BLOCKCHAIN TECHNOLOGY: ADDRESSING THE RISK OF DIGITAL ASSETS EXCHANGE

by

Mari Thomas

Thesis presented in partial fulfilment of the requirements for the degree of Master of Commerce (Computer Auditing) in the Faculty of Economic and Management Sciences at Stellenbosch University

Supervisor: Riana Goosen

March 2018

DECLARATION

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), the reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: March 2018

ACKNOWLEDGEMENTS

I am truly grateful to everyone who has contributed to making this research project possible. I would like to thank the following people in particular:

- To my heavenly Father, thank you God, for giving me the determination to complete this project;

- To my parents, who always believe in me. Special thanks to my mother for all her support and encouragement;

- To my family, my husband and my two boys, thank you for your support and understanding;

- To my supervisor, Riana Goosen, thank you for all your patience and guidance throughout the process.

ABSTRACT

Blockchain technology is a complicated and emerging technology affecting the way business is performed. Blockchain is a decentralised transaction and data management technology which was first introduced through the Bitcoin cryptocurrency. Ever since the introduction of Bitcoin in 2008, interest in the blockchain technology has grown significantly. This is mainly due to the fact that this technology has the ability to eliminate the role of trusted third parties with regards to security, anonymity and data integrity aspects.

The purpose of this study was to provide a matrix which can be used as a quick reference to indicate the various blockchain characteristics and how they address identified risks with the exchange of digital assets and subsequently assist in achieving the control objectives of a business. Furthermore, additional risks were identified which potential users need to take into consideration before implementing the blockchain technology.

The matrix was developed by first identifying the significant inherent risks of digital asset exchange, namely trust, repudiation, double-spending and theft, including fraud. An understanding of how the blockchain technology works was obtained through performing a detailed literature review, from which the key characteristics of the blockchain technology was identified. This was utilised to provide a matrix for potential users on how a specific blockchain characteristic has the ability to address the identified significant risks of digital asset exchange and to achieve the control objectives of a business. Additional risks were derived from the matrix and further literature work carried out to identify the additional risks which needs to be considered before the implementation of the blockchain technology.

By utilising the matrix provided, various industries will be able to evaluate whether the blockchain technology will assist them in addressing their specific risks and achieving their control objectives.

UITTREKSEL

Blockchain-tegnologie is 'n gekompliseerde en opkomende tegnologie wat die manier hoe besigheid uitgevoer word affekteer. Blockchain is 'n gedesentraliseerde transaksie- en databasis-bestuurstegnologie wat die eerste keer deur die Bitcoin-kripto-geldeenheid bekendgestel is. Sedert die bekendstelling van Bitcoin in 2008 het belangstelling in die blockchain-tegnologie aansienlik gegroei, hoofsaaklik vanweë die feit dat die tegnologie die vermoë het om die rol van vertroude derde partye uit te skakel met betrekking tot sekuriteit, anonimiteit en data-integriteit.

Die doel van hierdie studie was om 'n matriks te verskaf wat as 'n vinnige verwysing gebruik kan word om die verskillende blockchain-eienskappe aan te dui en te toon hoe dit die geïdentifiseerde risiko's met die oordrag van digitale bates aanspreek en gevolglik beheerdoelwitte van die besigheid bereik. Verder is die oorblywende risiko's geïdentifiseer wat potensiële gebruikers in ag moet neem voordat die blockchain-tegnologie geïmplementeer word.

Die matriks is ontwikkel deur eerstens die beduidende inherente risiko's van digitale bate-uitruiling te identifiseer, naamlik vertroue, repudiasie, dubbelbesteding en diefstal, insluitend bedrog. 'n Begrip van hoe die blockchain-tegnologie werk is verkry deur 'n uitgebreide literatuuroorsig te doen, waaruit die sleutelkenmerke van die blockchain-tegnologie geïdentifiseer is. Dit is aangewend om 'n matriks vir potensiële gebruikers te verskaf, wat verduidelik hoe 'n spesifieke blockchain-kenmerk die geïdentifiseerde beduidende risiko's van digitale bate-oordrag kan aanspreek en kan help om die besigheid se beheerdoelwitte te bereik. Oorblywende risiko's is afgelei van die matriks en deur die uitvoer van ʼn verdere literatuuroorsig is die oorblywende risiko’s geidentifiseer wat oorweeg moet word voor die implementering van die blockchain tegnologie.

Deur van die matriks gebruik te maak, sal dit verskeie industrieë in staat stel om te evalueer of die blockchain-tegnologie hul spesifieke risiko's sal aanspreek en hul beheerdoelwitte sal bereik.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

List of figures

List of tables

CHAPTER 1. INTRODUCTION AND RESEARCH OBJECTIVE

1.1 Introduction and background

When any transaction occurs between two transacting parties, risks are created when rights and obligations are transferred with the exchange of assets. The identified risks need to be mitigated through the implementation of internal controls. These risks involved in the exchange of physical assets are also present in the exchange of digital assets. The risks might even be higher in a digital environment. As such, the identified risks in a digital environment will be addressed not only through internal controls but also through the use of new technology innovations.

When assets are exchanged, a system is required to record the transactions. Money and payment systems are inherently interconnected. For an asset to perform the function of a medium of exchange it is important that the assets are transferred in a secure way, therefore a payment system is required. Furthermore, for any system other than the exchange of physical banknotes, the values need to be recorded; therefore a ledger is also required. Modern payment systems are computerised, resulting in money existing only as digital records on commercial banks' accounts. It is therefore necessary that digital records or digital assets be exchanged through a payment system and recorded in a ledger (Ali, Barrdear, Clews & Southgate, 2014).

There have been various attempts at introducing a monetary system that is based on public-key cryptography. For example, Chaum and Roijakkers (1990) introduced a payment system through which payments are performed anonymously and securely, but a trusted third party is still required. Chaum and Roijakkers (1990) were also the founders of DigiCashBV, which is the first company that provided a cryptographic digital currency. Another attempt at introducing a monetary system was Griggs's Triple Entry Accounting, a payment system which was primarily designed for the internal transfer of money (Chaum & Roijakkers, 1990). The abovementioned electronic systems are however all centralised, thus they are reliant on a trusted third party, who facilitates and controls the transaction.

Most payment platforms are reliant on private secure communication networks. Visa, for example utilises VisaNet, which connects to the Internet for processing, but the network is centralised because the nodes, both physical and virtual are owned by Visa (Khan, 2012). Currently all internet commerce is linked to a financial institution which performs the role of a trusted third party that processes and mediates all electronic transactions (Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman, 2016). The blockchain technology was developed to eliminate the need for a trusted third party. This was achieved by designing a system that ensures that the network participants agree on the order of the transactions processed without the mediation of a trusted third party (Crosby *et al.*, 2016).

Bitcoin, created by Satoshi Nakamoto in 2008, was the first decentralised electronic currency system (Skudnov, 2012). The key innovation of the digital currency Bitcoin is the underlying technology, blockchain. Blockchain technology utilises distributed ledgers. These distributed ledgers allow payment systems to operate in an entirely decentralised way, without the assistance of intermediaries such as banks. With the increased use of digital assets, the most significant risks need to be identified and addressed through technology developments. For example, digital currencies such as Bitcoin, that combine a new payment system and a new currency, hold various risks with the exchange of the digital assets. These risks need to be identified and addressed through internal controls and new technology innovations such as blockchain technology.

1.2 Historical review

Research on Bitcoin, the underlying technology blockchain, digital assets, cryptocurrencies and risks has been documented in various forms. The research conducted to date can be categorised in three types: (1) research performed with regard to the Bitcoin application and the analysing of the underlying technology on a technical level, (2) research performed based on the challenges and limitations of the blockchain technology and (3) research presenting applications based on the blockchain technology.

Most of the research has been performed on the Bitcoin application as this is the first and most well-known application of the blockchain technology and the application which first introduced the blockchain technology. The research conducted on the Bitcoin application is based on Nakamoto's study published in 2008. Other studies have been very technical, analysing the underlying blockchain technology on a technical level, for example Skudnov (2012), who conducted a technical study on the different Bitcoin clients. The different users of the Bitcoin application was categorised by Skudnov (2012) into different Bitcoin clients depending on the role they perform in a Bitcoin transaction. The technical concepts of the Bitcoin application were also discussed.

Extensive research has been conducted based on the technical challenges and limitations of the blockchain technology as identified by Swan (2015). Most research is performed on the security and privacy of the blockchain (Yli-Huumo, Ko, Choi, Park & Smolander, 2016). For example: research has been conducted by Vasek, Thornton and Moore (2014) on security aspects of the blockchain technology and four types of Bitcoin security incidents were investigated, while Lim, Kim, Lee, Lee, Nam-Gung and Lee (2014) analysed the trend of security breaches in the Bitcoin application, and its possible countermeasures.

Other research has focused on possible applications of the blockchain technology in various industries such as insurance, the financial sector, and smart contracts. Examples of studies include the following: Guo and Liang (2016) conducted a study on the possibilities of the blockchain technology in the banking industry; Bahga and Madisetti (2016) presented a decentralised peer-to-peer platform for Industrial Internet of Things which is based on the blockchain technology; and Abeyratne and Monfared (2016) discussed the potential benefits of the blockchain technology in the manufacturing supply chain.

Whilst valuable research has been conducted in these areas, the practical application has been limited since the discussions remain mainly theoretical or technically based in nature, or look at the possible application in a specific industry in isolation, or deal with specific aspects of the technology only. Thus, the research conducted in this study is aimed to be more practical where the blockchain characteristics were identified and discussed through the various levels of a general transaction and these characteristics were mapped to the risks identified with the exchange of digital assets – and furthermore linked to the control objectives of a business transaction.

The study was aimed at practical guidance. It provides evidence to the user on how the implementation of this technology could possibly address business risks and assist in achieving control objectives on a transaction level.

1.3 Research questions and research objective

This study sought to identify the significant risks of the exchange of digital assets and to investigate the manner in which the blockchain technology might address these risks.

It is important to note that this study addressed the following possible risks identified for the exchange of digital assets: trust, double-spending, theft (including fraudulent transactions) and repudiation. Although other related risks may be present in the environment that forms part of the topic of this article (exchange of digital assets), the abovementioned risks, and how blockchain technology addresses the risks is discussed in this thesis.

This study investigated the blockchain technology in general terms. It was not the purpose of this study to provide an in-depth technical analysis of blockchain technology nor did it aim to provide a complete list of possible applications. The research questions were therefore as follows:

- What are the most significant, inherent risks when digital assets are exchange?
- What are the underlying characteristics of the blockchain technology which could potentially address the most significant, inherent risks, identified?
- How is the blockchain technology utilised in a specific application, Bitcoin, to address these risks for a standard Bitcoin exchange transaction?
- What are the additional risks the users should be aware of before implementing the blockchain technology?

Lastly, this study did not intend to address any technical problems relating to the functioning of the blockchain technology, but merely provides a framework of how the characteristics of the blockchain technology could address these risks.

1.4 Scope limitations

The research reported in this thesis focused only on significant, inherent risks relating to the exchange of digital assets and did not intend to create an exhaustive list of all risks that may arise from the exchange of digital assets. Therefore, only the most differentiating characteristics of the underlying Blockchain technology addressing these risks were formulated.

Digital assets have a complex definition and were defined in the study, but the research was limited to digital commodities defined as assets, for example, Bitcoin.

1.5 Research motivation

As explained in section 1.2, most researchers have thus far focused on the various applications and possibilities of the blockchain technology in various industries, whilst others identified the risks within the blockchain technology which users and developers should consider for future application and development. However, considering that blockchain is a new technology, more specific research is required to allow management to understand how the blockchain technology could assist them in addressing the risks of digital asset exchange.

This research will assist management, IT professionals, auditors and other relevant role-players in understanding how the blockchain technology works and how it could potentially address the risks associated with the exchange of digital assets. The matrix developed contains the identified significant risks and how they are addressed by the specific blockchain technology characteristics. The additional risks that should be considered by users are also identified and will add value to potential users of the blockchain technology. Considering the increased use and necessity for the exchange of digital assets, this research will be both beneficial and crucial to future business trading and how to manage such types of exchange of digital assets.

1.6 Organisational structure of research

This research is presented in six chapters. Chapter two describes the design and methodology of the research. Chapter three contains a discussion of the risk identification process used to identify the most significant, inherent risks with the exchange of digital assets. Internal control and risk management are briefly discussed as measures to address such identified risks.

