and exchanging data over the air through NFC. In this system, vouchers are made available in electronic format on a NFC-compatible device, allowing the user to pay electronically by touching a merchant's payment terminal with the NFC device. The electronic voucher (e-voucher) system consists of three types of actors, namely e-voucher issuers, e-voucher users (beneficiaries) and owners of payment terminals (affiliates). A beneficiary receives e-voucher from issuer through SMS based communication. Exchange of data and transaction between beneficiary and affiliate is done through NFC communication. The researchers used 3DES, RSA and SHA-1 cryptography algorithms for securing the transaction.

The followings are identified as major drawbacks of this research work.

- The system relies on extra hardware elements called secured element that has limited storage capacity and designed to store small amount of data such as customer credentials and cryptographic information.

- SMS is used to perform transaction between the issuer and receiver. SMS is not considered secure since the SMS message is not confidential and exposed for several attacks like man in the middle attack, spamming, and phishing [77, 78].
- PIN based authentication is used to protect the e-voucher against unauthorized users and to verify the transaction. As discussed in section 2.3.2, this kind of authentication can easily be hacked through social engineering and brute force attack [34, 50].
- As discussed in section 2.4.3, the cryptography algorithms used are computationally intensive and resource intensive for limited environment such as SE and mobile phones [59, 61, 64]. To establish the connection and complete the transaction process, it requires too much time and too many steps. The main reasons for this overhead lie in the cryptographic protocols used. The overhead of using RSA is significant reason for the unsatisfactory timings. The evaluation result shows that half of the transaction time is spent to perform asymmetric key operations.

Bossi M. in [73] proposed a Peer-to-Peer Strong Local Authentication Protocol (P2PSLAP) for mobile banking transaction that implements a peer-to-peer architecture to provide local authentication mechanism between the customer and the agent only. It is designed to authenticate participants (i.e. customer and agent) with mobile phones at point of interaction. Bluetooth is used as short-range communication technologies. After keys are generated through service provider server, they are sent over the air to the customers and agents. Then these keys are used to secure the transaction.

The followings are identified as major drawbacks of this research work.

- Insecure channel for key distribution and privacy issue: Since private and public key pairs are generated by service provider and sent over the network, the secret information is exposed for cyber attack during transmission in order to access the key pairs especially the private key that has to be secret for the owner user only. Moreover, keys can also be accessed by service provider and used for impersonate attack.

- Bluetooth is used for communication in the mobile payment. It is exposed and susceptible for vulnerability and attacks since it is a large range wireless communication technology that is exposed for man in the middle attack[15] and eavesdropping attack[16]

Xiaohua and Wenxue [74] proposed mobile wallet system architecture based on NFC. Figure 3.5 depicts their system overall architecture. The overall architecture of the mobile wallet system involves mobile wallet platforms, bank counter system, acquiring system, account management system, and mobile client software. Mobile wallet platform adds online and offline accounts. Online account is a temporary account for mobile wallet cash, that is, does not write its balance into the mobile wallet accounts whereas the balance of offline account is written into mobile wallet account for offline consumption. Mobile wallet account deducts the corresponding funds when people consume offline payments. POS terminal sends the consumer records to the acquiring system, then the acquiring system sends it to the mobile wallet platform in the bank. When the records are validated by mobile wallet platform, the offline account will deduct the amount. Mobile wallet platform sends the request to the bank account management system, when users make transaction. Then the bank account management system processes the transaction accordingly. As a result, the amount of offline account in mobile wallet platform is increased. If the operation makes successful, the system will notice the client software, the amount of mobile wallet account has been increased finally.

Account management system manages the ledger of banking institutions. Enterprise Service Bus (ESB) controls routing, changeover message and exception handling. Mobile wallet business system manages the ledger of mobile wallet system, liquidating the account of offline consumption, checking the account with bank account management system. Key management system is responsible for continuously generating asymmetric keys. The China union pay root Certificate Authority (CA) system is responsible for issuing the bank's certificates. The WAP gateway is responsible for protocol conversion between the WAP and WWW. Acquiring system is responsible for generating and sends the offline transaction information to collect and submit billing data etc. Bank counter system is responsible for increasing or canceling mobile wallet service.

[15] https://en.wikipedia.org/wiki/Man-in-the-middle_attack
[16] https://www.owasp.org/index.php/Network_Eavesdropping

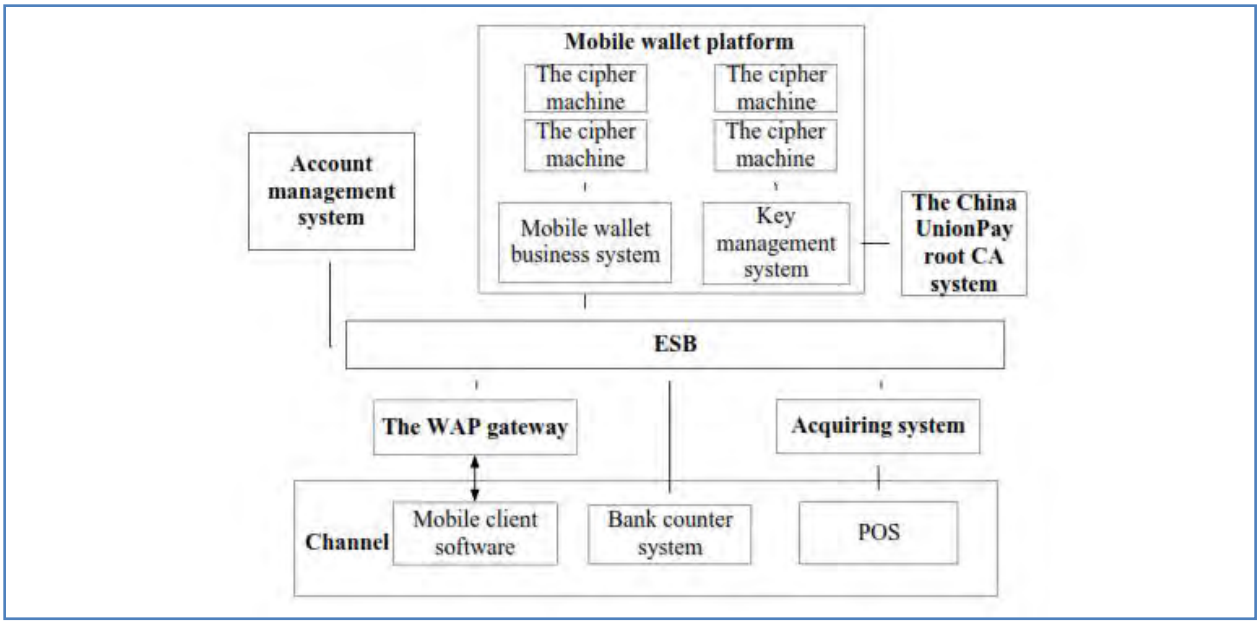


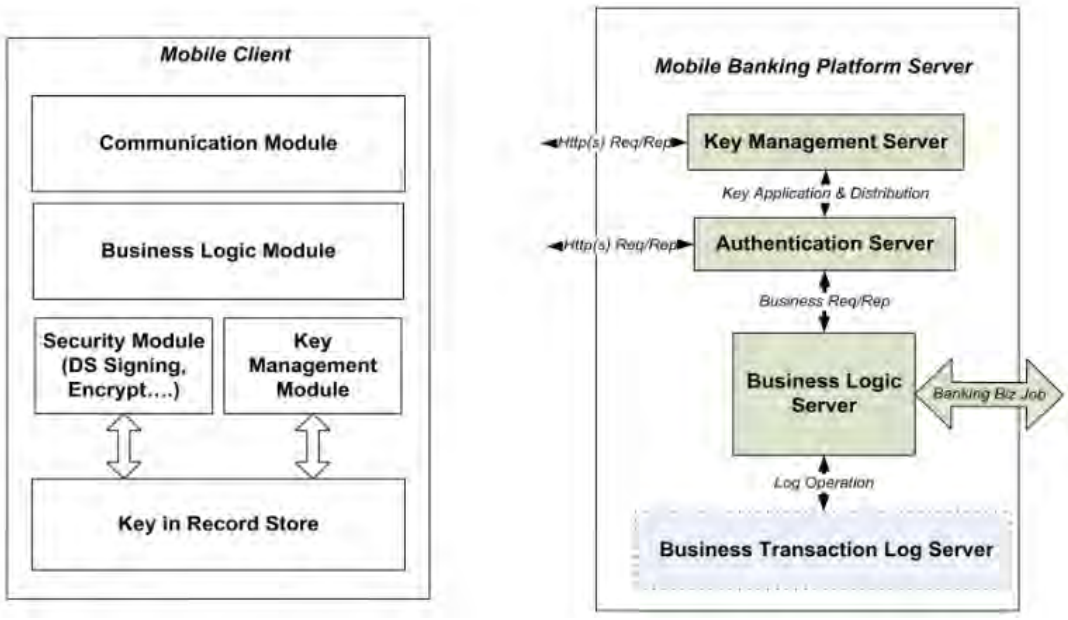
Figure 3.5: Overall Architecture of Mobile Wallet

The following are identified as major gaps of this research.

- High expensive infrastructure and communication is required to complete a given transaction. This system is mainly designed for the existing bank institutions that highly utilize expensive infrastructures such as POS, ATM, and bank branches in order to cash in and cash out. As a result, it is not accessible and used by the mass especially for those who are in the remote area where banks or ATMs are not accessible and available.
- It is not completely offline and cashes are not stored in the user mobile phone, that is, users cannot carry the digital money in their phone and use it for offline payment without third party involvement. PIN based authentication and authorization is also used in this system.
- The secret information is transferred through email that is exposed to spoofing and sniffing attack.

Y. Zhu proposed secured two-party mobile payments architecture between customer and payment service provider [75]. Figure 3.6 [75] (A) illustrates the detail architecture components of the mobile client application whereas Figure 3.6 (B) illustrates the detail architecture components of mobile banking platform server. The mobile client system consists of the business logic module for processing all business functions, the security module for handling security

issues, the communication module for handling information exchange between mobile client application and mobile banking platform server, and the key management module for managing, generating, and distributing keys.



(A) (B)

Figure 3.6: Mobile Client and Mobile Banking Platform Architecture Components

The mobile banking platform server consists of the business logic server to handle all business requests, the authentication server to provide the authentication service for the mobile banking platform server, the business transaction log server to create and maintain transaction log, and the key management server to store the public key, and initialize renewal process of a key pair.

Though this research work has strong security features, the followings are identified as major gaps of the proposed system.

- This research work only shows the communication and mobile money transaction between the client and the bank, that is, it has no any offline features for micro payments between customers.
- On the client side, nothing is stored except pairs of key, that is, digital money cannot be stored in the users' mobile phone and digital money is represented, transferred, and stored in the form of plain floating numbers which leads to inconvenience.

- The secret key is stored in a file without authentication that is exposed for attack. PIN is also used for user authentication and transaction verification.

Behzad P. et al proposed an architectural design for secure mobile banking [76]. The authors adopt and implement Secured Application for Financial Environment (SAFE) model. They also adopt account-based payment model, which is one of the payment models supported by the SAFE system.

This model includes customer, merchant, issuer or customer's financial service provider, and acquirer or merchant financial institution as an actor of the system. As the main features of the system, mobile pre-paid accounts (PPAs) are used to deposit and withdraw cash and for various mobile payments, so that a consumer can pay with an account associated with its mobile phone number through communication networks. When the customer intends to make a mobile payment transaction, he/she uses the wallet and select from which account they want to pay and the beneficiary account number. Then the value is debited from the account of the customer and is transferred to the merchant account.

Unlike the work proposed in [75], the sensitive information and cryptography keys are stored in removable secured hardware element and a location based authentication service is proposed.

The following are identified as major gaps of this research work.

- Specialized devices such as POS and SE are required in order to process transaction. Since SE is removable, it is exposed for improper use by an authorized user. During payment, the transaction is authenticated and authorized through users PIN that is easily breakable as mentioned before.
- SMS based communication is also used for exchanging sensitive information over the air that is easily breakable as mentioned before.
- The privacy of individuals is exposed and any other body can easily track them since the GPS service is always on for transaction services. Due to the fact that users are mobile, it is computationally infeasible to keep the records of all the locations of users during transaction to use it for verification and authentication.
- Bluetooth is also used to exchange sensitive information that can be discovered and targeted for attack by other Bluetooth enabled devices as mentioned before. In addition, mobile phone malware can be delivered through this channel.

3.4 Summary

In this chapter, gaps of different mobile money models and mobile payment system architectures that are related and relevant to our proposed system are investigated and analyzed. From the analysis of the related works, we came up with the following major problems of present day mobile money and its payment schemes.

- The mobile money is linked with paper money. As a result, the paper money is not totally eliminated from the market and replaced by mobile money.
- The current contactless mobile-based payments are designed for smart card emulation and POS systems used as a payment tool on the existing more sophisticated infrastructures that are accessible in developed markets only. As a result, a wide adoption of such kind of system for a broader set of population is too much expensive especially for developing market where huge amount of investment is required to extend the infrastructure.

In conclusion, our work is fundamentally different from the other works since we have proposed a new form of digital money what we call smart money as an active object based on the real world money abstract features in order to make the digital money smarter and understandable for users. We have also employed biometric features of users, offline payment scheme, and end-to-end secure communication techniques using appropriate cryptography algorithms considering the features, storage and computation capacity of the current smart phones.

Chapter 4

Modeling Mobile Money Wallet and Offline Payment

This chapter presents the overall design of the proposed model for smart mobile money wallet and offline payment. The components of the proposed model with their functionalities and interactions are identified and explained. First, the general conceptual design is presented and then detailed components of the model are followed.

4.1 The Conceptual Design

The smart mobile money wallet is conceived as a system that can run on smart phones. The smart mobile money server is a dedicated machine, which is designed to handle the requests coming from the smart mobile money wallets. The communication link between the wallets and the server is facilitated through Wireless Application Protocol (WAP). The payer-payee communication is an NFC-based data transfer between the smart phones on which the wallets reside. When users want to withdraw or deposit smart money, communication between the wallet and the smart mobile money server is established through WAP. Users can withdraw and hold any amount of smart money on their wallet, which they use to pay any other smart money user party. They can also deposit the smart money they have on their wallet to their account on the smart mobile money server at any time. As smart money is withdrawn, deposited or paid, the smart money is verified for validity. Both the wallet and the server have the capability to verify validity of the smart money.

Smart mobile money can be transferred offline without real time remote connection, third party involvement and authentication for processing payment. In case of offline payment, the payer/payee smart mobile money wallets communicate using Near Field Communication (NFC) when users tap their phones to each other after a payment instruction is made. The conceptual organization of the overall functioning of the smart mobile money wallet and the offline payment process is presented in Figure 4.1.

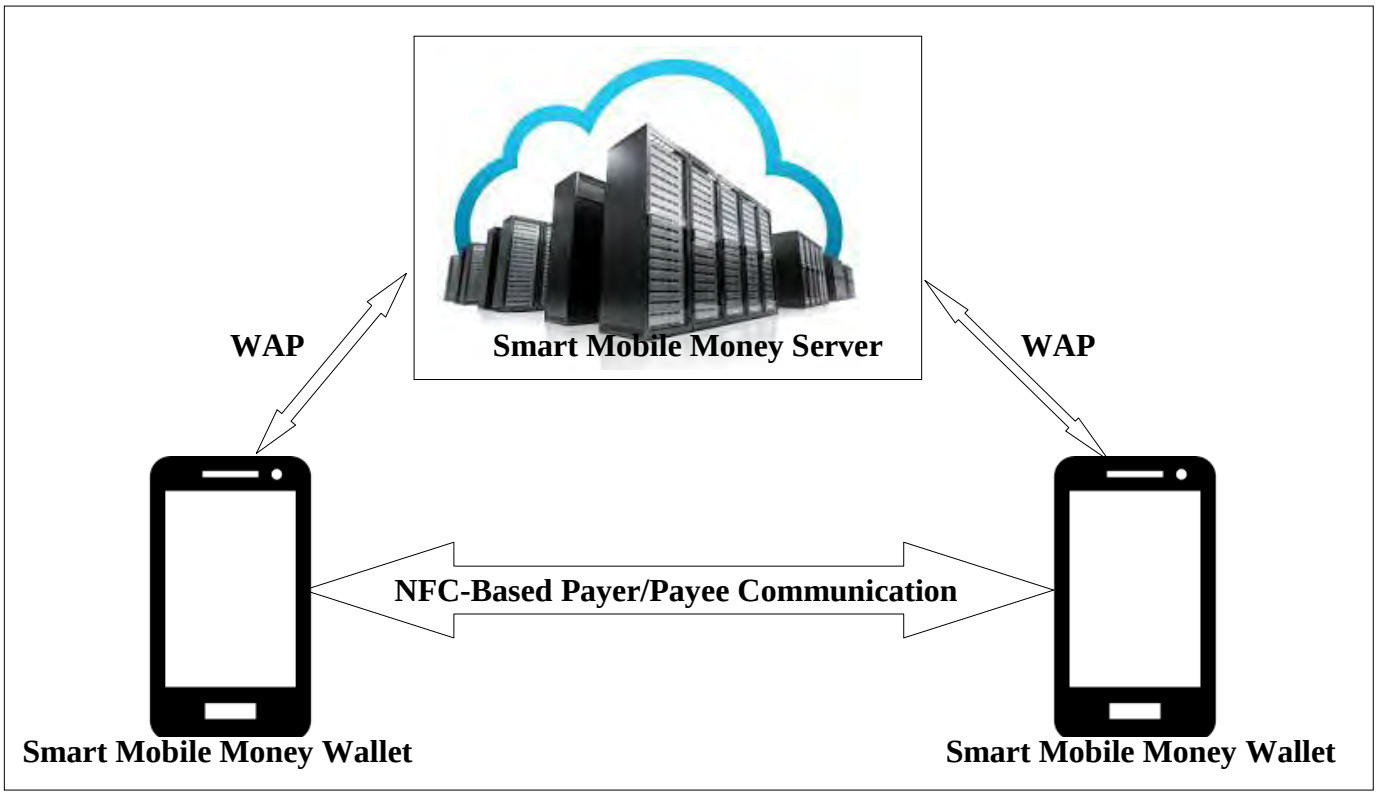


Figure 4.1: High Level Conceptual Design of the Smart Mobile Money System

4.2 The Model for the Smart Mobile Money Wallet and Offline Payment

This section presents and illustrates the components of smart mobile money and offline payment model as well as the interactions between the components. The proposed model operates on client-server based three-tier architecture and the communication between the client and the server takes place using wireless application protocol. The smart mobile money wallet lies on the client tier of the architectural model, which functions on a smart phone. The smart money is generated, processed and authenticated on the logic tier, where as the user registration records, the smart money records, and the transaction log are managed on the data tier.

The model is composed of different components distributed in the three layers. The presentation layer contains all the client-side sub-systems and functionalities that contain the major components: the user-interface, the client-side security subsystem and the mobile wallet subsystem. The user interface is composed of the smart mobile wallet application that permits the user to interact with the other system components. In addition, it also contains the fingerprint scanner component that serves as a biometric authentication of the user.

The security guard engine, fingerprint authentication engine, passkey authentication engine, Smart Money Detector, and Smart Crypto are identified as components of Client-Side Security Subsystem to perform security related operations during user interaction and communication with smart mobile money server. The Mobile Wallet Engine consists of Registration Engine, Withdrawal Engine, Deposit Engine, and Payment Engine in order to process and handle user registration, smart money withdrawal, smart money deposit, and smart money payment and reception, respectively. Wallet Database is also identified as a component of smart mobile money wallet in order to manage and store user's data and smart money. Communication Manger component handles the communication of smart phones during payment.

In the logic layer, the Smart Money Transaction Engine, the Smart Money Object Generator, and the Server-Side Security Subsystem are the major components that are designed to handle transaction requests sent from the client. The Message Authentication Engine, the Smart Money Detector, and Smart Crypto are the components of server-side security subsystem to make security measurements during data exchange with smart mobile money wallet. Note that both Smart Money Detector and Smart Crypto have similar functionalities both in the smart mobile money wallet and in smart mobile money server. However, both in the wallet and in the server, Smart Money Detector and Smart Crypto should be installed as components in order to detect smart money and perform cryptography operations, respectively. The Data layer consists of the database management that is required to manage the smart money. Figure 4.2 shows the model for the smart mobile money and offline payment. The proposed detail functioning of the components during the interactions of each of the components of the model are illustrated and described in the subsequent sub sections.

