University of Fort Hare

Together in Excellence

THE STUDY OF BLOCKCHAIN TOWARDS ITS APPLICATION TO THE SOUTH AFRICAN SOCIAL SECURITY AGENCY (SASSA)

by

Sthembile Mthethwa (201514844)

MSc in Computer Science

A dissertation submitted in fulfilment of the academic requirements for the degree of Master of Science in Computer Science

in the

Faculty of Science and Agriculture, Department of Computer Science,
University of Fort Hare

Supervisor:

Prof. M. Thinyane

Co-Supervisors:

Mr. E. Dube & Dr. G. Barbour

March 2017

Preface

The research discussed in this dissertation was carried out in the Faculty of Science and Agriculture, Department of Computer Science at the University of Fort Hare, Alice from January 2015 until November 2016 by Sthembile Mthethwa under the supervision of Professor Mamello Thinyane and co-supervision of Doctor Graham Barbour and Mr. Erick Dube.

As the candidate's supervisor, I, Mamello Thinyane, agree / do not agree to the submission of this dissertation.

Signed:_____ Date:_____

As the candidate's co-supervisor, I, Erick Dube, agree / do not agree to the submission of this dissertation.

Signed:_____ Date:_____

As the candidate's co-supervisor, I, Graham Barbour, agree / do not agree to the submission of this dissertation.

Signed:_____ Date:_____

I, Sthembile Mthethwa, hereby declare that all the materials incorporated in this dissertation are my own original work, except where acknowledgement is made by name or in the form of a reference. The work contained herein has not been submitted in any form for any degree or diploma to any other institution.

Signed:_____ Date:_____

Declaration - Plagiarism

I, Sthembile Nothando Mthethwa, declare that this thesis titled "The Study of Blockchain Towards its Application to the South African Social Security Agency (SASSA)" is my own work. I declare that:

- This dissertation submitted for the degree of Master of Computer Science at the University of Fort Hare has not been submitted for any degree or examination to another university.
- The work reported in this dissertation, except where otherwise indicated is my original work.
- I have acknowledged the work of other researchers included in this dissertation.

Signed:_____

List of Publications

I, Sthembile Nothando Mthethwa, declare that the following publications were produced from the work reported in this dissertation.

1. S. Mthethwa, M. Thinyane, and E. Dube, "The Applicability of the Blockchain Protocol to the Social Grant System." Work-in-Progress Paper in *The Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*, 6-9 Sept 2015, Arabella, Hermanus, Western Cape, South Africa, 2015.

2. S. Mthethwa, M. Thinyane, and E. Dube, "Can the Blockchain be Applied to the Social Grant System." Abstract Paper in *The South African Institute of Computer Scientists and Information Technologists (SAICSIT)*, 28-30 Sept 2015, STIAS Wallenberg Centre, Stellenbosch, South Africa, 2015.

3. S. Mthethwa, G. Barbour, and M. Thinyane, "An Improved Smartcard for the South African Social Security Agency (SASSA): A Proof of life Based Solution" presented in *2016 International Conference on Information Science and Security (ICISS), December 19th-22nd, Pattaya, Thailand, pg. 60-63, IEEE Xplore, 2016.*

Signed:_____

Acknowledgements

This dissertation would not have been completed without the help and the guidance of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this project. To them, I owe my sincere gratitude.

Firstly, I would like to thank the Lord Jesus for making this opportunity possible, for giving me the strength, sanity and grace to go through my masters.

I would like to extend my gratitude to the CSIR (Modelling and Digital Science) for providing the opportunity of doing my masters and the Department of Science and Technology for providing the funds to the CSIR.

I would like to thank my supervisors Professor Mamello Thinyane, Doctor Graham Barbour and Mr Erick Dube for their valuable input, advice and support throughout the duration of this project.

I would also like to thank the staff and fellow students at the CSIR (Modelling and Digital Science) for the assistance they gave.

Finally I would like to send my gratitude to my family and friends for their continuous prayers, support, love and advice throughout my studies.

This dissertation is dedicated to my late sister B.H Mthethwa and to my parents (my mother, T.R Mthethwa and my late father, P.Z Mthethwa).

THE STUDY OF BLOCKCHAIN TOWARDS ITS APPLICATION TO THE SOUTH AFRICAN SOCIAL SECURITY AGENCY (SASSA)

Abstract

In recent years, there has been a rapid improvement in the way currencies are perceived, which has led to a rise in digital currencies commonly known as cryptocurrencies (because they are secured by the use of cryptography). Bitcoin was the first successful cryptocurrency which allowed users to transact directly with each other without the involvement of the third party (the bank). Bitcoin introduced a new technology known as the blockchain which is considered to be the "next-generation technology". Blockchain is a chronological database used to store all the transactions that have occurred since the inception of Bitcoin.

A study of the Blockchain involving its application to the South African Social Security Agency (SASSA) is presented. This study assesses how the Blockchain functions. The Blockchain has been viewed as the next-generation technology. This study also assesses the application of the Blockchain to other systems other than cryptocurrencies or digital currencies. Recent studies in the literature have proposed applications of the Blockchain to other system (e.g. electronic voting, smart contracts, and intellectual property rights). Although these proposals have been put forward, none has been made specifically for SASSA.

This study also presents the problems that the Blockchain has (e.g. scalability, security). Recent literature has tried to solve the problem of scalability, by introducing new protocols like mini-blockchain. In addition, this study presents the challenges that SASSA is currently having and it provides details about the attacks that could succeed in the system. The study presents the analysis of the blockchain for its application to SASSA; the analysis includes scalability, performance and security. Based on the analysis, it is shown that the blockchain is not compatible to be applied to SASSA. However, this study proposes a solution to some of the challenges SASSA is currently facing.

Contents

List of Figures

List of Tables

List of Algorithms

Abbreviations

AES	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
ATM	Automated Teller Machine
BTC	bitcoins
CDG	Care dependency grant
CPS	Cash Paymaster Services
CPU	Central Processing Unit
CSG	Child support grant
CVM	Cardholder verification
DG	Disability grant
DES	Data Encryption Standard
DHA	Department of Home Affairs
ECB	European Central Bank
EMV	Europay, Mastercard, and Visa
FCG	Foster child grant
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standard
FNB	First National Bank
GDP	Gross Domestic Product
GIA	Grant-in-aid
ID	Identity document
inv	inventory message
IoT	Internet of Things

ISO	International Organizational for Standardazation
KByte	Kilobyte
MOC	Match on card
MTN	Mobile Telecommunication Company
NIST	National Institute of Standards and Technology
NPR	National Population Register
NPS	National Payment System
OAG	Old age grant
P2P	Person to Person
PASA	Payments Association of South Africa
PC	Personal Computer
PCH	Payment Clearing House
PIN	Personal Identification Number
POB	Proof of Burn
PoC	Proof of Concept
PoS	Proof of Stake
POS	Point of sale
POW	Proof of Work
RFP	Request for Proposal
SARB	South African Reserve Bank
SASSA	South African Social Security Agency
SOC	System on card
SOCPEN	Social Pension System
SRD	Social Relief of Distress
tps	transaction per second
UEPS	Universal Electronic Payments System
WVG	War Veterans grant

Chapter 1

Introduction

Currency is broadly defined as "[t]okens used as money in a country" [6]. The Financial Crimes Enforcement Network (FinCEN) an agency of the United States government defines currency as "the coin and paper money of the United States or of any other country that [6]:

- is designated as legal tender
- circulates
- is customary used and accepted as a medium of exchange in the country of issuance.

FinCEN terms these currencies as real currencies. Although currencies like the USD or Rands used to be backed by commodities such as gold. Today, most real currencies are fiat currencies, which are merely backed by their respective governments. By controlling the money supply, governments are able to influence the value of their currencies. Relatively stable currency values are achieved by public trust in the continued rational government manipulation of the money supply.

2008 marked a dramatic turning point in the way currencies are perceived, whereby a new type known as virtual currencies was introduced. The currency was named Bitcoin[1], which was introduced by a programmer with a pseudonym Satoshi Nakamoto [2]. Virtual currencies presented a way for two parties to transact directly with each other without

[1]Bitcoin represents the system and bitcoin is for the currency throughout this study

involving a bank. "Virtual currencies are sufficiently novel that the US government faces an "uncertainty paradox" in deciding whether and if so, how to engage in regulation [7]. It's not only the US but also other countries are sceptical about virtual currencies.

As the most popular virtual currency to date, Bitcoin has acted as the driving impetus for regulation- the case of the first impression [7]. Decisions made with Bitcoin in mind will shape the fundamental nature of virtual currencies going forward, acting as a deterministic model and setting the stage for future treatments by the government. Just as the structure of rules affects the outcome of the game, today's treatment of Bitcoin will shape the nature of virtual currencies and digital payments for years to come [7].

As the first cryptocurrency to be introduced, many perceptions have been made about Bitcoin, from lack of understanding mostly and because of scepticism. Regardless of the current perceptions and adoption, Bitcoin is gaining traction and most countries are beginning to use it even though it's not yet regulated [7]. Extensive growth has been noticed in the past few years of Bitcoin whereby most speculated that Bitcoin would not last for a long time. Places to exchange bitcoin's have been introduced in other countries e.g. ATM; bitcoins are accepted as payments in other countries and merchants. The success of Bitcoin led to the introduction of altcoins (cryptocurrencies) and the number has increased tremendously. Figure 1.1 shows the timeline of cryptocurrencies.

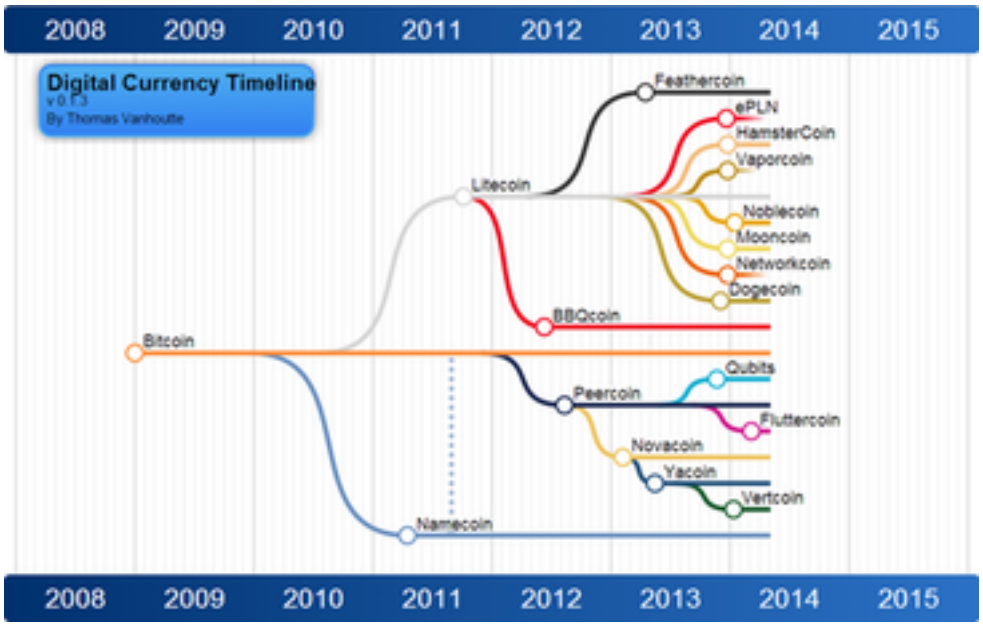

FIGURE 1.1: *Digital Currency Timeline (taken from [1])*

The main inherent risk to Bitcoin is volatility, which brings out a lot of scepticism. The main challenge facing these cryptocurrencies is the fact that they are not yet regulated by the government which makes it difficult for people to trust them as a form of payment. Because banks are not involved in these currencies, the government cannot regulate or control the supply.

1.1 What is Bitcoin?

Bitcoin is a decentralised peer to peer electronic system based on cryptography, thus the name cryptocurrency [8]. The currency unit is bitcoins. However, unlike other traditional currencies, it is not issued by a state or government or even a single entity (bank). The main aim of Bitcoin is to allow two or more peers to transact with each other without the involvement of a third entity or middleman. The Bitcoin economy has grown at an incredibly fast rate with a current estimated market capitalisation of about 3.5 billion US Dollars since the inception. The following section provides details of all the components in the Bitcoin system, adding details that will be required later.

1.1.1 Transactions

At an abstract level, a transaction is a process of moving coins from one or more accounts to one or more destinations [9]. In essence, accounts are represented by public and private keys. The private key is used for signing a transaction associated with a public key. When a transaction is created, it references inputs from a previous transaction output and subsequently becomes outputs for the next transaction [10]. Transactions should meet the following condition:

$$totaloutputs \leq totalinputs \tag{1.1}$$

The underlying information being tracked in the network, are the outputs and their status has to be consistent across all nodes in the network [4]. Outputs should meet the following criteria in order for transactions to be considered valid [4]:

1. An output may be claimed at most once;

2. New outputs are created solely as a result of a transaction;

3. Sum of inputs has to be greater or equal to the sum of outputs as shown in equation 1.1.

Once the transaction is published to the network, it must be verified before it is committed to the blockchain.

When nodes are verifying transactions, they check if the claimed coins are available in the account and whether the transaction has not been double spent [11]. Double spending attack is when two or more transactions attempt to transfer the same coin multiple times. If this attack occurs, Bitcoin resolves it by taking the first transaction to be received to be true and the other one fails [12]. Scripts are used to verify the transactions and they are in a stack based language. If at the end the contents of the stack yield to true, then the transaction is valid.

1.1.2 Blocks

A block contains a list of transactions that the node which created the block has committed since the previous block and the number of transactions differs based on the nodes creating the block [4]. Transactions become effective after they have been added to a block, which serves as the official record of executed transactions [13]. Only valid transactions get to be added to a block. The block is then distributed to the network so that other nodes may verify and then move on to create a new block.

For nodes to be able to add a block to the blockchain, they must find a solution to a proof of work problem. This consists of finding a value known as a nonce, whereby when combined with the block header it produces a hash that meets the target specified. The proof of work is calculated by using SHA-256 two times [14] to H, such that:

$$D = SHA256(SHA256(H)) \leq r, \tag{1.2}$$

where r is fixed, also known as the target, H is the header of the block of transactions collected, and D is the produced hash. To find the solution, different values must be tried

and this is difficult to get right away. The target is determined by the system in order to achieve an average of 10 minutes for blocks to be added to the chain. This target is adjusted after every 2 weeks in expectation.

The nodes responsible for finding a solution to the proof of work problem, are known as miners. Upon finding a solution, miners receive an incentive which comprises of:

1. transaction fees if specified or difference between inputs and outputs, and
2. newly minted coins which is 25 BTC and this value is halved after 4 years.

1.1.3 Blockchain

On their own, "blocks do not provide any added synchronisation on top of the individual transactions" [4]. But this is solved once the blocks are chained together (into a blockchain), thereby creating a chronological order over the blocks and therefore the transactions contained within them. Each block references the previous block, via a hash, therefore, organizing blocks in a directed tree. The root of the tree is known as the genesis block, this was hardcoded into the clients [15].

The blockchain is considered to be the longest chain from any block to the genesis block. Figure 1.2 depicts how the blockchain is structured and how blocks are chained together.

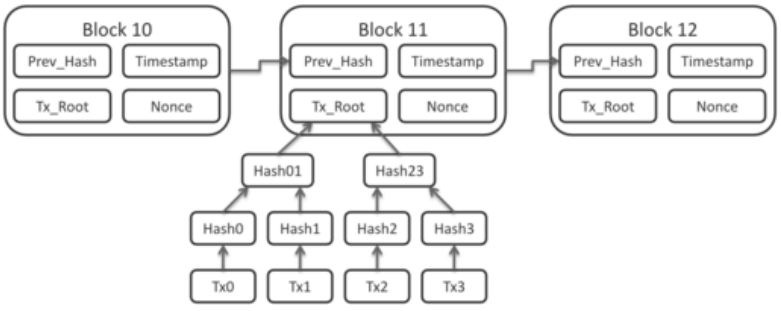

FIGURE 1.2: *Structure of the blockchain (based upon [2])*

Miners are required to build on top of the current or longest blockchain to avoid building on different branches. Figure 1.3 shows how the blockchain looks like when it has different branches.

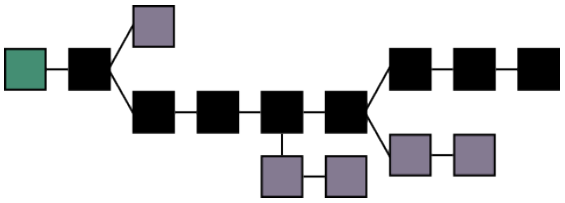

FIGURE 1.3: *A Graphical Representation of the Blockchain (take from [3])*

1.1.4 Blockchain Forks

At a certain point in time, it happens that the blockchain has multiple branches and this situation is known as a blockchain fork. This occurs when nodes in the network do not agree on which of the blocks is the current blockchain head. This disagreement actually happens when two nodes publish blocks at the same time, therefore leading to the blockchain being bifurcated producing two different branches. Different nodes receive these blocks differently and each node continues building up on the block they received first.

A blockchain fork may be prolonged as nodes continue adding blocks to their respective blockchains. But eventually this is solved, when one branch becomes longer than the other branch. Once this happens, all nodes switch to that block, therefore, everything is consistent in the network. The blocks discarded by this resolution are then referred to as orphan blocks. Transactions in the orphaned blocks that are not present in the accepted branch are added to the next block [3].

Blockchain forks may present an opportunity to attackers to try and change the transactions. An attacker has a chance only if they could control a majority (51% or more) of computational power on the network compared to honest nodes. In that way, they could actually revert the transactions and change the blocks leading to a longer branch such that nodes would switch on to the attackers branch. However, this has not been successful in the network. "One may argue that the existence of blockchain forks is the very reason that transactions are never definitively committed" [4]. Decker [4] mentions that blockchain forks not only slows down the confirmation time of transactions "but also limits it to be a probabilistic statement about the validity" [4]. It is mentioned that one should wait for their transaction to be 6 blocks deep in the blockchain which is approximately 1 hour for

the transaction to be considered confirmed. This is because it would become hard for an attack to change transactions once they are that deep in the blockchain. This presents a problem with regards to fast payments.

1.2 Problem Statement

A social grant system is a system that is controlled by the government and is designed to help underprivileged citizens in a country. The main aim is to take care of the social security and alleviate poverty in the country. In South Africa, the South African Social Security Agency (SASSA) is responsible for co-ordinating the process and distributing grants to beneficiaries on a monthly basis. SASSA does not have the internal capacity to distribute grants, therefore this task is outsourced to another organisation, Cash Paymaster Services (CPS). This forces SASSA to depend on trust about the information provided by the third party. SASSA still have challenges when it comes to the management and administration of grants which then leads to a loss of money.

One of the challenges is the fact that SASSA would like to know whether the beneficiaries being paid are the rightful ones or not. Therefore, SASSA requires beneficiaries to prove that they are still alive which is referred to as proof of life. To fulfil this requirement, the use of fingerprints has been proposed.The main limitation with this method is that fingerprints for payments are not regulated. Therefore, all the payments SASSA processes through this method do not go through the Payments Association of South Africa (PASA). This method is only used for offline payment methods e.g. cash pay points and biometric-enabled POS devices (found at certain shops e.g. Shoprite). Thus, SASSA still pays grants without proof that beneficiaries are still alive.

Depending on trust alone could be a problem when money is involved. However, in 2009 a new cryptocurrency know as Bitcoin was introduced. Bitcoin introduced a way for two parties to transact with each other without trusting and depending on a middleman [2]. It introduced two major innovations, which were solutions to two prevailing problems in computer science: the double spending problem and the byzantine general's problem. This

is the inability of a system (or component of a system) to detect when an unusual behavior occurs, namely when conflicting information is being sent to the system [16].

Therefore, SASSA can transact directly with beneficiaries without depending on CPS. Bitcoin's main innovation was the introduction of the blockchain, a peer-to-peer distributed timestamp server to record and order all the transactions chronologically. Many cryptocurrencies have been introduced which employs the blockchain introduced by Bitcoin [17].

Although blockchains are mostly used in cryptocurrencies, they are being studied in the context of non-cryptocurrency systems. A few systems have been proposed e.g. voting system (whereby blockchain is proposed to record all the votes during a voting process), smart contracts (which allows two people to agree on a contract), proof of existence (where a user add a document to the blockchain which would be timestamped proving that it belongs to a particular user) [18]. This shows that blockchain has the opportunity of being used in non-cryptocurrency systems. Therefore, the effectiveness of blockchain in SASSA's context needs to be investigated thereby the aim of necessitating this study.