Chapter four contains the literature review and includes the definition and explanation of theoretical and technical concepts. Chapter four also includes a discussion of the underlying characteristics of the blockchain technology, which is categorised in the various levels of a typical digital asset exchange transaction. The Bitcoin application is utilised to explain the blockchain characteristics in more detail. These identified characteristics, in the various levels of a digital asset transaction form the basis for the findings presented in Chapter five. Chapter five contains a risk-based characteristics matrix, linking the inherent risks identified in Chapter three to the blockchain characteristics identified in Chapter four. The matrix could be used as a quick reference guide as it indicates which specific blockchain characteristics address the identified risks. Chapter five also includes a discussion of the additional risks which potential users need to consider before implementing the blockchain technology as a control mechanism to address the risks of the exchange of digital assets. Chapter six provides an overview of the study by summarising the key findings. It concludes with the identification of potential areas of future research in the field of blockchain technology.

CHAPTER 2. RESEARCH DESIGN AND METHODOLOGY

2.1 Purpose of the study

The aim of this study was to identify the most significant, inherent risks for the exchange of digital assets and to obtain a comprehensive understanding of the blockchain technology and underlying characteristics which could potentially address these risks. A non-empirical, qualitative study was conducted together with an extensive literature review.

2.2 Literature study

The literature review included papers published in accredited research journals, articles in information technology publications and websites on a local and international front. The following areas were researched:

- Digital asset exchange and the inherent risks related to the transfer of ownership of assets;
- Gaining an understanding of the blockchain technology;
- Gaining an understanding of the Bitcoin application;
- Advantages of blockchain; and
- Risks of blockchain applications.

The methodology that was employed to address the research objectives is explained below.

2.3 Research methodology

With the aim of identifying the blockchain characteristics which could potentially address the most significant inherent risks with the exchange of digital assets, the following steps were followed:

Step 1: The most significant inherent risks with regards to the exchange of digital assets were identified and derived from the basic business assumptions of a transaction (control objectives).

Step 1.1: The basic business assumptions of a transaction were found to be in-line with the control objectives of a transaction, as defined by ISA 315, namely: completeness, accuracy, validity, integrity and privacy (International Standard on Auditing 315 (Revised), 2014).

Step 1.2: Through extensive literature research performed on the risks of the transfer of digital assets the most significant risks were identified. Although the risk in a traditional environment is different from the risks in a digital environment, the control objectives are the same.

Step 1.3: In the majority of research performed the following were the main risks identified that needs to be addressed with the transfer of digital assets. Trust (to achieve validity), double-spending (to achieve validity and integrity), theft (to achieve validity, integrity and privacy) and repudiation (to achieve validity). These risks are regarded as the most significant risks with the exchange of digital assets because if these risks are not addressed the control objectives will not be achieved. These key risks identified formed the basis of the research conducted. How the blockchain technology potentially address these risks, formed the subject of this study.

Step 2: The characteristics of the blockchain technology were identified through gaining a comprehensive understanding of the technology.

Step 2.1: These characteristics were best summarised through discussing the identified characteristics at the various levels of a general exchange of digital assets transaction and through using the Bitcoin application as an example.

Step 3: Mapping of blockchain technology characteristics to identified risks.

Step 3.1: Obtaining an understanding of how traditional controls are currently attempting to address identified risks with the exchange of digital assets.

Step 3.2: A mapping between the identified blockchain characteristics and the most significant, inherent risks of the exchange of digital assets and the control objectives of a transaction was performed.

Step 4: The additional risks, identified through mapping performed in step 3 and other risks identified during research performed in step 1.2, were grouped together to provide a list of additional risks users need to consider before implementing the blockchain technology.

2.4 Conclusion

The literature review provided a good theoretical foundation for an understanding of the risks in the exchange of digital assets; the Bitcoin application; and the underlying blockchain technology.

The methodology ensured that the most significant, inherent risks for the exchange of digital assets were identified and the characteristics of the blockchain technology were sufficiently explained through using the Bitcoin application as an example.

The research ultimately provides a quick reference matrix linking the most significant, inherent risks of the exchange of digital assets to the blockchain characteristics, addressing this risk, and the control objectives of a business transaction achieved.

CHAPTER 3. THE INHERENT RISKS OF DIGITAL ASSET EXCHANGE

3.1 Introduction

When any digital asset exchange transaction occurs between two or more transaction parties, there are various risks involved. These risks need to be identified through a risk assessment process and managed through the implementation of control procedures which could reduce the risks to an acceptable level. The inherent and most significant risks as well as other important aspects, when digital assets are exchanged, are discussed below.

When digital assets are exchanged between two transacting parties, various risks are created relating to rights and obligations of the underlying asset. Before these risks are discussed, the terms used in this chapter are first defined.

i) *Risk*

A risk is defined as any procedure, activity or occurrence which could have a negative effect on the entity in achieving its objectives (CICA, 1998). The King IV Report on Corporate Governance (IODSA, 2016) added to this definition by including that, the uncertain event can have both a positive and a negative effect on the entity's ability to achieve its objectives. Risk is furthermore seen as a function of the probability of a specific threat exploiting a potential vulnerability of the entity and the resulting effect of that undesirable event on the entity (Stoneburner, Goguen & Feringa, 2002).

Each entity needs to identity the specific risks it is exposed to through a risk assessment process. These risks will be dependent on a number of factors, including the industry in which the entity operates, the transacting parties and security risks, to name but a few. New, additional risks are introduced as a company changes its business processes, for example by moving from the physical exchange of assets to the digital exchange of assets (Butler, 2004).

Since risks differ in the various industries, the different types of business transactions, processes and systems utilised, this study was limited to one specific type of transaction, namely the exchange of digital assets between two transacting parties. Before the risks of the exchange of digital assets are discussed, it is necessary to define what physical and digital assets are.

ii) *Physical and digital assets*

Assets are broadly defined by the Conceptual Framework for financial reporting (2010) as a resource that is controlled by the entity, and which can be exchanged for other assets or utilised by the entity to generate income, ultimately resulting in the increase in economic benefits. Digital assets include stocks, bonds, gift cards and other forms of credit. However, digital assets have a more complex definition as noted by Windsor (2016), who concluded that there are generally three definitions of digital assets, summarised below:

- Media files such as photos and videos, which can be linked to metadata;
- A digital representation of an individual or entity and related metadata; and
- Digital commodities, represented as assets, for which the value is expressed by using metadata.

Metadata is data or information which provides information and details about the underlying data. It is of high importance and a necessary feature when digital assets are defined (Windsor, 2016).

The scope of this research was limited to the last element of the digital asset definition as described above, namely digital commodities as assets. One such commodity, namely Bitcoin, was the focus of this study. Bitcoin is a cryptocurrency, which is an example of a blockchain application, as discussed in Chapter four.

During a general exchange of digital asset transaction, the digital asset is transferred from the selling party to the buying party. For example: Party A will transfer three Bitcoins to party B. Risks will be present during the transfer of the digital asset, namely Bitcoins. Internal control measures and risk management as discussed below in section 3.2 and 3.3 are implemented to address the identified risks, as discussed in section 3.6.

3.2 Internal control

The risks present during the exchange of digital assets need to be sufficiently addressed through the implementation of internal control systems.

Internal control is defined by the COSO report (Internal Control – Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission, 1992) as the process which is implemented with the purpose of providing reasonable assurance that the entity will be able to achieve its objectives. The internal control process is implemented by an entity's board of directors, senior management and other staff members (Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission, 1992). Therefore, the risks identified during the exchange of digital assets need to be addressed through internal controls to ensure that the entity's objectives are achieved.

There are various forms of internal control measures which can be implemented to address identified risks. It is important to note that the most efficient internal control methods should be implemented to address a specific identified risk. The various forms of internal control methods to address identified risks are beyond the scope of this study. This study focused specifically on how the technology advances through the Blockchain application could possibly address such identified risks as a form of internal control.

3.3 Risk management

The processes by which risks are identified and addressed through internal controls are known as risk management. Risk management is defined by the King IV report (IODSA, 2016) under principle 4.1 as the process by which the governing body should manage risks and opportunities in such a manner that supports the entity in defining its main function, determining and achieving its strategic objectives.

Risk management has also been defined as the process by which management control the operational and economic costs of internal control procedures to ensure that the information technology systems and data are protected and support the entity's objectives (Stoneburner *et al.*, 2002).

Although the risk management process is the basis of the implementation of internal control measures to address identified risks, it was beyond the scope of the study. However, the characteristics of the blockchain technology could potentially be used as an internal control measure to address identified risks and to be utilised in the risk management process.

3.4 Criteria of business transactions

Romney and Steinbart (2003) concluded that any business transaction has three control objectives, namely validity, integrity and privacy. These terms can be explained as follows:

- Validity: A transacting party should be able to confirm the identity of the other transacting parties to ensure that the transaction is valid and enforceable.
- Integrity: Transacting parties need to ensure that the information contained in the transaction is accurate and has not been changed during the transmission process.

- Privacy: The privacy and confidentiality of business transactions and other information contained in the transaction message during the exchange needs to be maintained.

Traditionally, completeness and accuracy are also regarded as important control objectives in a manual business process. However, in a digital environment internal control measures have changed, to rather include the utilisation of other technology to address these identified risks and control objectives.

3.5 Risks within an electronic (digital) environment

The traditional risks within a manual system that prevent the achievement of business objectives are still applicable in a digital environment. The criteria of any business transaction, as discussed in section 3.4, are the same for the exchange of physical and digital assets. The internal control methods to achieve an entity's business objectives are, however, different in an electronic environment.

As stated previously, 'new' risks arise with a change in business models, thus when moving from the exchange of physical assets to the exchange of digital assets these 'new' risks need to be addressed in a different manner. When the environment in which the entity operates and the technology utilised for the business processes changes, the internal controls also need to be adjusted to ensure that the risks are adequately addressed.

In e-commerce transactions, for example, the exchange of digital assets is recorded through public networks, such as the Internet or peer-to-peer networks. Already, in 1999, Weber identified three problems with e-commerce transactions which are still a risk today, namely that transacting parties need to:

a. be able to determine each other's identity;
b. be able to protect the privacy of their transacting details; and
c. ensure that a secure exchange of money for goods and services can occur

These three problems are also related to the three fundamental criteria of any business transaction, namely validity (refer to a.), integrity (refer to b.) and privacy (refer to c.), as noted above (Romney & Steinbart, 2003). These fundamental criteria were utilised as the basis for the identification of the inherent risks, with the exchange of digital assets (see section 3.6 below).

3.6 Inherent risks with the exchange of digital assets

In any business transaction there are various risks involved and these risks differ among various business processes. Through the risk assessment process all the risks within a specific business process will be identified and addressed through risk management processes and the implementation of internal controls as required by King IV (IODSA, 2016).

In this study, the inherent risks with the exchange of digital assets were identified by using the fundamental criteria of any business transaction, namely validity, integrity and privacy as a basis (Romney & Steinbart, 2003). The process is discussed below.

Firstly, to achieve validity in a business transaction, non-repudiation needs to be ensured between transacting parties. Non-repudiation also forms part of the five categories of the Information Security Goals as defined by the International Organisation for Standardisation (ISO, 2013) and Tak, Lee and Park (2003). Therefore, the risk of repudiation is considered to be an inherent risk when digital assets are exchanged.

Secondly, in traditional payment systems, when assets have been exchanged for a monetary value, a trusted third party is required to ensure that the transaction is valid. Therefore, trust is an important element to ensure the validity of a transaction. Ratnasingham (1998) also concluded that trust or the lack thereof is one of the most significant risks between transacting parties when digital assets are exchanged.

Thirdly, to ensure the validity and integrity of a transaction, it is important that double-spending does not occur between transacting parties. Double-spending is regarded as a significant risk when digital assets are exchanged (Fan, Huang & Yu, 2013).

Lastly, in ensuring validity, integrity and privacy of a transaction, theft (including fraud) is always considered a risk when assets are exchanged. This aspect needs to be addressed at all times (Loster, 2005).

Although there are various risks involved in any business transaction, the four risks identified above, namely repudiation, lack of trust, double-spending and theft, including fraud, is considered the most significant, inherent risks, when digital assets are exchanged. These risks were addressed in this study. The identified risks are discussed in more detail below.