Unlike other mobile wallet architectures discussed in the related work, the proposed model mainly incorporates components such as smart money detector in order to detect smart money during transaction; smart crypto component in order to perform cryptographic operations and establish end-to-end secure communication; smart money object generator in order to generate smart money resembling real world paper money; withdrawal engine in order to facilitate smart money withdrawal process without accessing the physical bank or ATM; deposit engine in order to facilitate smart money deposit process without accessing the physical bank, payment engine in order to process offline smart money payment process without involvement of third party.

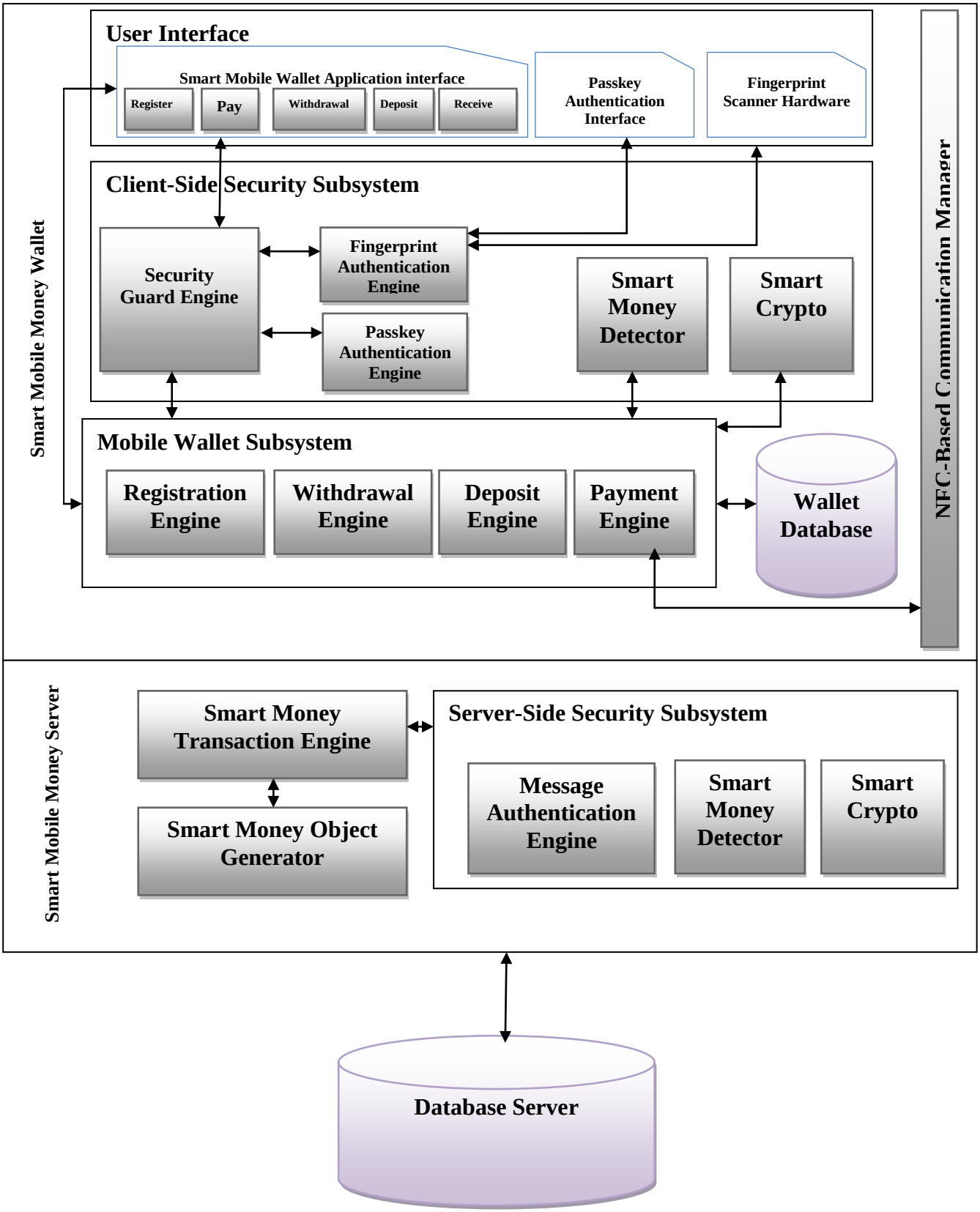


Figure 4.2: The Model for Smart Mobile Money Wallet and Offline Payment

4.2.1 User Interface Component

The user interface is a communication interface that enables the user to interact with the smart money system components. As a result, user interface component has three sub components, namely the smart mobile wallet application, passkey authentication interface and the fingerprint scanner hardware. Smart Mobile Wallet Application enables the user to withdraw, deposit, and pay smart mobile money. This includes the components that permit the user to register, receive smart money payments, deposit smart money, withdraw smart money, and pay smart money. Users can use fingerprint scanner hardware as an interface to scan their fingerprint for biometric authentication and they can use passkey authentication interface for passkey authentication.

4.2.2 Client-Side Security Subsystem

The proposed model uses security techniques and technologies to fulfill and achieve the current required security requirements. The major required security requirements are authentication, integrity, confidentiality, non-repudiation, privacy, and availability. Multi-layer authentication is employed in order to insure user authentication. The first layer of authentication is done through biometric-based authentication as an alternative to the knowledge-based authentication. The second layers of authentication is done through users' digital signature, which is used to authenticate a digital content to ensure that a known sender creates the message.

The proposed model ensures integrity of any transaction or message content to be done only by authorized parties to assure all system users, that is, the received messages have not been altered or modified in any way from the original message in transit. Generally, the original message with its signature is sent for the recipient to verify the integrity. The ECDSA cryptography technology is used to prevent modification of the message content and its signature.

The proposed model uses integrated encryption system to ensure confidentiality of any message sent to the recipient. The proposed model ensures that only authorized parties could access the message contents. In general, Elliptic Curve Integrated Encryption Scheme (ECIES) is used to achieve confidentiality of any message contents. Spongy castle and bouncy castle are used as a framework for the wallet and the server side respectively to implement ECIES.

A valid digital signature enables a recipient to believe that a known sender created the message and recipient can verify the message, such that the sender cannot deny having sent the message to ensure non-repudiation.

The proposed model prevents disclosure of any private personal information and keeps them secure to ensure users' privacy. Most relevant and private data like user's identity/fingerprint, passkey, and private key are not disclosed for any party including the service provider unlike current mobile money systems.

In general, in the user wallet, different security measurements are considered in order to secure the smart mobile wallet and exchanges of data. As a result, the Security Guard Engine, the Smart Money Detector, and the Smart Crypto are designed as major components of smart mobile money wallet security subsystem components to achieve the current security requirements.

A. The Security Guard Engine

The first time when users interact with the smart mobile wallet application or try to open the wallet, Security Guard Engine checks whether a user is already registered and security settings are configured in order to authenticate the smart mobile money wallet user as shown in Algorithm 4.1. If the wallet is not configured, the Security Guard Engine automatically initiates Registration Engine to start registration and configure the wallet. If the user is already registered and security settings are configured, Security Guard automatically initiates Fingerprint Authentication Engine in order to authenticate the user fingerprint. This is to mean that if and only if user's smart phone has fingerprint hardware with required API level and fingerprints are registered, the Security Guard Engine gives priority for fingerprint authentication and initiate Fingerprint Authentication Engine in order to prompt the user to scan his/her fingerprint and authenticate the user. Accordingly, the Passkey Authentication Engine is initiated in order to prompt the user to enter his/her passkey and authenticate the user through his/her passkey.

As a result, the contents or services of the wallet are accessed and the user gets permission to open and use the wallet if and only if both the authentication is successful.

```
Input: User fingerprint or passkey
Task: Authenticate user
Start
   User opens Smart Mobile Wallet
   Start Security Guard Engine
    If (Wallet is Valid)
       Start Fingerprint Authentication Engine
       Read user fingerprint
       Authenticate fingerprint
       Get fingerprint authentication result
       If (fingerprint is authenticated)
          Start Passkey Authentication Engine
          Read user passkey
          Authenticate passkey
          Get passkey authentication result
          If (passkey is authenticated)
             Start Smart Mobile Wallet Engine
          Else
             Warn the user and close wallet
       Else
        Warn the user and close wallet
    Else
     Start Registration Engine
 End Security Guard Engine
End
```

Algorithm 4.1: Algorithm to Authenticate Smart Mobile Money Wallet User

B. The Smart Money Detector

A Smart Money is virtual money encapsulating and resembling the most important features of the real world material money. The real world material money is modeled as an object in the computer world to be interactive and active. Once Smart Money is created as an object with its abstract features, it can be manipulated and stored in any computer system. As a result, a Smart Money object generated by the server with its abstract features is detected by Smart Money Detector component. The Smart Money Detector detects and verifies the validity of Smart Money signature signed by authorized Smart Money provider. Algorithm 4.2 shows the procedures to detect smart money.

```
Input: Smart Money Object
Task: detect Smart Money Object
Start
   Get Smart Money signature
   Connect to the database
   Get Smart Money provider public key
   Verify the signature using provider public key
   If (Signature is verified successfully)
      Real Smart Money is detected
   Else
      Counterfeit Smart Money is detected
End
```

Algorithm 4.2: Algorithm for Detecting Smart Money

C. The Smart Crypto

As discussed in Section 2.4.3, cryptography is used to design most modern security protocols and operations. Smart Crypto component is mainly designed to perform basic cryptography operations to apply cryptography algorithms during communication and message interpretation. Smart Crypto Component has various functions. The first one is creating key-pairs called private key and public key pairs which are very key elements in the cryptography security system. This process is used to create key-pairs of the client side. Each of this key pairs has 256-bit length. Once the private key and public key pairs are generated in smart mobile wallet, each of them is encoded by Smart Crypto component. The encoded private key is stored and embedded in the wallet since the private key needs to be secured and is private for the owner only. Even the smart mobile money wallet provider never know private keys of the users to ensure their privacy instead their encoded public key is dispatched and stored in the smart money wallet service provider database in order to use their public key to authenticate users during communication. The private key is used to sign any message to make sure that the message is created and owned by the owner of the private key whereas public key is used to verify message signature signed by associated private key. The private key is private for the owner only while the public key is distributed and available for the public so that anyone who has a public key of the sender of the signed message can easily verify whether it is sent from the original source or not. This key pairs are generated using elliptic curve algorithm. Creating signature for a message ready to be sent for the recipient is another major function of the Smart crypto component in the wallet. Whenever

any transaction request is generated and needs to be sent to the recipient, it should be first signed to make sure the integrity and authorization of the message so that the recipient can easily authenticate the message and ensure its integrity. ECDSA digital signature algorithm along with SHA256 hash algorithm is used to sign the message. As a result, after organizing and formatting the message, the smart mobile wallet should sign the message before sending it to the recipient.

Signing the message ready to be sent to the recipient is not enough to achieve all the current security requirements. Confidentiality is one of the major security requirements needs to be achieved in the proposed model. To ensure confidentiality, Smart Crypto component performs major operations such as generating secret key, encrypting message ready to be sent, and decrypt the message sent to the wallet during communication. Sharing secret key between two parties is the most critical task that needs to be handled seriously during an open-air communication. The proposed model achieves it using an integrated encryption scheme. ECIES is employed to integrate symmetric cryptography algorithms and asymmetric cryptography algorithms in order to share the secret key used for message encryption and decryption. As stated in Section 2.4.3, symmetric cryptography algorithms are used to encrypt and decrypt message content while asymmetric cryptography algorithms are used to sign and verify the content of the message. Smart Crypto component in the wallet generates 128-bit secret key and encode it. This secret key is used to encrypt the signed message ready to be sent in order to ensure that it cannot be decrypted and the message content cannot be disclosed without an authorized person only. AES symmetric cryptography algorithm is employed in order to encrypt and decrypt messages content during communication. Once the Smart Crypto encrypts the message content using the secret key, it encrypts secret key once again and attached to the message to be used later by the recipient in order to decrypt the content of the message. As a result, in order to achieve the secrecy of the secret key, Smart Crypto uses the public key of the recipient to encrypt the secret key used for message encryption so that the encrypted secret key cannot be decrypted without the recipient associated private key. This is to mean that the recipient first uses his/her private key to decrypt the secret key. Once the secret key is available at hand, the recipient again uses secret key in order to decrypt the content of the message. Then after, the recipient authenticate the message content using public key of the sender in order to make sure the original source of the message. Algorithm 4.3 shows the procedures how message is signed and encrypted using

Smart Crypto component in the smart mobile money wallet before sending any transaction request to the recipient.

```
Input: Plain message
Task: Encrypt plain message
Start
   Connect to the database
   Get sender private key
   Sign the plain message using sender private key
   Generate secret key
   Encrypt signed message using the secret key
   Get recipient public key
   Encrypt the secret key using recipient public key
End
```

Algorithm 4.3: Algorithm to Encrypt Plain Message

When transaction response is sent to smart mobile money wallet, Smart Crypto Component in the wallet first uses user private key stored in the wallet database to decrypt the secret key. Once the secret key is available at hand, the secret key is used to decrypt the content of the message as shown in Algorithm 4.4.

```
Input: Encrypted message
Task: Decrypt message
Start
   Connect to database
   Get recipient private key
   Decrypt secret key using the private key
   Decrypt the message using the secret key
End
```

Algorithm 4.4: Algorithm to Decrypt the Message

4.2.3 The Smart Mobile Wallet Subsystem

The smart mobile wallet subsystem is used to control user interaction and that responds accordingly in order to use the wallet and access services such as user registration, smart money withdrawal, smart money deposit, and smart money payment.

A. The Registration Engine

The Registration Engine facilitates the user registration process during new user registration. The Registration Engine interacts with Smart Crypto component in order to generate key-pairs for the registered user. Once the key-pairs are generated, the Registration Engine encodes user name, phone number, and public key of the user. Then the Registration Engine sends registration request to the smart mobile money server in order to register this new user in the database server. During registration, the smart mobile money server provides unique smart mobile money account number, the encoded smart mobile money service provider's public key for the new user and then sends the acknowledgement message back to Registration Engine. Once the acknowledgment message is received successfully by the wallet, the Registration Engine handles the response message to complete registration. The Registration Engine extracts the smart mobile money account number and smart money service provider public key from the response message sent from the server. The smart mobile money account number is a randomly generated number that uniquely indentifies the user to store smart money balance in the database server, whereas the smart mobile money service provider's public key is used to verify and ensure all the messages and the smart money created and signed by an authorized service provider. Then, the Registration Engine encapsulates all required information of the user and stores it in the wallet database that is embedded within smart money wallet application. The user's private key, user name, phone number, passkey, secret question, and the corresponding answer for secret question are all the required user information in addition to smart money account number and service provider public key sent from the server. The user's private key, passkey, and an answer for secret questions are private for the user only and can be accessed by the user only since they are stored and authorized. The passkey is an alternative knowledge-based authentication scheme in addition to biometrics-based authentication that is used to authenticate the user in order to access smart mobile money wallet service. During registration, the user will be prompted to enroll their fingerprint if user's smart phone has fingerprint scanner hardware so that the user can use his/her fingerprint based authentication as an alternative to passkey. The secret question and its associated answer is formulated by the user during registration in order to remind the passkey if the user forgets and unable to remember the passkey. In this case, the user is prompted to provide an appropriate answer for the secret question formulated before by him/her so that the passkey is displayed to the user if the answer is correct. Users are recommended to formulate strong

question and a corresponding answer that cannot be easily deduced. Algorithm 4.5 shows the processes to register the user.

```
Input: user name, phone number, passkey, secret question,
and answer
Task: Register user
Start
   Start Registration Engine
    Generates Key Pairs
    Encode user public key, user name and phone number
    Send user registration request
    Start Smart Money Transaction Engine
     Receive request message
     Decode user public key, user name and phone number
     Generate account number
     Register the user
     Connect to the Database Server
     Get service provider public key
     Encode user account number and provider public key
     Send user registration response
    End Smart Money Transaction Engine
    Receive the response message
    If (user is registered successfully)
     Decode user account and provider public key
     Store user details in the wallet
    Else
    Cancel registration
   End Registration Engine
End
```

Algorithm 4.5: Algorithm to Register a User

B. The Withdrawal Engine

In order to enable the user to easily understand and use smart money, real world material money is modeled and structured in the computer system which are not available in the digital money ecosystem so far. As a result, the user can randomly select smart money designed and displayed on the interface based on their preference in order to be signed by smart money service provider. Once authorized provider signs the smart money, it can be verified and detected during transaction more reliably than material money. As a result, the Withdrawal Engine facilitates smart money withdrawal process whenever users want to withdraw smart money from the server and store it in the wallet to pay it offline for purchasing goods and service.

When the user needs to withdraw and specify such amount of smart money having different economic values, Withdrawal Engine requests smart money objects encapsulating different economic values. Then, the Withdrawal Engine creates a withdrawal transaction request, encode transaction request, sign and encrypt transaction request using newly generated secret key, encrypt the secret key, and finally structure the message and send it to the smart mobile money server to be processed as shown in Figure 4.3. A transaction is composed of list of Smart Money needs to be withdrawn, the smart money account numbers of the user, and automatically generated random challenges. The challenge is used to protect replay attack so that there will not be the same transaction requests sent to the smart mobile money server.