1.3 Research Gap

In the attempt to understand the possible use of blockchain in other systems, various systems proposals have been introduced thus far e.g. proof of existence, smart contracts, electronic voting etc. Of these systems, none of them is based on the social grant system. The potential of utilizing blockchain to the social grant system has not been explored or studied; therefore the aim of this study is to bridge this gap.

1.4 Research Objectives and Questions

The overall objective of this study is to study the potential that the application of blockchain has on the social grant system (SASSA). Thus, it poses the following questions:

- **RQ1** — What are the challenges in the South African Social Security Agency (SASSA)?
- **RQ2** — Can the Blockchain be used to solve some of the challenges SASSA is facing?

From the main objective, the following sub-objectives arises:

- **ROBJ1** — To assess the South African Social Security System and identify the existing challenges
- **ROBJ2** — To evaluate the impact of blockchain on the SASSA challenges
- **ROBJ3** — To design a solution for the challenges identified

Table 7.1 links research questions, objectives, methodology and chapters where it is discussed.

TABLE 1.1: *Summary of research.*

Research Question	**Research Objective**	**Methodology**	**Section References**
RQ1	ROBJ1	Literature study and Case study	Chapter 4
	ROBJ1	Security threat model	Chapter 4
RQ2	ROBJ2	Extensive literature review	Chapter 2
	ROBJ3	Design possible solutions	Chapter 5

1.5 Research Contribution

This research seeks to make the following contributions:

1. It presents the overview of Bitcoin, thus leading to the analysis of blockchain.
2. It describes the system used by the South African Social Security Agency (SASSA), some of the flaws and challenges the system has.
3. It proposes solutions for the challenges identified.
4. Describes the analysis of blockchain towards the application to SASSA.

1.6 Thesis Layout

The rest of the chapters are structured with their own introduction, body and conclusion sections. The various aspects of Chapter 1 are expanded further in the following chapters:

1. **Chapter** 2 provides extensive literature to the study.
2. **Chapter** 3 discusses the methodology employed for this study.
3. **Chapter** 4 provides detailed analysis of SASSA's existing system.
4. **Chapter** 5 provides details of the proposed solution.
5. **Chapter** 6 provides details of the application of blockchain to SASSA.
6. **Chapter** 7 presents the research review and conclusions made from the research.

Chapter 2

Literature Review

This chapter provides a review of the literature in relation to the development of payment systems and their evolution. This is approached by discussing different types of payment systems.

2.1 Introduction

In general, two parties are involved in a payment i.e. payer and payee. Tom states the definition of payment as, "the transfer of funds which discharges an obligation on the payer's side vis-à-vis a payee" [19]. To assist with the process of payment, systems have been developed known as payment systems. According to Tom, a payment system may be defined as the complete set of instructions, intermediaries, rules, procedures, processes and interbank fund transfer systems facilitating the circulation of money in a country or currency area [19]. This definition indicates that, there are three elements involved in a payment system namely:

- Payment instruments - which are the means through which payments are authorized and submitted.
- Processing (includes clearing) - instructions being exchanged between banks or accounts concerned e.g. Payment Clearing House (PCH) is used in South Africa.

- Settlement for relevant banks e.g. the South African Reserve bank (SARB) is used as a third party for clearing debts between banks.

Well designed payment structures must contribute to the proper functioning of markets and helps to eliminate frictions in trade. The availability of reliable and safe payments mechanisms for the transfer of funds is therefore an important thing for the majority of economic interactions. In the past decades, payment systems have evolved drastically and the following section looks at the different types of systems that have been developed in the past.

2.2 The Evolution of Payment Systems

Different monetary systems have emerged under the influence of practical demand and developments in monetary policies throughout history. Initially, a bartering system was used whereby goods or services were exchanged for a certain amount of goods/services [20]. This process was good in that time but then it had problems, which are listed below:

- It is time consuming and involves a lot of work in the sense that one spends a lot of time looking for someone to trade with in order to get exactly what one wants.
- Deciding on an equal trade is difficult
- If one trades perishable goods, time becomes a big factor. One might be pressured into taking unfair deals.

Menger explains that "in many cases a direct exchange of commodities is not possible because some commodities are indivisible and thus the matching process of supply and demand is tedious, resulting in search costs" [21]. After bartering, commodity money was introduced and was based on the idea that the commodity itself has a special value in it. Amongst other examples of the earliest commodity money are: dyes, beads and shell jewellery. Gold and silver are probably the most famous forms of commodity money, which was swapped by Egyptians in a bar form and has taken the monetary functions throughout history [21]. Menger explains that the introduction of commodity money as a

form of money and unit of account was mostly in advanced civilizations [21]. White states that to further economize the costs involved in bartering through commodity money, the emergence of coinage was observed in an unregulated competitive environment [22].

A means of progress from commodity money, was the introduction of coin and paper money, which is fiat currency/money. Fiat currency is a type of currency whose value is backed by the government that issued it [23]. Paper money initially was in a form of a receipt that was issued by the bank to the depositor which was redeemable for whatever gold/silver they had stored. Money became popular, which led to other improvements i.e. the introduction of cards. This made it easier for people to make payments because there was no need to carry cash everywhere. The technological advancement in the world led to the improvement of payment systems to use technology. There was the introduction of mobile phones and people started using them more often. Therefore, it was a good idea for researchers to find a way of adapting the technological developments that were taking place. The use of Internet started gaining momentum and most people started using it more which led to the development of electronic money. According to the European Central Bank (ECB), electronic money is defined as an "electronic store of monetary value on a technical device e.g. mobile phone, which may be used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid bearer instrument" [24].

This is when mobile phones and the Internet are used to make payments reducing the risks that comes from carrying cash (fraud).

Today it is the norm for people to conduct payments and transactions without the need for physical cash. Today, payments have become more card and mobile based. This has actually made life much easier for individuals especially those in urban areas. Attempts have been made to try and make things easier even for those in rural areas. After the shift of electronic payment system, new payment systems/methods such as M-Pesa spiraled. M-Pesa is a payment system launched in Kenya in March 2007 [25]. This system was developed by a mobile phone operator Vodafone and was then launched by Safaricom its affiliate in Kenya. M-pesa can be accessed from an ordinary mobile phone and it's a "small-value electronic payment and store of value system" [25]. M-Pesa was originally conceived

as a way of microloans repayment. However, as it was market tested by Safaricom, the core proposition was then shifted from microloan repayments to helping people make person-to-person (P2P) transfers to friends and families [25]. M-Pesa's aim was to target the rural areas. M-Pesa is successful because of the three following reasons [25]:

- Demonstrated the promise of leveraging mobile technology to extend financial services to large segments of unbanked poor people.
- Demonstrated the importance of designing usage rather than float based revenue models for reaching poor customers to repay microloans.
- Demonstrated the importance of building a low-cost transactions platform which enables customers to meet a broad range of their payment needs.

M-Pesa is said to be amongst the successful payment systems in Africa [25]. From the success of M-Pesa other mobile payment systems were introduced in South Africa. Amongst those are "Instant Money" which was introduced by Standard Bank and it is a joint venture with the retailer Spar [26]. "Standard Bank also has a joint venture company called "Oltio" between itself and pan-African mobile network operator MTN which, through its "payD" platform enables customers to purchase products and services online and use their debit cards to pay for the purchase while making use of their mobile phones to enter their personal identification numbers (PINs)" [26]. First National Bank (FNB) also entered the fray and launched "e-Wallet" mobile money transfer, which allows the sending of money between South African customers with valid mobile phone numbers [26]. The table 2.1 compares different types of payment methods.

TABLE 2.1: *Summary of Payment Systems*

Payment Method	**Third Party Involvement**	**Anonymity**	**Limitations**
Bartering	No	No	Time consuming
Commodity money	No	No	Fraud
Cash	Yes	No	Theft
Cards	Yes	No	High interest rates
Mobile	Yes	Yes	Costly
Digital (Cyptocurrencies)	No	Pseudonymity	Limited acceptance

The method of mobile money bridged the gap of the unbanked community. Physical cash is slowly losing its attraction as technology improves [27]. Shultz continues to say that, "as the use of technology and Internet increases, new ways of paying are being introduced which makes things easier for individuals" [27]. From the electronic payment systems, a new payment system was introduced known as digital payment system. Digital payment systems have been studied in the past decade but are now gaining momentum. These are widely known as electronic cash or cryptocurrencies. The first successful digital payment system to be launched was Bitcoin. The following section discusses in detail Bitcoin as a payment system and the evolution thereof.

2.3 Origins of Bitcoin

This section is an overview of the ideas underlying cryptographic money over the past three decades, leading to the development of the first successful cryptocurrency known as Bitcoin. Two main aims that electronic money accomplishes are:

- anonymity — the condition of being anonymous. Cryptocurrency also introduced pseudonymity (whereby fictitious names are used), which may not entirely be anonymity but then a level of anonymity was introduced which the traditional/previous systems did not have.
- decentralization — is the process of redistributing or dispersing functions, powers, people or things away from a central location or authority. The main issue with the other methods from the section above is centralization, whereby the systems are being controlled by one central entity which is the bank. The introduction of cryptocurrency eliminated the need for a bank.

The motive for electronic cash is not something new [28]. Franco indicated that most of the ideas behind digital payment systems were brought forth by the cypherpunk movement [29]. Cypherpunk was launched in 1990, which were series of meetings that were attended by cryptographers and were based on the early cryptographic developments i.e. blind signature, public key cryptography. But then the movement didn't last very long.

Chaum [30] was the first one to introduce electronic money which was named e-cash and his aim was to introduce an anonymous system using blind signatures. In 1990, Chaum [31] proposed a modified version of the e-cash which was then targeting offline payments. Researchers gained interest and proposed refinements in 1993 [32], whereby Brands incorporated the property of untraceability of payments into offline electronic cash system and in 2005 [33], whereby Brands presented an efficient offline anonymous e-cash schemes where a user can withdraw a wallet containing coins each of which she can spend unlinkably (without the need for a bank).

Another payment system named Hashcash was introduced by Back, which was a method for spam limitation [34]. This system used a principle of solving a cryptographic puzzle which is similar to the one Bitcoin is using (proof-of-work) [35]. In 1998 two systems were independently proposed namely: bit gold [36] and b-money [37] which were similar. Their main idea was not to involve a third party and use a distributed database to store balances. These were just theoretical and were never implemented. Another system was introduced in 1999, which didn't involve third party but achieved full-anonymity as transactions were not linkable. In 2004, Finney made a generalization of Hashcash which was not tied to any application and can be spent freely and this was later discontinued [38]. Zerocoin [39]and zerocash [40] are recent approaches similar to hashcah.

The main problem posed by the above mentioned systems, was trust and dependence on a third party. But as a solution to this problem, Satoshi introduced Bitcoin [2]. Bitcoin made it easier for parties to transact with each other without the involvement of a third party. In his system, he solves the double spending problem by the use of peer-to-peer network that uses proof-of-work to record history of all transactions in a public ledger called blockchain, which was his innovation.

Bitcoin being the first successful cryptocurrency [41], triggered a number of researchers to study it [42]. Different components of Bitcoin has been studied e.g. its anonymity [43], double spending [44, 45], mining [46], transactions [9], and how to improve Bitcoin [10, 47]. Besides studying Bitcoin, other cryptocurrencies were introduced from it and are still being proposed e.g. Permacoin [48], Namecoin [14] and many more [49] and these are called altcoins. A few key ones are briefly discussed below.

1. **Litecoin**: This is the second largest cryptocurrency in the world, it was launched in 2011 by Lee [50]. It is also not controlled by any central authority just like the counterpart (Bitcoin), but uses scrypt as proof of work which is discussed in section 2.4.3.2. For mining CPUs can be used unlike Bitcoin which requires specialized ASIC computers. Transactions are confirmed very fast (2.5 minutes) [50].

2. **Darkcoin**: Duffield created Darkcoin which was launched in 2014 [51]. It is said to be the more anonymous version of Bitcoin. It works on a decentralized master-code network resulting in almost untraceable transactions, hence offering more anonymity [51].

3. **Peercoin**: It was launched in 2012 by King (a pseudonym) and Nadal [52]. It was the first cryptocurrency to utilize both proof of work discussed in 2.4.3 and proof of stake discussed in 2.4.4. The initial generation of coins is performed with proof of work. The proof-of-stake system was designed to address vulnerabilities that could occur in a pure proof-of-work system.

4. **Dogecoin**: It was launched in 2013 by Markus and Palmer. As a proof of work it uses scrypt. A block is generated every 60 seconds and the difficulty adjustment time is 4 hours.

5. **Primecoin**: It was developed by King, it is distinct because the proof of work used is based on prime numbers [53]. This proof of work scheme is concerned with finding Cunningham chains and bi-twin chains. These are special long chains of prime numbers. Primecoin offers easier mining and greater security to the network [53].

Table 2.2 shows a summary of some of the successful cryptocurrencies, whereby deflationary means whether the cryptocurrency causes economic deflation and details of the different types of proof of work is found in 2.4.3.

TABLE 2.2: *Summary of Cryptocurrencies*

Currency	**Deflationary**	**Blockchain**	**Proof of Work**	**Launched**
Bitcoin	Yes	Yes	SHA-256	2009
Litecoin	Yes	Yes	Scrypt	2011
Peercoin	No	Yes	SHA-256	2012
Primecoin	No	Yes	Cunningham chains	2013
Dogecoin	No	Yes	Scrypt	2013
Darkcoin	Yes	Yes	X11	2014

The number of cryptocurrencies that have been introduced shows that Bitcoin can somehow be useful in the future. It did not end with the introduction of cryptocurrencies, but other systems are being developed from the main innovation (blockchain) i.e. Ethereum [54]. The following section provide details about the Blockchain.

2.4 Blockchain

Prior to the innovation of Blockchain, the coordination of activities over the Internet without the requirement of a central entity was not extensive. A group of unrelated individuals were able to confirm an event that has occurred through the central authority. This concept was encapsulated in a well-known computer science problem from the early 1980's, commonly referred to as the "Byzantine Generals Problem". It questioned how consensus was reached by the distributed computer systems if they did not rely on a central authority, in such a way that the network of computers could resist an attack from ill-intentioned individuals.

Wright and Filippi say that the Blockchain came as a solution to this problem through a probabilistic approach [3]. It forces information to become more transparent and verifiable with the use of mathematical problems which requires computational resources to be solved. This makes it harder for attackers to corrupt the Blockchain unless they own 51%

computational power. The protocols in the system ensure that transactions added on the Blockchain are valid and that the system is running accordingly.

2.4.1 Definition

A Blockchain is the main innovation that was introduced by cryptocurrencies. Wright and Filippi define blockchain as a chronological database of transactions recorded by a network of computers [3]. It is made up of different blocks that are linked together. Every block contains a number of transactions, a reference to the preceding block, as well as an answer to a complex mathematical puzzle, which is used to validate the data associated with the block.

2.4.2 The Protocols

This section discusses the protocols ensuring that the system is secure. Goodman mentions 3 protocols in cryptoledgers: the network, transaction and consensus protocols [55].

2.4.2.1 Network Protocol

The network protocol in bitcoin is typically the gossip network that grants the broadcasting of transactions, the downloading and publishing of blocks, the discovery of blocks [55]. Decker and Waltenhofer explain fully how it works [4]. Each node in the Bitcoin network is required to keep a complete replica of the blockchain. Each node verifies information it receives from other nodes independently.

When a node joins the network it queries available peers participating in the network for a connection. A brand-new node only knows one block (the genesis block), which is statistically embedded in the client software. Once connected, the node learns about other nodes by probing their neighbours for known addresses and listening for spontaneous advertisements to new addresses. “Each node attempts to keep a minimum number of connections p to other nodes at all times. Should the number of open connections be

below p the node will randomly select an address from the set of known addresses and attempt to establish a connection" [4].

Transaction (Tx) and block (B_i) messages are relevant especially for the purpose of updating and synchronizing the blockchain. These messages are not forwarded directly to nodes, so as to divert from sending messages to nodes that already have them. Alternately their availability is broadcasted to the neighbours by sending the *inv* message once the transaction or block has been verified. The *inv* message contains a set of transaction and block hashes that have been received by the sender. A node, receiving an *inv* message for a transaction or block that it does not yet have locally, will issue a *getdata* message to the sender of the *inv* message containing the hashes of the information it needs. The actual transfer of the block or transaction is done via individual block or transaction messages. Figure 2.1 shows how messages are propagated throughout the network using the broadcast mechanism.

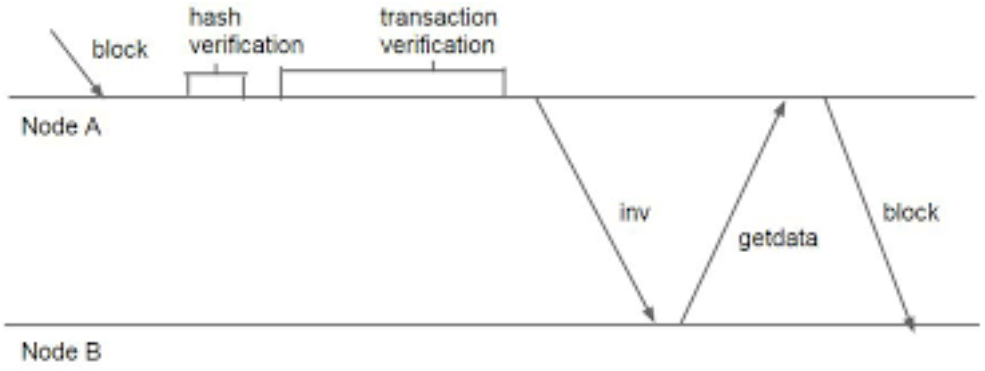

FIGURE 2.1: *Information Propagation (from [4])*

2.4.2.2 Transaction Protocol

Goodman defines this protocol as what makes a transaction valid which is defined through a scripting language [55]. Bitcoin nodes use scripts to validate transactions and there are two types of scripts:

- **Locking Script** — "A locking script is an encumbrance placed on an output, and it specifies the conditions that must be met to spend the output in the future" [56].

Commonly referred to as the scriptPubKey, because it contained a public key or bitcoin address.

- **Unlocking Script** — "An unlocking script is a script that "solves", or satisfies, the conditions placed on an output by a locking script and allows the output to be spent" [56]. Usually known as the ScriptSig, because it contained a digital signature. It is part of every transaction input and most of the time it contains a digital signature produced by the user's wallet from their private key.

Every bitcoin client will validate transactions by executing the locking and unlocking scripts together as depicted below.

$$< Sig >< PubK > DUPHASH160 < PubKHash > EQUALVERIFYCHECKSIG \tag{2.1}$$

2.4.2.3 Consensus Protocol

Consensus protocol describes how consensus is built around the most difficult chain and the miner schedules allowing miners to "draw transactions from the coinbase, dictates how difficulty changes, indicates which blocks are valid and which blocks are part of the main chain" [55].

As the blockchain is maintained by peers on the network, so Bitcoin requires that each block prove a significant amount of work was invested in the creation. To prove one did some extra work to create a block, one must create a hash of the block header which does not exceed a certain value. One can even estimate the probability that a given hash attempt will generate a number below the target threshold. Bitcoin assumes a linear probability that the lower it makes the target threshold, the more hash attempts (or average) will need to be tried.

New blocks will only be added to the blockchain if their hash is at least as challenging as a difficulty value expected by the consensus protocol. For every 2016 blocks, the network uses timestamps stored in each block header to calculate the number of seconds elapsed between generation of the first and last of those 2016 blocks [56].

- If it took fewer than 2 weeks to generate 2016 blocks, the expected difficulty value is increased proportionally (by as much as 300%) so that the next 2016 blocks should take exactly 2 weeks to generate if hashes are checked at the same rate.
- If it took more than 2 weeks to generate the blocks, the expected difficulty value is decreased proportionally (by as much as 75%) for the same reason.

Algorithm 2.1 depicts exactly how this protocol works:

Algorithm 2.1 The proof-of-work algorithm (from [57])

```
1: function POW(x,C)
2:     if C = ϵ then
3:         s ← 0                                  ▷ Determine proof of work instance
4:     else
5:         <s′, x′, ctr′ >← head(C)
6:         s ← H(ctr′, G(s′, x′))
7:     end if
8:     ctr ← 1
9:     B ← ϵ
10:    h ← G(s,x)
11:    while ctr ≤ q do
12:        if H(ctr,h) < D then        ▷ This H(.) invocation subject to the q-bound
13:            B ← <s,x,ctr >
14:            break
15:        end if
16:        ctr ← ctr + 1
17:    end while
18:    C ← CB                                     ▷ Extend chain
19: return C
20: end function
```

The algorithm works as follows. Given a chain C and a value x (to be inserted in the chain), these values are hashed to get h and initializes a counter ctr. Subsequently, it

increments ctr and checks to see whether $H(ctr, h) \leq D$ [57]. If a suitable ctr is found then the algorithm succeeds in solving the proof of work and extends chain C by one block inserting x as well as ctr (which serves as the POW). If no suitable ctr is found, the algorithm simply returns the chain unaltered [57].