3.6.1 Repudiation

One of the most significant risks when digital assets are exchanged between transacting parties is the risk of repudiation of the transaction by the initiator (sender/transferor) of the digital asset. Repudiation can be explained as the denial, refusal or renouncement of the sending transacting party of his/her commitment to exchange the digital asset or assets to the receiving party. Repudiation may result from unauthorised transactions or discrepancies and will be discussed below (Butler, 2004):

- Unauthorised transactions created, which are unknown to the initiating transacting party, while his/her details were used; and/or
- Discrepancies between the original transaction messages. This might result from unintentional mistakes, or intentional unauthorised changes which are made to the initial transaction after the initial transaction was accepted by the two transacting parties.

In summary, it can therefore be said that to ensure that transactions are not repudiated, the following important aspects need to be confirmed:

- The validity of the transaction, including the source it came from;
- The integrity of the transaction, to ensure that unauthorised changes were not subsequently made to authorised transactions.

To ensure the validity of a transaction, its authenticity also needs to be confirmed. Authenticity is the reliance upon establishing and preserving the identity and the integrity of a record from the time it was created and subsequently until it is deleted (Rogers, 2015). Digital records are generally maintained for a period of time in the system from which they were generated. The period of maintaining the record differs depending on the purpose of the record. For example, entities might have sufficient record management programs that include retention schedules or alternatively it might only be linked to the decommissioning of the system that generated the record. It is important that the system that originates the records also determines an identity for the records (Rogers, 2015). Determining an identity for the records is the process whereby the records are registered in a schedule and assigned an unique identifier (Rogers, 2015). These procedures, which are also specified in standard information technology security controls (ISO, 2013), entail that maintaining the recording system will help to ensure the integrity of the data within the system.

To conclude: non-repudiation within a digital environment requires that neither the sender nor the receiver of the message is able to disagree on the sending or receiving of the message. Thus, the receiver can prove that the message was sent by the assumed sender and the message was received by the assumed receiver (Stallings, 1995).

3.6.2 Lack of trust

Trust is generally defined as confidence in the character, ability, strength, or trust of someone or something. Trust is furthermore a condition of a relationship to which something is committed or entrusted to be cared for, in the interest of another party. Trust has also been defined by Ghosh (2001) as the confidence in the transacting party that the transacting party is reliable, has integrity and has qualities such as consistency, competence, honesty, fairness and responsibility. What it means with respect to trusting records and the conditions required to achieve trust, is still an open research question.

The discussion about trusted records or systems is linked to two concepts: reliability and authenticity (Mak, 2012). Reliability, with regard to records, is defined as the trustworthiness of a record based on the capabilities of the transacting party creating the record, the completeness of the record and the controls present when the record was initially created (Duranti & Rogers, 2012). Reliability of records is mandated by standards for record management. For example, ISO (2013) defines a reliable record as a record of which the contents can be trusted as an accurate and complete representation of the transaction or activities.

Determining trust is based on a risk assessment process where the following four items are evaluated (Duranti & Rogers, 2012):

- Reputation, which includes the evaluation of the transacting parties' past actions and conduct;
- Performance, which is the relationship between the current activities and activities required to complete the transaction;
- Competence, which is the knowledge, skills and talents required to perform the activities required; and
- Confidence, which is an expectation of the standard of the activities to be expected by the transacting party.

Trust and trust development are aspects discussed by Reyesa, Zhangb, Royc, Andersend, Whitmoree and Andersend (2013), who note that trust is generally seen as a two-party relationship in which one party accepts the inherent risk of a relationship with another party. Rousseau, Sitkin, Burt and Camerer (1998) mention three mechanisms associated with trust development, namely institutional trust, calculative trust and relational trust. Institutional trust refers to the existence of an institutional framework that regulates the relationship between the main parties, for example in terms of contracts, guarantees, laws and regulations. Calculative trust refers to the estimation of the risks and the benefits of the interaction with another party. Lastly, relational trust is the recognition of the trustworthiness of other parties in a repeated relationship. Compared to calculative trust, relational trust is influenced more by environmental changes. These three trust mechanisms are interrelated. For example, institutional mechanisms of trust reduce the risk associated with a particular transaction or relationship. Calculative trust is important in the beginning of a relationship, while relational trust is more important after repeated positive interactions between transacting parties (Rousseau *et al.*, 1998).

Trust is furthermore increased through traceability. When transacting parties know the elements of a transaction may be traced, trust is increased because potential problems, discrepancies and other disputes could possibly be resolved through working backwards in the transacting process and identifying where the problem occurred or who is responsible (Steinauer, Wakid & Rasberry, 1997).

Currently, transactions on the Internet are reliant on financial institutions to process electronic payments. These intermediaries fulfil the role of a trusted third party. Even though the system works well for most transactions, it still has the inherent risks of a trust-based model (Nakamoto, 2008). For example, non-reversible transactions are not really possible in a trust-based model because financial institutions cannot deny mediating disputes. When transactions are disputed by transacting parties, financial institutions will mediate the dispute process, which might result in reversal of the transaction. The cost of the mediation process increases transaction costs. With increased transaction costs, small transactions are not feasible as the costs of processing these transactions might be higher than the transacting amount (Nakamoto, 2008). Furthermore, with the possibility of the reversal of transactions, the need for trust increases.

It is therefore concluded that there is a need for a trusted third party or other mechanisms to fulfil the role of a trusted third party to address this risk.

3.6.3 Theft, including fraud

With internet transactions, a certain percentage of fraud is accepted as unavoidable. Currently the fraud risk is mainly controlled through trusted third parties, but with any human involvement there will always be an element of fraud risk (Nakamoto, 2008).

For digital currencies, such as Bitcoin, fraud is firstly a concern in the form of double-spending, as discussed in section 3.6.4 below. Furthermore, resulting from the nature of digital assets, theft is also regarded a significant risk. For example, these digital assets, such as Bitcoins, are stored on the internet, in digital wallets. When coins are transferred, a password, known as a private key, is required. These private keys are stored by the transacting parties on their personal computers, thus resulting in these digital assets being exposed to an increased risk of theft through the possible hacking of users' personal computer systems (Hanley, 2013).

This poses an increased risk for cryptocurrencies, resulting mainly from the fact that transactions are restricted to the Internet and consequently vulnerable to hacking (Mittal, 2017). Therefore, fraud, including theft, will always be a concern for cyber security which needs to be addressed through the implementation of internal controls.

3.6.4 Double-spending

Digital currencies, such as Bitcoin, are susceptible to double-spending. The fact that digital units have immaterial replication costs, results in the same units having the potential to be fraudulently claimed or spent multiple times (Koch & Pieters, 2017). In the literature on digital currency, this is known as the double-spending problem. The double-spending problem occurs when a digital representation of currency is used to create multiple copies resulting in the same digital currency being spent two or more times (Wayner, 1997).

Double-spending is closely related to fraud, as the transacting party attempts to transfer his/her digital assets more than once (Koch & Pieters, 2017). Currently, the problem of double-spending is addressed through a trusted third party who authorises a transaction, but the risk of double-spending could also be addressed through the implementation of blockchain technology.

3.7 Conclusion

In this chapter the risks relating to the exchange of digital assets were discussed. Although there are various risks when digital assets are exchanged, only the most significant, inherent risks were identified, based on the characteristics of a general business transaction.

The identified risks, namely repudiation, lack of trust, theft, including fraud and double-spending, formed the basis of this study. Even though there are more risks when digital assets are exchanged, depending on the business environment, industry and so forth, only the most significant risks were identified and addressed in this study. These identified risks were not intended to create an exhaustive list of risks, but were limited to generic inherent risks.

These significant risks identified in the exchange of digital assets need to be addressed through the implementation of internal controls and by technology innovations, such as blockchain.

In Chapter 4, the technology innovation, Blockchain, is discussed and the characteristics of this technology are explained, since this technology can be used as a form of internal control to address the abovementioned risks.

CHAPTER 4. LITERATURE REVIEW: DEFINITIONS AND EXPLANATIONS OF THE BLOCKCHAIN TECHNOLOGY INCLUDING THE BITCOIN APPLICATION

4.1 Introduction

Any electronic system that records data needs to have a specific format and location in which the data in the system is stored. Furthermore, records maintained in an electronic register list every transaction which has been recorded by the system. The blockchain is a digital register filled with transactions which is constantly growing (Condos, Sorrell & Donegan, 2016).

Blockchain is a distributed ledger, which can be seen as a database of transactions, recorded in a distributed manner, by a decentralised network of computers (Wright & De Filippi, 2015). As indicated by the name blockchain, it can be split two-fold, namely block and chain. The blocks are formed by grouping together transactions into smaller encrypted data sets. Each block includes a reference to the previous block and an answer to a complicated mathematical puzzle, which results in the validation of the transactions (Pazaitis, De Filippi & Kostakis, 2017). The chain is formed by organising the blocks into a linear sequence which represents a chain. The blockchain technology was developed from a combination of existing technologies, namely peer-to-peer networks, cryptographic algorithms, distributed data storage and decentralised consensus mechanisms (Wright & De Fillippi, 2015).

The blockchain technology is seen by Tapscott and Tapscott (2016) as a general-purpose technology which can be utilised by multiple systems that contain valuable information, including money, title deeds, intellectual property rights or even votes or identity register data. The system is also able to accumulate and save static documents, records and transactions (Lorenz, Munstermann, Higginson, Olesen, Bohlken & Ricciardi, 2016). Information recorded in the blockchain can never be deleted or altered, therefore the blockchain contains a verifiable record of every single transaction recorded within a specific blockchain (Crosby *et al*., 2016).

The Bitcoin application, which was developed by Satoshi Nakamoto in 2008, was the first application to introduce the underlying technology, blockchain. The Bitcoin application will be used as an example to explain and further expand the understanding of blockchain's characteristics, when discussed in chapter 4.

Bitcoin is a permissionless payment system. Thus any participant in the network can read on or write to the chain. The Bitcoin blockchain is maintained by a peer-to-peer network. A peer-to-peer (P2P) network is a network consisting of nodes that are directly connected with each other. Since the nodes within the network have equivalent status (Poelstra, 2014), any node is able to participate in any stage of the transaction process, for example by generating or validating transactions.

Bitcoin technology introduced two new solutions, namely the blockchain and the consensus protocol proof-of-work. Proof-of-work is the process of validating transactions before they are recorded in the blockchain. This process is known as mining (Pazaitis *et al*., 2017).

The cryptocurrency Bitcoin is used for transacting in the Bitcoin application, and the proof-of-work consensus system is used for validating transactions. Anonymity is one of the key characteristics of the Bitcoin application, and transaction fees are discretionary (Janusz, Sikorski & Markus, 2016).

Furthermore, Bitcoin is known as a peer-to-peer digital payment system which is set up for transactions between multiple parties without the inclusion of a trusted third party (Levin, 2017). Digital signatures and cryptography are technologies which are included in the Bitcoin application which enables this.

Blockchain will be explained through discussing and defining the different elements of a blockchain. Firstly, the various types of blockchain systems will be discussed in section 4.2. Secondly, relevant blockchain terminology will be defined in section 4.3. Blockchain technology will be explained through discussing the key fundamental characteristics of the technology in section 4.4 and lastly further advantages of the blockchain technology will be discussed in section 4.5.

4.2 Classification of blockchain systems

The blockchain technology is classified into three types, namely public blockchains, private blockchains and consortium blockchains (Buterin, 2015). The main characteristics of the classified blockchain systems are discussed below:

4.2.1 Public blockchain

Public blockchains have decentralised ledgers which are permissionless (O'Dair, Beaven, Neilson, Osbon & Pacifico, 2016). Public decentralised ledgers are available to all internet users and are characterised by the fact that the public is able to participate unconditionally in the process of adding blocks to the chain (mining) and the current state of the blockchain (Buterin, 2015). The Bitcoin application is based on the traditional blockchain, and is an example of a public blockchain which utilises decentralised ledgers.

4.2.2 Private blockchain

Private blockchains are controlled by a single entity which results in a centralised network. Private blockchains have permissioned ledgers, which monitor write-permissions through centralised decision making, while read-permissions are either public or restricted by predetermined protocols (Buterin, 2015). The consensus process is controlled by specific pre-determined nodes. Furthermore, transactions are visible to the nodes in the blockchain, but not to the public.

4.2.3 Consortium blockchain

In a consortium blockchain the consensus process is determined by a selection of nodes. The ledger is seen to be somewhere between a public and a private ledger and is therefore considered to be partly decentralised (Pilkington, 2015).

In summary: the type of blockchain system is determined by the specific blockchain application. The Bitcoin applications discussed in this chapter utilises public blockchains. The other types of blockchain systems are outside the scope of this study.