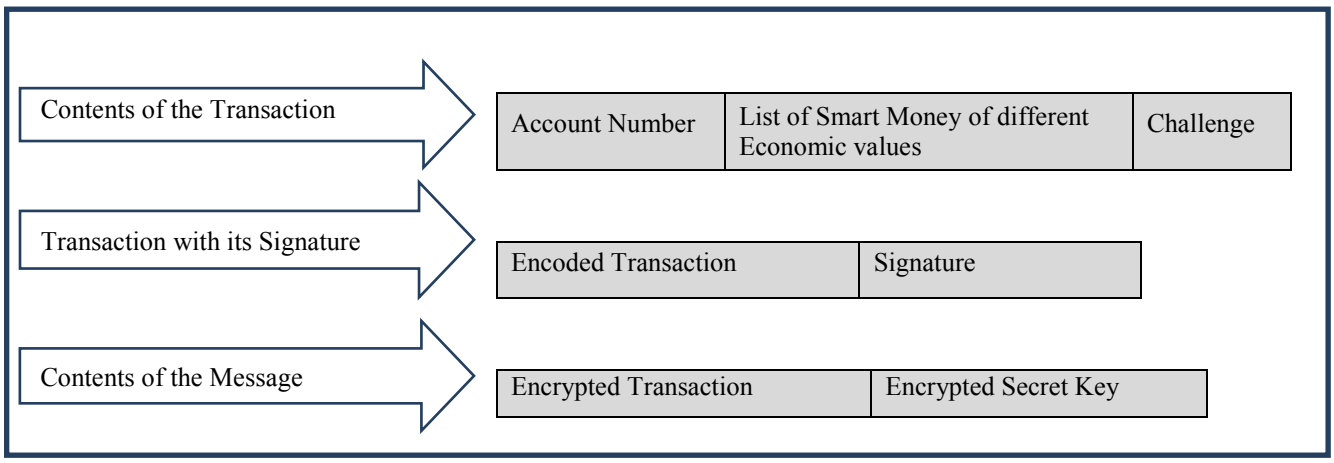


Figure 4.3: The Structure of the Withdrawal Transaction Request Message

As depicted on Figure 4.3, after transaction request, the encapsulating account number, the list of Smart Money with different economic value, and the random challenge are created, encoded and signed. Then, the encoded transaction with its signature is encrypted using the secret key to make it confidential. Finally, after the secret key is encrypted, the message is structured and sent to the recipient. After the smart mobile money server processes the transaction request, it signs the requested smart money and sends the response message back to Withdrawal Engine with an end-to-end secured channel. Then, the Withdrawal Engine interacts with the Smart Crypto component in order to decrypt the message sent from the smart mobile money server. Accordingly, the Smart Crypto first decrypts the secret key using smart mobile money server public key, then decrypts the contents of the message using the secret key, and finally returns the plain message to the Withdrawal Engine. Then, the Withdrawal Engine extracts the real smart money that are signed by smart mobile money server. In order to verify the validity of each smart

money, the Withdrawal Engine interacts with Smart Money detector. Then, the Smart Money detector detects and verifies signatures of each Smart Money. If one of the Smart Money is detected as counterfeit, the transaction is totally rejected and cancelled. If verification is completed successfully and each smart money is detected as valid money, the money will be stored in the wallet database to be used later to pay offline for purchasing goods and services. Algorithm 4.6 shows the steps of procedure for smart money withdrawal process. Annex C shows sequence diagram to process an example of Smart Birr withdrawal.

```
Input: List of different smart money economic values
Task: Withdraw smart money
Start
 Start Withdrawal Engine
    Connect to Wallet Database
    Get user account number
    Generate unique challenge
    Encode different economic values
    Create withdrawal transaction
    Encode withdrawal transaction
    Get user private key
    Sign the encoded withdrawal transaction
    Generate the secret Key
    Encrypt signed transaction
    Get recipient public key
    Encrypt secret key
    Encode request message
    Send the request message
    Start the Smart Money Transaction Engine
       Receive request message
       Decode request message
       Connect to Database Server
       Get service provider public key
       Decrypt secret key
       Decrypt withdrawal transaction request
       Decode withdrawal transaction request
       Get user public key
       Authenticate withdrawal transaction request
       If (authentication is successful)
          Get smart money economic values
          Compute withdrawal amount
          Get user account balance
          If (withdrawal amount is less than balance)
             Initialize smart money list
             For each smart money economic values
```

```
            Generate smart money
            Add smart money to the smart money list
          End for loop
          Debit user account balance
          Create and stores transaction log
          Encode list of generated smart money
          Generate secret key
          Encrypt encoded list of smart money
          Get the user public key
          Encrypt secret key
          Encode response message
          Send response message
        Else
          Cancel withdrawal transaction request
      Else
        Cancel withdrawal transaction request
    End the Smart Money Transaction Engine
    Receive response message
    Decode response message
    Get user private key
    Decrypt secret key
    Decrypt encoded list of smart money
    Decode list of smart money
    Initialize Verification to false
    For each smart money
      Verify smart money
      If (smart money is verified)
        Verification is true
      Else
        Verification is false
    End for loop
    If (Verification is true)
      Store list of smart money in the wallet
      Create transaction log
    Else
      Cancel transaction
  End the Withdrawal Engine
End
```

Algorithm 4.6: Algorithm for Smart Money Withdrawal Process

C. Payment Engine

Offline payment is a very important key feature of the proposed model that enables two parties, who have smart mobile money wallet to transfer or pay smart money. During the payment process, third party involvement and authentication is not required, that is, the payment can be

fully anonymous just like material money or can be made fully known based on an applied policy. The smart money, stored in the wallet and used for payment, exactly resembles the real world material money abstract features. This is achieved by creating smart money objects resembling the real world material money with its basic features such as serial number, economic value, nation identifier, icon, and signature. In the computer system, objects are secured, easy to manage, active and interactive. This is because everything is packed and data is encapsulated in to one entity called object. These smart money objects created in the digital world replace material money objects in the real world and acts like them. Then users can manage and use the smart mobile money in the same way as they can manage and use the real world material money by unlocking their physical leather wallet and use available money for any kind of payment. Unlike real world material money, smart mobile money has advanced features like advanced security, usability, durability, neatness, and profitability since printing, storing, moving, and managing real world material money is expensive.

The Payment Engine facilitates and handles the payment process between smart mobile money wallets. Payment Engine setups and controls everything to handle the payment process when users open the smart mobile money wallet and start payment. The Payment Engine automatically arranges and displays available smart mobile money in the user wallet when users want to pay/transfer smart money. Accordingly, the user can specify the amount of smart mobile money and make payment to other party. Then the Payment Engine encodes the smart mobile money and uses NFC-based communication channel in order to manage communication between the smart mobile money wallets.

During payment process, Payment Engine interacts with Smart Money Detector component in order to detect and verify the validity of the smart money being transferred to the recipient. Since each smart money stored in users wallet are generated as an active object and signed by an authorized smart money service provider in the smart mobile money server, the Smart Money Detector can verify the signatures of each smart money using the public key provided by the service provider. Algorithm 4.7 shows the steps of procedures for smart money offline payment process. Annex E shows the sequence diagram to process an example of Smart Birr payment.

```
Input: Smart money
Task: Pay smart money
Start
   Start Payment Engine
      Check NFC
      If (NFC is enabled)
         Encode smart money
         Encode payload message
         Prompt users to tap their smart phone to each other
         If (smart phones are tapped)
            Prompt the Payer to confirm payment
            If (payment is confirmed)
               Send encoded payload message to payee
               Payee receive payload message
               Decode payload message
               Decode list of smart money
               Initialize Verification to false
               For each smart money
                  Verify smart money
                  If (smart money is verified)
                     Verification is true
                  Else
                     Verification is false
               End for loop
               If (Verification is true)
                  Credit Payee wallet
                  Create Payee transaction log
                  Debit Payer wallet
                  Create Payer transaction log
                  Notify Payer and Payee
               Else
                  Cancel payment
            Else
               Cancel payment
         Else
            Cancel payment
      Else
         Prompt Payer to enable NFC first
  End the Payment Engine
End
```

Algorithm 4.7: Algorithm for Smart Money Offline Payment Process

D. Deposit Engine

When users want to deposit smart mobile money stored in their wallet to their account in the smart mobile money server, they can send deposit request to the smart mobile money server anytime. Unlike the real world traditional financial institution and the current mobile money services, no need to travel a long distance and access the physical bank to deposit or withdraw cash instead user can withdraw or deposit smart mobile money anytime being anywhere with Internet access.

The Deposit Engine facilitates and handles the smart mobile money deposit process between smart mobile money wallet and smart mobile money server. Deposit Engine setups and controls everything to handle the deposit process when users want to deposit smart mobile money into their accounts in the smart mobile server.

The Deposit Engine automatically arranges and displays available smart mobile money in the users' wallet when users want to deposit smart mobile money. Accordingly, users can specify the amount of smart mobile money that needs to be deposited into their account in the server. Then Deposit Engine creates a deposit transaction request, encode transaction request, sign and encrypt transaction request using newly generated secret key, encrypt the secret key, and finally structure the message and send it to the smart mobile money server to be processed as shown in Figure 4.4. Unlike withdrawal transaction request, deposit transaction is composed of a list of real smart money, account numbers of the user, and automatically generated random challenges.

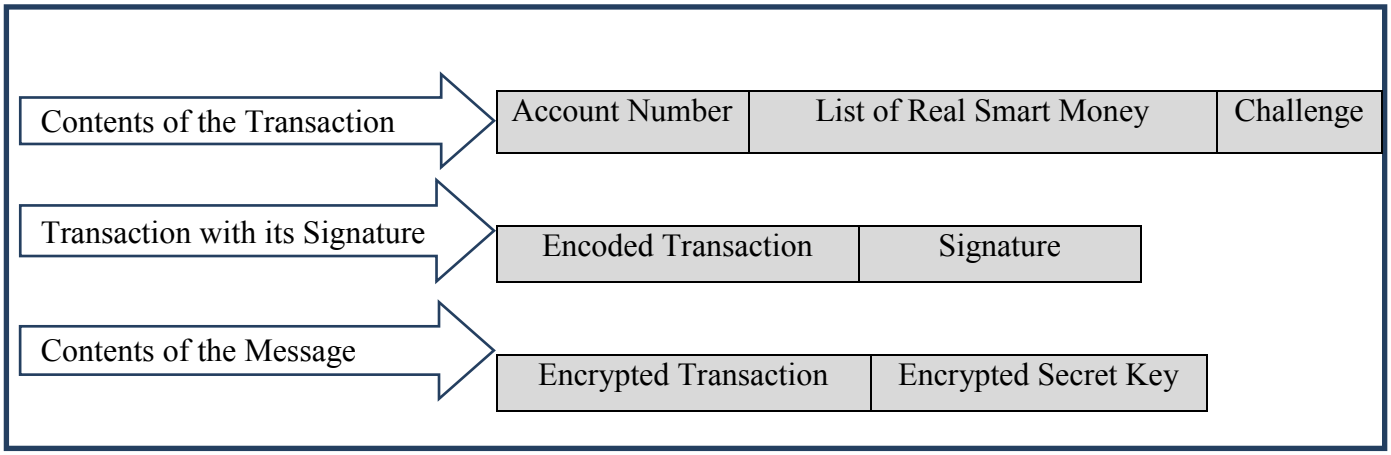


Figure 4.4: The Structure of the Message for Smart Money Deposit Request

Then Deposit Engine sends the request to the smart mobile money server. After the smart mobile money server processes the request, it sends the acknowledgment message back to the

withdrawal Engine using end-to-end secured channel. Like Withdrawal Engine, Deposit Engine interacts with Smart Crypto component in order to extract and interpret confidential acknowledgement message sent from the smart mobile money server so that the Deposit Engine confirm it and debit smart mobile money wallet and notify users. Algorithm 4.8 shows the steps of procedures for smart money deposit process. Annex B shows the sequence diagram to process an example of Smart Birr Deposit.

```
Input: Smart money
Task: Deposit smart money
Start
 Start the Deposit Engine
    Connect to the Wallet Database
    Get user account number
    Generate unique challenge
    Encode list of smart money
    Create deposit transaction request
    Encode deposit transaction request
    Get user private key
    Sign encoded deposit transaction request
    Generate secret key
    Encrypt signed deposit transaction request
    Get recipient public key
    Encrypt secret key
    Encode request message
    Send request message
    Start Smart Money Transaction Engine
       Receive request message
       Decode request message
       Connect to Database Server
       Get service provider public key
       Decrypt secret key
       Decrypt deposit transaction request
       Decode deposit transaction request
       Get user public key
       Authenticate deposit transaction request
       If (authentication is successful)
          Decode list of smart money
          Initialize Verification to false
          For each smart money
             Verify smart money
             Check the smart money status
             If (the smart money is verified and already spent)
                Verification is true
             Else
```

```
            Verification is false
        End for loop
        If (Verification is true)
           Connect to the Database Server
           Compute deposit amount
           Update each smart money status
           Credit user account
           Create transaction log
           Create acknowledgment message
           Generate secret Key
           Encrypt acknowledgment message
           Get user public key
           Encrypt secret key
           Encode response message
           Send response message
        Else
           Cancel transaction
      Else
         Cancel transaction
   End Smart Money Transaction Engine
   Receive response message
   Decode the response message
   Get user private key
   Decrypt secret key
   Decrypt acknowledgment message
   If (the acknowledgment message is successful)
      Debit wallet
      Update Transaction Log
   Else
      Cancel transaction
 End the Deposit Engine
End
```

Algorithm 4.8: Algorithm for Smart Money Deposit Process

4.2.4 Smart Money Transaction Engine

The smart mobile money wallets send a transaction request to the smart mobile money server when users want to withdraw or deposit smart money from and to their account. The smart mobile money server then handles the request sent from smart mobile money wallet and responds accordingly. As a result, Smart Money Transaction Engine is identified as a key component to be mapped on smart mobile money server in order to handle and process the requests sent from smart mobile money wallets. Smart Money Transaction Engine mainly

handles and processes withdrawal or deposit transaction requests sent from smart mobile money wallet. Then the request message is first decrypted and authenticated using Smart Crypto and Message Authentication Engine components respectively before processing the request message to ensure integrity and authorization of the message, that is, it is to make sure that the message is sent from an authorized party and not modified in transit. If message is authenticated successfully, Smart Money Transaction Engine starts to interpret and process withdrawal or deposit transaction request.

In the case of withdrawal transaction request, Smart Money Transaction Engine extracts and interprets the amount of smart money needs to be generated and user's account number from the request message. Then, before generating requested smart money, Smart Money Transaction Engine make sure that the account number has sufficient balance or not. If the balance is sufficient, Smart Money Transaction Engine interacts with Smart Money Object Generator in order to generate the requested amount of smart money. Accordingly, Smart money Transaction Engine interacts with Smart Crypto component in order to encode the message and encrypt it using the recipient public key so that the message is only disclosed through the associated recipient private key. Then the associated user account is debited and withdrawal transaction response message is sent to smart mobile money wallet.

In the case of deposit transaction request, Smart Money Transaction Engine extracts and interprets the amount of real smart money needs to be deposited and associated user's account number from the request message. Then, before associated user account is credited, each smart money is detected and verified using Smart Money Detector component. If counterfeit smart money is not detected and verification is completed successfully, Smart Money Transaction Engine debits associated user account and send encoded and encrypted acknowledgment message back to the smart mobile money wallet.

4.2.5 Smart Money Object Generator

Smart money, in the proposed model, is structured and created as an object resembling the real world material money important features. As discussed in Section 2.1, the current digital money lacks digital money structure and never abstracts the real world material money important features in the computer system instead the digital money is represented in floating numbers. In the proposed model, the real world material money is modeled and created as an active object in

the computer system. In order to create smart money, the proposed model considers the important features of the real world money like security features, serial number, icon, economic value, and nation identifier. This enables the user to easily understand and identify smart money as real world material money.

As a result, Smart Money Object Generator generates smart money objects encapsulating serial number, economic value, nation identifier, icon, and signature as shown in Algorithm 4.9. Each smart money serial number is automatically generated and universally unique that is used to identify each smart money uniquely. Then nation identifier represents the nation that generates the smart money. Economic value represents the value of each smart money object as the real world currency notes have different economic value. For example, Ethiopian material money are categorized into different economic values like100 birr, 50 birr, 10 birr, 5 birr, 1 birr, 50 cent, 25 cent , 10 cent, 5 cent, and 1 cent. In the case of smart money, an icon is an encoded binary data that encapsulates smart money serial number, economic value, nation identifier, and automatically generated random challenge that is used to generate unique signature for each smart money so that generating or reproducing such kind of smart money again is quite difficult and not possible. Smart money signature is a digital signature used to validate each smart money. As a result, Smart Money Object Generator generates smart money objects that satisfy all these abstract features. In general, as discussed in Section 2.1, the smart money satisfies the three criteria of money in order to serve as a store of value, unit of account, and medium of exchange.

```
Input: Smart Money economic value
Task: Generate Smart Money
Start
   SERIAL_NUMBER = Generate serial number
   CHALLENGE = Generate random challenge
   NATION_IDENTIFIER = assign nation identifier
   ECONOMIC_VALUE = assign economic value
   ICON    =    assign    encoded    SERIAL_NUMBER,    CHALLENGE,
                NATION_IDENTIFIER, and ECONOMIC_VALUE
   SIGNATURE = generate signature
   SMART_MONEY = create Smart Money object
   Set  SERIAL_NUMBER,  NATION_IDENTIFIER,  ECONOMIC_VALUE,  ICON,
         and SIGNATURE to SMART_MONEY object
End
```

Algorithm 4.9: Algorithm to Generate Smart Money Object

4.2.6 Server-Side Security Subsystem

The Smart Crypto, Smart Money Detector, and Message authentication components are identified to be mapped onto the smart mobile money server to make security measurements.

The server-side Smart Money detects counterfeit smart money and verifies the validity of smart money sent from smart mobile money wallets.

Server-side Smart Crypto is used to generate an authorized smart mobile money service provider key-pairs namely the private key and public key so that the smart mobile money server uses the private key to sign the smart money objects. In order to send message to the smart mobile wallets from the server, the Smart Crypto first generates secret key randomly and encrypt the message using this secret key. Then the secret key is again encrypted using recipient public key and then the message is encoded and sent to smart mobile wallets. In contrast, when message is sent to the smart mobile money server from the smart mobile money wallets, the Smart Crypto first decrypts the secret key using recipient public key, that is, the service provider public key and then decrypts the content of the message using this secret key.

The Message Authentication Engine component facilitates and handles message authentication when request message is sent from the smart mobile money wallets. After the content of request message is decrypted via Smart Crypto, the message is then authenticated via Message Authentication Engine using the public key of the sender in order to make sure whether the request message is sent from an authorized user or not as shown in Algorithm 4.10.

As discussed in Section 2.3.2, the current mobile money payment systems use either PIN based or token based authentication method in order to authenticate users. In this case, the authentication is very weak and easily attackable since it can be deduced. Moreover, service providers know users' private data since the actual PIN is stored in the service providers' database that is exposed to impersonate attack. Unlike these authentication methods, digital signature based authentication is used in the proposed model in order to authenticate users using their signature. Since any transaction request message is signed by users' private key, users can be authenticated by verifying their signature without disclosing their private data.

```
Input: Encrypted message
Task: Authenticate message
Start
   Connect to the database
   Get recipient private key
   Decrypt the secret key using the recipient private key
   Decrypt the message using the secret key
   Get the signature of the request message
   Get sender account number
   Get public key of associated sender account number
   Verify message signature using sender public key
   If (signature is verified)
      Message is authenticated
   Else
      Authentication is failed
End
```

Algorithm 4.10: Algorithm to Authenticate Request Message Sent from Users

4.3 Database Design

This section presents and shows the database designs for Smart mobile money wallet and offline payment model both in the smart mobile money wallet and server. For more clarity, the entity relationship diagram and database model are designed and illustrated in order to show how the real world objects with their attributes are represented and stored in the database system.

Note that shaded rectangle represents name of the entities while the oval symbol represents their associated attributes in the entity relationship diagram. In the database model, table icon on the right corner of the diagram refers to a relation/table created in the database. In addition, primary key attributes are indicated with "PK" while unique attributes are indicated with "UQ"

4.3.1 Wallet Database Design

In the smart mobile money wallet, SQLite relational database system is used to store smart money and user information since it is embedded SQL database engine and an integral part of the application program so that the data is embedded in the smart mobile money wallet.

Wallet database stores two major entities, namely Smart Money and User with their attributes as it is depicted in Figure 4.5.

The Smart Money entity has five major attributes, namely serial number, nation identifier, economic value, icon, and signature in order to store associated values for each smart money in the wallet.

The User entity has seven major attributes, namely smart mobile money account, user name, phone number, device id, user signature, user signature detector, and provider signature detector. In the wallet, it is allowed to store only one user and this user is only authorized to authenticate the wallet. Once all these relevant user details are stored and embedded in the wallet, user is not required to fill these details during any transaction since the wallet automatically retrieves the required details for any transaction if and only if the user authenticates the transaction through his/her fingerprint or passkey only.

Figure 4.6 shows models of each entity in the wallet database with their constraints. Serial number is a primary key attribute for smart money.