The following sections describe the available algorithms used to keep the blockchain secure.

2.4.3 Proof of Work (POW)

Proof of Work (POW) is a cryptographic puzzle used to ensure that a party has performed a certain amount of work [58]. POW is based on the idea from Adams Back Hashcash. POW has two basic properties, firstly, it ensures that the party providing the proof of work has invested a predefined amount of effort in order to create the proof and secondly, that the proof is efficiently verifiable. Typically, finding a solution to a POW puzzle is a probabilistic process with a success probability depending on the predefined difficulty. In Bitcoin, the hashing algorithm is double SHA-256 and the predefined structure is a hash less or equal to a target value T. A few types of proof of work have been discussed in the sections below.

2.4.3.1 SHA-256

The main aim of a miner in the Bitcoin network, is to find a solution to a computational puzzle. The computational puzzle requires finding a partial pre-image for SHA-256, a cryptographic hash function [59]. The puzzle is to find specifically a block that consist of a list of transactions, the hash of the previous block, a timestamp and a version number, plus an arbitrary nonce value, whose SHA-256 hash is less than a target value. The aim is to find a hash that starts with x consecutive zero bits therefore, trying different random nonces until the solution is found [59].

2.4.3.2 Scrypt

A scrypt is a type of proof of work system/scheme; which has been utilised by a number of cryptocurrencies. First implemented in 2011 by an anonymous programmer called Artforz in Tenebrix followed by Fourbrix and the first cryptocurrency was Litecoin [60]. Mining of cyptocurrencies that use scrypt is often performed on graphics processing units (GPUs). Since GPUs tend to have significantly more processing power compared to CPU. This led to shortages of high end GPUs, due to the rising price of these cryptocurrencies in months of November and December 2013. As of May 2014, specialized ASIC mining hardware is available for scrypt based cryptocurrencies.

2.4.3.3 Cunningham Chains

Cunningham chains were introduced in 2013 by Sunny King, after the realisation that searching for prime chains could potentially be an alternative of a proof of work system. With some effort, a pure prime number based proof of work has been designed, providing both minting and security for cryptocurrency networks [52]. Similar to Hashcash type of proof of work, the project is named primecoin [52].

2.4.3.4 X11

X11 is more complicated than a SHA-256 ASIC implementation. The use of this algorithm will prevent the use of ASIC miners for a short-term to mid-term in the future [51]. It will also allow for a longer period of mining for CPU/GPU users. GPU miners that mine with the X11 algorithm are currently experiencing reduced power usage (up to 50%) and reduced heat generation compared to scrypt [51].

2.4.4 Proof of Stake (PoS)

One popular alternative to proof of work is frequently proposed as a mechanism for a cheaply distributed consensus [61] and was first introduced in Peercoin [52]. Because proof of work is said to be expensive due to the fact that it requires a lot of computational

power to solve, the purpose of developing proof of stake was to get rid of that challenge [62]. Proof of stake use "coin age"; currency amount times holding period. Similar to energy, coin age as a source is expensive to a mass in huge quantity for an attacker to accumulate enough coin age to attack the distributed network, he/she either has to buy on the open market, a large amount of the very currency one is trying to attack, driving up the price during the process and diminishing one's economic incentive or hold coins for a very long time, reducing the frequency of his/her own attacks [62]. One useful feature of PoS is the significant saving in energy consumption. Another main feature is the better alignment of incentives between miners and stakeholders because miners are now the stakeholders. Proof of stake has several limitations e.g. initial distribution, hoarding, full nodes, and mining on multiple forks [62].

2.4.5 Proof of Burn (POB)

Another algorithm which presents a solution to the drawbacks of proof of work algorithm mining was introduced and it is known as the proof of burn (POB). This algorithm utilizes the idea of burning coins to reduce the need of powerful computational power or resources when mining. Proof of burn introduces a solution to the dependency of powerful hardware. What is needed in this algorithm is for some coins to be burned so as to acquire mining power, instead of waiting for days or months on end. The first cryptocurrency to be introduced that utilized this algorithm was Slimcoin [63]. The process of burning coins is considered as proof of mining. This process consists of sending coins to a predetermined address which is not owned by anyone and these coins are considered to be "burnt" therefore they cannot be retrieved. This process of burning coins is said to be parallel to buying hardware for proof of work mining [63].

2.4.6 Applications of the Blockchain

"Blockchain is regarded as a next-generation information technology with many potential upsides in a number of fields beyond digital currencies" [64]. The section below discusses further applications of the blockchain.

2.4.6.1 Smart Contracts

The term smart contract appeared in 1994 when Nick Szabo who described a computer program with the structure of interacting with the real world [14]. Smart contracts represent the implementation of a contractual agreement, whose legal provisions are formalized into programming code verified through a network of peers [3]. To set up a smart contract one needs to choose an event or condition which triggers the transaction expected in the contract, and then checks whether the event or condition has occurred with the program and then the contracts are added to the blockchain. An example of a smart contract might be a bet made by two users about the maximum humidity level for the following day. Therefore, the event for this example would be humidity levels. On the day of the bet, the contract is automatically completed by a software program checking the humidity levels provided by a qualified weather service as stated by the contract, reading and transferring funds from the loser's to the winner's accounts.

The main purpose of this project was to create an independent platform where, using a programming language, the users can create a virtual contract between them for any purpose they want. Provided with the reliance of source codes, users are now able to model contractual performance and simulate the agreement effectiveness before it is execution [3]. The use of the smart contract is not limited to the financial and commercial sector. It can be used to confirm a real estate transfer playing the role of the notary. At the same time, a user can write his/her own will on the platform and the contract will be executed after their death without the intervention of a third party [65].

There are 3 distinctive properties of smart contracts:

- Autonomous — once they are added to the blockchain, "they no longer need heed of their creators" [14].
- Self-sufficient — overtime they could accumulate capital e.g. digital currencies or physical assets.
- Decentralized — no one person controls them.

A few projects started developing programing languages for the easy creation of smart contracts [54]. Currently, there are two main projects related to smart contracts, namely Namecoin and Ethereum.

2.4.6.2 Electronic Voting

Voting procedures remain, in many countries, a controversial issue; as incidence of electoral fraud (invalid/inaccurate vote, multiple registration) and the big percentage of abstentions often shape the final result. The voting members or electorate could connect to a PC-based system through their computer, laptop or smartphone, using open source code that is open to editing using a kind of authentication (biometric, written) to prove their identity to the program. This will increase reliability and the convenience of access to the voters [65].

An electronic vote is essentially an electronic transaction whereby a voter, provided with some voting credits, will spend them in favour of one or more candidate recipients. Candidate recipients could be people like in a presidential election or options to choose from. Therefore, the blockchain is used to log the votes and audit results. The proposed method involves the use of Merkle trees for voters' list verification and block explorers for vote count checking [66]. A Merkle tree is a tree in which every non-leaf node is labelled with the hash of the labels or values of the child nodes. Basically, two nodes are grouped together and hashed and at the end they would be one node left. The main advantage of Merkle trees, is that they allow efficient and secure verification of the contents of large data structures. Because votes contain large amount of data, this method is appropriate.

This proposed method does not solve all the issues associated with electronic voting, but it provides the following benefits [66]:

- Free, open-source peer-reviewed software
- Ubiquitous
- Secure
- Protecting the secrecy of the ballots

- Allowing free, independent audits of the results
- Minimizing the trust level required from the organizers

2.4.6.3 Smart Property

The key objective of smart properties, is the assertion of ownership rights for an asset through the registration in the blockchain, secured by means of a private key [14]. Therefore, one requires a private and public key. The public key would be used to verify whether the assets belongs to them. The one in possession of the private key is therefore the owner of the asset. The owner can sell or give someone the assets by giving the new owner the corresponding private key e.g. through the use of smart contract.

With the case of physical assets which are more prone to fraud, a uniquely identifiable tag or chip could be attached to it and this would be added to the blockchain. If the tag or chip is compromised in any way, therefore the smart contract would not be guaranteed. An example of a smart property is with the introduction of proof of existence, which is discussed below.

- **Proof of Existence**: Proof of existence created by Manual Aruoz, is a web-based service used to prove the authorship of things such as software or documents. The information contained in a document would not be revealed and it can be used to show that a particular document was added on the blockchain at a certain time [14]. The system computes a digest of the contents of the document using cryptographic hash function and later on the digest is inserted into a block of the blockchain. Therefore, the block's timestamp becomes the document timestamp. A modified version of the document would present a different hash digest which then presents a limitation of this process.

2.4.6.4 Land Titles

Land titles can be beneficial as it would reduce the bureaucracy and the corruption that is connected with the real estate industry. Authentication of the holders would be easier and land transfer would require less capital [64].

Many companies including IBM have started investigating blockchain. IBM released a paper in 2015 about saving the future of Internet of things (IoT) [67]. ADEPT is an effort to prove the foundational concepts around a decentralized approach, one that will offer greater scalability and security for the IoT. "The cryptocurrency space is actively engaged in investigations on optimizing different aspects of the technology including addressing challenges like scalability" [67]. The application of the concept of blockchain in the domain of IoT would bring fascinating possibilities. Once the IoT is blockchain based, the possibility of maintaining product information, the history, product revisions, warranty details and end of life in the blockchain means the blockchain itself can become the trusted product database.

2.4.7 Advantages of the Blockchain

As a payment system, Bitcoin has certain benefits over existing electronic systems. This section discusses advantages that can be attained from the use of the blockchain.

- Transparency — As has been discussed, all transactions are cleared in the Blockchain and it records all the transactions. The blockchain is public, therefore all the transactions can be tracked and traced. Everyone in the network can get access to the information of the system [68].
- Irreversibility — Regarding the payments made via intermediaries, human or software errors can be easily reversed by appealing to the intermediary. In a blockchain, things are infinitely more complicated. Once a block has been confirmed and new blocks are being added to the chain, an attacker can reverse any of the transactions by being in possession of 51% of the processing power to engage in a 'hard fork', which is not easy, thus making it difficult to reverse any transactions [69].

- Decentralised — The main aim of the Bitcoin network is decentalisation, therefore the blockchain is decentralised. There is no single entity controlling the system which limits the susceptibility to fraud and failure of the system.
- Network security — Blockchain is secured due to the use of cryptography. It is protected using proof of work which is performed by the nodes in the network.

2.4.8 Problems with Blockchain

The debate as to whether Bitcoin should be considered currency or commodity continues and it remains unclear with which perspective the average consumer and the monetary authorities will eventually view Bitcoin. The section below discusses aspects of Bitcoin that hinder it from being accepted easily and also presents problems that the Blockchain has.

2.4.8.1 Acquiring Bitcoin

Bitcoin is not yet widely accepted in the business community, but numerous merchants now accept bitcoins as payments. The means and ways to use bitcoins for payments is still ongoing research and development. Bitcoins need to be acquired before being used as payments, and these are the ways that bitcoins can be obtained:

- buying from an exchange,
- getting them from someone who is in possession of them,
- recieving a reward from successfully mining a block.

The last option is very difficult, because one needs to have enough computational power to start the process of mining.

2.4.8.2 Scalability

Scalability is an important issue when it comes to any system. Considering the number of transactions processed by the current electronic system such as Visa which takes approximately 2000tps (transaction per second) [70]. The question that arises then is whether Bitcoin can accommodate such volumes of transactions? This is a critical concern for the following reasons:

- The maximum size of a block is currently 1MB [28], approximately 7 transactions per second. The average size of a Bitcoin transaction is 250 bytes, which means at most an average of 4194 transactions can be incorporated into each block.
- All full nodes keep the entire copy of Blockchain which is currently about 65GB [71] and grows every 10 minutes on average. Increasing the size of the block to accommodate more transaction results in an increase in the rate at which the size of the blockchain increases. Consequently, the power (storage and processing) of full nodes will have to be increased. This raises the cost of having full nodes, which in turn, has a centralizing effect as less powerful nodes will eventually leave the network. Increasing the block size limit has long been an issue of contention in the Bitcoin community.
- Transactions in a block are only considered confirmed (tentatively) when the block is 6 blocks deep into the blockchain [70]. This means a transaction will only be confirmed on average after an hour. This would then be a problem when it comes to fast payments, For example, if a customer is making a purchase online using bitcoins, do they have to wait for an hour before the purchase is confirmed?

The above limitations warrant serious concerns in the event that Bitcoin is widely accepted for use [70]. A number of solutions have been proposed for the above issues such as using sidechains [72] and; mini blockchain [73].

2.5 Conclusion

This chapter presented the evolution of payment systems and how this led to the development of Bitcoin. Additionally, the different applications from Bitcoin have been discussed and details about problems facing Bitcoin have been argued. This would make a huge impact when it comes to deciding whether the Blockchain can work for SASSA. In Chapter 3 the methodology employed for this study is presented.

Chapter 3

Methodology

3.1 Introduction

This research was conducted in order to achieve the objectives set in Chapter 1. To recap, these are the questions specified in Chapter 1.

- **RQ1** — What are the challenges in the South African Social Security System (SASSA)?
- **RQ2** — Can the Blockchain be used to solve some of the challenges SASSA is facing?

The objectives for this study are as follows:

- **ROBJ1** — To assess the South African Social Security System and identify the existing challenges
- **ROBJ2** — To evaluate the impact of blockchain on the challenges
- **ROBJ3** — To design a solution for the challenges identified

Thus, this chapter provides a detailed methodology implemented in this dissertation. This includes research design, research methods employed for data collection and the data evaluation methods used.

3.2 Research Design

There are two basic types of research, namely; applied and fundamental. Applied research (referred to as action research) aims at finding a solution for an immediate problem facing a society or an industrial/business organisation [74]. In contrast, a fundamental research is mainly concerned with generalisations and with the formulation of a theory. Research aimed at certain conclusions (say, a solution) facing a concrete social or business problem is an example of applied research. Thus, the central aim of applied research is to discover a solution for some pressing practical problem, whereas fundamental research is directed towards finding information that has a broad base of applications and thus, adds to the already existing body of scientific knowledge [74]. The experimental research approach is the quantitative approach designed to discover the effects of presumed causes. The key feature of this approach is that one thing is deliberately varied to see what happens to something else, or to discover the effects of presumed causes. Therefore, the applied/action/experimental research was adopted for this work. The purpose of this approach is to develop and employ a model which is a solution pertaining to the problem.

Saunders explains how a research is structured using what he calls a research onion. The research onion is depicted in the figure 3.1.

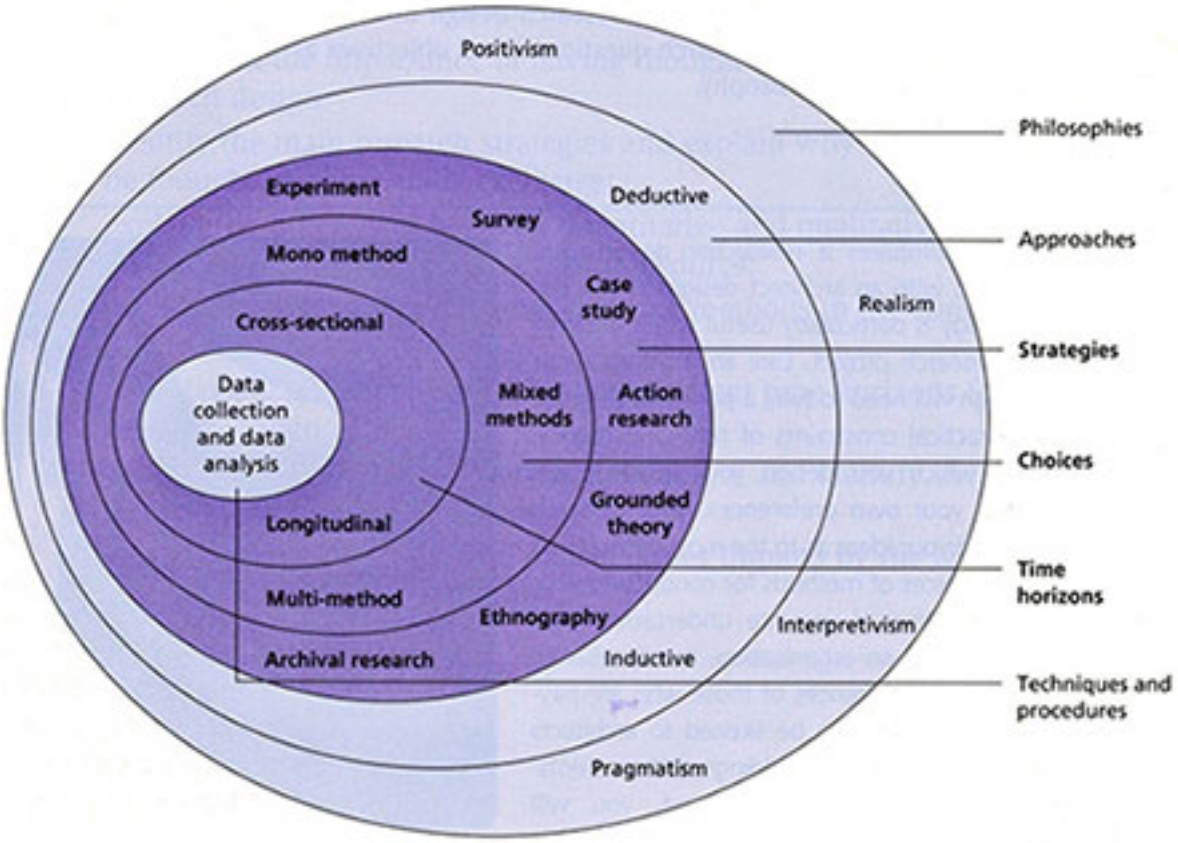

FIGURE 3.1: *Research Onion Diagram (from [5])*

The onion is made up of 6 layers, which are further divided into different parts. Based on Saunders, this research would employ the following:

- Layer 1(Philosophical Stances) — In this layer, this research would employ positivism. Positivism generates hypothesis or questions that can be tested and allows explanations. This is appropriate for this research because we have questions that need to be answered which were presented in Chapter 1.

- Layer 2 (Approaches) — The deductive approach was employed for this study. In this approach, a researcher starts with a question and sets out to answer it at the end and the main task would be to conclude with a yes or no response for the question. As the questions for this research were presented in Chapter 1, at the end of this research the aim was to provide answers to them. The main question at hand for this research is: Can the blockchain be applied to SASSA?

- Layer 3 (Strategies) — A case study was employed as the strategy. The case study involves extensive study of one or more individuals or cases in a real life context and the main case of this study was SASSA. More details would be provided in the sections below.
- Layer 4 & 5 (Choices and Time horizons) — These two layers were not employed in this research because this study would not be using quantitative and qualitative methods.
- Layer 6 (Techniques and procedures) — For data collection this research used the security threat model and for data analysis simulations/statistical modelling would be used. Further details are provided in the sections below.

3.3 Methodology

The study employed the following methods, namely extended literature review, case study approach, evaluative research, security threat modelling and simulations/ statistical modelling for the collection and analysis of data. These methods are discussed in the sections below linking them to the questions and objectives they aim to answer.

3.3.1 Extended Literature Review

An extended literature review approach was undertaken to provide an answer to the following objective:

- **ROBJ2** — To evaluate the impact of blockchain on the challenges

Therefore the aim of this method was to provide an overview of blockchain in the aspect of payment systems or any other system in general. The main reason behind this approach was that, Bitcoin is still at the inception stage and it brought a lot of promises through the technology, blockchain. Therefore, the aim was to study the technology and the use within other systems and this was achieved through the use of extended literature review.

This method was also applied to accomplish the following objective:

- **ROBJ1** — To assess the South African Social Security System and identify the existing challenges

The main aim for this was to gain an understanding of SASSA, how the system is structured and how it works in general.

3.3.2 Case Study

The second method was the case study; Zainal mentions that a case study allows a researcher to thoroughly scrutinize the data within a specific context [75–77]. Based on the above definition, this study was examining one unit which was SASSA. Therefore, the aim was to meet the following objective:

- **ROBJ1** — To assess the South African Social Security System and identify the existing challenges

The aim was to understand how SASSA works, how the system is structured so that it is easier to move on to the second part of the objective which was to determine the challenges. The underlying principle behind the selection of this method is [75]:

- It is capable of providing in-depth knowledge and insight for informed decision making. It facilitates an understanding of a complex, interdependent and dynamic social phenomenon like natural resource conflicts, in which multiple actors compete for scarce resources.
- It provides a platform for multi-perspective analysis during which researchers consider not only the views of actors but also the interactions between them.
- Case studies are well applicable for an exploratory research approach i.e., when one tries to better understand causal or complex relations in a certain environment without so much of theoretical background serving as the basis of hypothesis.
- The case study method is effective when in depth knowledge is required of any particular case for whatever reasons.