4.3 Blockchain technology and Bitcoin application definitions (terminology)

The following definitions are applicable to both the blockchain technology and the Bitcoin application.

4.3.1 Blockchain participants (Nodes)

Blockchain participants are known as nodes. A node is any device which is part of the blockchain network, and has a unique network address. Nodes in a blockchain network have the following characteristics: they are not identifiable and they can leave and rejoin the network at any stage during the process. Nodes have the ability to express their acceptance of valid blocks by working on extending the chain and can ultimately establish a single, but distributed, agreed history of each transaction (Nakamoto, 2008). The nodes in the Bitcoin application who complete the consensus mechanism process are known as miners (refer to 4.3.4 below).

4.3.2 Decentralised network

A decentralised network exists when various users connect to a blockchain network through a node which has an installed blockchain client. The nodes distribute data to the network after validating the data (Zheng, Xie, Dai & Wang, 2016*).*

4.3.3 Blockchain fork

A so-called fork is formed when a blockchain is split into two or more chains. A fork originates when two or more nodes publish a valid block at more or less the same time (refer to section 4.4.6 ii) (Swanson, 2015).

4.3.4 Consensus mechanisms

Consensus mechanisms are the processes whereby the transactions contained in a block are verified, after which the blocks are published. The consensus process is determined by the specific blockchain applications protocol. For the Bitcoin application, the nodes (miners) compete to solve a mathematical puzzle which requires computing power. When the puzzle is solved, the new block of transactions is added to the chain and accepted by the network. The miner is rewarded with newly generated coins (Vukolić, 2016). The proof-of-work consensus mechanism will be discussed in more detail in section 4.4.3.

4.3.5 Nonce

A nonce is an arbitrary number which is used only once in cryptographic communication. The nonce is part of the block header which is used by miners to solve the mathematical problem. Refer to section 4.4.3 where the function of the nonce during the consensus process will be discussed.

4.3.6 Hash

Hash functions are any functions which could be utilised to map data of random size to data of fixed size. For example, transaction data which is of random size are inputted into the hash function to produce a hash value. The hash value or output consists of a fixed size of numbers and symbols determined by the hash function (Lewis, 2015).

4.3.7 Merkle tree

A Merkle tree root hash is a representation of the hash value of all the transactions in the block. The merkle tree root is calculated by using hash functions to calculate the hash values of all the leaves and eventually obtaining only one value for the root branch. Instead of storing entire transactions in the block header, only the Merkle root is included. The Merkle root is the root hash of the Merkle tree, which is calculated from all the transactions to be included in the block (Shudnov, 2012).

4.3.8 Cryptographic algorithm

Cryptography is used by the blockchain technology in two-fold, namely the verification process and the payment process. The specific cryptographic processes used by the blockchain technology are dependent on the protocol of the application of the blockchain technology. Two cryptographic processes are mainly used by the blockchain technology. They are known as digital signatures and cryptographic hash functions (Badev & Chen, 2014). These cryptographic processes are discussed in section 4.4.1.

4.3.9 Bitcoin application

Bitcoin is described by Badev and Chen (2014) as a type of payment system because it also enables the transfer of value between parties. Traditional payment systems are based on the transfer of value which is denominated in a currency, for example Euro. Bitcoin, however, has its own metric of value, known as Bitcoin. Within a Bitcoin payment system, entities transact directly with each other without any mediation by a trusted third party, for example banks (Badev & Chen, 2014).

4.3.10 Bitcoin

Bitcoin is a cryptocurrency which is defined by general dictionary definitions as a digital currency which operates independently of a central bank or authority. The generation of the units of currency and the verification of the transfer of funds is regulated through encryption techniques.

Furthermore, Bitcoins are a fiduciary currency. Fiduciary currencies have no intrinsic value; their value is derived from either government fiat or from the belief that they may be accepted by other transacting parties.

4.3.11 Peer-to-peer network

A peer-to-peer network consists of Bitcoin miners which are informally connected without any central co-ordination. The Bitcoin protocol determines that all messages transmitted across the network needs to be shared with the network participants' immediate peers. This result in transactions not being broadcasted to the entire network at the same time, but alternatively is shared haphazardly with random peers first, which is then shared to their peers, and so forth.

4.4 Fundamental characteristics of the blockchain technology

The blockchain technology will be explained through a discussion of the various levels in a blockchain transaction and the analysis of the characteristics of the blockchain technology in that specific level.

The aim of this study was not to provide an in-depth analysis of the underlying technology but to explain the underlying buildings blocks that provide the foundation of the blockchain technology. As illustrated in Figure 4.1 below, a blockchain transaction is grouped into the following levels:

Level 1: Transaction initiation, which includes the following sublevels:

- i) Transaction encryption
- ii) Verification of transactions

Level 2: Transaction creation, to form online blocks, which include the following sublevels:

- i) Blockchain blocks content
- ii) Timestamping

Level 3: The block generation process, which includes one sublevel:

- i) Consensus mechanisms

Level 4: The broadcasting of the block to the entire network

Level 5: Network participants approving and validating transactions

Level 6: The block is added to the blockchain and the digital asset is transferred. The following sublevels are involved:

- i) Consensus mechanisms
- ii) Blockchain maintenance
- iii) Blockchain forking

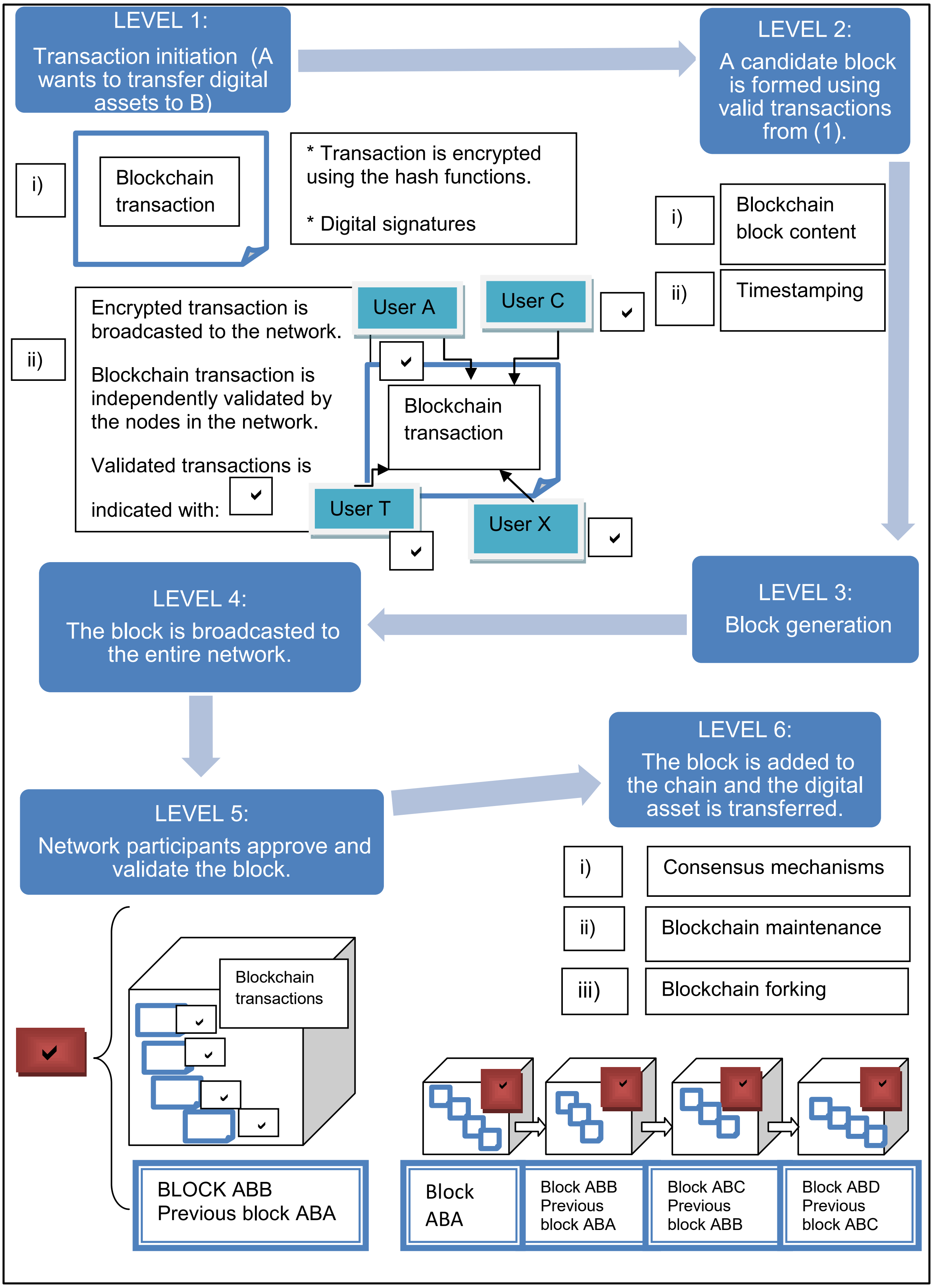

LEVEL 1:
Transaction initiation (A wants to transfer digital assets to B)
i)
Blockchain transaction
* Transaction is encrypted using the hash functions.
* Digital signatures
ii)
Encrypted transaction is broadcasted to the network.
Blockchain transaction is independently validated by the nodes in the network.
Validated transactions is indicated with: ✓
User A
User C
✓
Blockchain transaction
User T
User X
✓
✓
✓
LEVEL 2:
A candidate block is formed using valid transactions from (1).
i)
Blockchain block content
ii)
Timestamping
LEVEL 3:
Block generation
LEVEL 4:
The block is broadcasted to the entire network.
LEVEL 5:
Network participants approve and validate the block.
✓
Blockchain transactions
✓
✓
✓
✓
BLOCK ABB
Previous block ABA
LEVEL 6:
The block is added to the chain and the digital asset is transferred.
i)
Consensus mechanisms
ii)
Blockchain maintenance
iii)
Blockchain forking
✓
✓
✓
✓
Block ABA
Block ABB Previous block ABA
Block ABC Previous block ABB
Block ABD Previous block ABC

Figure 4.1 The blockchain process

Source: (Adapted from Kakavand, De Sevres & Chilton, 2017)

4.4.1 Transaction initiation (Level 1)

Level 1, the initiation of a transaction, can be further analysed through the following two sublevels: the encryption of the transaction message through hashing and digital signatures, after which the encrypted transaction is broadcasted to the network; and the verification of the transaction, which is performed by the nodes in the network. Blockchains are based on two core cryptographic measures, namely cryptographic hash functions and digital signatures (Harz, 2017). Cryptographic hash functions are utilised to implement discipline when transaction records are recorded in the public ledger and digital signatures ensure accurate payment instructions between transacting parties.

i) Transaction encryption (through hashing and digital signatures)

The initiation of a transaction takes place, for example, when an initiating party wants to transfer a digital asset (or assets) from a node's address (or addresses) to another node's address (or addresses), in the blockchain network (O'Diar *et al.*, 2016). When transaction parties want to send the 'message' of the proposed transaction over the network, the transaction first needs to be encrypted.

To ensure that the message is securely sent, the message needs to be encrypted by the initiating party. Encryption of information is one of the essential elements of digital security. Encryption is the translation of data, through using a mathematical algorithm, which ensures that the original data is concealed and only accessible to the intended recipients. The receiving party will decrypt the message to recover the original message. The algorithms for encryption and decryption are generally known, while the encryption and decryption keys are confidentially maintained. There are two types of encryption, namely symmetric encryption algorithms and cryptographic hashing. These encryption methods are discussed below (Harz, 2017).

- Symmetric encryption algorithms

When data is encrypted using one-for-one translation, data is translated from one set of data to another set of data. When both transaction parties use the same key for encryption and decryption, it is known as a symmetric encryption algorithm (Skudnov, 2012).

- Cryptographic hashing

Cryptographic hashing is the encryption method used by the blockchain technology. During the cryptographic hashing process, the contents of a transaction, including a few pieces of metadata, such as timestamps (refer to 4.4.2 ii) and transacting parties, are encrypted through utilising a mathematical algorithm. The output is known as a hash, which is a short digest of the original data (Condos *et al.*, 2016).