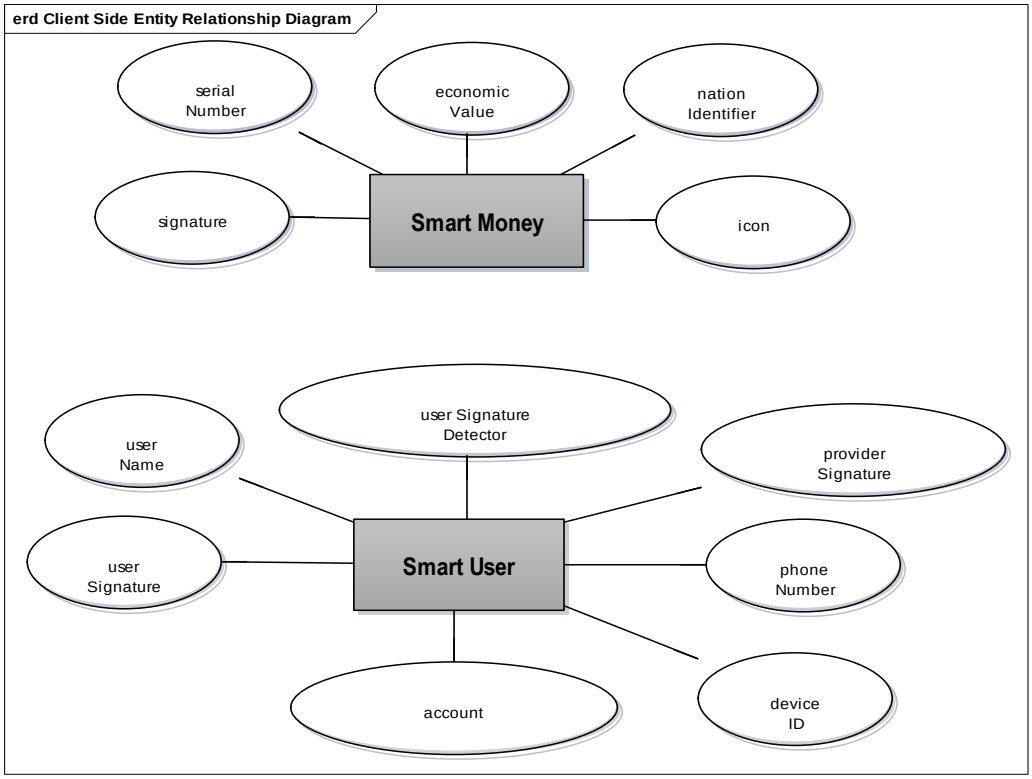


Figure 4.5: Smart Mobile Money Wallet Entity Relationship Diagram

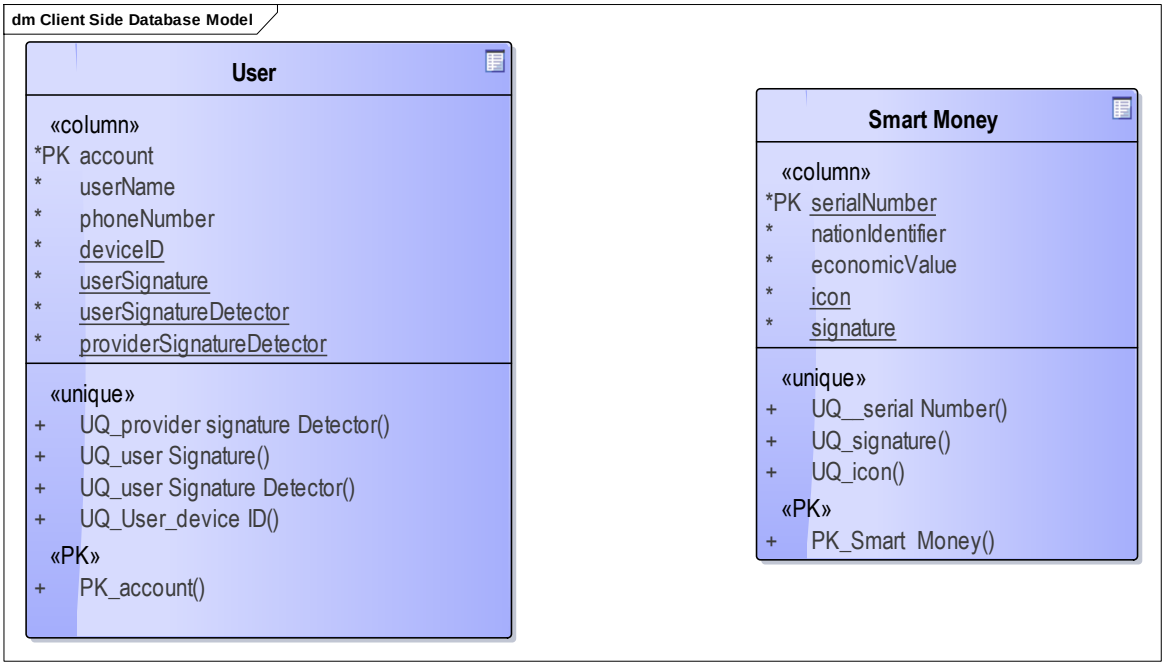


Figure 4.6: Wallet Database Model

4.3.2 Server Database Design

In the server side, MySQL relational database management system is used to store detail information related to different real world entities.

Server side application stores four major entities, namely Smart Money and User, Transaction Log, and Service Provider with their attributes as it is depicted in Figure 4.7.

Service Provider entity has four main entities, namely provider ID, provider name, provider signature (private key), and provider signature detector (public key).

In case of server side database, Smart Money has additional attribute called “status” in order to store the status of each smart money in order to identify whether they are spent or returned so that double spending attack can be easily detected. In the same fashion, User entity has additional attributes called “balance” in order to manage the balance when smart money is debited or credited by the user.

The User creates one-to-many relationship with Transaction Log entity since users create one or more transactions. So that, when users make transaction its associated transaction log is created.

Transaction Log entity has four main attributes, namely transaction ID, transaction amount, transaction type and timestamp. Transaction amount is the amount of transaction debited or credited while transaction type can be either withdrawal or deposit. Timestamp is used to stamp the time when the transaction is created or executed.

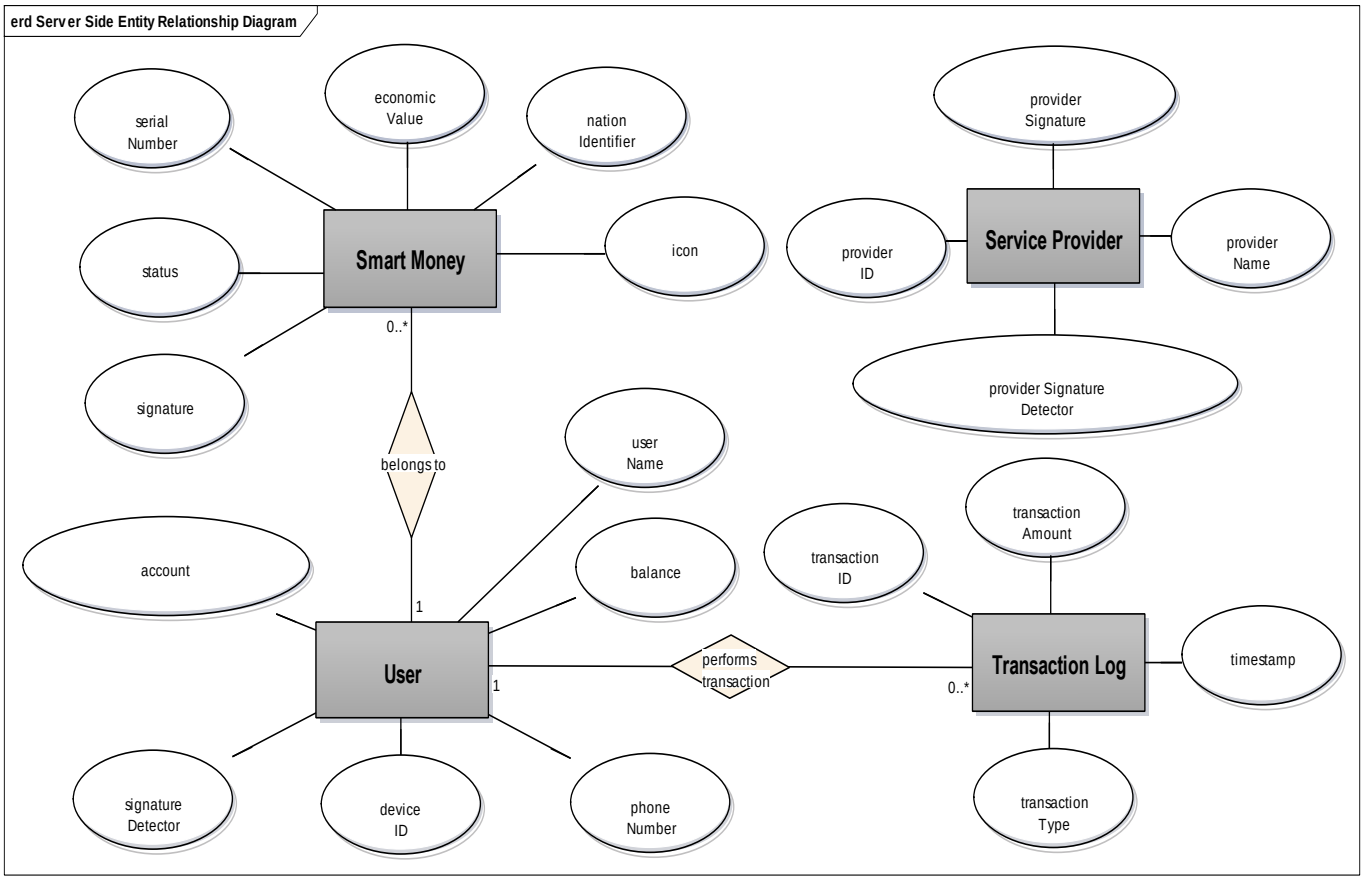


Figure 4.7: Server Side Entity Relationship Diagram

Figure 4.8 shows server side database model in order to show the relations with their constraints and relationships with other relations. Account, serial number, transaction ID, and provider ID are specified as primary key for the User, Smart Money, Transaction Log, and Service Provider entities, respectively. The primary key and foreign key relationship between the User and Transaction Log shows that "userAccount" is specified as foreign key attribute for Transaction Log relation where its value is inherited and referred from the user primary key attribute called "account". In the same manner, User and Smart Money are associated and primary key and foreign key mapping is shown.

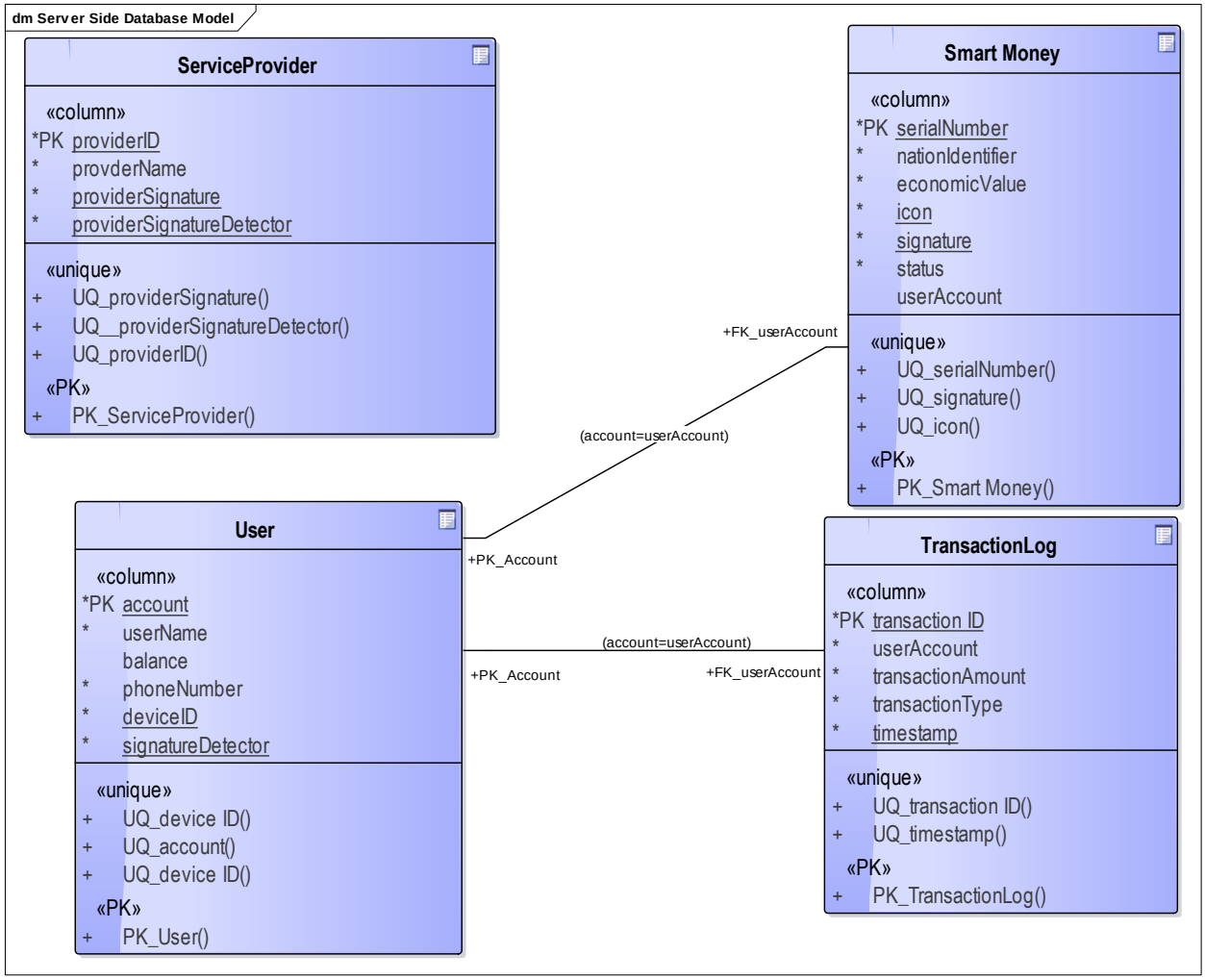


Figure 4.8: Server Side Database Model

4.4 Summary

Since money is like our blood flowing in our daily life, a broader set of people keep the material money in the leather wallet and put in the pocket so that without any third party involvement and transaction cost, they can use it for any kind of payment to purchase goods and services in the real world. In the same fashion, this work proposed digital wallet resembling leather wallet to store smart money resembling real world material money in order to use it for any kind of anonymous offline payment for purchasing goods and services whenever necessary.

In this chapter, the components of the proposed model for smart mobile money wallet and payment with their operations and interactions are presented and discussed. An end-to-end secured communication technique for open-air communication is also employed.

The proposed model components includes Security Guard Engine, Fingerprint Authentication Engine, Passkey Authentication Engine, Smart Money detector, Smart Crypto, Registration Engine, Withdrawal Engine, Deposit Engine, Payment Engine, Message Authentication Engine, Smart Money Transaction Engine, and Smart Money Object Generator.

In order to achieve the current security requirements digital signature, advanced encryption standard, hybrid encryption scheme, and multi-layer authentication scheme are employed.

As a result, the new proposed model enables the users to:

- Withdraw or deposit smart mobile money from and to authorized smart mobile money provider anywhere and anytime via Internet without traveling a long distance and access the physical bank or agents in the real world.
- Store and carry the smart mobile money in their smart phone.
- Understand and handle the smart mobile money easily like real world material money
- Make fully anonymous offline payment in order to purchase goods and service without third party involvement and interference.

In general, the proposed model is expected to play a great role in the digital money ecosystem in order to enable a broader set of people including less educated users to be the part of digital money ecosystem and extend the mobile money service especially in the remote area where expansion of traditional banks infrastructure is challenging problem and unavailable.

Chapter 5
Experiment

This chapter briefly presents each of the proposed model components prototype implementation along with their demonstration details. This chapter also briefly lists and explains tools and technologies that have been used to implement the proposed model prototype and why they were selected. Moreover, experimental procedures, requirements of testing environment and performance of the proposed model prototype from different perspectives are also presented and discussed in detail.

5.1 Tools and Technologies used for Development

Appropriate and advanced technologies are used to develop both the smart mobile money wallet and smart mobile money server application. The followings are major technologies with their brief and precise description used for development.

Java Programming Language

Java programming language has been used to write computer instructions for client side and server side application. Java is one of the most popular programming languages used to create web applications and platforms. It was designed for flexibility, allowing developers to write code that would run on any machine, regardless of architecture or platform. According to the Java home page[17], more than 1 billion computers and 3 billion mobile phones worldwide run Java. So java is everywhere, that is, it's on desktop, on mobile, on card, almost everywhere. Moreover, Java[18] is object-oriented, multithreaded, interpreted, distributed, dynamic, robust, secure, architecture-neutral, portable, and executes with high performance. That is why Java is preferable programming language for implementing the proposed model prototype.

[17] https://www.java.com
[18] http://www.c4learn.com/java/java-characteristics-features/

NFC

NFC is near field communication technology used to transfer smart money in proximity distance. As discussed in Section 2.4.2, NFC is appealing choice and has been used as communication technology during offline payment for proposed model prototype since it has three primary advantages over other mechanisms. First, NFC has a very short range communication channel making it hard for intruders to intercept communications. Users can clearly see anyone trying to intercept a transaction; in contrast to longer range protocols such as WiFi and Bluetooth that are exposed for intruders. Second, it is quick and easy to set up a NFC connection with another nearby NFC smart phone by tapping one smart phone over the other. However, in case of Bluetooth, peering the smart phones together is tedious and slow to set up. Third, NFC has a straightforward conceptual model for users so that they know exactly what device they are communicating with, as opposed to longer-range wireless protocols.

SQLite Database Management System

SQLite[19] is an embedded SQL database engine and an integral part of the application program used for Smart Birr[20] wallet development. It is an in-process library that implements a self-contained, server less, zero-configuration, and transactional SQL database engine. Its transactions are Atomic, Consistent, Isolated, and Durable (ACID) even after system crashes and power failures. As a result, SQLite is an appealing choice as embedded database for our Smart Birr wallet development.

Android Operating System

Android[21] is a mobile operating system currently developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smart phones and tablets. Android user interface is mainly based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual keyboard for text input. Android based smart phones have been selected to develop the prototype and later researchers will plan to extend the research to develop

[19] http://www.sqlite.org/
[20] Smart-Birr is a smart money used as system prototype for Ethiopian Birr
[21] http://www.android.com/

compatible application with all kinds of smart phone operating systems. Android 5.1 (lollipop) installed on Samsung Galaxy Note 4 has been used to test the prototype.

Android Studio

Android studio[22] is the official Integrated Development Environment (IDE) for Android application development, based on IntelliJ IDEA[23]. On top of the capabilities of IntelliJ, Android studio offers dominant features such as app sighing capabilities, flexible gradle-based build system, rich layout editor, tools to catch performance, usability, version compatibility, and other problems. Android studio 1.5.1 with Android SDK version 23.2 has been used for smart mobile money wallet development.

Cryptography Technology

As discussed in Section 2.4.3, ECDSA is the appealing choice and has been used as asymmetric cryptography technology used for digital signature due to its greater security, effectiveness, less power consumptions, low computing power, less memory utilization, less key size, high performance, and compatibility with lightweight devices. In addition to ECDSA, for end-to-end security, Elliptic Curve Integrated Encryption Scheme (ECIES)[24] and Advanced Encryption Standard (AES)[25] are used. AES is symmetric cryptography technology used for encryption while ECIES is a hybrid encryption scheme which provides semantic security for exchanging secret key. Moreover, bouncy castle framework[26] and spongy castle framework[27] are an appropriate choice for providing lightweight cryptography APIs. Bouncy castle framework is a collection of lightweight APIs and Java Cryptography Extensions (JCE) that has been used for server side cryptograph implementation while spongy castle framework is an extended and customized version of bouncy castle framework designed for android development and has been used for client side cryptograph implementation.

[22] http://developer.android.com/tools/studio/index.html
[23] https://www.jetbrains.com/idea/
[24] https://en.wikipedia.org/wiki/Integrated_Encryption_Scheme
[25] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[26] https://bouncycastle.org/
[27] https://github.com/rtyley/spongycastle

Biometrics

As it is discussed in Section 2.3.2, the traditional technologies available to achieve a positive recognition and authentication include knowledge-based methods and token-based methods. Both Knowledge-based and token-based methods are easily attackable as compared with biometrics based authentication [26]. In computer security, biometrics[28] refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods. There are several types of biometric identification schemes[29] such as facial recognition, voice recognition, signature recognition, iris recognition, and fingerprint, and hand geometry. Among these schemes, fingerprint recognition[30] technique is one of the most developed biometric technology and most economical authentication technique in the biometric market since it has very high level of accuracy, simplicity, small storage space, and high range of deployment environments.

Due to this fact, fingerprint recognition scheme has been selected and implemented in order to authenticate users in addition to traditional knowledge-based methods.

Enterprise Architect

Enterprise architecture (EA)[31] is a well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of architectures. It is used as UML design and business analysis tool for modeling, documenting, reverse engineering, building, and maintaining object-oriented software systems. It has been continually developed, enhanced and refined to meet the emerging needs of programmers, business analysts, enterprise architects, testers, project managers, designers, and others in order to comfortably scale from small single user models to large team based repositories and even to globally distributed Cloud based solutions[32]. Due to this fact, Enterprise architect version 11 is used for designing the proposed model prototype class model and sequence diagram with detail flow of interaction and dependency between each component.

[28] https://en.wikipedia.org/wiki/Biometrics
[29] www.biometricsinstitute.org/pages/types-of-biometrics.html
[30] http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/types/strengthen
[31] https://en.wikipedia.org/wiki/Enterprise_architecture
[32] http://www.sparxsystems.com/products/ea/

Java Script Object Notation (JSON)

JSON[33] is a lightweight data-interchange format which is easy for machines to parse and generate. It is text format that is completely language independent. This property makes JSON an ideal data-interchange language. JSON has been used to construct data format during exchanging of information between two different entities such as the server and the client in the proposed model prototype.