3.3.3 Simulation/statistical modelling

Another method adopted was the simulation/statistical modelling, and the aim was to answer the following question:

- **RQ2** — Can the Blockchain be used to solve some of the challenges SASSA is facing?

Also, to accomplish the following objective:

- **ROBJ3** — To design a solution for the challenges identified

Basically this method was to simulate the solution proposed for the attacks.

Maria [78] describes the process of producing a model; a model is a representation of the construction and working of some system of interest. A model is similar to but simpler than the system it represents. One purpose of a model is to enable the analyst to predict the effect of changes to the system. A model should be a close approximation to the real system and incorporate most of the salient features. Maria explains simulation as the operation of a model of the system. Simulation is a tool to evaluate the performance of a system, existing or proposed, under different configurations of interest and over long periods of real time. A simulation experiment is a test or a series of tests in which meaningful changes are made to the input variables of a simulation model so that we may observe and identify the reasons for changes in the performance measures. The procedure consists of 4 steps:

1. Simulation model development — whereby the development tool is chosen. For this study, MATLAB was to be used as it is a good tool when it comes to simulations.
2. Designing the simulation experiment — writing the detailed design of the simulation including how the simulation should be like at the end of the process.
3. Simulation/output analysis — this is how we plan to analyse the simulation at the end if it is correct or not. The aim was to test it against the attacks presented from the security threat model.

4. Formulating conclusions, and making decisions to alter the system under study — at the end conclusions are made whether the simulation is appropriate or not for the system and these were to be made based on the challenges.

Figure 3.2 depicts the schematic of a simulation study.

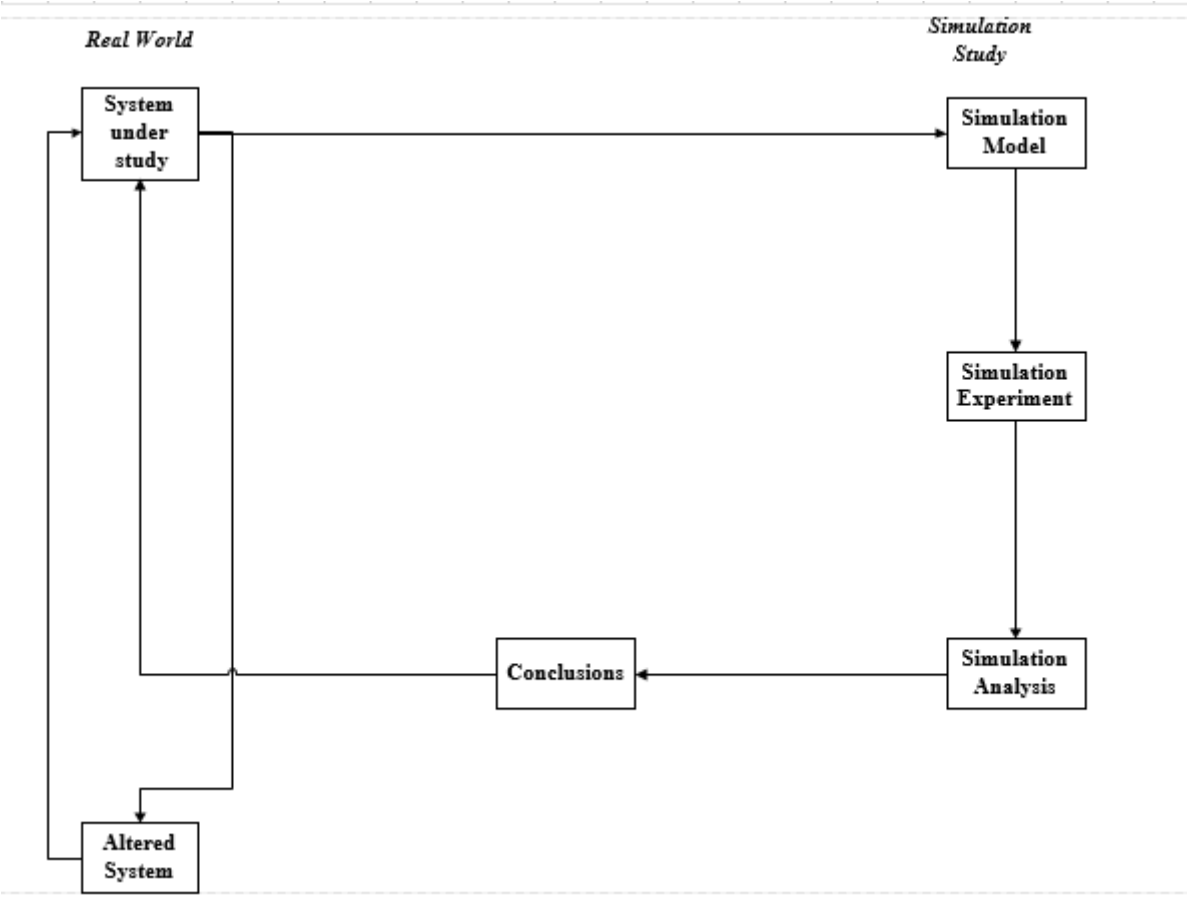

FIGURE 3.2: *Schematic of a Simulation Study*

When used accordingly, simulation modelling and analysis make it possible to:

- Obtain a better understanding of the system by developing a mathematical model of a system of interest, and observing the system's operation in detail over long periods of time.
- Test hypotheses about the system for feasibility.

- Studying effects can be done without disrupting the real system and significantly reduces the risk of experimenting with the real system.

This process of simulation also has pitfalls, which includes the following:

- time consuming — planning for a simulation takes a lot of time especially with designing.
- Simulation model may be too complex or too simple — the model could be too complex to understand and make conclusions on or too simple. Therefore, it is imperative to spend a lot of time with designing.
- Using simulation when an analytical solution is appropriate — it might happen that this method is used whilst it is not appropriate for that particular problem.

Simulations are dependent on the results of the analysis. If the analysis proves that blockchain could be applied to SASSA, therefore, simulations would be performed, otherwise this process would not performed.

3.3.4 Security Threat Model

The last method used was the security threat model. "Threat modelling involves understanding the complexity of the system and identifying all possible threats to the system, regardless of whether or not they can be exploited" [79]. This method aims to answer the following question:

- **RQ1** — What are the challenges in the South African Social Security System (SASSA)?

This model was used for the identification of possible threats in the SASSA system that would then make it easier to decide whether the proposed solution solves the threats identified. Comprehensive information about this method is discussed in the Chapter 4. Table 3.1 provides a summary by linking methodologies, questions and objectives.

TABLE 3.1: *Linking methodologies with questions and objectives*

Methodologies	**Questions**	**Objectives**
Extended Literature	RQ1	ROBJ1 and ROBJ2
Case Study	RQ1	ROBJ1
Security threat modelling	RQ1	ROBJ1
Simulation/statistical modelling	RQ2	ROBJ3 and ROBJ2

3.4 Conclusion

In this chapter methods utilized in this study have been presented, in order to formulate conclusions at the end of the study. It also presented in detail the analysis method and why it was preferred for analysing data but the simulations were not performed as a way of using blockchain to eliminate the identified challenges was not found. The following chapter discusses in detail one of the methods mentioned here called security threat modelling.

Chapter 4

Security Threat Modelling Using Attack Trees

This chapter introduces the process of threat modelling performed on the South African Social Grant System (SASSA). Whereby possible attacks that could happen in the system are identified and discussed in details.

4.1 Introduction

Designing a secure computer system is difficult. Attackers often break into systems and this has led to, software vendors providing security as a necessary feature for their products and network systems [79]. Powerful techniques to solve a wide array of security problems have been developed from years of research. An important question that needs to be asked; is "Are the security features of the system necessary, and do they meet the system's needs" [79]?. Security measures should be selected carefully and not arbitrarily in order to suit the entire system. Schneier [80] mentions that security is "a chain, it is only as secure as the weakest link. Security is a process, not a product."

The design of a system security is best done by the utilisation of a systematic engineering approach. Systems security engineering is concerned with identifying security risks, requirements and recovery strategies [81]. This is the process that involves developing

security mechanisms. Ideally, security engineering should be incorporated into the system design process as early as possible, from the initial architectural specifications if possible. The earlier security concerns are addressed, the less time consuming and costly it is to fix future security problems.

One view of security engineering process is given in figure 4.1. "Threat modelling involves understanding the complexity of the system and identifying all possible threats to the system, regardless of whether or not they can be exploited." [79].

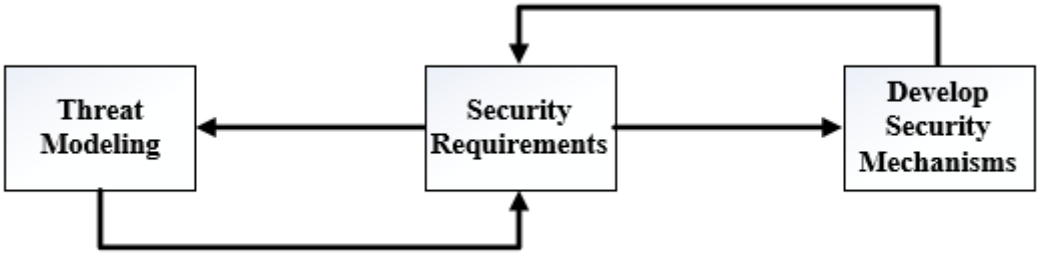

FIGURE 4.1: *System Security Engineering Schematic*

Threat modelling is also defined as "a systematic and structured security technique, used to identify the security objectives, threats and vulnerabilities of a system to help make design and engineering decisions and determine where to prioritise efforts in designing, developing and deploying secure applications" [79]. If the process of threat modelling is done well, it produces the following benefits:

- It provides a clear view across a project that justifies security efforts.
- It allows security decisions to be made rationally, with all the information available.
- It produces an assurance argument that can be used to explain and defend the security of an application or a system. An assurance argument starts with a few high level claims, and justifies them with either sub claims or evidence.

The system of concern here is SASSA, so the threat model mentioned here would be applied to this system in order to identify threats.

4.2 SASSA'S Payment Structure

South Africa has one of the largest cash transfer systems in Africa [82]. In total as of September 2015 [83] 16,938,608 grants were being paid out monthly. Social grants are considered an important instrument in fighting poverty in South Africa. SASSA is a national agency that was created to administer the application, approval and payment of social grants in South Africa. SASSA's main motto is "paying the right social grant, to the right person, at the right time and place. NJALO!" [84]. In total SASSA offers 8 types of grants namely: Old age grant (OAG), War veteran's grant (WVG), Disability grant (DG), Grant in aid (GIA), Child support grant (CSG), Foster child grant (FCG), Social Relief of Distress and Care dependency grant (CDG) [85]. Figure 4.2 depicts the structure of the payment system used by SASSA.

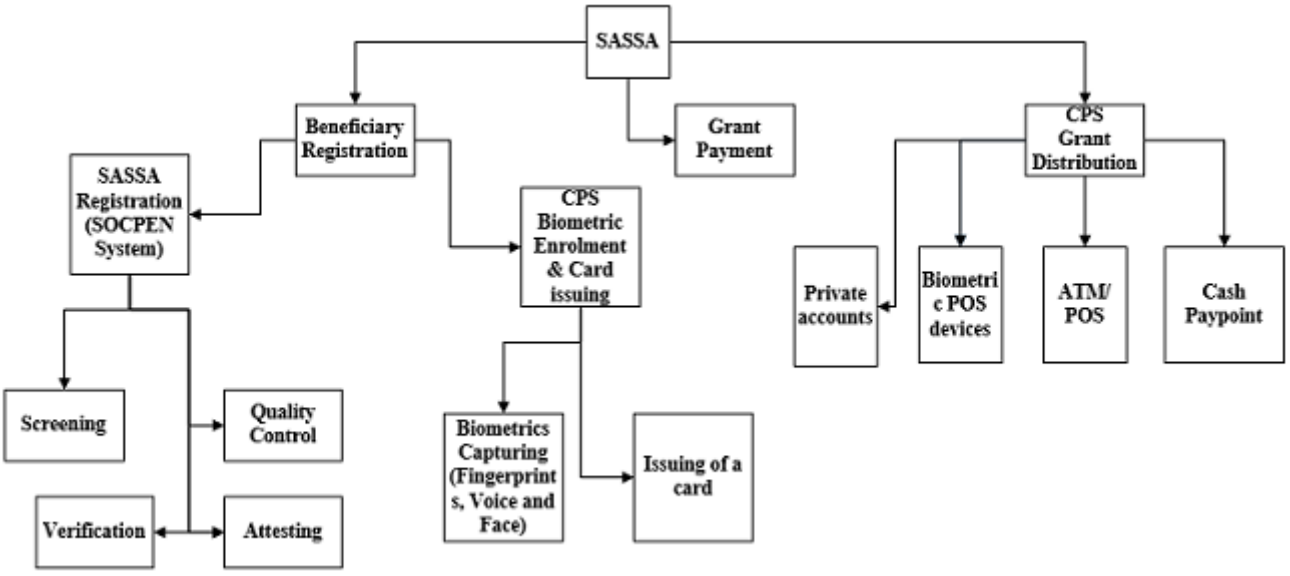

FIGURE 4.2: *SASSA'S Registration Payment Structure*

The first process involves the beneficiary registration, which takes place after a beneficiary has applied for a social grant. SASSA subcontracts the issuing of social grants to distribution companies which carry out the identification and the verification processes in different parts of the country [86]. Registration occurs in two stages, one performed by SASSA which involves four stages and the other by Cash Paymaster Services (CPS) which involves the capturing of biometrics and issuing of a card [87]. The four steps performed

by SASSA include screening, testing, quality control and verification. All of these four steps are performed in a system called the social pension system (SOCPEN) [88]. In January 2012, the Request for Proposal (RFP) was awarded to the Cash Payment Services (a subsidiary of Net1), who partnered with Grindrod Bank [89]. As the designated issuer, Grindrod Bank turned to MasterCard as the payment partner of choice. A biometric technology was used as a solution. Together, Net1 and MasterCard were able to integrate Net1's Universal Electronic Payments System (UEPS) biometric technology with MasterCard's EMV chip technology to create a solution that successfully operated in both online and offline environments.

Net1's UEPS biometric technology and MasterCard's EMV technology were combined onto a single chip that supports two sets of instructions:

- supports identification and grant approval
- supports grant access and spending

There are three types of biometrics captured in the first process, namely; fingerprints, voice and face [87].

The second process in the system called grant payment is the process of receiving funds and allocating them to beneficiaries so that they can access them on a monthly basis. This process includes the creation of a file that determines which beneficiaries are eligible for payments and the value they should be receiving that month. SOCPEN is used for generating the list of beneficiaries to be paid every month. Once the grants have been distributed by CPS, a financial reconciliation file is created of the paid and unpaid grants [87].

The third process in the payment system is known as grant distribution. This process describes how grants are distributed to beneficiaries and it is controlled by CPS [87]. There are four channels that beneficiaries can use to receive their grants which are:

- private bank accounts – money is sent via EFT
- ATM or Point-of-sale (POS) devices – pin-based cardholder verification (CVM)

- Biometric-enabled POS devices – uses biometrics for CVM to authorise transactions
- Biometric-enabled cash pay points – distribution of raw cash

4.3 Challenges/Concerns

During the process of studying and analysis of SASSA's processes, a few flaws were detected in the system. SASSA has challenges and some of them are listed below.

4.3.1 Authentication

Login details do not provide complete non-repudiation. If a person gains access to a user's login details, they could use these to fraudulently administer a particular step. Although this may be picked up during quality control checks, it would still be preferable if a higher level of non-repudiation could be achieved.

4.3.2 Integrity

This process of checking documentation is manual and it relies on the honesty and vigilance of the SOCPEN user. In addition the quality control may not detect that a particular document has been faked, e.g. a medical assessment. It is for these reasons that some applications do still have missing or incorrect documents even after approval. Even if the applicants do have all supporting documentation, there is a manual process involved in storing and retrieving files, which allows the possibility for documentation to go missing.

4.3.3 Fabrication, Authentication and Integrity of Identity Numbers

When applicants are not in possession of a valid ID number, they are required to provide alternative identification, there is a possibility that this may be faked and also that multiple grants may be applied for using the same alternative identification [86].

4.3.4 Offline Systems

A compromise in the NPR (The National Population Register) inherently affects the SASSA registration process since the DHA NPR is used to check the applicant's details. If there are cases where a person has been registered under multiple identities in the NPR, this would allow them to apply for multiple grants at SASSA. A similar problem applies to all other external information systems that SOCPEN uses. The SOCPEN interface to NPR is also offline, thus it may take some time to discover that a new beneficiary is not on the NPR.

4.3.5 Rightful Owner

The beneficiary must be in possession of a valid grant award letter and an ID book, which is automatically compared to the captured ID number and must match in order for the registration to proceed. However, there does not appear to be any visual verification to confirm that the person presenting the ID is in fact the rightful owner. Therefore, if a person gains access to a beneficiary's award letter and ID book after the SOCPEN registration process, they may be able to fraudulently enrol their biometrics and be issued with the beneficiary's card, since the biometrics are currently not checked against the DHA database. There is also insufficient evidence to indicate whether CPS checks the biometrics for duplicates, so they may not be able to pick up multiple identities.

4.3.6 Actual Capture of Biometrics

The quality of biometrics capture is not controlled for all the biometrics, which makes their usability questionable. The capturing of fingerprints is guided by the operator and the quality is ensured by the fingerprint scanner which does not capture an image unless it is of sufficiently good or readable quality. However, similar measures are not in place for the face and voice biometrics. The face and voice biometrics are currently not used by SASSA [90].

4.3.7 Children Fingerprints

Fingerprints are also captured from children, when in fact it is not clear whether these can be reliably used for recognition. As the child grows older, it may happen that fingerprints change but they are not re-captured. Again, it is unclear whether the children's fingerprints are used at all by CPS and SASSA.

4.3.8 Reconciliation

The current reconciliation process is reliant on the information from CPS. The main aim of the reconciliation file is to determine which beneficiaries were paid. However, there is no proof to indicate whether or not the information provided by CPS is genuine.

4.3.9 Proof of Life Methods

CPS has two mechanisms in place which could be used by beneficiaries to provide proof-of-life using biometrics:

- Voice proof-of-life (Beneficiaries call a toll free number and repeat phrases as prompted).
- Fingerprint proof-of-life (beneficiaries use the biometric-enabled payment channels which automatically provide proof-of-life since a fingerprint is required to authorise payment).

However, the above methods are not monitored, in that no information is provided to SASSA of which beneficiaries have provided proof-of-life or not. As a result, SASSA uses the NPR as their sole source for determining if a beneficiary is still alive. If a death is not registered with DHA, a person could continue to fraudulently claim the grant of a deceased beneficiary or deceased child dependent. When an ATM is used as a channel for receiving grants no biometrics are used, therefore proof-of-life is not practised.

4.3.10 Bypassing of the National Payment System

The current biometric-enabled distribution channels make use of a biometric-based CVM which is not standardised in South Africa and the payments therefore bypass NPS. Payments at these distribution channels do not meet PASA (Payments Association of South Africa) regulations, which is a major concern for SASSA.

4.3.11 Fraud and Corruption

This is the most dangerous challenge SASSA is facing which leads to money loss.

4.4 Players involved

The following provides details of all the stakeholders participating in all the processes involved in the system.

- **Cash Paymaster Service (CPS)** — After the payment cycle for each month, CPS must submit a reconciliation file listing all the beneficiaries who have been paid as they are the ones responsible for the payment process. CPS can submit a wrong reconciliation file to SASSA. Fraudulently lying about the profit accumulated from the money in their account before being distributed to beneficiaries. Offer beneficiaries loans which they are not supposed to take. Using beneficiary's confidential information without their consent.
- **CPS Official** — They are responsible for distributing grants whereby they distribute cash. To attack the system, they could fraudulently deprive beneficiaries their grants especially those using the cash pay points and claim that they were not paid that month. Reporting wrong information to SASSA. Registering biometrics of a beneficiary who is not the rightful owner of the ID number presented.
- **SASSA'S Official** — They are responsible for registering beneficiaries on the system. To defraud the system, the official has an option of stealing another official's

login details which would then lead to one gaining access to where they are not supposed to. The SASSA official may not be vigilant enough in the process of verifying the documents provided by the client registering for a grant. The official could fraudulently register a beneficiary that does not exist. He/she may deny someone a grant just because of personal issues with them. Denying the quality service to beneficiaries that they deserve.