A cryptographic hash function has the ability to take an input of random length, and provide an output, a sequence of predetermined length. A fundamental characteristic of the hash function is that the same hash will always be produced from the same input message. Furthermore, the hash will not be able to be reversed to the original message (Badev & Chen, 2014). A perfect cryptographic hash function, as discussed above, has the following characteristics (Rogaway & Shrimpton, 2004; Lewis, 2015):

- It is very difficult to derive the original data from the hash function.
- When there are any changes to the original data, no matter how immaterial, the hash will change significantly. The new hash is completely different from the old hash and appears unrelated to the previous hash.
- A hash is unique, thus it is not possible for the same hash to be derived from two different inputs.

These advantageous characteristics result in it being nearly impossible to determine, through guessing, what the original content of a hash was. The output of a hash function is very random and there is currently no known technique to reverse-engineer the original content from the calculated cryptographic hash. For example, envision a file containing a range of numbers, for example: 07 16 27 41 72 91. Hashing a document is similar to performing a mathematical calculation on the numbers. For example, the sum of the aforementioned numbers is 254. When given the sum of the numbers it is impossible to determine what the original numbers were. When one of the numbers in the range are changed, the hash will change. This is similar to the hashing of an electronic document, except the original input is thousands of numbers, and the mathematical calculation is more complex than a straightforward sum function. For example: take the sum, divide by 40, take the square root, add 80, and with 300 more steps (Condos *et al.*, 2016).

After the encryption of the transaction data, the message needs to be signed by the transacting (initiating) party, through the use of digital signatures.

Digital signatures (Asymmetric cryptography)

All transacting parties own a pair of keys, a private and a public key. Private keys are kept secret, similar to a password, and are used to sign messages. Public keys are visible to the network and are used to access the original message. These keys can be seen as digital certificates that are stored on the user's computer system, which allows for the encryption and decryption of data.

Digital signatures are a form of asymmetric cryptography (they use one private and one public key), which is used in an untrusted environment as a mechanism to validate the authentication of transactions (Christidis & Devetsikiotis, 2016).

To build a digital signature scheme, three algorithms are required (Harz, 2017):

- an algorithm which will create a public and a private key. The two keys are paired, based on their key size. The private key is used to sign messages, while the public key on the message can be verified by anyone in the network;
- a sign algorithm which will create a signature, based on the private key, and a message; and
- a verifying algorithm which will evaluate the validity of the message, based on the public key, and the signature.

Figure 4.2 below shows an example of a digital signature used in a blockchain transaction. The digital signature is involved in two parts of the transaction: the signing and the verification part. For example, when a user A signs a transaction, she will firstly generate a hash value, which is calculated from the transaction. The calculated hash value will now be encrypted by using her private key, then she sends the encrypted hash, which includes the original data (the transaction), to user Bs (all the nodes in the network). User Bs (nodes in the network) will verify the received transaction through comparing the decrypted hash (through using user A's public key) and the hash value of the received data (using the same hash function as user A).

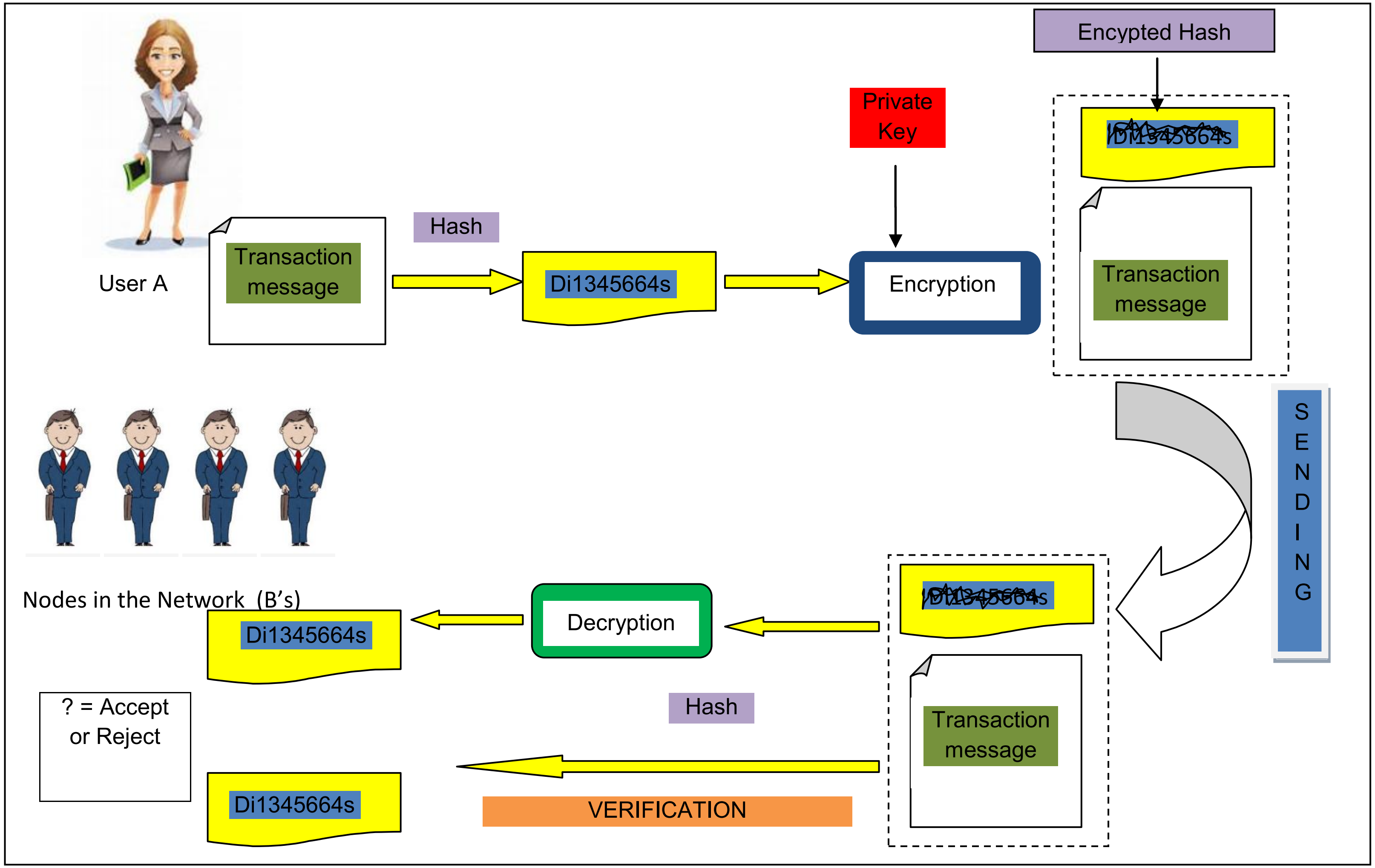


Figure 4.2 The blockchain digital signature (Asymmetric cryptography)

Source: (Adapted from Zheng *et al.*, 2016)

Therefore, a valid digital signature results in the authentication and validation of a transaction. The validation of the transaction illustrates and confirms that the transaction was created by a known sender, the sender cannot deny sending the transaction, and the message was not altered in transit.

Therefore, digital signatures are utilised to ensure that a message between a sender and a receiver is validated (Badev & Chen, 2014). Through the validation of the message the following risks are addressed:

- authentication – the recipient can verify that the message came from the sender;
- non-repudiation – the sender cannot deny sending the message; and
- integrity – the message has not been altered or edited in transit.

Bitcoin application

The initiation of a transaction occurs, for example, when an initiation party wants to transfer Bitcoins to another party within the Bitcoin network. Entities generally own a set of Bitcoin addresses, called their wallet, which is used for transacting on the Bitcoin network. Each transaction record will consist of one or more sending addresses and one or more receiving addresses and the amount of Bitcoins sent and received per address will differ. Thus there is a possibility of multiple receiving addresses from one Bitcoin sending address. This process is illustrated in Figure 4.3 below.

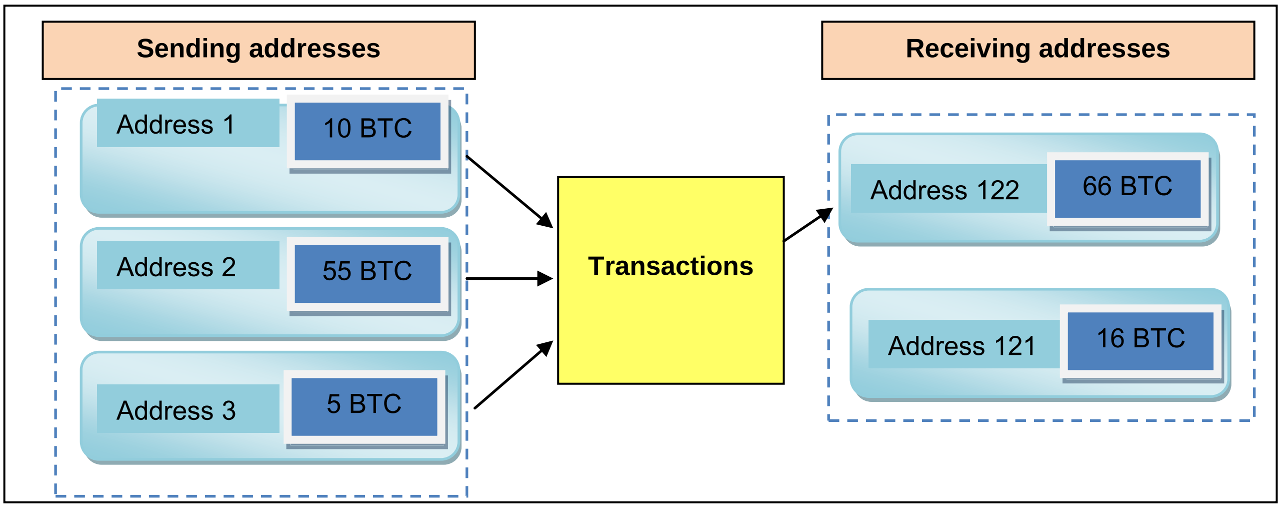


Figure 4.3 A Bitcoin transaction

Source: (Badev & Chen, 2014)

From the Bitcoin transaction illustrated in Figure 4.3, two important features are noted, namely that serial numbers cannot be assigned to Bitcoins to trace their path in the Bitcoin network, since there are multiple sending and receiving addresses per transaction. Secondly, even though the ledger is public, the changing of ownership of Bitcoins cannot be directly observed since the identity of the network nodes are protected and only public keys are visible (Badev & Chen, 2014).

During the Bitcoin transaction process, cryptography is used by the Bitcoin application in three fold, namely the verification process; the payment process; and to manage the number of Bitcoins (Badev & Chen, 2014).

The cryptographic hash function utilised by the Bitcoin application is SHA-256, which is a type of secure hash algorithm. SHA-256 was designed by the National Security Agency and published by the National Institute of Standards and Technology (Dang, 2012).

The type of digital signatures used by the Bitcoin application is called the elliptical curve digital signature algorithm (ECDSA). Elliptic curve digital signature algorithms have several advantages, including smaller key sizes and faster computation, while the security factor quality remains the same (Skudnov, 2012).

For the Bitcoin application, the public key of the digital signature is used to identify the users. A user can create identities or addresses and is allowed to create multiple addresses (Nakamoto, 2008; Wood, 2014). On the other hand, in permissioned blockchains, the process of creating identities is controlled by a membership service which authorises new identities (Cachin, 2016).

The Bitcoin balance of every Bitcoin address is public information and can be calculated by any participant in the Bitcoin network, because the transaction history is recorded in a public ledger. Therefore, every previous or proposed (newly broadcasted) transaction can be verified and the availability of the proposed amount of Bitcoins for a particular Bitcoin address can be confirmed by the network nodes (Badev & Chen, 2014).

To conclude, the sender uses its key to encrypt the transaction data. The transaction will now be broadcasted to the entire network for the verification process to start. The verification process is discussed below.

ii) Transactions are broadcasted to the network and verification process can start

The digitally signed transactions are broadcasted to all the participating nodes in the network. The recipients in the network, receiving the encrypted message, use their public

keys to decrypt the information and validate the transaction based on the blockchain protocol. The transactions are recorded in the public ledger after the verification process.
The process during which the integrity of a transaction is verified and the availability of funds is confirmed, is a complex process. The maintenance of records and the verification of transactions are regarded as a central part of any electronic payment system. These functions are generally performed through private ledgers which are maintained by trusted third parties. A decentralised payment system, such as Bitcoin, replaces third party intermediaries and the records are maintained in a public ledger through a distributed information system. The public ledger allows for a decentralised approach in the verification of transaction messages (Badev & Chen, 2014).