Apache Tomcat server

Apache tomcat server[34] is an application server that provides a pure Java HTTP web server environment for java code to run in. Apache tomcat server 8.0 has been used as an application server for the proposed model prototype.

Jersey RESTful Web Services framework

Jersey[35] is a framework used for developing Representative Stateless Transmission (RESTful) web services application in Java. Jersey 2.2 framework has been used to develop web service application in the proposed model prototype.

MySQL

MySQL[36] is an open source relational database engine used as a back end to manage data for server side development. MySQL 5.7 has been used as a server side relational database engine in the proposed model prototype.

Eclipse IDE

Eclipse[37] is an IDE used to develop java program. It contains a base workspace and an extensible plug-in system for customizing the environment. Eclipse is written mostly in Java and its primary use is for developing Java applications. Eclipse 4.5 is used as development environment for server side web service application.

[33] www.json.org/
[34] https://tomcat.apache.org
[35] https://jersey.java.net/
[36] https://www.mysql.com
[37] https://eclipse.org

5.2 Proposed Model Components, Implementation Details and Demonstration

This section presents the demonstration and implementation details of each components of smart mobile money wallet and offline payment model.

5.2.1 Smart Birr wallet Security Guard Engine

As it is briefly explained and discussed in Section 4.2.2, Security Guard Engine is responsible to authenticate the Smart Birr users before they access all the services provided by the wallet. Security Guard is initiated and activated whenever user opens Smart Birr wallet installed in their smart phone. As shown in Figure 5.1, a user uses Smart Birr wallet icon to open the application. The design of the Smart Birr icon shows that each Ethiopian material money currency notes are modeled and represented in the smart mobile money wallet, as they can be stored in the leather wallet in order to use and manage smart money just like material money.

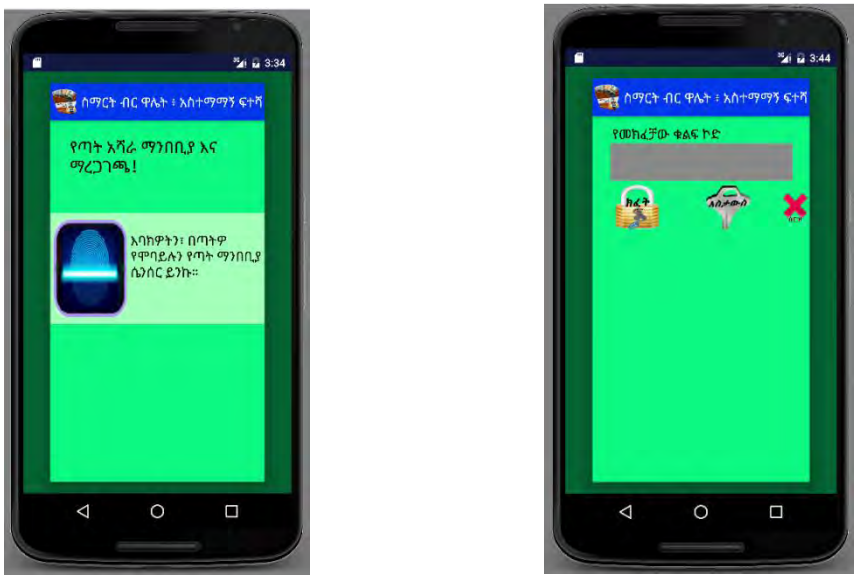
Figure 5.1 Smart Birr Wallet Icon

Figure 5.2: Smart Birr wallet Welcome User Interface

Once a user clicks on the icon shown in Figure 5.1, Security Guard engine automatically displays welcome screen shown in Figure 5.2 and prompts the users to open Smart Birr wallet by clicking on it in order to authenticate them and provide access to the services of Smart Birr wallet.

If fingerprint is already enrolled, Security Guard Engine prompts the user to scan their fingerprint in order to authenticate and permit access to the wallet as shown in Figure 5.3 (A). And then, Security Guard Engine uses passkey authentication scheme in order to prompt the user to enter the passkey and authenticate the user before allowing the user to access the services provided by the wallet as shown in Figure 5.3 (B). If both of these two-authentication schemes are done successfully, the security guard directs the user to Smart Birr wallet service user

interface as shown in Figure 5.5 and permits the user to access the services otherwise users will be directed to registration processes. Once a user gets an access to Smart Birr wallet services, he/she can perform transactions.



(A) Fingerprint Authentication Screen (B) Passkey Authentication Screen

Figure 5.3: User Authentication User Interface

5.2.2 Smart Birr wallet Registration Engine

As it is briefly discussed in Section 4.2.3, Registration Engine is one of the central component and controller to process user registration. Once a user fills all required information as shown in Figure 5.4 and sends a registration signal to the Registration Engine, the Registration Engine handles registration process.

Once the registration is completed successfully and security settings are configured, notification message is sent to the user and user is redirected to the main user interface for authentication before accessing the services. In this case, for demonstration purpose, Biritu is registered as a user successfully. Once Biritu is registered and authenticated successfully, Smart Birr wallet services user interface shown in Figure 5.5 is displayed to enable Biritu to make different transactions.

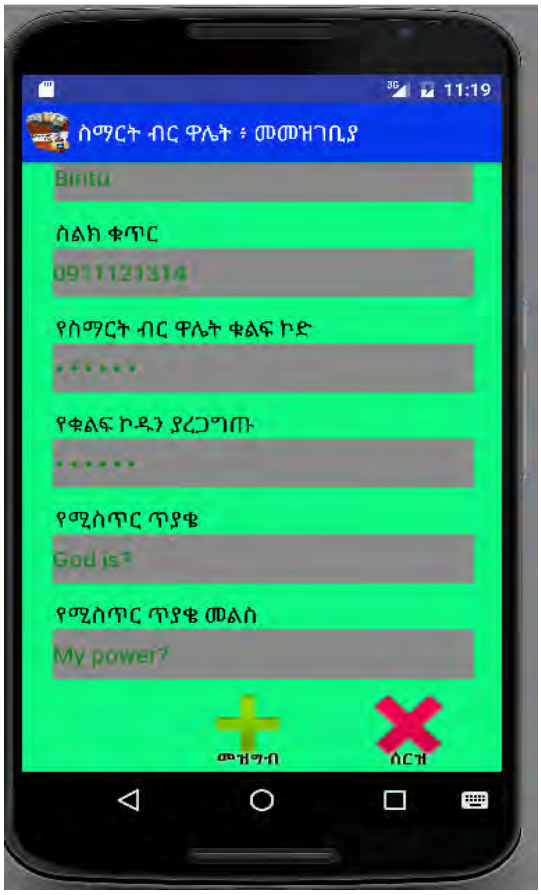


Figure 5.4: User Registration User Interface

Figure 5.5: Smart Birr Wallet Services User Interface

There are mainly five major services provided by Smart Birr wallet and each service is represented with unique icons and labels in order to easily identify each of them as shown in Figure 5.5. The first one represented with number 1 is a withdrawal service that allows the user to withdraw Smart Birr from his/her smart mobile money account in the server and store it in the wallet. Once Smart Birr is downloaded, users can use them for payment or purchasing goods and services. The second one represented with number 2 is a deposit service that allows the user to deposit Smart Birr into his/her smart mobile money account in the server. The third one represented with number 3 is a payment service that allows the user to pay for goods and services. The forth one represented with number 4 is transaction controller service that shows the flow of transaction in detail. Finally, a key exchanger service represented with number 5 is another service provided by Smart Birr wallet in order to allow users to change their key pass whenever necessary.

5.2.3 Smart Birr wallet Withdrawal Engine

Whenever a user, in this context Biritu, clicks on a withdrawal service icon represented by number 1 Figure 5.5, Withdrawal Engine component of a Smart Birr wallet is started and withdrawal service user interface is displayed as shown in Figure 5.6. The withdrawal interface has four main sections. The first section represented with number 1 shows ordered Ethiopian currency notes that enable the user to select any of Ethiopian currency notes required to be generated and downloaded from the server or service provider. When a user selects one of any currency notes, Withdrawal Engine encodes economic value of selected currency notes. For example, if Biritu selects currency notes with 100 birr and 50 birr, Withdrawal Engine encodes these economic values and requests the service provider in order to generate real Smart Birr with its economic value of 100 and another Smart Birr with economic value of 50. The second section represented with number 2 displays currency notes selected by the user. The third section represented with number 3 displays the total amount of Smart Birr for withdrawal. Finally, the last section represented by number 4 enables the user to send a withdrawal command to Withdrawal Engine. Then, Withdrawal Engine creates a transaction and sends Smart Birr withdrawal request to the server through end-to-end secured channel. Accordingly, the server processes the request if and only if the request is authenticated successfully, that is, the user is legal and authorized. Then the server checks Biritu's balance. If Biritu has sufficient balance, the server generates Smart Birr objects encapsulating universally unique serial number, economic value, nation identifier, icon, and signature and sends the response back to the Withdrawal Engine. A java code used to generate Smart Birr is provided in Annex B. When the response is arrived in the wallet to Withdrawal Engine, Withdrawal Engine verifies each Smart Birr sent from the server. If each Smart Birr is valid, Withdrawal Engine stores each Smart Birr in the smart mobile money wallet.

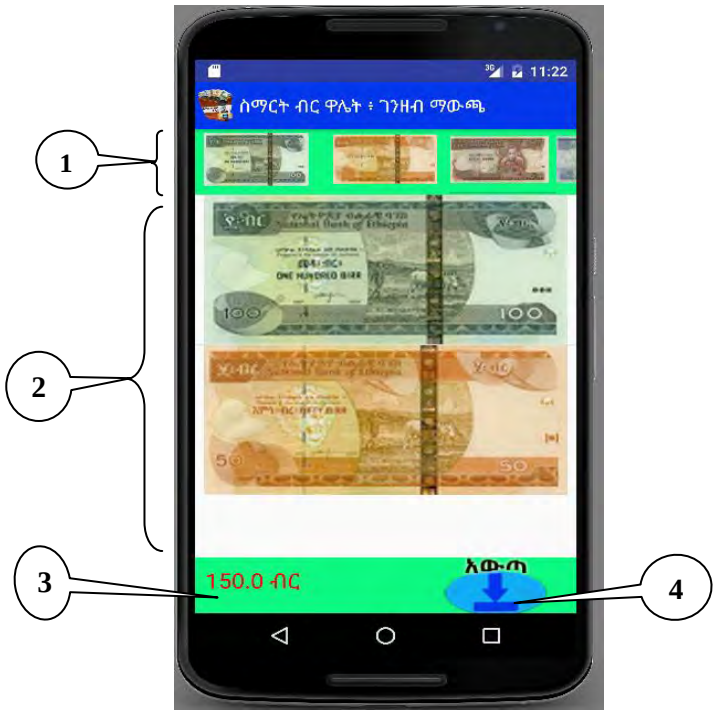


Figure 5.6: Smart Birr Withdrawal Service User Interface

5.2.4 Smart Birr Wallet Payment Engine

If real Smart Birr is available in the wallet, a user can pay/transfer them to purchase goods and services offline. This can be done with in a very short range of NFC communication between the Payer and the Payee using Smart Birr wallet by tapping their smart phones each other. Figure 5.8 shows Smart Birr payment interface that enables the user to transfer Smart Birr to purchase goods and services. Parts of payment interface represented by number 1 displays only available Smart Birr in the wallet. In this case, Biritu has only one hundred birr and fifty birr currency notes downloaded from her account in the server.

Since one hundred birr currency note has already been selected and be ready for payment, the Payment Engine automatically shows that only one hundred birr note is available in the wallet and allows the user to select it only once. A section of the payment interface represented by number 2 shows selected currency notes ready for payment while number 3 shows total amount of values to be paid. In this case, only one hundred birr is ready for payment. Once all required currency notes are arranged and ready for payment, a user can send payment command for Payment Engine by clicking on the icon indicated by number 4. Consequently, Payment Engine

encodes the Smart Birr ready to be transferred and prompts the user to tap the smart phone with Payee's smart phone.

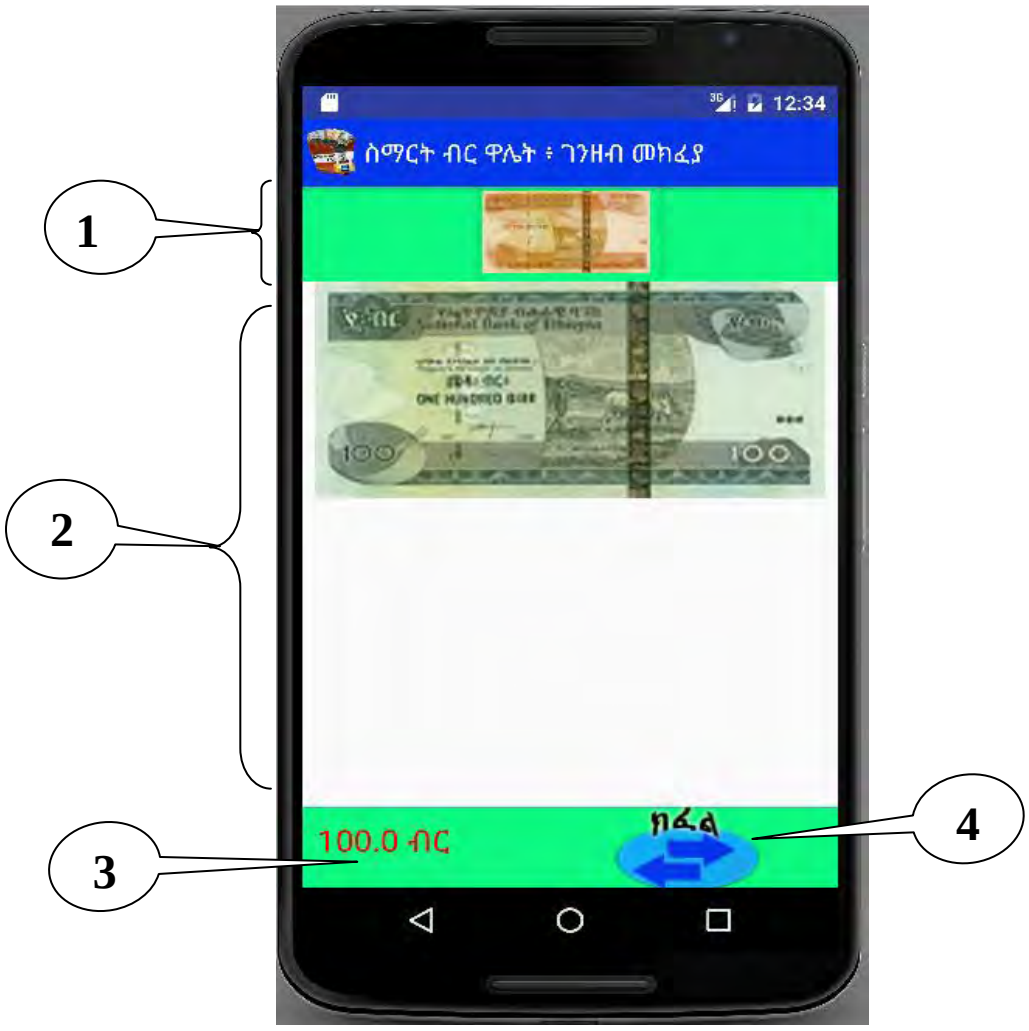


Figure 5.7: Smart Birr Wallet Payment Service User Interface

For demonstration, assume that Biritu wants to pay one hundred birr for Biru to purchase flash disk. When Biritu confirms the payment, after the Smart Birr is detected as valid by Smart Birr Detector successfully, Payment Engine credits Biru's wallet, debits Biritu's wallet and send notification message. Then Payment Engine displays transferred Smart Birr on Biru's smart mobile money wallet. Once Biru received verified real Smart Birr, he can use it for another payment or deposit to the server.

5.2.5 Smart Birr Wallet Deposit Engine

Whenever a user wants to deposit Smart Birr into his/her account in the server, he/she can use Smart Birr wallet deposit service. Figure 5.8 shows Smart Birr wallet deposit interface that enables a user to interact with the wallet in order to deposit real Smart Birr into his/her account in the server. When a user opens Smart Birr wallet deposit service, Deposit Engine automatically displays available Smart Birr only stored in the wallet. A section of the interface represented by 1 is empty to indicate that no other Smart Birr are available in Biru's smart mobile money wallet except the one which is received from Biritu. As indicated with number 2 in Figure 5.7, selected currency note is displayed for the user and number 3 indicates total amount of Smart Birr ready for deposit. Then a user can click on the icon indicated by number 4 in order to send a deposit command for Deposit Engine. Accordingly, Deposit Engine creates and encodes a transaction encapsulating list of selected Smart Birr and a user account number, and finally sends deposit request to the server through an end-to-end secured channel. When the request arrives in the server, the server then authenticates the request and processes the transaction. If the server verifies each Smart Birr and approves the validity of each Smart Birr, the server credits users account and sends acknowledgement message back to the wallet. Consequently, when the acknowledgement arrives in the wallet, Deposit Engine debits the wallet and notifies the user.

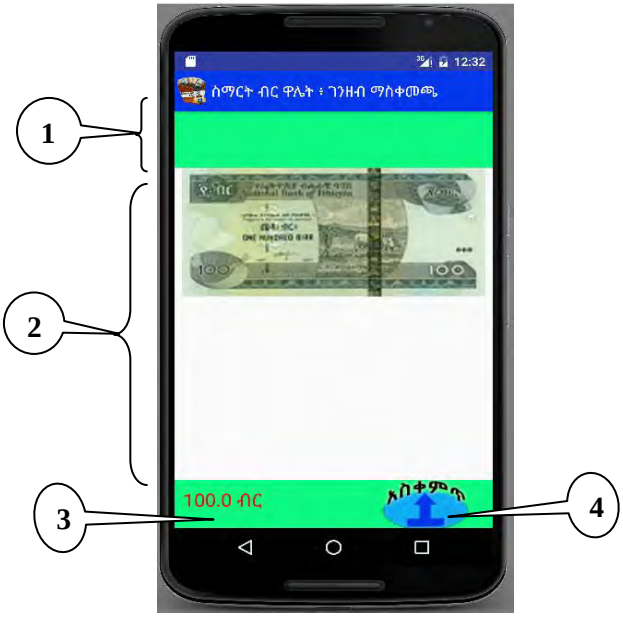


Figure 5.8: Smart Birr Wallet Deposit Service User Interface

For demonstration, assume that Biritu has transferred one hundred birr to Biru and Biru wants to deposit this one hundred birr to the server. When Biru opens Smart Birr wallet deposit service, the wallet only shows, as shown in Figure 5.8, one hundred birr stored in the wallet. Accordingly, he can select it and deposits to his account in the server.

Whenever users make a transaction, associated transaction log is created and stored in the wallet. Transaction log mainly encapsulates transaction number, amount, transaction type, date, and flow of particular transaction. Figure 5.9 shows user interface to control flow of transactions. Smart Birr may flow from server to wallet during withdrawal, wallet to server during deposit, and wallet to wallet during payment. The first section of the interface represented by number 1 displays general information related to user account balance in the server, Smart Birr wallet balance, and total amount of balance stored both in the wallet and in the server. The second section of the interface represented by number 2 shows the flow of transactions done in the last month starting from the recent one in decreasing order.

For demonstration, assume that Biritu has saved seventy five thousand birr in her account in the server and she withdraws one hundred fifty birr from the server and pays one hundred birr to purchase flash disk. Based on these transactions, Figure 5.9 shows the transactions made by Biritu.