- **Beneficiary** — The potential beneficiary registers for a grant and if approved an award letter is issued and used to register for a card. A cyber attacker could steal someone's identity and use it to register for a grant. A beneficiary may receive a grant of someone who has passed on. One may lie while taking the means test in order to receive a grant whilst they do not qualify. One may fraudulently apply for fake ID numbers. One may receive grants for children who do not exist. One may bribe an official in order to get registered for a grant or bribe a medical doctor in order to qualify for a grant.
- **Medical Doctors** — For disability grants, doctors are required to do a check-up on the applicant and decide whether they qualify for the grant or not. To defraud the system, doctors could forge a medical report that qualifies a beneficiary to receive a grant.

4.5 Possible Attacks

The following gives a description of possible attacks that might affect the system.

- **A1: Identity theft between officials at SASSA** — This may be used to gain access where that official does not have access to the system.
- **A2: Bribery of SASSA officials** — The aim of this may be to help with the approval of grants in the case where applicants are not eligible for that grant.
- **A3: Registering non-existing beneficiaries** — This is successful when a beneficiary is in possession of a fake certificate/ID and use those to apply for grants. This has been encountered in the case of children.

- **A4: Beneficiaries bribing medical doctors to get medical approval** — Some of the grants offered by SASSA requires a medical doctor to confirm the eligibility of that beneficiary. Beneficiaries end up bribing the doctor in order to become eligible for such a grant.

- **A5: Beneficiaries using fake identities (identity theft)** — This method allows beneficiaries to receive grants that they are not eligible for.

- **A6: Approving and disapproving grants fraudulently** — This can happen when the official has been bribed to do so, or they know the client applying for the grant.

- **A7: Using someone's award letter to enrol/capture biometrics and get a card (identity theft)** — A beneficiary can only get a card when they have the award letter whereby they are required to capture their biometrics. Someone can steal the award letter and successfully capture their biometrics. This is possible because the biometrics captured are not verified with the ones stored at the Department of Home Affairs, to make sure the information on both sides matches.

- **A8: Beneficiary file being lost due to e.g. fire** — Whenever a beneficiary registers for a grant, a physical file is created and it is stored in a warehouse. if something happens to the warehouse, then SASSA losses the files like in the case where the warehouse was burnt.

- **A9: CPS using beneficiary's confidential information** — CPS has access to beneficiary's information, and they might use the information for something else which is not approved.

- **A10: CPS offering beneficiaries loans/ other benefits illegally** — SASSA does not allow beneficiaries to be allowed to take loans and use their grants for paying back. It only allows deductions like funeral covers.

- **A11: CPS not being honest about the interest gained before the money is paid to the beneficiaries** — CPS receives money before the payment process begins, and they are accountable for returning the interest gained on that money to SASSA. Once again SASSA relies on the information provided to them.

- **A12: CPS submitting a fraudulent reconciliation file to SASSA** — the reconciliation file consists of beneficiaries that were paid and those who did not collect their grants for that month. SASSA has to rely on the information provided by CPS.

The following section would give details on how the above attacks or threats can be performed in the system using attack trees to depict it.

4.6 Attack Tree

"Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, it represents attacks against a system in a tree structure, with the goal as a root node and different ways of achieving that goal as leaf nodes" [91]. The basic steps to create an attack tree are as follows:

- **Decide on the representation** — There are AND trees, where the state of a node depends on all of the nodes below it being true, and OR trees, where a node is true if any of the sub-nodes are true. For this study the OR tree was adopted, as it represents different ways a certain attack could be achieved.
- **Create a root node** — The root node can be the component that prompts the analysis, or an adversary's goal. Some attack trees use the problematic state (rather than the goal) as the root. For this case the problematic case has been adopted.
- **Create sub-nodes** — The relationship between sub-nodes can also be AND or OR, and the OR would be used. The list of sub-nodes would be provided below.
- **Consider completeness** — The aim for this step is to determine whether the set of attack trees is complete enough. An attack tree may be checked for quality by iterating over the nodes, looking for additional ways to reach the goal.
- **Prune the tree** — In this step, one goes through each node in the tree and consider whether the action in each sub-node is prevented or duplicative.

- **Check the presentation** — One should aim to present each tree or subtree in no more than a page. If the tree is hard to see on a page, it may be helpful to break it into smaller trees.

4.6.1 Sub-Nodes

The following section describes the possible attacks in the system which are depicted and numbered in figure 4.3 below.

1. **Fraud and Corruption** — This occurs when users of the system are not honest in using the system according to the rules stipulated. For this study, 4 types have been identified and labelled in figure 4.3.
    - **Identity fraud** — Usually occurs when one steals someones personal information e.g. open credit card accounts. Three types have been identified.
        - Login Details — Whereby credentials are stolen and used to defraud the system.
        - Id Numbers — ID numbers are stolen and used to register for social grants.
        - Rightful Owner — When someone steals an award letter from the rightful owner and use it to register for a card.
    - **Insider fraud** — Whereby people working in a system are responsible for defrauding the system.
        - Beneficiary registration — SASSA officials could be involved in registering false or non-existing beneficiaries in the system.
        - Beneficiary file handling — Officials manipulating or not handling the files appropriately.
        - Beneficiary enrolment — CPS officials could manipulate the process of enrolment.
        - Beneficiary bank account (CPS) — Withdrawing money from beneficiaries accounts e.g. for airtime or loans. SASSA prohibits any of these activities.
        - Fraudulent reconciliation file — Tampering with the reconciliation file e.g. not providing all the list of beneficiaries paid for that payment cycle.

  - Medical reports — Doctors receiving bribes and faking medical reports.

2. **Payments** — presents attacks that could happen during the payment process and it is divided into 2 parts.

   - **Proof-of-life methods** — this is a way beneficiaries prove they are still alive.
     - Utilisation of voice and face biometrics — voice and face are supposed to be used by beneficiaries to provide proof of life, but this is not clearly monitored. These are captured during the process of registration but it is not clear as to when they are utilised in the system.
     - PIN security — PINs are used for cardholder verification methods and this could be a problem because most of the beneficiaries are old so it would be difficult for them to memorise a PIN.
   - **Standardisation** — in South Africa, PASA is responsible for the standards and regulations.
     - Bypassing NPS — for offline methods, SASSA use fingerprints for cardholder verification methods which is not regulated by PASA therefore, it bypasses the standardisation.

3. **File Handling** — for every social grant registration, a file is created for each beneficiary. The physical file is stored in a warehouse.

   - File Access — access to these files must be monitored because it contains personal information.
   - File confidentiality — contents of the file should be confidential so that it is protected from fraudulent activities.
   - Confidentiality of private information — if anyone has access to beneficiaries private information, they could use it for fraudulent activities.

Figure 4.3 depicts different ways in which fraud and corruption can be achieved in the system.

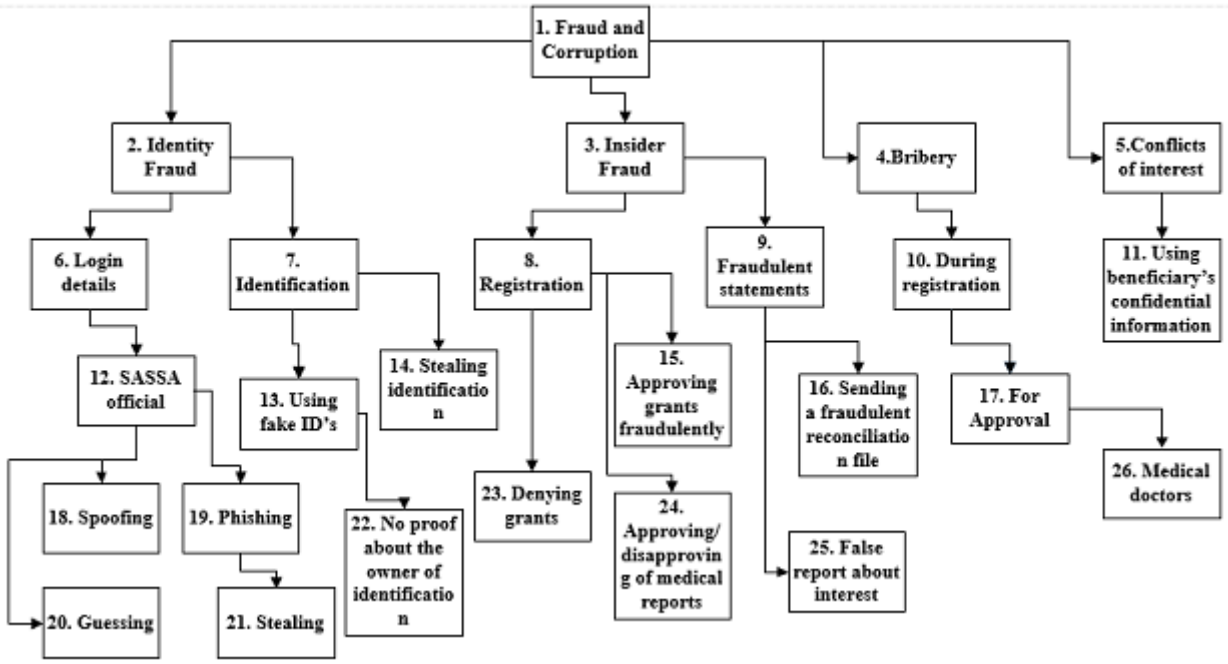

FIGURE 4.3: *Attack Tree*

4.7 Conclusion

Threat modelling is an important process that helps in the identification of threats in a system; it has been used to identify the possible threats presented here. This chapter presents the use of attack tree in order to depict some of the attacks that could happen in the system leading to the main attack identified as fraud and corruption and the damage caused thereof. This makes it easier to propose solutions to the threats identified.

Chapter 5

Proposed Solution

5.1 Introduction

South Africa currently spends over 4% of the gross domestic product (GDP) on social grants and the minister of Finance, Pravin Gordhan has announced that social grants will receive an additional R11.5 billion to protect low-income households [92]. This was announced in the budget speech, February 2016 [93]. According to the budget review, the reprioritisation and spending reductions have been designed to minimise negative consequences for low-income households [93]. This statement is because many households depend on social grants. However, corrupt people are misusing the main aim of social grants which actually leads to a loss of money. This has been encountered, whereby 14 people have been arrested for defrauding SASSA of more than R2.3 million involving more than 400 social grants [94].

It was reported on the 28th of May 2016, that Hawks (Directorate for Priority Crime Investigations) have caught a social grant fraud syndicate [94]. Amongst the arrested includes, SASSA officials, CPS officials and members of the public. The report mentions that 8 SASSA officials that are responsible for capturing and verifying social grants on SASSA's SOCPEN system were arrested [94]. During the arrest the following items were found:

- Laptops

- Scanners
- Copying machines
- ID's
- ID copies
- ID templates
- CPS enrolment machines
- Printers
- Electronic storage devices
- Bank cards
- SASSA cards

This means that they were able to register for fraudulent grants, with fraudulent ID's and get SASSA cards in order to receive grants. These are prominent security flaws that are costing SASSA a lot of money. The section below provides details on the hypothesis made from this attack.

5.1.1 Hypotheses

After the analysis of the attack leading to SASSA losing money, the following hypothesis was made and details on how it may have been successful are provided below.

1. "SASSA is vulnerable to attacks when officials using the SOCPEN system are corrupt because they could capture and verify grants."
2. "Attacks are more prone at SASSA when fake identities exist because attackers can get fraudulent ID's."
3. "Devices used for the registration process at SASSA have a lot of impact on fraud because they can be duplicated."

During the process of registration, SASSA officials use the SOCPEN system to capture applicants information, process applications and verify social grants. Therefore for hypothesis 1 to be successful, officials need to work hand in hand with the attackers. Access to the SOCPEN system, makes it easier for the following to be successful:

- applying for fraudulent grants, and
- fraudulently verifying grants

This means that the officials were able to apply and verify fraudulent grants because they already have access to the system.

During the arrest described in the section above, IDs were found. To register for a social grant, an ID is required therefore it means that the IDs found were used in order to register for grants. It may be possible that these we acquired due to identity theft or fake IDs. Information gathered during identity theft could be used to register for fake IDs, therefore, application of grants [95]. The green barcoded identity document used has been said to be prone to fraudulent instances. Attackers could get hold of fake IDs if they are working with people from the Department of Home Affairs and if they get access to the system used for IDs [96]. It has been reported that people have found a way to the National Population Register system and therefore acquired green barcoded IDs fraudulently. This makes hypothesis 2 to be successful.

After the registration process is complete and successful, the applicant proceeds to CPS to get a card. Before a card is issued, fingerprints must be captured. Therefore, if attackers have access to these devices, it becomes easy for them to issue SASSA cards. It would be easy to know how the system works because they work together with CPS officials. This means that they can issue fraudulent cards and then receive grants leading to the success of hypothesis 3.

The proposed solutions for the attacks identified in Chapter 4 and the ones identified in this section, are presented. The proposed solution is categorised based on the attacks mainly because the attacks require different solutions. In what follows, a brief description of the attacks as well as the solutions.

5.2 Attacks

This section provides a brief explanation of the attacks identified in Chapter 4. These attacks were identified during the process of security threat modelling, discussed in details in Chapter 4. The broader categories of the attacks are provided below and only those attacks that would get a proposed solution are discussed below. This is because not all the attacks identified would be solved, but only those of significant impact to SASSA would be discussed, limiting the scope for this study. This was assessed based on the impact that could be caused to the system when an attack occurs e.g. if it is something that would not have any difference in the system, therefore they was no need to add this attack.

5.2.1 The Reconciliation File Attack

The main aim of the reconciliation file is for CPS to provide SASSA with a list of beneficiaries that have been paid. SASSA cannot prove the validity of the information contained by the reconciliation file as discussed in Chapter 4. The reconciliation file is merely based on trust. This attack can allow CPS to tamper with the reconciliation file and submit a fraudulent one. This attack can be possible because SASSA has no way of verifying the information on the file.

5.2.2 Receiving Double Spending Attack

For the offline payments, everything is registered to the reconciliation file at the end of payment cycle (which is at the end of a business day). For this attack, the question is: What is stopping a beneficiary using the offline payment to collect their grant from one pay point and shortly after going to another pay point to collect the same grant?

5.2.3 Award Letter Attack

Once a social grant has been approved, a beneficiary is provided with an award letter which is presented for the process of capturing fingerprints and card registration. CPS

is responsible for this process. With this attack, nothing is stopping an attacker from stealing someone else's award letter and presenting it for card registration.

5.2.4 Proof of Life Certification Attack

This is a way for SASSA to know whether a beneficiary is still alive or not. SASSA incorporated the use of fingerprints to serve as the cardholder verification. The challenge is that it is only available for offline payments which are considered to be outside the regulations of the National Payment System(NPS). As described in Chapter 4, other means exist to provide proof of life but these are not monitored. SASSA has a challenge with beneficiaries using the online payment systems because there is no way for beneficiaries to provide proof-of-life. This opens a gap for an attack, whereby someone receives a grant for a beneficiary that has passed away only if they are not yet registered in the NPR database, which is the only way SASSA knows if a beneficiary is still alive.

5.3 Proposed Solution

This section provides solutions to the attacks presented above. Details on how the proposed solutions work for SASSA are also provided.

5.3.1 Solution to the Reconciliation File Attack

This solution proposes that two keys (public and private key) per the rules of digital signatures must be generated during the enrolment process. When a beneficiary receives a card, the private key is stored on the card. During the process of signing the transaction record, the private key is employed to create a digital signature. The public key is mainly for SASSA to use during the process of verification which commences after the payment cycle. As a solution to this attack, we propose the use of digital signatures. Digital signatures are good when it comes to integrity checking and it allows users to provide assurance for the receiver that the data was infact sent by the assumed party. The digital

signature scheme allows users to produce 2 keys (private and public key) [97]. Generally, digital signature scheme $DS = (K, Sign, VF)$ consists of 3 algorithms as follows [97]:

- The randomized key generation algorithm K (takes no input) returns a pair (pk, sk) of keys, the public key and matching secret key respectively.
- The signing algorithm $Sign$ takes the secret vkey sk and a message M to return a signature $\sigma\epsilon[0, 1]$. The algorithm may be randomized or stateful. We write $\sigma \leftarrow Sign_{sk}(M)$ or $\sigma \leftarrow Sign(sk, M)$ for the operation running $Sign$ on inputs sk, M and letting σ be the signature returned.
- The deterministic verification algorithm VF takes a public key pk, a message M, and a candidate signature σ for M to return a bit. We write $d \leftarrow VF_{pk}(M, \sigma)$ or $d \leftarrow VF(pk, M, \sigma)$ to denote the operation running VF on inputs pk, M, σ and letting d be the bit returned.

For the solution, we propose the use of this method. The two keys discussed above would be generated during the process of registration or capturing of biometrics and issuing of a card. The private key would be sent to the smartcard because it needs to be safe and not be compromised in any way. The public key would be stored in a file which would be kept at SASSA which would be used for verification. On their own smartcards provide a layer of authentication, but we want to add another layer of authentication that would make it difficult to break or forge contents or information, because the private key would be stored on the smartcard [98]. Therefore, it is important that the smartcard be secured and safe enough to store the private key thereby it requires a strong security protection and authentication [99]. The Advanced Encryption Standard (AES) for smartcards would be used for the proposed solution as it is considered to be amongst the secured algorithms for smartcards [100] [101].

AES was announced by the National Institute of Standards and Technology (NIST) as US FIPS PUB 197 (FIPS 197) in November 2001. It is a symmetric key encryption which comprises 3 block ciphers: AES-126, AES-192, AES-256 adopted from a larger collection originally published as Rijndael [101]. Each of these ciphers has a 128-bit block size,

with key sizes of 128, 192 and 256 bits, respectively [100]. The AES ciphers have been analysed extensively and are now used worldwide, as the case with the predecessor, the Data encryption Standard (DES).

One issue that arises in software implementations is the basic underlying architectures. The performance of AES or any other encryption algorithm depends on a particular high-level language used. In most cases, software strongly affects the performance [100]. Users need to prove their identity before using the card and currently this is only used for the offline payment methods, whereby beneficiaries use fingerprints unlike for online payments who use PIN's and there is no way to prove identity using this method.

There are two main approaches involved when using biometrics.

- **Fingerprint matching** - where the smartcard stores a template of the user's fingerprint and requires the user to present a matching template before it will sign messages on the user's behalf [102].
- **Fingerprint mapping** - where a fingerprint is used to obscure the private key, without storing a template. The private key can only be recovered and consequently used to sign an authentication message if a valid fingerprint is provided [102].

For the proposed solution, we propose the use of fingerprint matching as it is already incorporated in the current system. The diagram 5.1 below shows the schematic of our proposed solution.

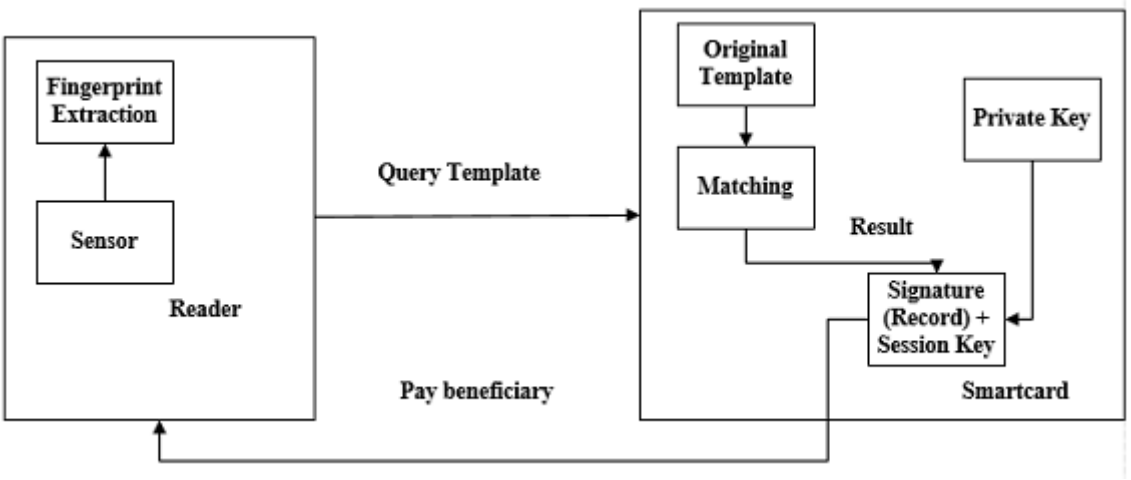

FIGURE 5.1: *Offline Solution*

The user presents the smartcard to a machine or terminal, then a fingerprint scanner is used to capture the fingerprint image. Storing a raw fingerprint or any biometric data typically requires substantially more memory e.g. a complete fingerprint image will require 50 to 100 kbytes, while a fingerprint template requires only 300 bytes to 2kbytes [103].The method used here is known as match-on-card (MOC), whereby the process of data acquisition and feature extraction is done at the reader while the matching is performed inside the smartcard [102]. During the stage of enrolment , the original template constructed at the reader is stored in the card. During matching, the reader will construct the query template which is then sent to the smartcard for matching . The final matching decision is computed inside the smartcard and the original template is not released from the smartcard.