When transactions are verified, the following needs to be checked by the verifying nodes:

- The digital asset is owned by the spender, which is checked through ensuring that the transaction was signed by the initiating party, known as 'digital signature verification of transactions'.
- The spender (initiating party) has a sufficient amount of the digital asset (for example cryptocurrencies) in his account. This will be checked through checking every transaction performed on the spender's account or 'public key' which is registered in the ledger. This process will ensure that the spender has an adequate amount of the specific digital asset in his account to complete and finalise the transaction (Crosby *et al.*, 2016).

Bitcoin application

The Merkle tree is utilised to verify transactions in the Bitcoin application. As discussed in section 4.4.2 i) the block consists of a block header which includes a Merkle tree root hash.

Bitcoin utilises the Merkle tree structure through a method known as 'simplified payment verification' (SPV). Franco (2014) concluded that through applying the block header, Bitcoin proposes an easier way to verify whether a transaction should be included in a block or not. The block header is formed through the Merkle root, which includes the nonce (included by the miner) and the hash of the previous block (Franco, 2014). Each SPV client maintains copies of the block headers from the longest proof-of-work chain, which could be obtained through enquiry to the network until the SPV client is satisfied that it has the longest chain, which is regarded as the valid chain (refer to section 4.4.3). When an SPV client wants to verify that a specific transaction belongs in the block, they will be able to download a specific branch in the Merkle tree. This specific branch in the Merkle tree, which includes the connection between particular transactions to the specific block header, named a Merkle branch, will be used to validate the transaction (Levin, 2017).

4.4.2 Candidate blocks are formed using validated transactions (Level 2)

After transactions have been initiated, encrypted through cryptographic hashing and digital signatures, broadcasted to the network, and validated by the network participants, these transactions are now valid. Nodes in the network will now group transactions into blocks.

In Level 2, the blockchain blocks are discussed, which includes the contents of a block, namely the block header, block body and the timestamping of blocks.

i) Blockchain blocks

Firstly, a block is a file in which data, for example transactions or events, are recorded (Condos *et al.,* 2016). These blocks are added together to form a blockchain, which then constitutes a complete list of all the transactional records (Chuen, 2015). In this string or chain of blocks, every block refers to the previous block through a reference known as a hash value. The previous block is called the parent block, while the first block of a blockchain is referred to as the genesis block. Figure 4.4 is a simplified explanation of a blockchain. The first block is known as the genesis block, the sequence of blocks is ordered backward, based on the hash value of the previous blocks.

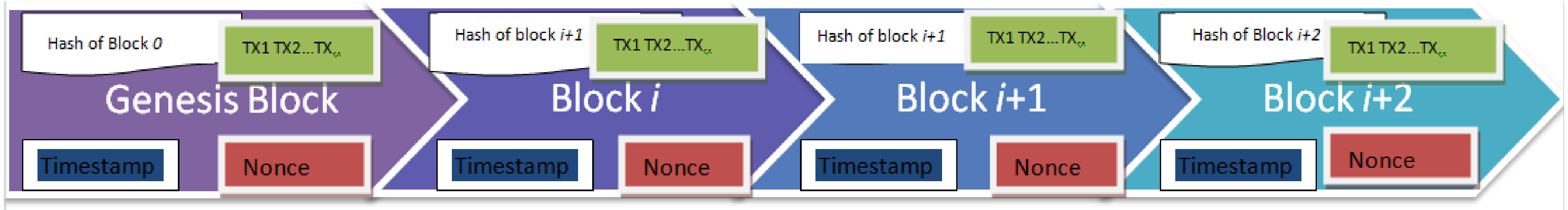


Figure 4.4 An example of a blockchain

Source: (Zheng *et al.*, 2016)

Blocks, which contain the transaction information, are used to match information across all nodes in the network. The content of a block is grouped together as a block header and a block body (Zheng *et al.*, 2016).

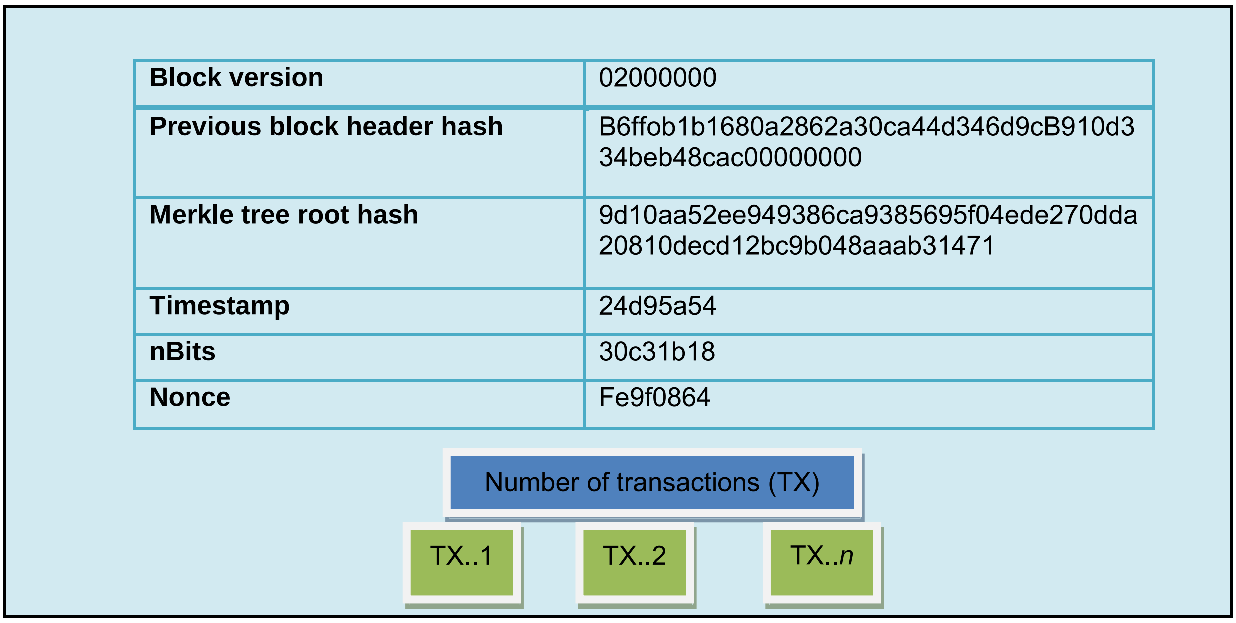
Block header (header hash)

A block header (or a header hash) is a hash value calculated from the information included in a block's header. This header hash is used by the next block to link back to the previous block. The content of the header hash in the blockchain application is dependent on the specific blockchain application protocol. The following are the minimum contents of a block header:

- Blockchain version number, which specifies which set of 'consensus rules' should be followed;
- Header hash of the previous block;
- Merkle tree root hash, which is the hash value of all the transactions in the block;
- Timestamp (current 'timestamp' as seconds in universal time since 1 January 1970);
- nBits (compact representation of the 'target' of a valid block hash); and
- The 'nonce' (the value which will be changed during the consensus process to obtain the 'target' hash. It is a 4-byte field, generally starts with 0, and increases with every hash calculation).

All transactions are not included in the block header, only the Merkle root is. The Merkle root is the root hash of the Merkle tree, which is calculated using all the transactions to be included in the block as input to the hash function. A Merkle tree is a binary tree which is formed through using hash values. One of the major advantages of Merkle trees is the verification of transactions. When a node wants to verify that a transaction belongs to a block on the blockchain, the node does not need to recalculate the hashes of the entire chain, but only the hashes from the leaf and upwards towards the root branch (Levin, 2017).

A Merkle tree is generated by performing the following procedures: first, hashes of all the transactions are calculated; then these calculated hashes are paired together and hashed again, resulting in a new, smaller group of hashes. This step is repeated numerous times until only one hash is left. Finally, this hash, which is called the root hash, or the Merkle root, is included in the block header (Skudnov, 2012). The precise procedure for calculating the Merkle tree was beyond the scope of this study. Figure 4.5 below provides an example of the contents of a block.



Block version	02000000
Previous block header hash	B6ffob1b1680a2862a30ca44d346d9cB910d3 34beb48cac00000000
Merkle tree root hash	9d10aa52ee949386ca9385695f04ede270dda 20810decd12bc9b048aaab31471
Timestamp	24d95a54
nBits	30c31b18
Nonce	Fe9f0864

Figure 4.5 An illustration of the contents of a block

Source: (Zheng *et al.*, 2016)

Block body

The block body includes the number and collection of transactions. The validation of these transactions is discussed above, in section 4.4.1 ii) (Level 1).

ii) Timestamping

A timestamp is the connection between the individual blocks. The timing of a transaction in the blockchain and the recording thereof is a critical step in the forming of the blockchain. During the verification process, a node will check (among other things) timestamps of previous transactions. This is done to ensure that transacting parties attempting to transact and record the same unit twice, at for example at 12:00 and 12:01 will be regarded as invalid by the nodes in the network during the validation process. Furthermore, timestamping enables data stored in the blockchain to be stored in chronological order. The timestamp of the current block also refers back to the timestamp of the previous transactions, resulting in a 'chain' of transactions. Individual timestamps are furthermore encrypted and obtained from a trusted timestamp server. Consequently, each block which are added to the chain is mathematically linked to the previous block, as well as to the subsequent blocks (Condos *et al.*, 2016).

4.4.3 The block-generation process, through consensus mechanisms (Level 3)

After transactions have been created and validated in Level 1 and a block is formed by the nodes in the network in Level 2, the block needs to be generated and added to the blockchain. This is performed by participants or nodes which will compete to record the transaction in the blockchain (Badev & Chen, 2014). A system is required to ensure that the 'correct' block is added to the blockchain, as there could be multiple blocks created by different nodes at the same time. The blocks in the blockchain are generated through a consensus process. The Bitcoin blockchain relies extensively on hashes and hash functions during the consensus process (Pilkington, 2015). The consensus process is performed through the use of a mathematical puzzle, whereby blocks would only be accepted to the blockchain once a very special mathematical problem is solved. For example, a node will be required to find a nonce which will provide a hash with a certain number of leading zeros when it is hashed with both transactions and hashes of the previous blocks (Crosby *et al*., 2016). The mathematical puzzle which needs to be solved by the node is adjusted to ensure that a block in the network takes more or less 10 minutes to be generated by a node. There is still a very small probability that more than one block will be generated by two nodes at a specific point in time, which will result in a fork (Crosby *et al.*, 2016). (Refer to a discussion of forks in section 4.4.6 ii.)

A distributed method to mitigate the forks in a blockchain is required because various nodes might have different views of the network. There are different approaches to obtain consensus. The following six mechanisms are representative of modern consensus algorithms (Vukolić, 2016):

- Proof of work (POW)
  In short, the proof-of-work process requires a node wanting to generate a block to prove that it has sufficient computing resources to solve a mathematical puzzle.
- Proof of stake (POS)
  Proof of stake is a consensus mechanism in which the generation of blocks depends on the amount of currency owned by the nodes. Verification is performed by the nodes with the highest stake in the network; hence the nodes with the largest amount of currency will perform the verification process. This is based on the assumption that the nodes with the highest stake would ensure that the verification process is performed correctly because this is in their best interest.
- Practical byzantine fault tolerance (PBFT)
  Practical byzantine fault tolerance was initially a system devised for a storage system, it could be utilised in digital asset management, which does not require a large amount of throughput, but does demand many transactions. Through PBFT, each node in the network will publish a public key. The node will sign the message coming through to verify its format. The transaction is regarded valid when sufficient identical responses are reached. Thus trust is confirmed through the total number of nodes agreeing to the transaction and no hashing power is required as per POW.
- Delegated proof of stake (DPOS)
  Delegated proof of stake is similar to POS, whereby nodes are able to create blocks based on their stake (amount of currency held by them). The difference between DPOS and POS is that in DPOS the stakeholders are able to choose delegates who may generate and validate a block.
- Deposit-based POS
  In deposit-based consensus protocols participants are required to register a security deposit for them to be able to provide the consensus for producing blocks.
- Roundrobin
  Roundrobin is used for private blockchains. There is consequently an amount of trust between the participants and consensus is achieved without difficult computations.

The specific blockchain protocol determines the consensus mechanism which needs to be performed by network participants (Pilkington, 2015). The Bitcoin application utilises the POW consensus mechanism for the block-generation process (Level 3), which is discussed below. The detailed working of the other modern consensus mechanisms, named above, is beyond the scope of this study.