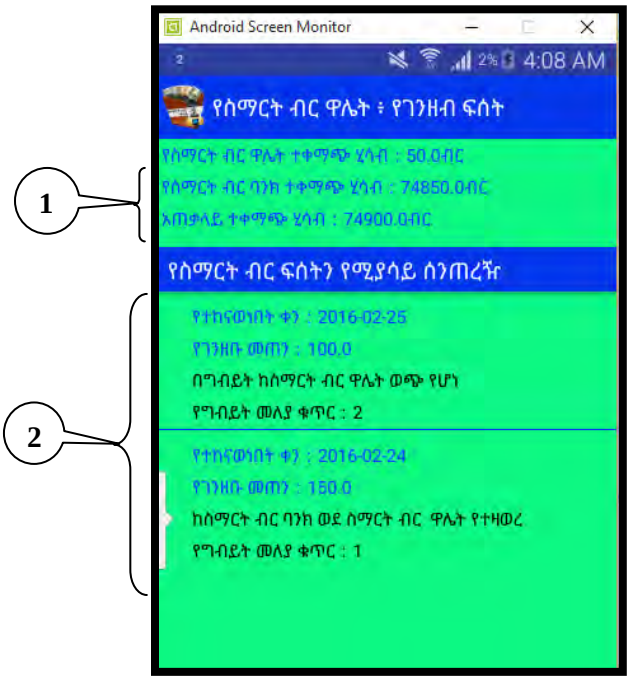


Figure 5.9: Smart Birr Wallet Transaction Flow

5.3 Proposed Model prototype Performance Evaluation

In computer system, the performance of an application is usually measured by evaluating the processing time required to complete a give task and the memory capacity required to be reserved while processing this task. It is known that Central Processing Unit (CPU) and Random Access Memory (RAM) are the most precious and limited resource of the computer system that are highly used for computing power.

As a result, critical and major tasks of the proposed model prototype are identified in order to measure the processing time required to complete the task. In addition, the memory size required to be reserved for each Smart Birr during processing of different transactions is measured and quantified. In this context, processing time is the amount of time measured in milliseconds for which CPU was used for processing instruction of a given task or transaction of the Smart Birr wallet while memory size is the amount of storage space reserved for each Smart Birr objects during the execution of a given task or transaction.

The amount of the processing time for a given task is evaluated in milliseconds programmatically by computing the difference of the starting and ending execution time of a given task. The amount of the memory size for a given Smart Birr object is measured programmatically by computing the difference of free total memory before memory space is reserved for Smart Birr object and free total memory after memory space is reserved for Smart Birr object during execution using Java runtime environment.

The processing time required to process withdrawal, deposit, and payment transaction for each Smart Birr is evaluated 50 times in the experiment until satisfactory result is obtained so that an average processing time required to process each transaction is computed and quantified. In the same manner, an average processing time required to generate and detect each Smart Birr is computed and quantified. Communication time is considered as an external factor that may vary the experiment result depending on the communication technology used.

As Table 6.1 shows, the experiment was operated on Samsung Note 4 smart phone with NFC, 2.7 GHz quad-core processor, 3GB RAM, Wi-Fi, and android lollipop 5.1 operating system. On the server side, the experiment was operated on Dell Inspiron 5537 with Virtual router for Wi-Fi hotspot, Intel (R) Core i7 2.8 GHz processor, 8 GB RAM, 64 bit Windows 10 operating system as shown in Table 6.2.

Table 5.1: Client Side Testing Environment Requirements

Items	Requirements
CPU	Quad-core 2.7 GHz processor
RAM	3 GB
Operating System	Android lollipop 5.1
Wi-Fi	Yes
NFC	Yes
Development Tools	SQLite, Spongy Castle 1.5,Android Studio 1.5.1, and Apache HTTP client 4.5.1

Table 5.2: Server Side Testing Environment Requirements

Items	Requirements
CPU	Quad-core 2.8 GHz processor
RAM	8 GB
Operating System	64 bit Windows 10
Router	Virtual Router
Development Tools	MySQL server 5.7, Jersey 2.2, Apache, Tomcat Server 8.0, Apache HTTP client 4.5.1, Bouncy Castle 1.5, and Eclipse 4.5

A. Processing Time to Generate Smart Birr

In order to generate Smart Birr, the server processes different tasks like generating universally unique serial number, signature, and unique icon. For this mater, the processing time required to generate particular Smart Birr is measured and evaluated by testing five times for each particular Smart Birr. Figure 6.1 shows the time difference of processing time for each five tests.

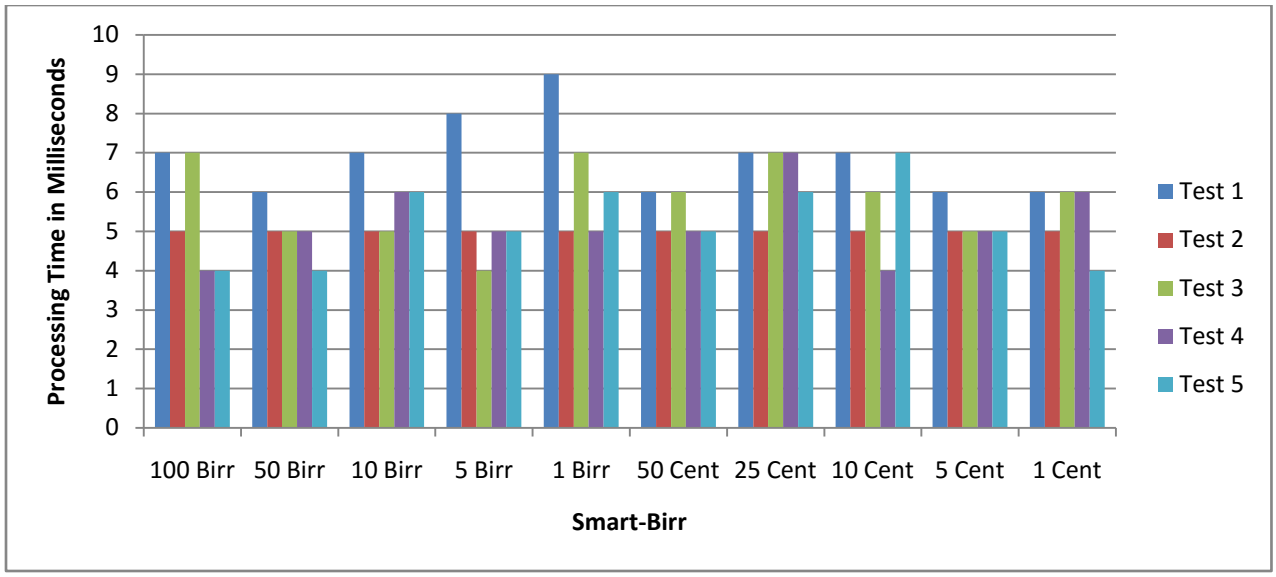


Figure 5.10 : Evaluation of Processing Time for Generating Smart Birr

As a result, approximately 5.62 milliseconds processing time is required to generate a particular Smart Birr.

B. Processing Time to Validate Smart Birr

Each Smart Birr is validated in each transaction to avoid counterfeit. As a result, the processing time required to detect particular Smart Birr is measured and evaluated by testing five times for each particular Smart Birr. Figure 6.2 shows the time difference of processing time for each five tests used to detect each particular Smart Birr.

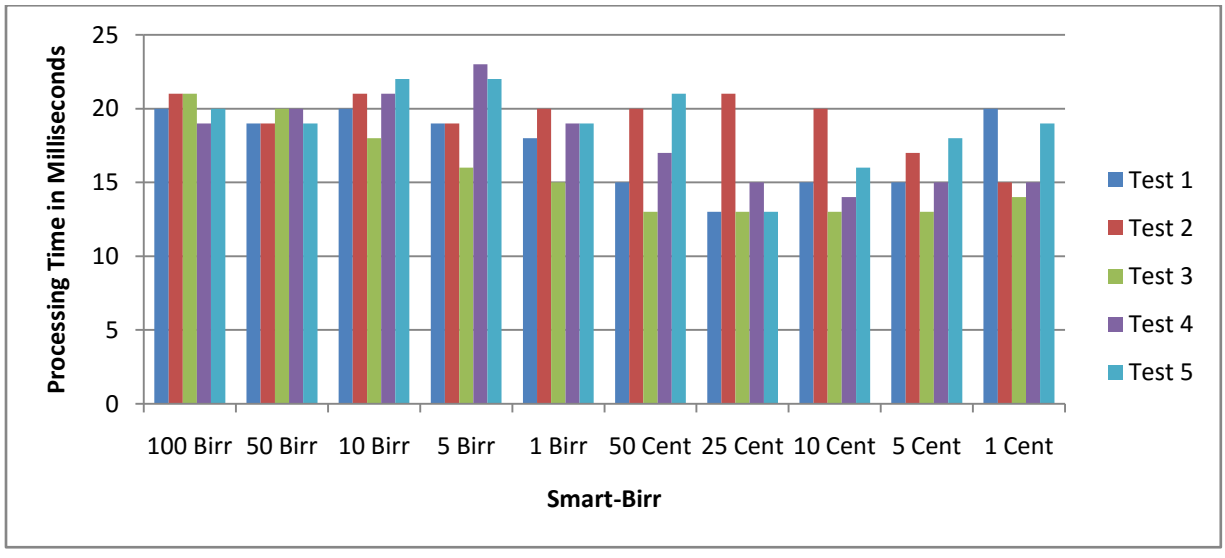


Figure 5.11: Evaluation of Processing Time for Validating Smart Birr

As a result, approximately 17.8 milliseconds processing time is required to detect each of the Smart Birr.

C. Smart Birr Withdrawal Processing Time

During Smart Birr withdrawal, various operations are executed both in the client and server side. The performance of the system required to process each Smart Birr withdrawal starting from the withdrawal request up to the completion is measured and evaluated as shown in Figure 6.3.

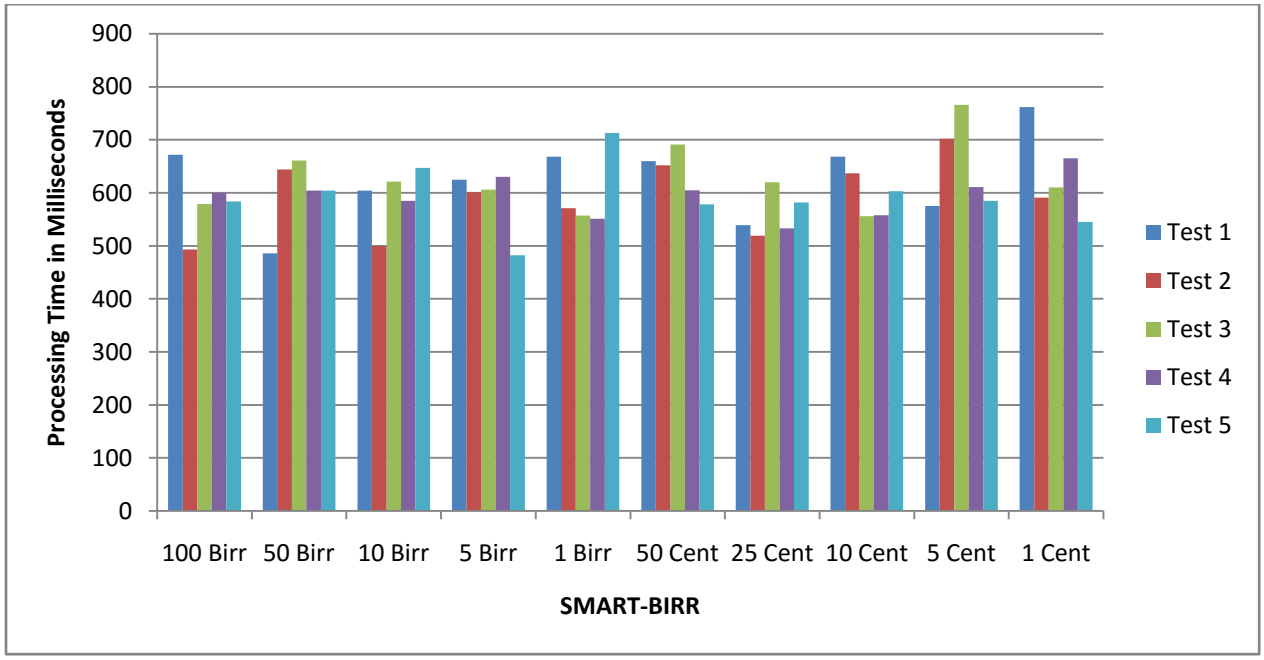


Figure 5.12 : Evaluation of Processing Time for Processing Smart Birr Withdrawal

As a result, approximately 606.02 milliseconds processing time is required to withdraw particular Smart Birr.

D. Smart Birr Deposit Processing Time

Like Smart Birr withdrawal, there are various computations expected to be computed both in the client and server side such as business computation, security computation like cryptographic computations, and communication via wireless network in the testing environment. The performance of the system required to process each Smart Birr deposit starting from the deposit request up to the completion is measured and evaluated as shown in Figure 6.4.

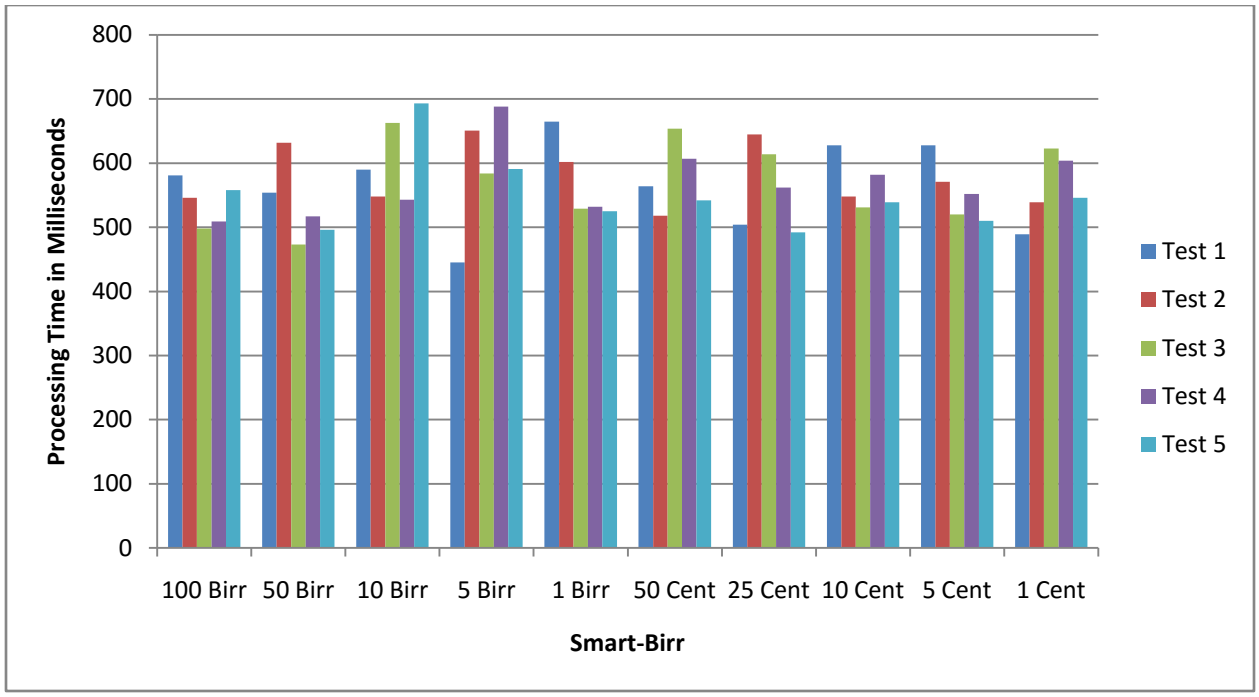


Figure 5.13: Evaluation of Processing Time for Processing Smart Birr Deposit

As a result, approximately 566.5 milliseconds processing time is required to deposit particular Smart Birr.

E. Smart Birr Payment Processing Time

Unlike Smart Birr withdrawal and deposit, the payment is taken place using NFC with in very short range communication line without the interference of third party. However, there are also various computations both in the Payer and Payee side such as business computations, security computations, and communication via NFC to complete payment process. The performance of the system required to process each Smart Birr payment starting from payment initialization up to its completion is measured and evaluated as shown in Figure 6.5.

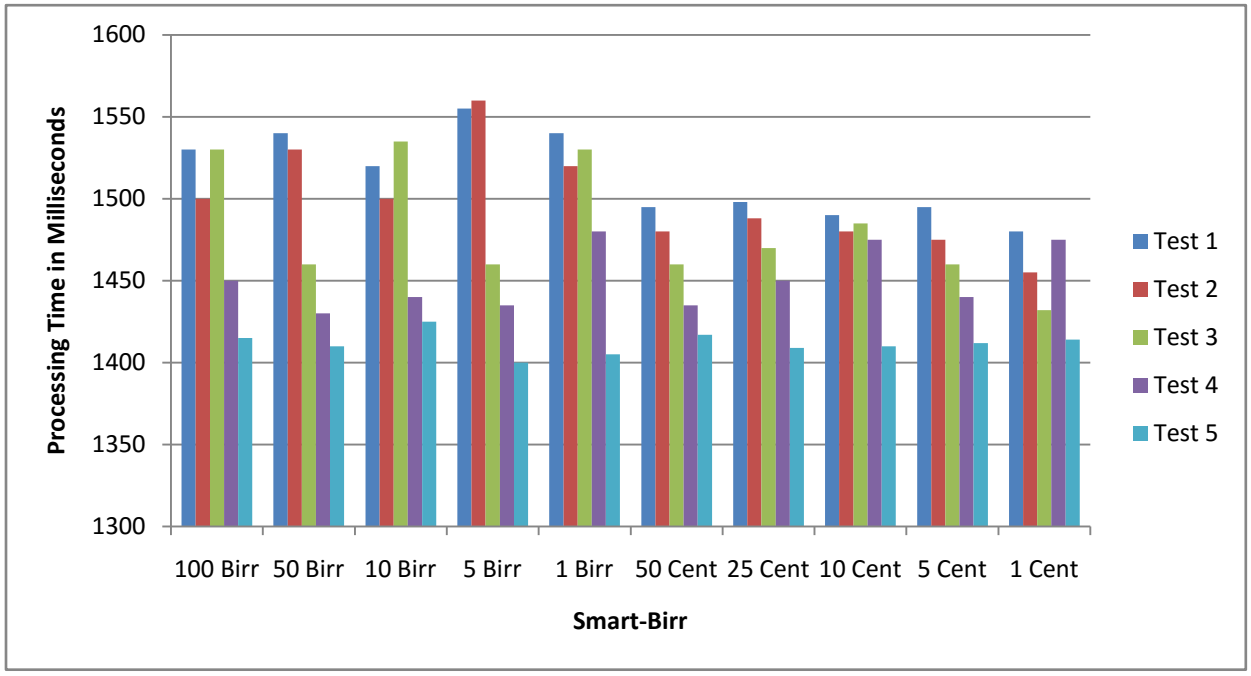


Figure 5.14: Evaluation of Processing Timefor Processing Smart Birr Payment

As a result, approximately 1471.6 milliseconds processing time is required to pay particular Smart Birr.

F. Smart Birr Memory Size

The real world Ethiopian currency notes are modeled and created as an object in side computer system. These objects reserve a computer memory that is scarce resource and has a great factor for the performance of the computer especially for lightweight devices such as smart phone. As a result, memory size required to be reserved during each Smart Birr processing is measured and evaluated. As a result, an average memory size required to be reserved during each Smart Birr processing is 536 byte.

5.4 The Prototype Usability Testing

In this section, usability of Smart Birr wallet from different perspective is evaluated from different users' perception. Smart Birr wallet needs to be highly usable by a large cross section of the population to be feasible.

The following usability criteria are used in order to evaluate usability of the prototype

Simplicity: Smart Birr wallet needs to be easy to use by broader set of people of different ages and technical competency and literacy.

Accuracy: Smart Birr wallet needs to be accurate enough for any kind of transaction with various amount and types of Smart Birr.

Security: Smart Birr wallet needs to be secured for any transaction.

Speed: Smart Birr wallet needs to be fast to use even as compared with real world material money.

In order to evaluate users' perception about the simplicity, accuracy, security, and speed of Smart Birr transactions, participants are selected purposely from different occupations. As a result, selected participants were composed of 7 students, 7 merchants, 7 instructors, 7 housewives, and 7 bank workers from technical and non-technical majors. Each participant was asked to complete a short demographics survey to determine his or her familiarity with smart phone technology and technical competency. The demographic survey questions prepared and provided for participants are shown in Annex A - Questionnaire Table 6.1.