Algorithm 5.1 below shows the process of matching.

Algorithm 5.1 Offline Solution.

```
1: function COMPARE(Q,S)
2:     if Compare = True then
3:
4:         function CHECK-PAYMENT-FILE(Payment file, ID number)
5: return X
6:         end function
7:     end if
8:     if X then = true
9:
10:        α ← Signature_sk(record)
11:        break
12:    end if
13: return α + record
14:
15: end function
```

Therefore, features would be extracted and sent as a request or query template which is in a form of a text file to the smartcard for the process of matching as shown in figure 5.1. If the process of matching is successful, a payment file is checked which is stored on the terminal or computer being used else the process stops or terminates. If the beneficiary is not in the payment file the process stops, else a transaction record is sent to the card to create a digital signature.

During the process of creating a digital signature, the private key inside the card is used to compute this function

$$\sigma \leftarrow Sign_{sk}(Record)$$

, where sk is private key and $record$ is what is stored in the payment file (i.e. Name, surname, ID number, Amount etc). The output (signature or σ) would be stored on the card which would be recorded in the reconciliation file along with the record.

We also propose the use of a session key, which would be an integer number generated after the digital signature has been created. This key would be used as a representation that a beneficiary has claimed the grant, therefore, preventing double spending. This session key would be stored in the card. Once this process is complete, the beneficiary is then paid and a reconciliation file is created. Because offline methods do not have access to the database, this process of a reconciliation file would be completed offline then later added to the main reconciliation file.

As we have seen the proposed solution above, caters mostly for offline payment methods. This is because fingerprints are not regulated for online payment methods instead PINs are used. The process remains the same mostly, but what we need to consider for online payment methods, is the fact that they are not allowed to withdraw all their grant allocation at the same time. But then the grant is only released to their accounts once and all the grant is paid to them. More solution proposed for the online payment method would be presented in the sections below.

5.3.2 Solution to the Double Spending Attack

The solution to a double spending attack that is described in 5.2.2 is presented here. This attack could only be performed by beneficiaries using offline payment methods and for this, we propose the use of session keys as described in the section above. Therefore if a beneficiary tries to go to another payment station after getting paid, the machine first checks if a session key already exists in the card and if it does the process stops. Figure 5.2 shows how this solution would work for this attack.

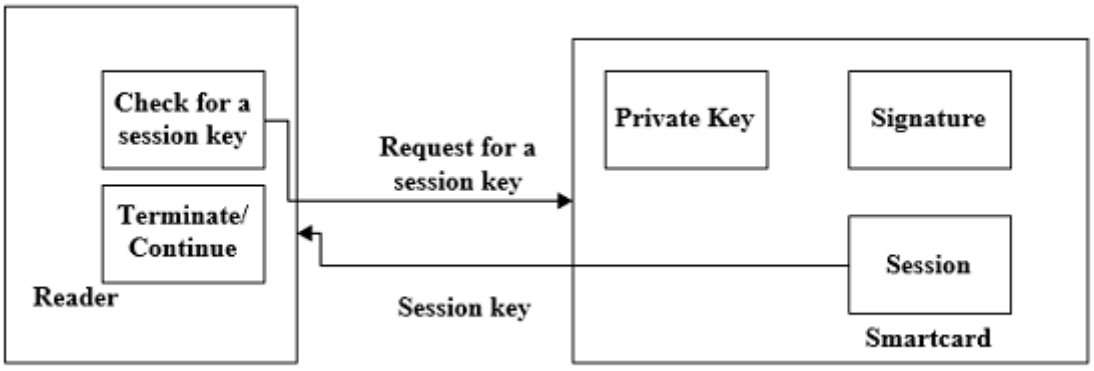

FIGURE 5.2: *Double Spending Solution*

5.3.2.1 Verification

Once the payment process ends, CPS has to submit a reconciliation file to SASSA. Upon receiving the file, SASSA can verify the contents in the file by the use of decryption. Therefore, SASSA uses the public key to decrypt and compute this function:

$$d \leftarrow VF_{pk}(M, \sigma)$$

as described in 5.3.1, where M is the record, σ is the signature and pk public key. This would show if the contents of the file have been tampered with.

Thus far the problem of proof of life certification for beneficiaries using online payment methods has not been solved, and the section below describes the proposed solution for this attack.

5.3.3 Solution to the Award Letter Attack

Currently, there is nothing stopping an attacker from taking someone's award letter and use that to register for a card in order to receive a grant, if that award letter has not been used as described in 5.2.3. The solution we are proposing is, to start checking beneficiaries' fingerprints with the ones stored at home affairs. During the process of enrolment, when fingerprints are captured those fingerprints would be checked with the home affairs

database to see whether they bring up the same information. If the information is not the same, it means something is wrong otherwise, there should be a match. In this way, it would mean that the department of Home Affairs database needs to be up to date so as to prevent any errors when it comes to checking of the fingerprints.

5.3.4 Solution to the Proof of Life Certification Attack

Proof of life certification is a way in which a beneficiary must prove that they are still alive before their grants are paid out. Details about this attack have been presented in 5.2.4 above. Fingerprints are used for offline payment methods, but for online methods nothing has been implemented with regards to the use of biometrics. Because banks use PINs instead of fingerprints, therefore anyone with access to the PIN can withdraw the grant. The diagram 5.3 below depicts the general security levels available.

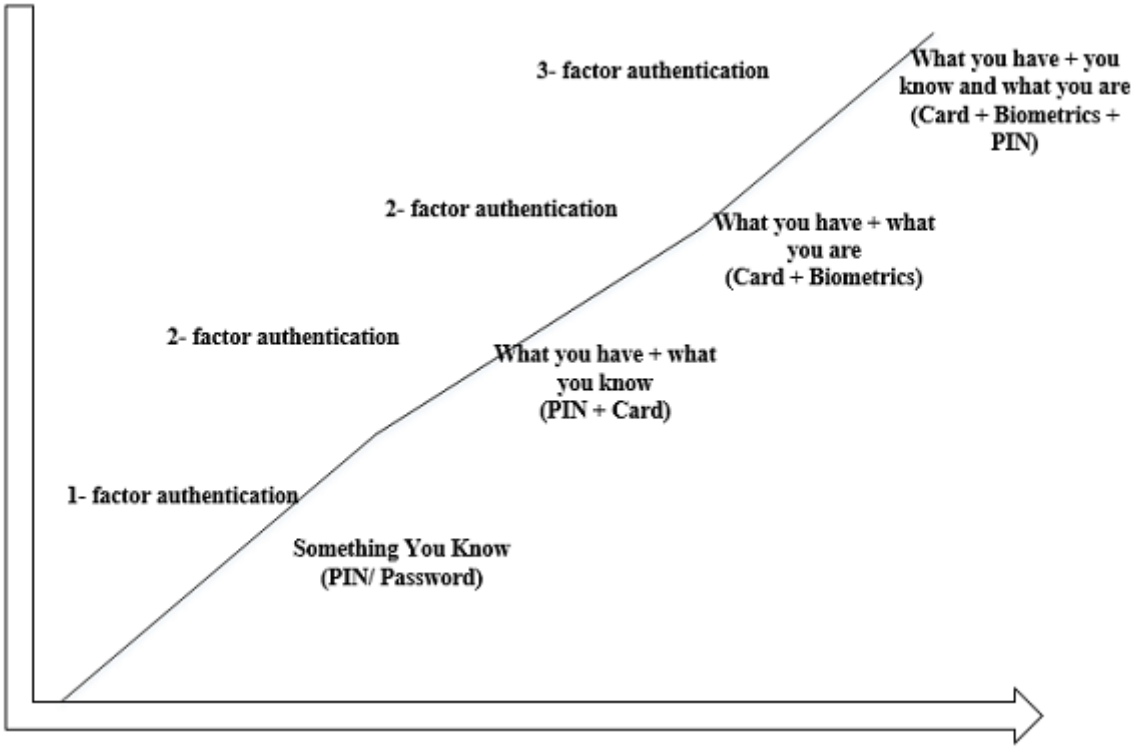

FIGURE 5.3: *Security Levels of Authentication*

Currently, SASSA falls in the category of two-factor authentication as shown in the above diagram. As a solution to this attack, we propose moving from two-factor to three-factor

authentication by the use of a new smartcard. This new smartcard has been seen in the Smartmetric whereby it allows Bitcoin users to withdraw at ATMs. This new card allows users to activate the card using fingerprint before inserting it into the ATM. This new card has also been proposed for credit cards in Britain whereby fingerprint scanners would be used instead of PINs.

Therefore, we propose the same smartcard for SASSA which would present SASSA the opportunity of knowing exactly which beneficiaries are still alive as discussed in [104]. This is because the card can only be used by the owner and no one else which might be a drawback for beneficiaries because they cannot send someone to withdraw on their behalf. This card might even present an opportunity of reducing the risk of card fraud. Diagram 5.4 shows how the new card would look like.

FIGURE 5.4: *Proposed Card*

The card would comprise of a CPU, memory,and a fingerprint reader including a sensing surface (preferably towards the edge of the card for easier access) [105]. When an individual inserts the card into the ATM, the query template of the fingerprint is compared with the template stored in memory during the process of registration. If the matching process is successful, the card is enabled and the user is allowed to enter their PIN and continue with the process of transacting or withdrawing. Diagram 5.5 depicts how the solution would look like and the matching.

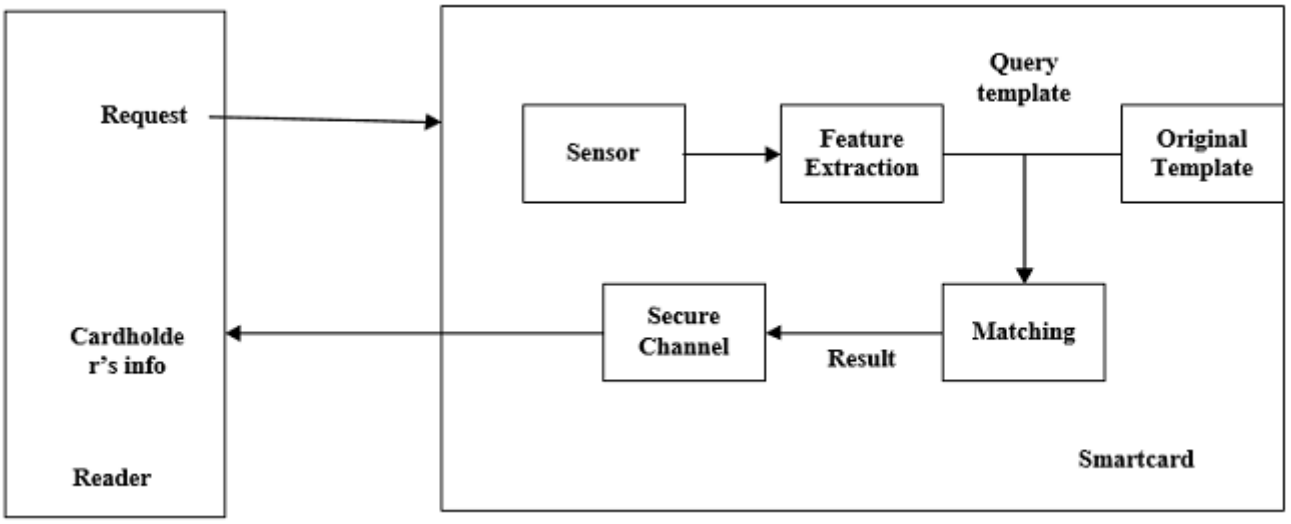

FIGURE 5.5: *Solution for Online Methods*

The technology used here is known as system-on-card (SOC), whereby the smartcard incorporates the entire biometric information, processor and algorithm [102]. Therefore, the entire process of biometric data acquisition, feature extraction and matching is done inside the card as shown in figure 5.5. The sensor we are proposing to use is from FPC sensor technology with a slim package which would be a perfect fit for smartcards. This company is known for the best sensors even for smartphones. The reasons for choosing this technology are listed below:

- Lower power consumption
- Thin compact form factor (ISO compliant)
- 3D image quality which leads to superior biometric performance

The ATMs used currently would not be required to be changed at all. The section below presents advantages and disadvantages to the system.

5.3.4.1 Advantages and disadvantages of the model

Like any other technology, biometrics have their own advantages and disadvantages. These are some of the advantages that would be presented by the model:

- Strong authentication — because authentication mechanisms are always with the user, there is no need of memorising or frequently changing passwords or PINs [106].
- Easy to operate — the sensor is positioned in a way that it is easier to access.
- Secure against card fraud — the card cannot be used by anyone else other than the cardowner, therefore if the card is stolen it would be difficult for someone else to use it.
- Links every transaction to the card owner — because only the cardholder can use the card it means every transaction performed on the card, the cardowner can account for it.
- Provides proof of life certification to SASSA — SASSA would have proof that the cardholder is still alive because they are still withdrawing their grants.

Some of the disadvantages include:

- Costs — changing the current smartcards and including sensors.
- Fingerprints fading because of age — as people grow older, fingerprints tend to fade and when this happens it becomes difficult for them to be used for authentication.
- Not being able to send someone to withdraw on your behalf — this would be a disadvantage especially when it comes to elderly beneficiaries because they may want to send someone on their behalf at a certain point to withdraw for them.

5.3.5 Solution to CPS Enrolment Machines

The use of digital signatures proposed above for the other attacks is proposed for this attack. We propose the use of public/private key pairs, to be assigned to the devices used for the enrolment of cards. For the private key to be secure, it must be stored on the device so that it is used by that device only. We propose the involvement of certificate authorities for the assigning of keys and we propose that SASSA serves as the certificate authority for themselves and use digital certificates for the internal certificates.

During the process of enrolment (which was discussed in Chapter 4), biometrics are captured and a card is issued to the beneficiary. Thereafter, the beneficiary's information is stored on the card. What we propose is that the beneficiary's information be signed using the private key stored on the device to produce a digital signature. This digital signature would be stored on the beneficiary's card along with other information i.e. name, surname, ID, beneficiary's private key etc. Figure 5.6 below depicts how the proposed solution would work.

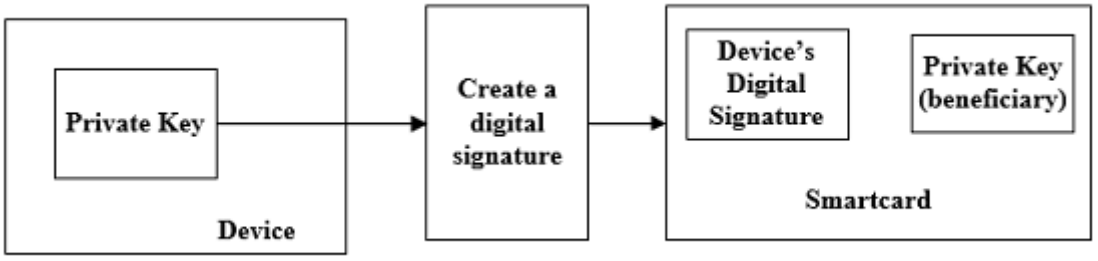

FIGURE 5.6: *Solution to Enrolment Devices*

When the card is inserted into a machine or ATM, the digital signature would be decrypted using the associated public key. If it does not work then it means the device used to issue the card is not the one certified by SASSA. Figure 5.7 shows how the process of verification would work. This would allow only devices certified by SASSA to carry out the enrolment and issuing of cards process.

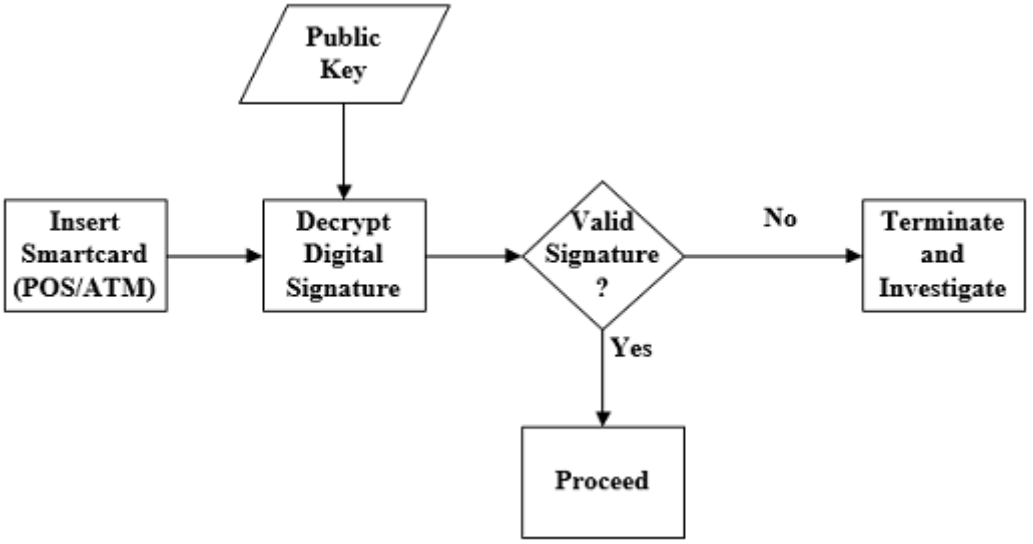

FIGURE 5.7: *Verifying Devices Digital Signature*

Proposed solutions have been presented but not to some of the attacks and the section below discusses that.

5.4 Conclusion

Attacks that involve the officials being corrupt have not been presented with the proposed solutions. It is difficult to stop people or officials from acting corruptly, there will always be that one person who wants to do things against the rules. In the case whereby fake identities are used to register for grants, it is difficult to mitigate that because the root of the problem is the NPR database. Someone already registered in the database becomes very easy to apply for a grant and chances are high for the grant to be approved.

This chapter has presented possible solutions to some of the possible attacks presented in Chapter 4 and details on how we propose to use the solutions for SASSA.

Chapter 6

Application of Blockchain to SASSA

6.1 Introduction

There are various (often conflicting) categorisations of blockchain types that have been discussed in the research community [107]. The following section gives a brief discussion of these types.

6.1.1 Different Types of Blockchains

For the purposes of this chapter, we will discuss the types of blockchains based on whether authorization is required for the nodes participating in the network and whether access to the blockchain is public or private. For the first category we have:

- **Permissionless blockchains** — where anyone is allowed to participate in the verification process; i.e. no prior authorisation is required and computational power is utilised, usually in return for a monetary reward [108].
- **Permissioned blockchains** — whereby verification nodes are preselected by central authority or consortium [108].

For the second category we have:

- **Public blockchains**- where anyone can read and submit transactions to the blockchain [107].
- **Private blockchains**- where this permission is restricted to users within an organization or group of organisations [107].

The intention for most permissioned blockchains is to restrict data access to the company or consortium of companies that operate the blockchain.

The blockchain used in the Bitcoin network falls under the permissionless blockchain. Whereby, permission refers to the authorisation for verification, and anybody can join the network to be a verifier without obtaining any prior permission to perform such network tasks [107]. These verifiers are encouraged through the issuance of new currency once they have verified a block of transactions to encourage their participation.

A permissionless blockchain is advantageous, in that, it can both accomodate anonymous or "pseudonymous" actors [108] and protect against sybil (i.e. identity-forging) attack [109]. On the other hand, the incentive mechanism has to be carefully developed in order to ensure that verifiers are incentivized to participate. The main disadvantageous aspect is that; the algorithm used to ensure security in the network, is very costly in terms of computation and further details have been discussed in Chapter 2.

Permissioned blockchains are intended to be purpose-built, and can thus be created to maintain compatibility with existing applications. They can be fully private or consortium blockchains. Because the actors in the network are named, the intention is that, they are also legally accountable for their activity [18]. In terms of the transactions these blockchains handle, it will be predominantly off-chain assets (such as digital representations of securities, fiat currency and titles of ownership), rather than on-chain assets, such as virtual currency tokens [108]. An advantage of a permissioned blockchain is scalability. In a permissionless blockchain, the data is stored on every computer in the network, and all nodes verify all transactions. It is obvious that once the number of transactions increase substantially, the users that are able to perform this type of processing and verification will decrease, leading to more centralisation [18]. In a permissioned blockchain, only a

smaller number of preselected participants will need to operate, and if these come from large institutions they will be able to scale their computing power in line with the increase in the number of transactions. However, because of the smaller number of participants, it is much easier for a group of users to collaborate and alter the rules, to revert transactions. In addition, it is easy for them to reject transactions and in this sense it is not "censorship resistant" as a permissionless blockchain would be. Examples of permissioned blockchains include Eris, Hyperledger, Ripple [110] and others.