Bitcoin application

As discussed above, digital signatures are utilised to verify that the transaction was signed by the transacting party claiming to be signing the message. However, this does not solve the problem that one person might send the same bitcoin twice, since it is possible to create valid signatures for both transactions (Nakamoto, 2008). In a decentralised system such as Bitcoin, network participants need to agree on the validity of transaction to prevent double-spending. This is done through a distributed consensus protocol.

A distributed consensus protocol includes the following factors: a network has ‘x’ nodes of which an arbitrary ‘k’ number of nodes might be faulty or malicious. The consensus protocol needs to ensure that firstly, all honest nodes agree with one value, as well as the transactions in a block, and secondly, that this value was created by honest nodes. Bitcoin utilises the consensus algorithm, Proof of work (POW), which is based on the fact that the chain with the most computational work is regarded to be the valid chain (Nakamoto, 2008).

The Bitcoin POW consensus mechanism is activated by nodes which compete to record the transactions in the blockchain. The nodes are called miners and the processes when the nodes compete to add a block to the blockchain are known as mining. The Bitcoins’ POW consensus mechanism is based on hashcash. Hashcash is a type of POW system which aims to ensure that competing computers use a defined number of computing resources to reach a predetermined target (Back, 2002; Nakamoto, 2008; Franco, 2014).

To reach the predetermined target, a complicated computational process is used for the validation of transactions. During this computational process, also known as the hash function, each miner in the network will calculate a hash value of the constantly changing block header. As explained in section 4.3.5, a nonce is a value starting from 0 which increases with each hash calculation. The POW consensus mechanism determines that the calculated value be equal to or smaller than a certain target value. For Bitcoin, which utilises a decentralised network, miners have to calculate the hash value continuously by using different nonces until the target hash value is reached. The hash target is determined by the blockchain protocol, which is a range of predetermined criteria.

If the hash value produced is below a certain threshold, the POW is complete and the transaction has been verified. If the target hash value has not been reached, the miner needs to try again through using another value for the nonce. Miners are forced to cycle through a series of nonce values on a trial and error basis because it is impossible to determine whether the value of the nonce, when combined with the other two inputs, will result in a acceptable hash value. For example, the Bitcoin protocol requires that miners combine three inputs and enter them into a SHA-256 hash function by including the following:

- a reference to the previous block;
- details of their proposed block of transactions; and
- a special number called a nonce.

When the appropriate value is obtained by a miner, the block is timestamped and all other nodes need to confirm the accuracy of the value. The range of transactions used for the calculation is the validated result, which is used by the new block in the blockchain.

The POW consensus mechanism utilised by the Bitcoin application causes the time taken to successfully verify a block of transactions to vary depending on the difficulty of obtaining the correct nonce. The time duration for the verification of a block will decrease when for example new miners connect to the blockchain network, or existing miners invest in faster computers. In order to allow time for information of each successful block to spread across the entire network, the difficulty of obtaining the correct nonce is periodically adjusted (Velde, 2013). This is done to ensure that the average time for adding blocks to the chain remains approximately stable at 10 minutes, resulting in payments not being instantaneous. This adjustment is done every two weeks to ensure that the rate at which blocks are added to the chain is six times per hour. Thus, if more miners are added to the network, the computing power will increase, resulting in the increased difficulty of resolving the mathematical problems in a timely manner (Velde, 2013).

To prevent fraudulent transactions on the blockchain, the adding of a block to the chain is an expensive process. 'Expensive', in terms of mining, refers to computer hardware required, electricity consumed and time expended. For POW schemes, the mathematical problem is difficult to solve, but the solution is easy to verify (Velde, 2013). Because the solution is easy to verify, the POW consensus system is balanced in favour of transaction verification, resulting in fraudulent transaction being easily identified.

The consensus process, known as mining for the Bitcoin blockchain, during which the nodes compete to add the block to the blockchain, is illustrated In Figure 4.6 below. A hash, called a digest, is obtained through inputting the data of a block of newly broadcasted transactions into the cryptographic hash function. The digest, together with a nonce, are inputted into another hash function, which result in a blockchain hash of the new block. The task that the nodes need to solve consists of finding a nonce, which will result in the blockchain hash for the new block having certain properties (target hash). When the first node finds the nonce to solve the problem and reach the target hash, it is broadcasted to the rest of the network and the ledger is updated (Badev & Chen, 2014).

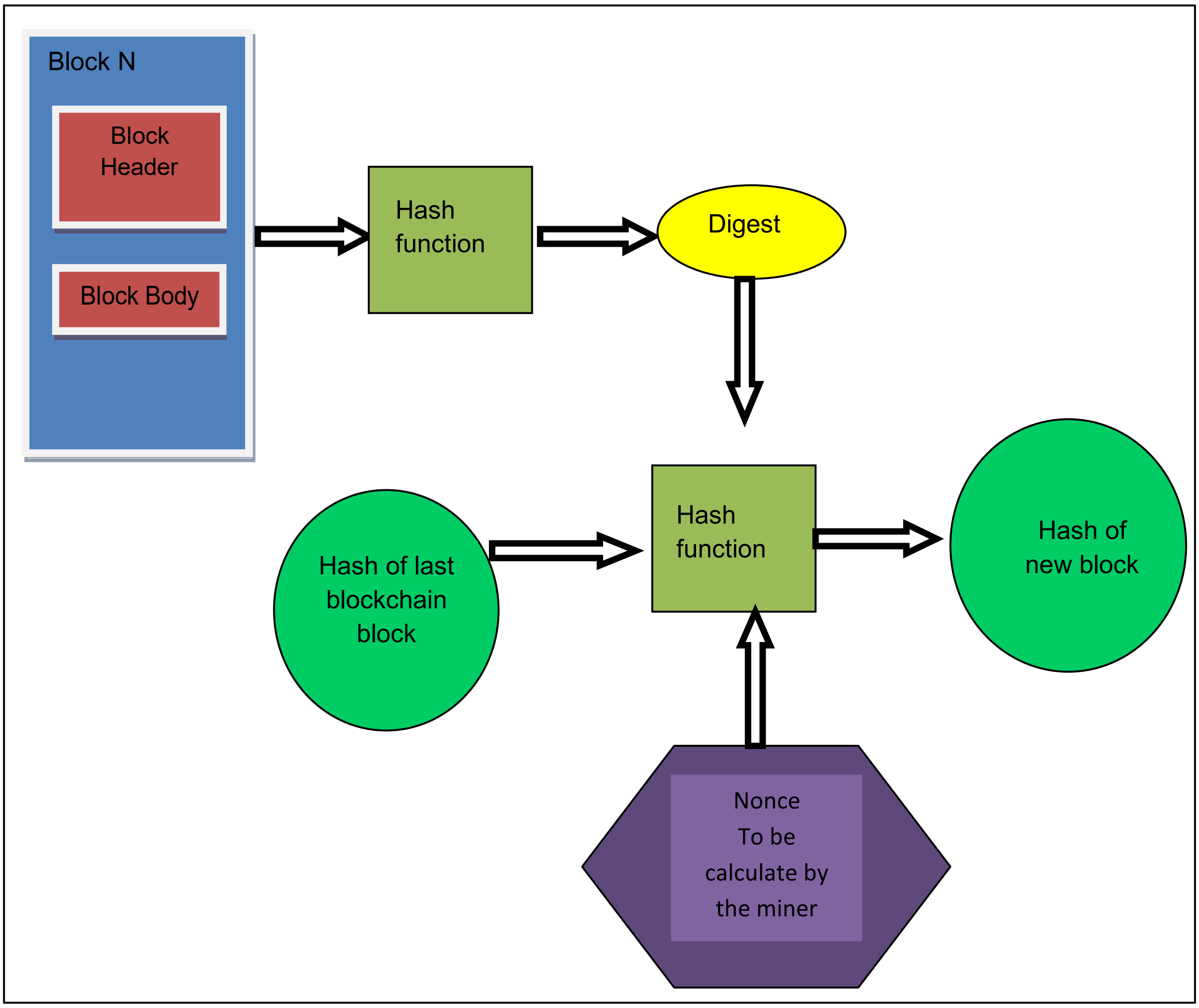


Figure 4.6 The consensus mechanism – mining process

Source: (Back, 2002)

Miner incentives and Bitcoin supply

The POW algorithm which is used as a consensus mechanism in Bitcoin is fundamental to the validation of transactions; hence, the miners performing this process are currently rewarded for their participation. The rewards are two-fold: firstly, a transaction fee is paid to miners, and secondly, newly generated Bitcoins are rewarded to miners who successfully solve the mathematical problem (Badev & Chen, 2014).

Transacting parties has the option to include a transaction fee; this fee will be distributed to the miner who successfully adds to the block to the blockchain (Velde, 2013). Initially, Nakamoto (2008) included the transaction fees with the idea that this would replace the newly minted Bitcoin reward to miners. The transaction fees are however not compulsory and willingly allocated by the sender of the transaction and currently this is an insignificant portion of the overall reward.

The reward of newly generated Bitcoins was initially 50, but the reward is halved every 210 000 blocks (which is every four years based on an average rate of six blocks per hour). This confirms that the total number of Bitcoins will increase to, but never exceed, 21 million. Thus, mining is becoming unprofitable for miners (Velde, 2013) and is considered to be a risk for the validation process of the Bitcoin application. Additional risks are discussed in more detail in chapter five.

4.4.4 The block is broadcasted to the entire network (Level 4)

After the block has been generated and the target hash solved, the block is broadcasted to the entire network. Before the block is added to the network, the network participants need to approve and validate the block, as explained in section 4.4.5 below.

4.4.5 Network participants approve and validate the block (Level 5)

The verification by the rest of the network that ‘proper work’ was done by the node is a very simple and a fast process since the inputs have to be hashed only once to determine if the output has the correct number of leading zeros and consequently confirming that the target has been reached.

The following steps are performed to confirm that a block is valid (Buterin, 2015):

- Check if the previous block, referenced by the current block, exists and is valid.
- Check that the timestamp of the block is greater than that of the previous block.
- Check that the POW on the block is valid.

If the validity of the block has been confirmed, the new block, which contains the grouped transactions, is added to the public ledger of the version of the blockchain held by the specific node who solved the mathematical problem. Acceptance of the block by the network participants is indicated by the nodes through working on creating a new block in the chain and by using the hash of the previous (accepted) block in the generation of the new block.

4.4.6 The block is added to the blockchain and the digital asset is transferred (Level 6)

After the block has been added to the network and the transaction is completed, it is important that the public ledger is maintained.

i) Blockchain maintenance

The determining factor for a valid ledger is the ledger which required the most cumulative work to be generated. The 'work' that is performed by the nodes is a function of the difficulty in obtaining an acceptable nonce which produces the predetermined target and the hash (discussed above in section 4.4.3). The work that is done to encrypt a block, through computational power, is also added to the overall work of the blockchain to which it is added (Badev & Chen, 2014). The incremental difficulty of a block is based on the number of leading zeros in its nonce. With the increase in the number of leading zeros of the nonce, the incremental difficulty of the block increases. The cumulative difficulty of the blockchain is furthermore determined by the sum of the incremental difficulty of all the blocks in a chain. In Figure 4.7 below, '*d'* indicates the incremental difficulty of each block.

The process of reaching consensus on the correct, valid ledger is demonstrated in Figure 4.7. Assume that Block A is the current block and the nodes are competing to add to this block. The successful node will broadcast a new block B to the network, which will be added to the chain, adding to its difficulty. The blockchain with the highest cumulative difficulty will be considered the valid ledger. Therefore, an attacker wanting to manipulate the ledger will need to produce a ledger with a higher cumulative difficulty than the main, validated ledger. This is highly unlikely, since the attacker will only be successful if he has the ability to obtain more computational power than all the other nodes in the network (Badev & Chen, 2014).

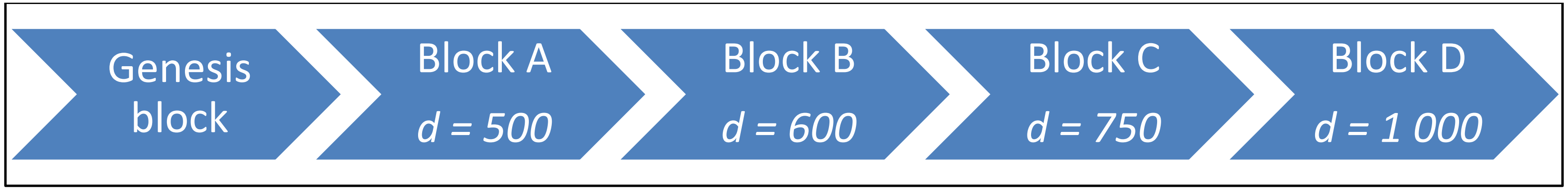


Figure 4.7 Blockchain maintenance

Source: (Badev & Chen, 2014)

ii) Blockchain forking

In a decentralised network, branches or forks may form as a result of the fact that valid blocks are generated simultaneously by numerous nodes finding the right nonce at more or less the same time. These branches or forks are shown in Figure 4.8 below.