Based on the answers given, participants are categorized into three groups namely novice, intermediate, and expert. Table 6.3 shows the participant demographics. Participants were provided with smart phones, basic training in how to use the phone and the NFC capability, and instructions for each activity in Smart Birr wallet before experiment. The training is equally provided for the three groups how they can use the Smart Birr wallet one by one. During the training, it is observed that the novice participants can easily learn and quickly adapt the Smart Birr wallet activities as easy as intermediate and expert participants adapt. It is also observed that participants with different education level can easily learn and adapt the Smart Birr wallet after the training is provided equally that implies the education level has no a great factor to learn and use the Smart Birr wallet.

For the experiment, all categories of participants are ordered to make Smart Birr withdrawal, deposit, and payment transactions. For experimenting payment transaction, an experimenter played the role of the other person involved in the Smart Birr payment transaction. As a result, all the three categories of participants namely novice, intermediate and expert users performed all the transactions successfully.

Table 5.3: Demographic Statistics of Participants for Usability Testing

Total number	35
Education Level	No Education (0) , Elementary (2), Secondary (3), Preparatory (3) , Certificate (4) , Diploma (4), BSc (12), MSc (6), PHD (1)
Proficiency level	Novice (8), intermediate (11), Expert (16)
Types of Phone	Smart phone (16)

After the completion of all experiments, participant perceptions are measured through a simple questionnaire provided in Annex A - Questionnaire Table 6.2 considering four major criteria such as simplicity, accuracy, security, and speed of Smart Birr wallet relative to cash transactions. Figure 6.6 shows experiment results.

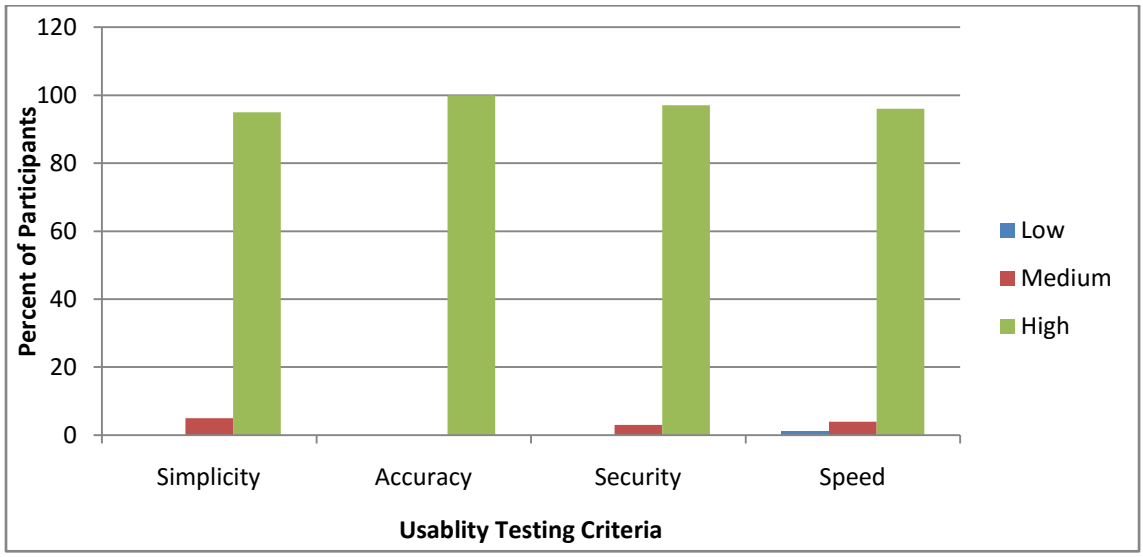


Figure 5.15: Usability Testing Experiment Result

According to the experiment result, 95% of participants have agreed that Smart Birr wallet has higher simplicity; 100% of participants have agreed that Smart Birr wallet has higher accuracy; 97% of participants have agreed that Smart Birr wallet has higher security; and 96% of participants have agreed that Smart Birr wallet has higher speed than cash based transaction. To

sum up, approximately 97% of 35 participants have agreed that Smart Birr wallet has higher usability than cash based transaction.

5.5 Summary

In this chapter, appropriate tools and technologies used to develop the proposed model prototype are briefly presented and described. Next to that, demonstration and implementation details of major components of the proposed model prototype are illustrated and presented.

As the prototype shows, an easy-to-use and interactive user interface is designed that can be easily learned and adapted by users including less educated users who have basic computer literacy but cannot read and write.

Processing Time experiment result shows that 5.62 milliseconds, 17.8 milliseconds, 606.02 milliseconds, 566.5 milliseconds, and 1471.6 milliseconds processing time are required in order to generate, detect, withdraw, deposit, and pay particular Smart Birr respectively. Moreover, in usability testing experiment result, 97% of 35 participants have agreed that Smart Birr wallet has higher usability than cash based transaction. In the experiment, it is observed that novice, intermediate and expert users can equally perform Smart Birr transactions easily. In addition to this, it is also observed that users' education level has no great factor to learn and adopt Smart Birr wallet.

In general, Smart Birr wallet has achieved simplicity with accuracy and end-to-end security. Several features are implemented in Smart Birr wallet in order to make it as usable as cash payments while preserving strong security.

Chapter 6
Conclusions and Future Works

Currently, smart phones with ever-increasing features and capabilities are being manufactured and massive amount of population throughout the world is highly dependent on technologies in order to make their life simple and smarter. As a result, creating innovative ideas and providing most important capabilities of smart phones in order to manage money and designing easy-to-use digital money user interface is key and novel idea. This chapter presents the summary of various works presented in this thesis and the vital contribution of the research work in the digital money ecosystem that creates a new capability to the smart phones in order to manage smart money. Moreover, the future works of the research are presented in this chapter.

6.1 Conclusion

This work proposed smart mobile money wallet and offline payment model which enables the user to withdraw smart money and store it in the mobile wallet. Once smart money is stored in the wallet, users can use them for offline payment without needing online connection and an involvement of a third party. When users want to save or deposit this smart money into their account in the smart mobile money server, they can make use of it anywhere and anytime they get online connection. In this work we have accomplished the following tasks:

We proposed a novel model for smart mobile money wallet and offline payment in order to address the gaps identified in the current mobile money systems. The different components of the proposed model and their operations, interactions, and associated algorithms are presented in depth in chapter 4. This includes the components of the model: Registration Engine, Withdrawal Engine, Deposit Engine, Payment Engine, Smart Crypto, Smart Money Detector, Smart Money Transaction Engine, Message Authentication Engine, Smart Money Object Generator on the client and server side of the smart mobile money wallet.

We then implemented the model for Ethiopian currency. As a result, a Smart Birr, is created. Very recent and proven technologies are used to develop the Smart Birr Wallet. The developed

system is tested on Android Smart Phone. The biometric authentication is tested on an Android emulator.

Finally, Processing Time evaluations and experiments are conducted. The Processing Time experiment result showed that 5.62 milliseconds, 17.8 milliseconds, 606.02 milliseconds, 566.5 milliseconds, and 1471.6 milliseconds processing time is required in order to generate, detect, withdraw, deposit, and pay particular Smart Birr respectively which are affordable by the current computing devices. In the usability experiment, 97% of participants have agreed that Smart Birr wallet has higher usability than cash based transaction. As a result, the real world material money or cash payment is properly modeled while preserving strong security.

6.2 Contributions

The followings are the main contribution of this thesis:

1. A novel generic model for smart mobile money wallet and offline payment is proposed.
2. Algorithms for the implementation of each components of the proposed model are designed.
3. A multi-layer authentication scheme that is proven to be effective is employed.
4. An end-to-end secured communication technique is employed.
5. A new approach to withdraw or deposit smart money anytime and anywhere without appearing physically to the banks, agents, or ATMs unlike the existing digital money systems and the traditional financial institutions is proposed.
6. A new approach of digital money structure (smart money) that resembles the real world material money abstract features is proposed.
7. Smart money detector that detects the validity of smart money during transaction is proposed.

6.3 Future Works

In the future, we plan to extend the existing work to address the following issues:

1. Authentication is one of the major security requirements that every computer system should improve and achieve. Due to this fact, in the future, researchers would like to extend the research to incorporate and integrate other biometric identification such as

multi-modal biometrics authentication techniques like voice recognition in addition to fingerprint.

2. Once again, security is every ones major question and crucial problem in the computer system that cannot be satisfied 100% perfectly. Due to this fact, security holes should be identified and an improvement should be done all the time to enhance security of any system. As a result, researchers would like to extend the research to incorporate and integrate double spending detector system in order to detect attempts of cloning, copying, and spending Smart Birr.
3. During real deployment of the proposed model, researchers would like to incorporate a trusted third party in order to certify digital signatures.
4. Currently, online withdrawal and deposit transactions between the user and service provider/ smart bank, and offline payment between users are designed and implemented. In order to provide full services in the real world, this research has to be extended to design and implement online smart money transfer between users.
5. In the real world, huge investment is required to open branches of traditional financial institutions. In our case, there would not be such branching demanding huge investment instead the researchers will dig more in the future to create smart bank/virtual bank that facilitates banking services virtually. As a result, users can be customers as a banker since they do have a branch of virtual bank in their pocket in order to handle the flow of smart money and extend the smart mobile money services for the broader set of people.

Reference

[1] GSMA Intelligence, "The Mobile Economy," Report, 2015, retrieved from http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf, Last accessed on March 03, 2016.

[2] Jenkins B., "Developing mobile money ecosystems," International Finance Corporation and Harvard Kennedy School, Washington, DC, 2008.

[3] GSMA Intelligence, "The Mobile Economy," Report, 2014, retrieved from http://www.gsmamobileeconomy.com/GSMA_ME_Report_2014_R2_WEB.pdf, Last accessed on January 08, 2015.

[4] Matthew R., Nicholas J., Mark N., Thecla M., and Guillermo E., "Maximizing Digital Service Opportunities," Informa UK Ltd, 2013.

[5] Seungjae S. and Wonjun L., "A Comparative Study of Smartphone User's Perception and Preference Towards Mobile Payment Methods In The U.S. and Korea," *The Journal of Applied Business Research* , Vol. 30, No. 5, 2014, pp. 1365-1376.

[6] Santi R., "Advanced Mobile Payment," White paper, 2012, retrieved from https://atos.net/content/dam/global/ascent-whitepapers/ascent-whitepaper-advanced-mobile-payment.pdf, Last accessed on January 08, 2015.

[7] Mesfin Woldemariam, Gheorghita Ghinea, and Solomon Atnafu, "Towards A Digital Money Structure for Illiterate Users," *Twenty Second European Conference on Information Systems*, Tel Aviv, 2014.

[8] Zanita Z. , Stuart H., Philippa W., and Mark G., "Perceived risk and Chinese consumers: Internet banking Service Adoption," *International Journal of Bank Marketing*, Vol. 26, No. 7, 2008, pp. 505-525.

[9] Wondwossen Taddesse and Tsegai G. Kidan, "E-Payment: Challenges and Opportunities in Ethiopia," United Nations Economic Commission For Africa, 2005, retrieved from http://www.ethioconstruction.net/sites/default/files/Law/Files/ePayment%20Study.pdf, Last accessed on January 1, 2015.

[10] Mohammad O., "Factors Affecting Adoption of Electronic Banking: An Analysis of the Perspectives of Banks Customers," *International Journal of Business and Social Science* Vol. 3, No. 17, 2012, pp. 294-309.

[11] Haruna I., "Challenges of Electronic Payment Systems in Ghana: The Case of e-ZWICH," *American Journal of Business and Management*, Vol.1, No. 3, 2012.

[12] Belaynew Asrie and Venkati P., "Electronic Commerce: Opportunities and Challenges of general importers in Addis Ababa," Unpublished Masters Thesis, Addis Ababa University, 2012.

[13] Taiwo Olufemi, Tajudeen John and Ebenezer Yemi, "Electronic Payment System In Nigeria: Implementation Constraints And Solutions," *Journal of Management and Society*, Vol. 1, No. 2, 2011, pp. 16-21.

[14] Akudo C. Anyanwu, Absalom E. Ezugwu and Sale E. Abdullahi , "Electronic Payment System (EPS): Facilitating the Development and Adoption in Nigeria", *International Journal of Computer Science Issues*, Vol. 9, No. 1,2012, 462-467.

[15] Gardachew Worku, "Electronic-Banking in Ethiopia Practices, Opportunities and Challenges," *Social Science Research Network*, 2010.

[16] Tu'emay Aregawi, "The Anti-Money Laundering and countering Terrorist Financing Regime in Ethiopia," Second Assessment Report, Center on Global Counterterrorism Cooperation, 2013, retrieved from http://www.globalcenter.org/wp-content/uploads/2013/03/13Feb27_EthiopianFIC-SecondAsmntRpt_TAD_Final.pdf, Last accessed on January 20, 2015.

[17] International Organization for Migration, "Mobile Money Service: A bank in your pocket overview and opportunities," 2014, retrieved from https://publications.iom.int/books/mobile-money-services-bank-your-pocket#sthash.8fPbgdrc.dpuf, Last accessed on January 25, 21015.

[18] Kazan, Erol, Damsgaard, and Jan, "An Investigation of Digital Payment Platform Designs: A Comparative Study of Four European Solutions," *Twenty Second European Conference on Information Systems*, Tel Aviv, 2014.

[19] Isaac Mbiti, David N. and Weil, "Mobile Banking: The Impact of M-PESA in Kenya," National Bureau of Economic Research, Massachusetts Avenue, Cambridge, 2011, retrieved from www.nber.org/papers/w17129.pdf, Last accessed on January 25, 2015.

[20] M. Yasmina, McCarty and Roar Bjaerum, "Easy paisa: Mobile Money Innovation in Pakistan," 2014, retrieved from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/07/Telenor-Pakistan.pdf, last accessed on January 25, 2015.

[21] Cisco, "MTN Mobile Money Service", 2012, retrieved from https://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1058/Cisco_MTN_CS.pdf, Last accessed on January 25, 2015.

[22] Brian Richardson, "WIZZIT," retrieved from http://cab.org.in/ICTPortal/Lists/International%20Experience/Attachments/9/wizzit_may07_presentation.pdf, Last accessed on January 25, 2015.

[23] Institute for Money, Technology and Financial Inclusion, "Mobile Money as A Complementary Form of Savings," retrieved from http://www.imtfi.uci.edu/files/2012-7_nandhi_flyer_2.pdf, Last accessed on January 25, 2015.

[24] GSMA Intelligence, "Mobile Money for Unbanked", 2014, retrieved from http://www.gsma.com/mobilefordevelopment/wp-content /uploads/2014/05/MMU_Cote_dIvoire_Turnaround_Story.pdf, Last accessed on January 25, 2015.

[25] Katharine M., Michelle K., and Jamie M., "Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks", 2015, retrieved from http://www.cgap.org/sites/default/files/Focus-Note-Doing-Digital-Finance-Right-Jun-2015.pdf, Last accessed on January 25, 2015.

[26] World Bank Development Research Group, "The Opportunities of Digitizing Payments," 2014, retrieved from https://docs.gatesfoundation.org/documents/G20%20Report_Final.pdf, Last accessed on January 26, 2015.

[27] Llewellyn D. W. Thomas, Antoine Vernet and David M. Gann, "Digital Money: How Ready are Countries to Adopt?," *DRUID Society Conference*, Copenhagen, 2014.

[28] Carolyn Wilkins, "Money in a Digital World," Wilfrid Laurier University Waterloo, Ontario, 2014.

[29] Heinz Kreft, "Cashing Up With Mobile Money – The FairCASH Way," Institute for Informatics, University of Kiel, 2005.

[30] "Electronic Payment System", retrieved from http://ocw.metu.edu.tr/pluginfile.php/354/mod_resource/content/0/Lecture_4.pdf, Last accessed on May 12, 2015.

[31] Norman Lonergan and Jonathan Dharmapalan, "Mobile Money: An overview for global telecommunications operators," EYGM Limited, 2009, retrieved from

http://www.ey.com/Publication/vwLUAssets/Mobile_Money./$FILE/Ernst%20&%20Young%20-%20Mobile%20Money%20-%2015.10.09%20(single%20view).pdf, Last accessed on May 12, 2015.

[32] ITU-T Technology Watch Report, "The Mobile Money Revolution: NFC Mobile Payments," Part 1, 2013, retrieved from https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200001PDFE.pdf, Last accessed on May 12, 2015.

[33] ITU-T Technology Watch Report, "The Mobile Money Revolution: Financial Inclusion Enabler," Part 2, 2013, retrieved from https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200002PDFE.pdf, Last accessed on May 12, 2015.

[34] "Mobile Money: For Business Development in the east African community, A Comparative Study of Existing Platforms and Regulations," United Nations Publication, 2012, retrieved from http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf, Last accessed on May 12, 2015.

[35] Eric K. A., Raymond S. M. and Maung K. S., "Mobile Money Security," Masters Thesis, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 2013, retrieved from

[36] Sarah Rotman, "Bitcoin Versus Electronic Money," CGAP Publication, 2014.

[37] Guilin Wang, "Digital Cash," The School of Computer Science, University of Birmingham, 2010.

[38] European Central Bank, "Virtual Currency Scheme," 2012, retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, Last accessed on May 16, 2015.

[39] Benton E. Gup, "What Is Money? From Commodities to Virtual Currencies/Bitcoin," Alternative Investment Analyst Review, University of Alabama, 2014, retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172, Last accessed on May 16, 2015.

[40] Otieno Linah , "Mobile money transfer: A focus on the impact and usage", Masters Thesis, Department of Management, Laurea University of Applied Sciences, 2013, retrieved from https://www.theseus.fi/xmlui/bitstream/handle/10024/59926/Thesis%20Linah.pdf?sequence=1, Last accessed on May 16, 2015.

[41] Smart Card Alliance, "The What, Who and Why of Contactless Payments," White Paper, 2006, retrieved from http://www.smartcardalliance.org/publications-contactless-payments-what-who-why/, Last accessed on May 16, 2015.

[42] United States Agency for International Development, "Standards and Practices Report for Electronic and Mobile Payments," White paper, 2012, retrieved from http://solutionscenter.nethope.org/case_studies/view/standards-and-practices-report-for-electronic-and-mobile-payments, Last accessed on May 16, 2015.

[43] ISACA, "Mobile Payments: Risk, Security and Assurance Issues," White Paper, 2011, retrieved from http://www.isaca.org/groups/professional-english/pci-compliance/groupdocuments/mobilepaymentswp.pdf, Last accessed on May 16, 2015.

[44] Erin F. Fonté, "Mobile Payments In The United States: How Disintermediation May Affect Delivery Of Payment Functions, Financial Inclusion And Anti-Money Laundering Issues," *Washington Jornal of Law Mobile Money Symposium*, Vol. 8, No. 3, 2013.

[45] Suzanne Cluckey, "Mobile Payments," 2011, retrieved from http://www.mobilepaymentstoday.com/whitepapers/mobile-payments-101-retail/, Last accessed on May 16, 2015.

[46] Emmanuel A. and Jacobs B.,"Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services," Radboud University Nijmegan, The Netherland, 2007, retrieved from www.cs.ru.nl/mtl/scripties/2007/EmmanuelAbunyangScriptie.pdf, Last accessed on July 12, 2015.

[47] Tang, J., Terziyan V. and Veijalainen J., "Distributed PIN verification scheme for improving security of mobile devices," Mobile Networks and Applications, vol. 8, 2003, retrieved from http://link.springer.com/article/10.1023%2FA%3A1022289231864#/page-1, Last accessed on July 12, 2015.

[48] Luo H., Kong J., Zerfor P., Lu S., and Zhang L., "Providing robust and ubiquitous security support for mobile adhoc networks," 2001, retrieved from http://netlab.cs.ucla.edu/wiki/files/ICNP01-jkong.pdf, Last accessed on July 12, 2015.

[49] Agarwal S., Khapra M., Menezes B., and Uchat N., "Security Issues in Mobile Payment Systems," Citeseer, 2007, retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.8225&rep=rep1&type=pdf, Last accessed on July 12, 2015.

[50] Anil K., Arun R., and Salil P., "An Introduction to Biometric Recognition, Appeared in IEEE Transactions on Circuits and Systems for Video Technology," Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, 2004.

[51] Pual B., "Examining Mobile Payments – Now and in the Future," Cotignac Synopsis, 2014.

[52] Marianne C. and Elisa T., "Mobile Phone Technology: "Smarter" Than We Thought," Federal Reserve Bank of Boston, 2012.