Hence, this study proposed the use of permissioned and private blockchain for SASSA in order to restrict access to the blockchain. The section below presents and analyse possible ways that blockchain could be applied to SASSA.

6.2 Application

For digital currencies, blockchain is mainly used for storing or keeping a record of all transactions in the system. Only the hash of the transaction is stored in the blockchain. What happens is that, when transactions are published in the network, miners group them together to create a block. Each block contain a block header, which is hashed twice using the SHA-256 algorithm [111]. The output is a hash, which is later recorded to the blockchain.

The hash contains details of all the transactions included in the block. The use of hashes helps to limit the amount of data stored in the blockchain [112]. The main aim here is to analyse whether the blockchain could be applied to SASSA. Hence, this analysis is divided into sections according to how the blockchain could be applied to SASSA and that would be analysed and conclusions would be made based on the analysis. The following sections present this analysis in details.

6.2.1 Recording Data to the Blockchain

For this first application, we would like to see whether blockchain would function accordingly when used for the purposes of recording data for each beneficiary that registers for

a social grant. Different types of information or documentation are required based on the type of social grant being applied for, but the basis of them all is the Identity Number (ID). These documents are used in determining whether an applicant is eligible to receive a particular social grant.

In chapter 4, attacks have been presented and amongst those is the issue of identity theft. Whereby, attackers use information that does not belong to them for fraudulent reasons like applying for social grants they are not eligible to receive. Therefore, we would like to test if the use of blockchain could eliminate this attack or in any way prevent it from occuring. To tackle this attack, the assumption that duplicate ID numbers does not exist in South Africa has been made.

Since the blockchain stores hashes of data, the plan is to do the same thing when it is used for SASSA. During registration, information like name, surname, ID number and fingerprints are captured. It would be more effective only if fingerprints could be hashed. Tulyakov, Farooq and Govindaraju claim that hashing the whole fingerprint proves to be impractical with respect to minutia sets [113]. They mention that, even the slight difference in minutia sets of two prints of the same finger will produce significant difference in hash values [113]. This would then present a problem when used for SASSA, because when someone tries to defraud the system, it would not be picked up. Only if a way to hash fingerprints properly were found this would have been used and be recorded to the blockchain so that the next time when someone comes to register for a grant a fingerprint would be used to check any existence in the blockchain. The lack of hashing fingerprints, would not allow the system to pick up when the same person is using the system. Researchers are still trying to explore this direction. With this limitation, an alternative has to be proposed and we propose the use of ID numbers. Just like the blockchain used in Bitcoin, we propose the use of block headers and the hash of the headers would be stored in the blockchain. The header would be formed by information such as name, surname, hash of an ID number and fingerprints.

The reason behind hashing the ID number, is that it would be used as a unique identifier, so we want to make sure that the next time a user uses the same ID number it produces the same hash and that the previously stored information is still the same. This would

limit ID numbers to belong to one person only. Figure 6.1 below depicts how this would actually work for SASSA.

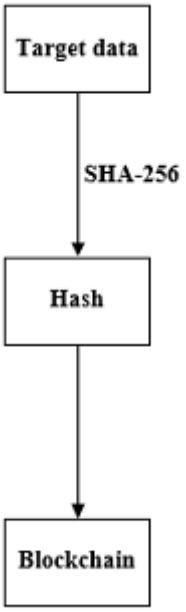

FIGURE 6.1: *Recording Data to the Blockchain*

As the blockchain records information that cannot be tampered with or changed for the entire existence, the hash of the ID number would be registered, timestamped and details of the owner would be stored. If it happens for some reason that someone losses their ID card and they get hold of a new ID number, it would be proved because the fingerprints stored in the first one would be checked for a match with the ones presented. When someone tries to use someone else's ID number the blockchain would recognise this, because the information registered against this ID number would not match especially the fingerprints. Unless if they share the same fingerprints, which is rare.

Record accuracy and trustworthiness, especially in the context of electronic records, is critical to the usefulness of the record [18]. Hence, the following section presents some challenges with using the blockchain to record data.

6.2.1.1 Challenges of recording data to the Blockchain

A record that cannot be trusted effectively cannot be used [114]. The measure of trustworthiness is primarily based on the reliability, accuracy and authenticity of the record [17]. Reliability is defined as the "trustworthiness of a record as a statement of fact based on the competency of the author, the completeness, and the controls on the recording of content and the transmission and authenticity is defined as the trustworthiness of a record as a record, meaning that the records is what it purports to be, free from tampering or corruption, based on the competence of the keeper(s) through time (i.e. creator and/or preserver) and on the reliability of the records system in which it resides" [115].

Blockchain technology does not address the reliability or accuracy of a digital record. Instead, it can address a record's authenticity by confirming the party or parties submitting a record, the time and date of the submission, and the contents of the record at the time of submission [17].

6.2.2 Using Blockchain to Bridge the Gap between Two Parties

This section looks at a way blockchain could be used to bridge the gap between SASSA and CPS. Bitcoin introduced a way that parties may interact with each other without the necessity of trusting each other. Yet, SASSA still operates with trust when it comes to CPS. As CPS is responsible for paying beneficiaries, at the end of each payment cycle, they must send a report to SASSA with the list of beneficiaries paid for that cycle. But then, SASSA does not know for sure that this report is true and has not been compromised in any way and this means that SASSA has to trust that the report is true.

Thus said, we propose the blockchain which would act as a way for SASSA to know for sure that these beneficiaries listed on the report have been paid because they (SASSA) would know and see every transaction as it occurs. The blockchain would serve as a live system for all the transactions. What would happen is that whenever a beneficiary claims their grant, a transaction record would be created and then a hash of the record would be created. It is the hash that would be added later to the blockchain and figure 6.2 depicts how this proposal would look like.

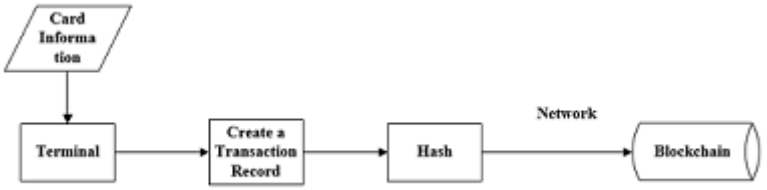

FIGURE 6.2: *Bridging a Gap between SASSA and CPS*

As it has been discussed in the beginning of this chapter that; a permissioned and private blockchain is suitable for SASSA. This means that, SASSA would have full access to the blockchain. Therefore, during the process of payment, a record is created containing name, surname, Id number, grant type and; amount etc. The record is then hashed using the SHA-256 algorithm and the hash is then sent to the blockchain to be recorded. This then affords SASSA the opportunity of knowing transactions when they actually occur in real time rather than waiting for a report. Someone operating the blockchain at SASSA can verify the transaction at that point. This can be achieved by checking information stored in the transaction (hash) and check it against the payment file that was sent to CPS at the beginning of the payment cycle as shown in figure 6.3.

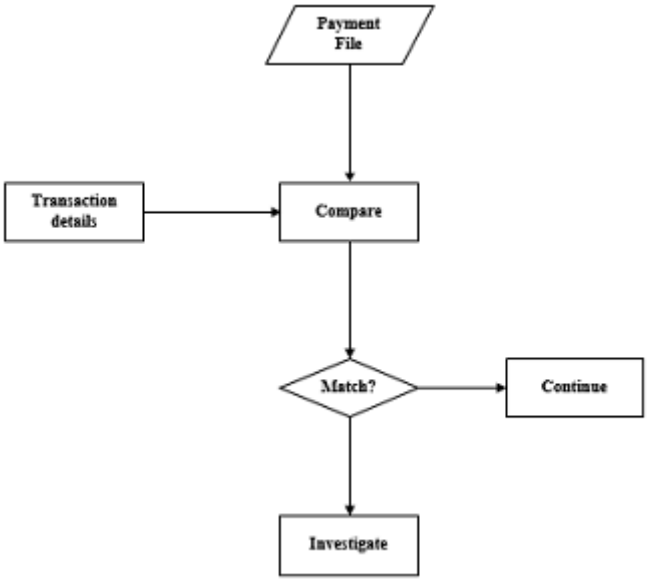

FIGURE 6.3: *Verifying a Transaction in the Blockchain*

If this information cannot be verified, then action could be taken at the same time. This would present a better way for SASSA to verify the report created by CPS at the end of the payment cycle.

As Mastercard is involved with payments, their approval might be required in order to take information during the process of payment and sending it to SASSA. The only limitation that might occur with the use of this method, is the fact that it caters only for beneficiaries using online payment methods. Therefore, SASSA still would not know with regards to offline payment methods. This might be a huge drawback, but then for online methods it would work perfectly. The main reason that blockchain would not be compatible when used for offline payment methods is that, blockchain is an online system that requires the use of the network other than that it would not work.

6.3 Drawbacks that Hinders the Application of Blockchain to SASSA

Having laid the technicalities of blockchain, now the focus can be shifted to analysing the application to SASSA. A few components are of vital importance with regards to the application of blockchain to other systems. These components have the potential of limiting the applicability of blockchain to other systems. The goal here is to address existing limits for the use case (SASSA) analysis of the section

6.3.1 Scalability

In any system, scalability is of significance [8]. According to [116], the general two definitions of scalability are as follows:

- "Scalability is the ability to handle increased workload (without adding resources to a system)."
- "Scalability is the ability to handle increased workload by repeatedly applying a cost effective strategy for extending a system's capacity."

Both these definitions show that scalability usually refers to the combination of computing hardware and software. A lot of concern has been raised about the ability of cryptocurrencies to scale [70]. There are two attributes that can affect scalability in a system and the following section provides details about them.

6.3.1.1 Throughput

This is the maximum number of transactions that a system can take per second. Currently, Bitcoin can approximately reach up to a maximum of 7 tps [117]. The number of transactions is constrained by the maximum block size which is enforced by the protocol for security purposes [118]. The block size has brought a debate in the Bitcoin community, whereby others seem to think that the use of sidechains or off chain can be utilized in order to store the many tiny transactions in the Bitcoin network [119]. Figure 6.4 shows the average block size from August 2015 up until the time of writing.

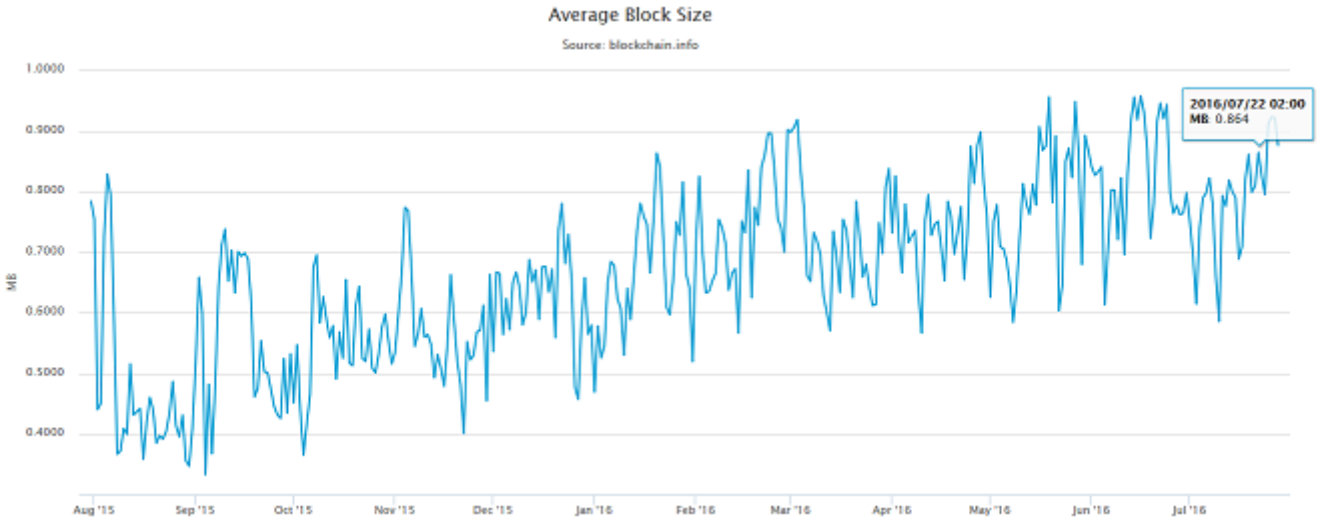

FIGURE 6.4: *Average Block Size (based upon Blockchain Info 2016)*

The average fluctuating of transactions in a block is clearly depicted in figure 6.5.

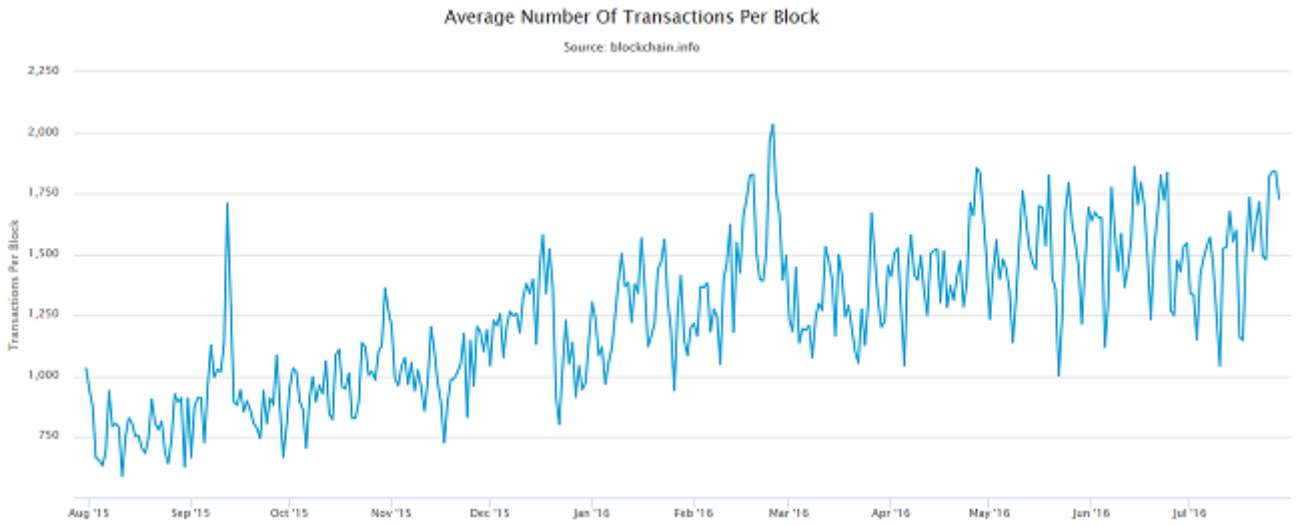

FIGURE 6.5: *Average Number of Transactions in a Block (based upon Blockchain Info 2016)*

By contrast, to Visa which processes approximately 2000 tps on average [70]. This clearly shows a huge gap between Bitcoins throughput and the one of Visa. Therefore, this gap presents questions whether the blockchain can actually be scaled up to match the throughput of systems like Visa, and as to how to attain that [70].

6.3.1.2 Latency

Latency is the time taken for a transaction to be confirmed and for Bitcoin, a transaction is considered confirmed when it is recorded in the blockchain [70]. The average time for confirmation is 10 minutes and for security purposes, it is highly recommended for the transaction until it is 6 blocks deep in the blockchain which is approximately one hour [118]. The main reason is to lower the probability of a double spending attack being successful. The Bitcoin protocol is responsible for enforcing the confirmation time to maintain the average of 10 minutes. By contrast, transactions are confirmed in seconds with systems like Visa.

Approximately 16 million beneficiaries are paid monthly, with the scalability of the blockchain, using blockchain to distribute grants would be a problem. Because transactions would not be confirmed in time, thus beneficiaries would have to wait a long time before receiving

their grants. Considering the details discussed above, it suffices to say as that as it stands now blockchain would not be able to scale up to accommodate transactions that SASSA is responsible for.

6.3.2 Privacy

Bitcoin users are not required to use their true identities when using the system, rather they use pseudonyms. Therefore, Bitcoin does not know the identity of the person using the system making transactions not to be traceable in case of fraud. With SASSA, the use of pseudonyms may not work as they are required to know their customers and they must be able to trace transactions to a specific person so that when fraud occurs it can be easy for them to track.

The blockchain is public, therefore everyone has access to the information stored in the blockchain. If the blockchain is used for recording or storing information for beneficiaries, it should not be public as this information is critical. Therefore, the best way would be to use a private blockchain so that information stored could be kept private.

6.3.3 Size and Bandwidth

As of July 2016, the size of the blockchain is above 75GB [71] and it grows approximately about 5GB per year [118]. Figure 6.6 visualises the size of the blockchain during the time of writing.

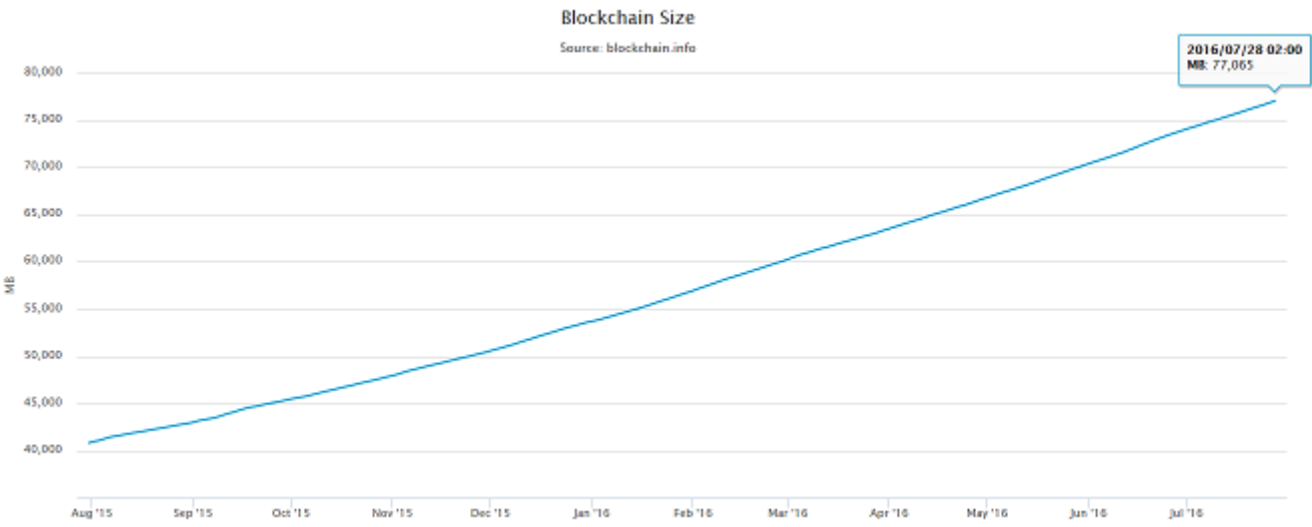

FIGURE 6.6: *The Blockchain Size (based upon Blockchain Info 2016)*

In systems whereby the transaction rate is high, the amount of data could become a challenge [118]. Nonetheless, within SASSA's context, this might not affect it that much, as the data stored would not be increasing tremendously to the point where it affects the blockchain size. Because it would store details of one organization, it can be used but requires understanding before being used so as to prevent any malfunctions or problems at the end.

6.3.4 Security

Blockchain is kept secure by the nodes participating in the network, thus their honesty in the network is vital. "Bitcoin network is considered secure to a threshold and design assumption that network majority is controlled by fair entities following the protocol" [118]. This means that the blockchain is secured if a majority of the nodes are honest. Dishonest nodes could compromise the security of the system if they control 51% or more of computational power and could successfully perform a double spending attack [120]. Computational power is the amount of power used to solve the proof of work algorithm as it is providing security to the system. The process of finding a solution to a proof of work problem requires a lot of computational power, which might pose challenges to systems that might want to use blockchain.

Blockchain is considered to be more resilient to cyber-attacks in comparison to centralized systems [118]. With regards to SASSA, they would require having participants that would utilise a lot of computational power to solve and keep the blockchain secure. Yet, SASSA could use internal participants to keep the blockchain secure.

6.4 Conclusion

An analysis of the application of blockchain to SASSA, on how it would work and how it might be a challenge has been presented in this chapter. Overall, a way on how the blockchain could be explored further for the implementation to SASSA has been presented. The following chapter presents a conclusion from the analysis presented in this study and gives suggestions of potential future work.

Chapter 7

Conclusions and Future Work

This chapter gives an overview of the research, limitations and contributions made by this research. After which, the author gives conclusions based on the analysis made. Finally, some ideas for future work are discussed.