[53] Smart Card Alliance, "The Mobile Payments and NFC Landscape: A U.S. Perspective," White Paper, 2011, retrieved from http://www.smartcardalliance.org/resources/pdf/Mobile_Payments_White_Paper_091611.pdf, Last accessed on July 12, 2015.

[54] Leila E., Zeinab B., and Mohammad A., "A Survey on Mobile Payment Systems Security," *Research Journal of Applied Sciences, Engineering and Technology,* Vol. 4, 2012, pp. 4043-4050.

[55] Stinson D. R., *Cryptography: Theory and Practice (Third Edition)*, CRC Press, Boca Raton, 2006.

[56] Kessler G. C, "An Overview of Cryptography", 2010, retrieved from http://www.garykessler.net/library/crypto.html, Last accessed on September 27, 2015.

[57] Stallings W., "Cryptography and Network Security: Principles and Practice (Fourth Edition)," Pearson Prentice Hall, Upper Saddle River, 2006.

[58] Shafi G. and Mihir B., "Lecture Notes on Cryptography," Cambridge University, 2008. Retrieved from https://cseweb.ucsd.edu/~mihir/papers/gb.pdf, Last accessed on September 27, 2015.

[59] Kristin L., "The Advantages of Elliptic Curve Cryptography for Wireless Security," IEEE Wireless Communications, 2004, retrieved from http://www.msr-waypoint.com/en-us/um/people/klauter/ieeefinal.pdf, Last accessed on September 27, 2015.

[60] Nigel S, "Cryptography: An Introduction (Third Edition)," University of Bristol, 2008, retrieved from www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf, Last accessed on September 27, 2015.

[61] Al Imem A., "Comparison and Evaluation of Digital Signature Schemes Employed in Ndn Network," *International Journal of Embedded systems and Applications (IJESA)*, Vol.5, No.2, 2015, pp. 15-29.

[62] Milanov, “The RSA Algorithm”, 2009, retrieved from https://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf, Last accessed on September 27, 2015.

[63] Don J., Scott V., and Alfred M., "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Certicom Corporation, 2001, retrieved from http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf, Last accessed on September 27, 2015.

[64] Asvhini S., Junaid A., and Mudassar A., "A Study on Elliptic Curve Digital Signature Algorithm (ECDSA) for Reliable E- Commerce Applications," Smart Computing Review, vol. 2, No. 1, 2012, pp. 71-76.

[65] Leo A., "Customer Adoption and Financial Literacy in Mobile Financial Services Case Study in Uganda," Masters Thesis, Bruxelles University, 2012.

[66] Cynthia M., "Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments," White Paper, 2010, retrieved from https://www.frbatlanta.org/-/media/Documents/rprf/rprf_resources/wp0810.pdf, Last accessed on October 16, 2015.

[67] Booz, Allen, Hamilton, "Mobile Financial Services Risk Matrix," United States Agency for International Development, 2010, retrieved from http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf, Last accessed on October 16, 2015.

[68] Timothy R., Gautam I., and Stefan S., "Use of Agents in Branchless Banking for the Poor: Rewards, Risks, and Regulation," Consultative Group to Assist the Poor, 2006, retrieved from https://www.cgap.org/sites/default/files/CGAP-Focus-Notes-Use-of-Agents-in-Branchless-Banking-for-the-Poor-Rewards-Risks-and-Regulation-Oct-2006.pdf, Last accessed on October 16, 2015.

[69] William J., Tavneet S., and Mit S. , "The Economics of M-PESA," Georgetown University , 2010, retrieved from www.nber.org/papers/w16721.pdf, Last accessed on October 16, 2015.

[70] Temitope O., Pavol Z., Ron R., and Dale L., "Security Modeling Of Mobile Payment System Architecture," Department of Information Systems Security Management, Concordia University, Canada, 2013.

[71] Sylvain G.t, Jean-Philippe A., The future of contactless mobile payment: with or without Secure Element, Nextendis, 2015, retrieved from http://www.nextendis.com/wp-

content/uploads/2015/06/Future-contactless-payment-WP-by-Nextendis.pdf, Last accessed on October 16, 2015.

[72] Gauthier V., Karel W., Hakan K., and Bart P., "Offline NFC Payments with Electronic Vouchers," ACM, 2009.

[73] Bossi M., "A Need For Peer-To-Peer Strong Local Authentication Protocol (P2PSLAP) In Mobile Banking," *International Journal of Network Security & Its Applications (IJNSA)*, Vol. 5, No. 6, 2013, pp. 31-39

[74] Xiaohua M. and Wenxue W., "The Architecture of Mobile Wallet System Based on NFC ," *Research Journal of Applied Sciences*, 2014, pp. 2589-2595.

[75] Yunpu Z., and J.E. Rice, "A New Architecture For Secure Two-Party Mobile Payment Transactions," Masters Thesis in Computer Science, University Of Lethbridge, 2010, retrieved from https://www.uleth.ca/dspace/handle/10133/2488, Last accessed on October 16, 2015.

[76] Behzad P., "A System for Secured Mobile Payment," Master Thesis, Department of Information and Communication Systems Security, KTH Information, 2013, retrieved from www.diva-portal.org/smash/get/diva2:616934/FULLTEXT01.pdf, Last accessed on October 16, 2015.

[77] William E., Patrick T., Patrick M., and Thomas L., "Exploiting Open Functionality in SMS Capable Cellular Networks ", ACM, 2005.

[78] Collin M., Ravishanchar B., Patrick S., and Jean P., " SMS-Based One-Time Passwords: Attacks and Defense ", Springer, 2013.

Annexes

Annex A: Questionnaires

Table 6.1: Demographic Survey Questionnaire

Demographics Questions	**Possible Answers**
Education Level:	☐No Education ☐Elementary ☐Secondary ☐Preparatory ☐Certificate ☐Diploma ☐BSc ☐MSc ☐PHD
1. Which kind of phone do you have?	☐ Smart phone ☐ Normal phone ☐None
2. Have you used MMS on your phone?	☐ Yes ☐ No
3. Have you connected your phone with any computer?	☐ Yes ☐ No
4. Have you transferred file from your phone to other phone?	☐ Yes ☐ No
5. Have you installed applications on your phone?	☐ Yes ☐ No
6. Have you browsed the Internet from your phone?	☐ Yes ☐ No
7. Have you used your phone for financial transaction?	☐ Yes ☐ No
8. Have you backup and restored your phone?	☐ Yes ☐ No
9. Have you used antivirus to scan your phone?	☐ Yes ☐ No

Table 6.2: Usability Survey Questionnaire

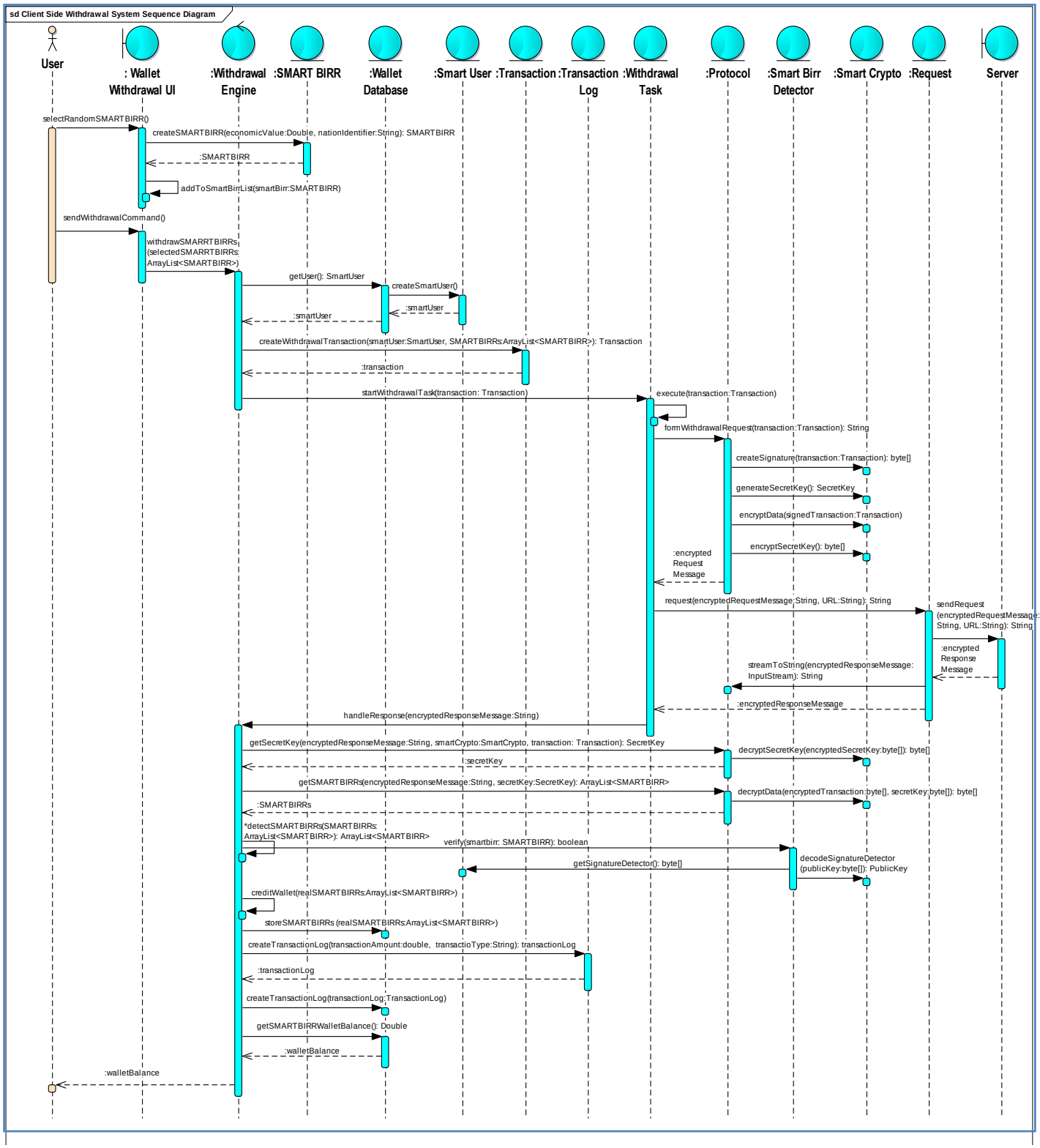
Questions	Possible Answers
1. What is the degree of Smart Birr wallet simplicity relative to material money?	☐ Low ☐ Medium ☐ High
2. What is the degree of Smart Birr wallet security relative to material money?	☐ Low ☐ Medium ☐ High
3. What is the degree of Smart Birr wallet accuracy relative to material money?	☐ Low ☐ Medium ☐ High
4. What is the degree of Smart Birr wallet speed relative to material money?	☐ Low ☐ Medium ☐ High

Annex B: Java Code Used to Create Smart Birr

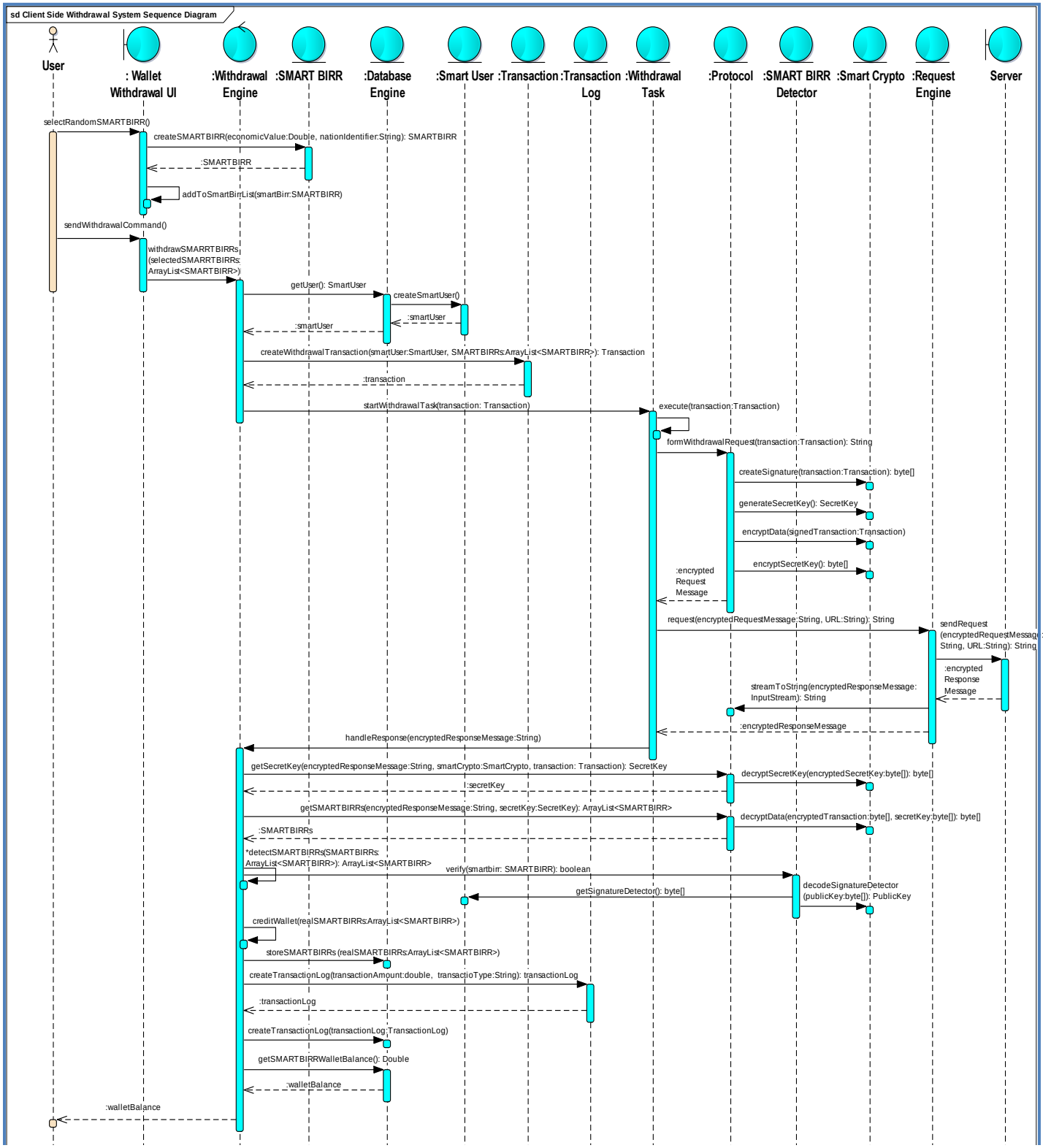
```
//Java Code used to create Smart Birr
public class SMARTBIRR {

    private String serialNumber;
    private double economicValue;
    private String nationIdentifier;
    private byte[] icon;
    private byte[] signature;

    public SMARTBIRR() {
    }
    public SMARTBIRR(double economicValue, String nationIdentifier) {
        this.economicValue = economicValue;
        this.nationIdentifier = nationIdentifier;
    }
```

```
    public SMARTBIRR(double economicValue, String nationIdentifier, String
serialNumber, byte[] icon, byte[] signature) {
        this.economicValue = economicValue;
        this.nationIdentifier = nationIdentifier;
        this.serialNumber = serialNumber;
        this.icon = icon;
        this.signature = signature;
    }
    public double getEconomicValue() {
        return economicValue;
    }
    public void setEconomicValue(double economicValue) {
        this.economicValue = economicValue;
    }
    public String getNationIdentifier() {
        return nationIdentifier;
    }
    public void setNationIdentifier(String nationIdentifier) {
        this.nationIdentifier = nationIdentifier;
    }
    public String getSerialNumber() {
        return serialNumber;
    }
    public void setSerialNumber(String serialNumber) {
        this.serialNumber = serialNumber;
    }
    public byte[] getIcon() {
        return icon;
    }
    public void setIcon(byte[] icon) {
        this.icon = icon;
    }
    public byte[] getSignature() {
        return signature;
    }
    public void setSignature(byte[] signature) {
        this.signature = signature;
    }
}
```

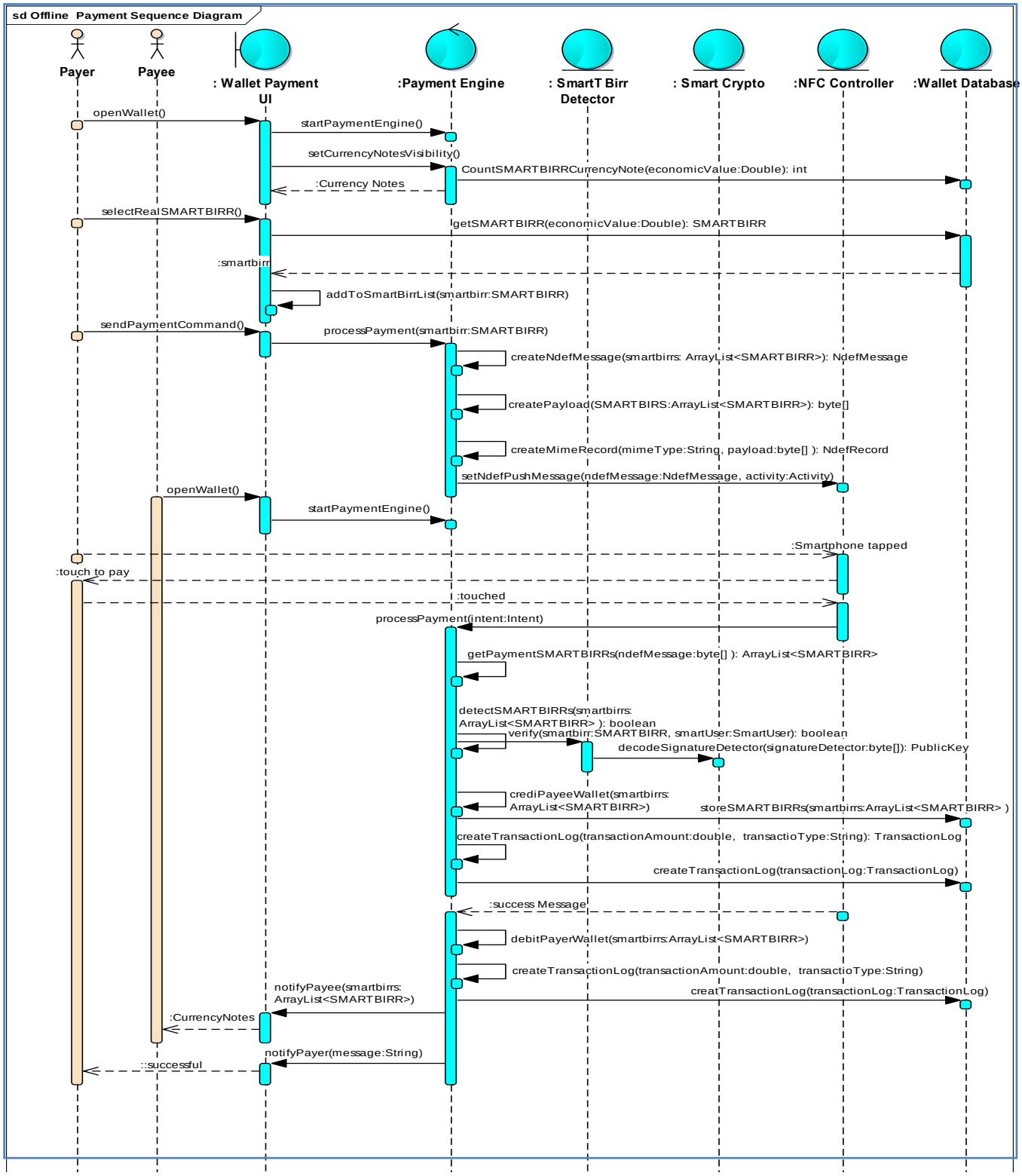
Annex C: Sequence Diagram to Process Smart Birr Withdrawal



Annex D: Sequence Diagram to Process Smart Birr Deposit



Annex E: Sequence Diagram to Process Smart Birr Payment



I, the undersigned, declare that this thesis is my original work and has not been presented for a degree in any other university, and that all source of materials used for the thesis have been duly acknowledged.

Declared by:

Name: Tadegew Bogale Mole

Signature: _____

Date: _____

Confirmed by advisor:

Name: Solomon Atnafu (PhD)

Signature: _____

Date: _____