7.1 Research Overview

The purpose of this research was to study the suitability of the application of blockchain to SASSA. At the beginning of this study, two questions were identified and the first question was:

- **RQ1:** *What are the challenges in the South African Social Security Agency (SASSA)?*

This research question is linked to the following objective:

- **ROBJ1:** *To assess the South African Social Security System and identify the existing challenges*

To accomplish the research objective stated above and answer the question associated with it, a security threat model was performed. In Chapter 4, a detailed analysis of SASSA's system has been presented. Possible attacks were clearly discussed and to aid

with understanding attacks, an attack tree was used to visualize the attacks as shown in figure 4.3.

The second research question was:

- **RQ2:** *Can the blockchain be used to solve some of the challenges SASSA is facing?*

This question was linked to the following objectives:

- **ROBJ2:** *To evaluate the impact of blockchain on the SASSA challenges*
- **ROBJ3:** *To design a solution for the challenges*

To answer research question 2, the blockchain needed to be understood and this was accomplished through the use of extensive literature review which was presented in Chapter 2. The main aim was to provide details on how the blockchain functions. Moreover, strengths and weaknesses of the blockchain were presented. Blockchain has been proposed to non-cryptocurrency systems and this has been detailed in this chapter e.g. electronic voting, smart contracts and more. Thus, the aim of this research.

Chapter 6 accomplished objective 2, whereby possible applications of blockchain to SASSA were presented. Strengths and weaknesses of each application were presented moreover, analysis was done to determine whether blockchain could work to eliminate the challenges identified.

Objective 3 was fully analysed in Chapter 5, whereby proposed solutions were discussed in detail for some of the attacks identified in Chapter 4. This chapter clearly identified each attack and the proposed solution for that particular attack. Digital signatures were proposed as one of the solutions for the attacks. Not all of the attacks have been presented with solutions. For example, no solution has been provided for the attacks involving officials being corrupt.

Table 7.1, shows a summary of the actual procedure that was adopted to find the answers to each of the research questions and objectives respectively.

TABLE 7.1: *Summary of research.*

Research Question	**Research Objective**	**Procedure Adopted**	**Section References**
RQ1	ROBJ1	Literature study was done on SASSA to understand how the system works	Chapter 4
	ROBJ1	Security threat model to find possible attacks and challenges	Chapter 4
RQ2	ROBJ2	Extensive literature review was done to understand the blockchain	Chapter 2, Chapter 6
	ROBJ3	Proposing possible solutions for the attacks identified	Chapter 5

The section below provides a detailed discussion on conclusions made from this study.

7.2 Conclusions

The main objective of this research, was to analyse whether blockchain could be applied to the South African Social Security Agency (SASSA). Moreover, the research aimed to study the system used by SASSA and detect attacks or challenges in the system.

The analysis of the blockchain was made and the blockchain was studied thoroughly, the components, how it functions and the challenges. The blockchain of interest for this research was the one used by the Bitcoin system, as it was the first one to be introduced when cryptocurrencies gained popular support and usage. Detailed analysis of the blockchain was presented in Chapter 2. With the blockchain, 3 components were of interest e.g. security, performance/scalability and the acquisition of bitcoins. These were analysed and compared with the requirements of SASSA as they play a major role in the adaptation of blockchain. Yet, these components might affect the application of blockchain but they can be modified in order to suit any purpose of blockchain.

Thus, these components might hinder the adaptation but it does not hinder the compatibility of the blockchain for SASSA.

The second objective was to study SASSA and find challenges in the system. This was successfully accomplished and details of the attacks were clearly discussed in Chapter 4. Whereby, the security threat model was used to find or identify the attacks. From these attacks and the analysis of blockchain, it is clear that blockchain might be used at SASSA i.e. for recording data or bridging a gap between SASSA and CPS as discussed in Chapter 7. Some challenges still exist even when this method is used, like the fact that it does not target the entire group of beneficiaries but only those beneficiaries using online payment methods.

Therefore, it is concluded that, blockchain cannot be applied to SASSA's system in order to solve the challenges identified in this thesis because it does not bring a solution to them. Yet, blockchain can be applied for other means at SASSA but not specifically for these challenges. Thus, leading to the incompatibility of blockchain towards solving the challenges identified in this study.

The second part of this objective was to propose a solution to these attacks. Therefore, the proposed solutions have been clearly discussed in Chapter 5. Because the solutions were not implemented, to validate them the attacks had to be performed to determine if they are still successful.

7.3 Significance and Contribution of Research

This section describes the contribution or signficance obtained from this research.

- This research presented a thorough review of Bitcoin, thus leading to the review of the blockchain adding to the body of knowledge on how the blockchain functions.
- Analysis of the system used by SASSA has been analysed and presented along with possible attacks. This would be beneficial to SASSA, as it pinpoints possible attacks in the system.
- Proposed solutions on the identified attacks have been identified. These solutions might be of interest to SASSA because they give out solutions to attacks encountered by SASSA currently. These solutions could be adopted for these attacks.

- As the aim of the study was to analyse whether blockchain might impact on the attacks identified for SASSA. Therefore, this research presented a possible application of blockchain to SASSA and precisely how the blockchain cannot be applied to solve the identified attacks. With this, simulations were not performed because of the lack of applicability of the blockchain to the attacks identified.

7.4 Limitations

As the research focuses on a real used system and organisation SASSA, some information could not be found easily. Information about the system is very critical, therefore some of the information was not exposed for everyone and some of the flaws published are removed from websites. Finding information was not necessarily easy, but at the end means were made in order to get that information.

7.5 Future Work

From the conclusion presented above and from the work presented in this dissertation, a few avenues for potential future work were identified:

- Firstly, it would be interesting to see how the proposed solutions perform after being implemented for SASSA.
- Secondly, it would be of valuable interest to put more research on the proposed smartcard for the potential it might have in other systems e.g. healthcare systems, access controls etc.
- Finally, it would also be of interest to put more research on the blockchain, by taking into consideration other blockchains used by other cryptocurrencies. Compare them and design a hybrid blockchain that would be suitable for SASSA but still maintain the security and also researching how the blockchain might be of use to other systems as it is considered to be the next generation technology [65].

References

[1] T. Vanhoutte, "Digital currency timeline," 2008.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *Available at SSRN 2580664*, 2015.

[4] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on.* IEEE, 2013, pp. 1–10.

[5] G. Wedawatta, I. Bingunath, and A. Dilanthi, "Case study as a research strategy: Investigating extreme weather resilience of construction smes in the uk," *7th Annual International Conference of International Institute for Infrastructure, Renewal and Reconstruction*, 2011.

[6] L. M. Kien-Meng, "Coining bitcoin's legal-bits: Examining the regulatory framework for bitcoin and virtual currencies," *Harv. JL & Tech.*, vol. 27, p. 587, 2013.

[7] E. D. Jeans, "Funny money or the fall of fiat: Bitcoin and forward-facing virtual currency regulation," *J. on Telecomm. & High Tech. L.*, vol. 13, p. 99, 2015.

[8] M. Mwale, "Modelling the dynamics of the bitcoin blockchain," Ph.D. dissertation, Stellenbosch: Stellenbosch University, 2016.

[9] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security.* Springer, 2013, pp. 6–24.

[10] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better—how to make bitcoin a better currency," in *Financial cryptography and data security*. Springer, 2012, pp. 399–414.

[11] F. Reid and M. Harrigan, *An analysis of anonymity in the bitcoin system*. Springer, 2013.

[12] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, "Tampering with the delivery of blocks and transactions in bitcoin," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 692–705.

[13] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *Financial Cryptography and Data Security*. Springer, 2013, pp. 34–51.

[14] P. Forte, D. Romano, and G. Schmid, "Beyond bitcoin-part i: A critical look at blockchain-based systems," 2015.

[15] C. Lustig and B. Nardi, "Algorithmic authority: the case of bitcoin," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. IEEE, 2015, pp. 743–752.

[16] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[17] J. Condos, W. H. Sorrell, and S. L. Donegan, "Blockchain technology: Opportunities and risks," 2016.

[18] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," *Available at SSRN 2692487*, 2015.

[19] T. Kokkola, "The payment system," *Payments, Securities and Derivatives, and the role of the eurosystem. Frankfurt am Main: ecB*, 2010.

[20] V. Walter, *Essential Guide to Payments*. Veritas Books, 2013.

[21] C. Menger, *On the Origins of Money.* Creative Commons Attribution, 1892.

[22] L. H. White, *Free banking in Britain: Theory, experience, and debate, 1800-1845.* Cambridge University Press, 1984.

[23] M. D. Bordo, R. D. Dittmar, and W. T. Gavin, "Gold, fiat money, and price stability," *The BE Journal of Macroeconomics*, vol. 7, no. 1, 2007.

[24] E. C. Bank, "Report on electronic money," 1998.

[25] I. Mas and D. Radcliffe, "Mobile payments go viral: M-pesa in kenya," 2010.

[26] V. A. Lawack, "Mobile money, financial inclusion and financial integrity: The south african case," *Wash. JL Tech. & Arts*, vol. 8, p. 317, 2012.

[27] B. L. Shultz and D. Bayer, "Certification of witness: Mitigating blockchain fork attacks," 2015.

[28] M. Möser, "Anonymity of bitcoin transactions: An analysis of mixing services," in *Proceedings of Münster Bitcoin Conference*, 2013.

[29] P. Franco, *Understanding Bitcoin: Cryptography, engineering and economics.* John Wiley & Sons, 2014.

[30] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[31] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proceedings on Advances in cryptology.* Springer-Verlag New York, Inc., 1990, pp. 319–327.

[32] S. Brands, "Untraceable off-line cash in wallet with observers," in *Advances in Cryptology—CRYPTO'93.* Springer, 1993, pp. 302–318.

[33] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Compact e-cash," in *Advances in Cryptology–EUROCRYPT 2005.* Springer, 2005, pp. 302–321.

[34] A. Back *et al.*, "Hashcash—a denial of service counter-measure, 2002," *Available from World Wide Web: http://www. hashcash. org/papers/hashcash. pdf*, 2007.

[35] B. Laurie and R. Clayton, "Proof-of-work" proves not to work; version 0.2," in *Workshop on Economics and Information, Security*, 2004.

[36] N. Szabo, "Bit gold," *Website/Blog*, 2008.

[37] W. Dai, "B-money," *Consulted*, vol. 1, p. 2012, 1998.

[38] H. Finney, "Rpow: Reusable proofs of work. cypherpunks," 2004.

[39] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *Security and Privacy (SP), 2013 IEEE Symposium on.* IEEE, 2013, pp. 397–411.

[40] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Security and Privacy (SP), 2014 IEEE Symposium on.* IEEE, 2014, pp. 459–474.

[41] C. A. Vyas and M. Lunagaria, "Security concerns and issues for bitcoin," *International Journal of Computer Applications (IJCA)*, pp. 10–12, 2014.

[42] T. Moore and N. Christin, "Beware the middleman: Empirical analysis of bitcoin-exchange risk," in *Financial cryptography and data security.* Springer, 2013, pp. 25–33.

[43] F. Reid and M. Harrigan, *An analysis of anonymity in the bitcoin system.* Springer, 2013.

[44] G. Karame, E. Androulaki, and S. Capkun, "Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin." *IACR Cryptology ePrint Archive*, vol. 2012, p. 248, 2012.

[45] M. Herrmann, "Implementation, evaluation and detection of a doublespend-attack on bitcoin," 2012.

[46] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Financial Cryptography and Data Security.* Springer, 2014, pp. 436–454.

[47] J. Clark and A. Essex, "Commitcoin: Carbon dating commitments with bitcoin," in *Financial Cryptography and Data Security.* Springer, 2012, pp. 390–398.

[48] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE, 2014, pp. 475–490.

[49] C. Media, "Map of coins," 2016. [Online]. Available: http://mapofcoins.com/

[50] T. Gibbs and S. Yordchim, "Thai perception on litecoin value," *World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, vol. 8, no. 8, pp. 2613–2615, 2014.

[51] E. Duffield and K. Hagan, "Darkcoin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proofofwork system," 2014.

[52] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.

[53] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," *July 7th*, 2013.

[54] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, 2014.

[55] L. Goodman, "Tezos: A self-amending crypto-ledger position paper," 2014.

[56] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies.* " O'Reilly Media, Inc.", 2014.

[57] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology-EUROCRYPT 2015*. Springer, 2015, pp. 281–310.

[58] K. Okupski, "Bitcoin developer reference," *Availabl e at http://enetium. com/resources/Bitcoin. pdf*, 2014.

[59] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 104–121.

[60] C. Percival, "Stronger key derivation via sequential memory-hard functions," *Self-published*, pp. 1–16, 2009.

[61] A. Poelstra, "On stake and consensus," 2015.

[62] L. Ren, "Proof of stake velocity: Building the social currency of the digital age," *Self-published white paper*, 2014.

[63] P4Titan, "Slimcoin: A peer-to-peer crypto-currency with proof-of-burn "mining without powerful hardware"," 2014. [Online]. Available: www.slimcoin.org

[64] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," 2015.

[65] J. Mattila, "The blockchain phenomenon the disruptive potential of distributed consensus architectures," 2016.

[66] N. Pierre, "Using the bitcoin blockchain for secure, independently verifiable electronic votes," 2014.

[67] P. Sanjay, N. Sumabala, B. Paul, and P. Veena, "Adept: An iot practitioner perspective," 2015.

[68] K. Scholer, "An introduction to bitcoin and blockchain technology," 2016.

[69] S. H. Ammous, "Blockchain technology: What is it good for?" *Browser Download This Paper*, 2016.

[70] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, and E. Gün, "On scaling decentralized blockchains," in *Proc. 3rd Workshop on Bitcoin and Blockchain Research*, 2016.

[71] B. Info, "Size of the bitcoin blockchain," *Blockchain Info.(last accessed 29 April, 2016)*, 2016.

[72] A. Back, G. Maxwell, M. Corallo, M. Friedenbach, and L. Dashjr, "Enabling blockchain innovations with pegged sidechains," 2014.

[73] J. Bruce, "The mini-blockchain scheme," 2014.

[74] C. R. Kothari, *Research methodology: Methods and techniques.* New Age International, 2004.

[75] Z. Zainal, "Case study as a research method," *Jurnal Kemanusiaan*, vol. 9, 2007.

[76] K. B. M. Noor, "Case study: A strategic research methodology," *American journal of applied sciences*, vol. 5, no. 11, pp. 1602–1604, 2008.

[77] R. K. Yin, *Case study research: Design and methods.* Sage publications, 2013.

[78] A. Maria, "Introduction to modeling and simulation," in *Proceedings of the 29th conference on Winter simulation.* IEEE Computer Society, 1997, pp. 7–13.

[79] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Symposium on requirements engineering for information security (SREIS)*, vol. 2005, 2005, pp. 1–8.

[80] B. Schneier, *Secrets and lies: digital security in a networked world.* John Wiley & Sons, 2011.

[81] I. Sommerville and G. Kotonya, *Requirements engineering: processes and techniques.* John Wiley & Sons, Inc., 1998.

[82] M. Chitiga-Mabugu, R. Mabugu, I. Fofana, B. Abidoye *et al.*, "Assessing the general equilibrium effect of social grants in south africa," 2014.

[83] M. S, *A Statistical Summary of Social Grants in South Africa.* SASSA, 2015.

[84] SASSA, *Annual Performance Plan.* SASSA, 2015.

[85] V. Barca and R. Chirchir, "Single registries and integrated miss: De-mystifying data and information management concepts," *Barton ACT: Department of Foreign Affairs and Trade*, 2014.

[86] S. Flowerday and G. Ranga, "Identification now and in the future: Social grant distribution process in south africa," in *New Approaches for Security, Privacy and Trust in Complex Environments.* Springer, 2007, pp. 457–459.

[87] SASSA, "Sassa/cps service level agreement," 2012. [Online]. Available: http://www.sec.gov/Archives/edgar/data/1041514/000106299312000404/exhibit99-2.htm

[88] M. Samson, M. O. Babson, C. Haarmann, D. Haarmann, M. G. Khathi, K. Mac Quene, and I. van Niekerk, "Social security reform and the basic income grant for south africa," *Report commissioned by the International Labour Organization (ILO) and produced by the Economic Policy Research Institute (EPRI)*, 2002.

[89] K. P. Donovan, *The biometric imaginary: standardization & objectivity in post-apartheid welfare*. University of Cape Town, 2013.

[90] H. van de Haar, D. van Greunen, and D. Pottas, "Biometrics in social grants: Separating myth from reality," in *2015 IEEE International Symposium on Technology and Society (ISTAS)*. IEEE, 2015, pp. 1–8.

[91] B. Schneier, "Modelling security threats," *Dr. Dobb's Journal*, 1999.

[92] P. Gordhan, "Budget speech," *Republic of South Africa, Pretoria: Government Printers*, 2016.

[93] F. Louise, "Factsheet: Social grants in south africa – separating myth from reality," 2016. [Online]. Available: https://africacheck.org/factsheets/separating-myth-from-reality-a-guide-to-social-grants-in-south-africa/

[94] C. . Courts, "Hawks nail social grants fraud syndicate," 2016. [Online]. Available: http://www.iol.co.za/news/crime-courts/hawks-nail-social-grants-fraud-syndicate-2027463

[95] S. Tessa, "Identity theft," 2016. [Online]. Available: http://www.bowman.co.za/eZines/Custom/Litigation/MarchNewsletter/IdentityTheft.html

[96] D. O. H. AFFAIRS, "Statement on alleged smart id card fraud," 2015. [Online]. Available: http://www.dha.gov.za/index.php/statements-speeches/686-statement-on-alleged-smart-id-card-fraud

[97] J. Zhou and K.-Y. Lam, "Securing digital signatures for non-repudiation," *Computer Communications*, vol. 22, no. 8, pp. 710–716, 1999.

[98] R. J. Sullivan, "Can smart cards reduce payments fraud and identity theft?" *Economic Review-Federal Reserve Bank of Kansas City*, vol. 93, no. 3, p. 35, 2008.

[99] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication," in *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*. ACM, 2003, pp. 45–52.

[100] P. Juthamas and T. Witit, "Aes implementation on smart card."

[101] D. Selent, "Advanced encryption standard," *Rivier Academic Journal*, vol. 6, no. 2, pp. 1–14, 2010.

[102] Y. W. Yun and C. T. Pang, "An introduction to biometric match-on-card," 2005.

[103] L. Mohammed, A. R. Ramli, V. Prakash, M. B. Daud *et al.*, "Smart card technology: past, present, and future," *International Journal of The Computer, the Internet and Management*, vol. 12, no. 1, pp. 12–22, 2004.

[104] S. Mthethwa, G. Barbour, and M. Thinyane, "An improved smartcard for the south african social security agency (sassa): A proof of life based solution," in *2016 International Conference on Information Science and Security (ICISS) December 19th-22nd, Pattaya, Thailand*. IEEE, 2016, pp. 60–63.

[105] S. Mandal, "A review on secured money transaction with fingerprint technique in atm system," *arXiv preprint arXiv:1307.8043*, 2013.

[106] L. A. Mohammed, "Use of biometrics to tackle atm fraud," in *Proc. 2010 International Conference on Business and Economics Research*, vol. 1, 2011.

[107] M. Pilkington, "Blockchain technology: Principles and applications," *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar*, 2016.

[108] T. Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems," Working paper. 6 April. Retrieved from http://www. ofnumbers. com/wp-content/uploads/2015/04/Permissioned-distributedledgers. pdf, Tech. Rep., 2015.

[109] J. R. Douceur, "The sybil attack," in *Peer-to-peer Systems*. Springer, 2002, pp. 251–260.

[110] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," in *Trust and Trustworthy Computing*. Springer, 2015, pp. 163–180.

[111] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in *Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, 2016.

[112] J. Mattila *et al.*, "The blockchain phenomenon–the disruptive potential of distributed consensus architectures," The Research Institute of the Finnish Economy, Tech. Rep., 2016.

[113] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2427–2436, 2007.

[114] R. O'Dwyer, "The revolution will (not) be decentralised: Blockchains," *Commons Transition*, 2015.

[115] M. Mainelli and M. Smith, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," *The Journal of Financial Perspectives*, vol. 3, no. 3, pp. 38–69, 2015.

[116] C. B. Weinstock and J. B. Goodenough, "On system scalability," DTIC Document, Tech. Rep., 2006.

[117] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments. 2016," *URl: https://lightning. network/lightningnetwork-paper. pdf (visited on 2016-04-19)*, 2015.

[118] M. Biella and V. Zinetti, "Blockchain technology and applications from a financial perspective," UniCredit, Tech. Rep., 2016.

[119] G. Caffyn, "What is the bitcoin block size debate and why does it matter?" 2015. [Online]. Available: http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/

[120] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," *arXiv preprint arXiv:1507.06183*, 2015.