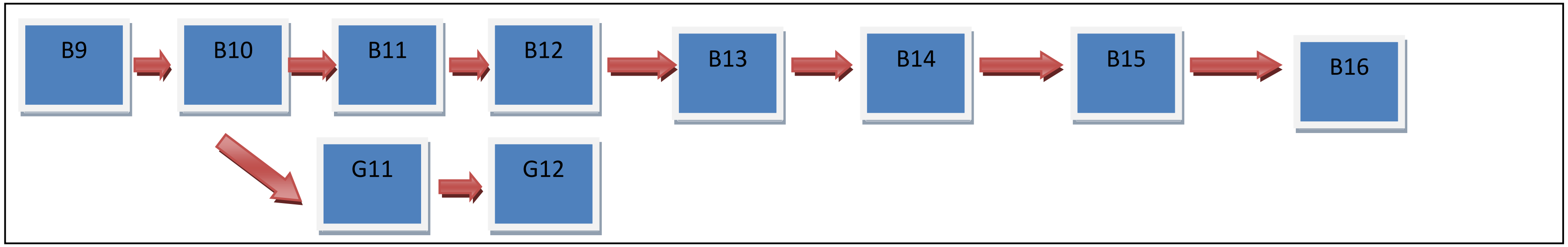


Figure 4.8 Blockchain forks

Source: (Johnson & Vanstone, 2001)

The POW protocol stipulates that the longest chain generated after the fork is regarded to be the valid chain. Generally, when more or less six blocks are generated, the relevant blockchain is regarded to be validated (Johnson & Vanstone, 2001). For example, by referring to figure 4.8, assume blocks B11 and G11 were validated simultaneously. Nodes will work on both the forks to add new blocks to both of them. But when B12 is added to B11, miners that were working on G11–G12 will switch to B12 and continue with that chain. Block G11–G12 is known as orphan blocks.

Bitcoin application

The maintenance of the Bitcoin blockchain could be jeopardised through possible attacks on the Bitcoin network. A possible way the system can be attacked is through obtaining sufficient computing power to be able to verify fraudulent transactions. This would however result in trust problems for the entire system which will consequently result in the decrease of the value of possible Bitcoins the attacker could steal. It therefore would be more sensible for anyone who is able to obtain sufficient computing power to rather contribute to the system than attacking it (Levin, 2017).

An example of an attack on the Bitcoin system would be an attempt to build a fraudulent chain faster than the honest chain is originating. However, this attack would most likely fail because honest nodes would not accept an invalid transaction or add a block to the blockchain that contains invalid transaction. An alternative form of an attack would be for an attacker to adjust their own transaction history, thus trying to respend coins used in previous transactions (Levin, 2017).

Nakamoto (2008) argues that the race between honest and fraudulent chains can be viewed as a Binomial Random Walk. The process can furthermore be seen as an attempt to catch up continuously. When the honest chain validates a block which is added to the chain, the gap between the honest and the fraudulent chain is extended by +1. Furthermore, for each block that is added to the attacker's chain the gap is decreased by -1. This process is similar to the Gambler's Ruin Problem, which in short, is the calculation of the probability of an attacker to catch up to the honest chain from a certain deficit. For example, if a gambler with an unlimited credit starts off with a deficit and plays an infinite number of games, with the goal of trying to break even, it will be possible to calculate the probability that the gambler has to break even, or in the case of blockchain, for the attacker from the fraudulent chain to catch up to the honest chain (Levin, 2017).

As discussed above, there are ways to attack the Bitcoin network but the probability of succeeding is low in large blockchains such as Bitcoin, where the computational power required to process fraudulent transactions is very high.

4.5 Further advantages of the blockchain technology

The blockchain characteristics discussed above are the specific characteristics identified which could potentially address the significant risks with the exchange of digital assets, as discussed in Chapter 3. However, the blockchain technology has further characteristics and advantages which could be beneficial to any user implementing the technology in various industries.

The list of benefits provided below is not an exhaustive list, but includes what is regarded to be the most important advantages differentiating this new technology innovation from other current technology innovations.

- **Redundancy**

Decentralised networks used by the blockchain technology are more durable than centralised networks because the risks are distributed between all the nodes and are not subject to single point of failure as per a centralised network (Abeyratne & Monfared, 2016).

- **Anonymity**

Users or entities interacting with the Bitcoin blockchain network utilises a generated address (through the public key), which does not disclose the identity of the user of entity. Even though complete privacy preservation cannot be guaranteed, this mechanism ensures a certain amount of privacy on the transactions included in the blockchain (Shrier, Larossi, Sharma & Pentland, 2016).

- **Auditability**

Verification and tracing previous records are made possible through timestamps and the fact that any node in the distributed network can be accessed. This undoubtedly improves the traceability and the transparency of the data stored in the blockchain (Shrier *et al.*, 2016).

- **Availability**

The network of participating nodes makes the blockchain and its contents highly available to users, regardless of their location (Wilson, 2016). Blockchain enables transactions to be processed unconditionally, without limitations to aspects such as time and location. This availability could be utilised for automated interactions which will result in decreasing or even eliminating transaction costs.

- **Transparency**

All transactions executed on the blockchain are visible to the public, making it possible for all nodes to agree on the status of the ledger (Wilson, 2016).

- **Permissionless**

The Bitcoin network is permissionless, thus no registration is required before participants can start transacting or mining (Wilson, 2016).

4.6 Conclusion

The characteristics of the blockchain technology were discussed in this chapter through explaining the various levels in a blockchain transaction. The Bitcoin application was utilised as an example of the blockchain technology to further enhance the understanding of the characteristics of the underlying technology.

In summary, this chapter found the following: the Bitcoin application and the underlying blockchain technology is a unique technology innovation which can be differentiated from other distributed systems by two characteristics. Firstly, Bitcoin attempts to ensure that each transaction is transparent, which will complicate falsification, and secondly, Bitcoin proposes a solution to the double-spending problem through utilising a peer-to-peer network together with consensus algorithms and a distributed timestamp server. Each transaction is timestamped and hashed into a continuous chain of hashes, by making use of the POW consensus algorithm. This results in blocks which cannot be adjusted by external parties without reperforming the POW (Levin, 2017).

In chapter five, the findings of how the characteristics of the blockchain technology, as discussed in this chapter, address the most significant identified risks with the exchange of digital asset, as discussed in chapter three are mapped. Additional risks were also identified during the mapping process, which users need to consider before implementing blockchain technology.

CHAPTER 5. HOW BLOCKCHAIN TECHNOLOGY ADDRESSES THE IDENTIFIED KEY RISKS AND THE IDENTIFICATION OF THE REMAINING (Additional) RISKS

5.1 Introduction

A discussion follows on how to manage the four main risks identified when digital assets are exchanged, as discussed in chapter three. This is done by discussing the current available technological developments which are aimed at addressing these identified risks. Next, the specifically designed blockchain technology characteristics, as discussed in chapter four, are mapped to these identified risks. As a result of the abovementioned mapping performed, a summary of the remaining, unaddressed or so-called additional risks is also included.

5.2 Risks identified when digital assets are exchanged

The procedures in addressing the identified risks, as noted in chapter three, are discussed using traditional controls. This is followed by a discussion on how the specific blockchain technology characteristics identified in chapter four could potentially address these risks in a possibly more effective and efficient manner.

These results are summarised in Table 5.1 where the blockchain characteristics are mapped to the identified risk. This was furthermore linked to the control objective achieved when the specific risk is addressed.

5.2.1 Trust

Traditional procedures addressing the trust risk

Currently, all internet commerce, which includes the exchanged of digital assets, is exclusively linked to a financial institution, central bank or central trusted agency. These trusted third parties process and mediate transactions, including the validation, safeguarding and preservation of transactions (Crosby *et al*., 2016). Because a certain percentage of fraud is unavoidable in online transactions (including digital asset exchange), mediation is needed, which is currently supplied by a trusted third party. This results in high transaction costs and possible bottlenecks at central servers (Crosby *et al.,* 2016).

Blockchain characteristics addressing the trust risk

With blockchain technology, each transaction is collectively verified and validated by the network participants, resulting in the elimination of intermediaries. Furthermore, the transacting parties do not need to trust each other since the transaction is publicly processed in the network by all network participants.

The following blockchain-specific characteristics address the trust risk:

- Peer-to-peer network, through which all transactions processed on the blockchain are public, resulting in no intermediary being required to ensure trust between transacting parties (Nakamoto, 2008).
- Distributed ledgers, which provide greater traceability and transparency, resulting in increased trust, without a trusted third party governing the transacting process (Shrier *et al*., 2016);
- Consensus process, whereby data is validated and grouped into blocks, which are only added to the chain after consensus is reached by the nodes in the blockchain (Lorenz *et al*., 2016).

5.2.2 Double-spending

Traditional procedures addressing the double-spending problem

Even though digital signatures are currently trying to address the double-spending problem, a trusted third party is still required to try to prevent double-spending of digital assets (Nakamoto, 2008).

Blockchain characteristics addressing the double-spending problem

Blockchain is the first solution to the double-spending problem that does not require a central administrator or clearing agent (Lorenz *et al.,* 2016).

The double-spending problem is one of the main issues that blockchain is aiming to solve, through the following:

- Asymmetric cryptography as identified by Pilkington (2015): Asymmetric cryptography, of which digital signatures are an example, is used to ensure the validity of digital messages. Asymmetric cryptography therefore ensures validity, integrity and non-repudiation of transactions (Christidis & Devetsikiotis, 2016). Digital signatures specifically address unauthorised transactions, as private keys of network participants would need to be stolen before unauthorised transactions can be processed;
- Timestamping of transactions during the validation process (Nakamoto, 2008): The validation process includes the agreement by the nodes in the network on the order of transactions (Lemieux, 2016);

- Immutability of blocks: After blocks are added to the chain it is very difficult to modify them. To modify previous broadcasted blocks would be computationally infeasible as this would require the overtaking of the rate at which new blocks are currently added to the chain in order to re-write the entire history (Wilson, 2016).

5.2.3 Repudiation

Traditional procedures addressing the risk of repudiation

Currently, one of the fundamental instruments in digital security is the encryption of information through digital signatures or e-sign technologies. Digital signatures entail the translation of one piece of data into another through utilising a mathematical algorithm, to ensure that the original data is concealed and can only be accessed by the intended users (Condos *et al.*, 2016). E-sign technologies work on a similar basis, as public and private keys which are used for the encryption and decryption of data are stored on a user's computer system (Condos *et al.*, 2016).

Blockchain characteristic addressing the risk of repudiation

Even though participants in the Bitcoin blockchain have anonymity, repudiation of transactions is still addressed through the following characteristics:

- Asymmetric cryptography (refer to 5.2.2);
- Cryptographic hashing, which is an encryption method that is similar to traditional encryption methods used. Cryptographic hashing ensures the encryption of the contents of a transaction, through a mathematical algorithm (Christidis & Devetsikiotis, 2016); and
- Immutability of blocks, the fact that approved records cannot be altered, which furthermore addresses the non-repudiation risk and specifically discrepancies and ensures that transactions cannot be altered after initial processing (Wilson, 2016).

5.2.4 Theft (including fraud)

Traditional procedures addressing the risk of theft (including fraud)

Encryption of information, through digital signatures, is currently mostly used to address theft and fraud of digital assets. Furthermore, fraud is seen to be limited through mediation by a trusted third party (Crosby *et al.,* 2016).

Blockchain characteristic addressing the risk of theft (including fraud)

The blockchain innovation, which ensures that transactions are computationally impractical to reverse, results in the protection of sellers against fraud (Nakamoto, 2008). Although fraud will never be completely addressed by this method, the following characteristics of blockchain are aimed at decreasing the risk:

- Decentralised network: Because all or most of the nodes in the blockchain network have a copy of the valid chain, an attacker will not be able to negatively influence the entire system. This was confirmed through research performed by Nath (2016), who noted that the blockchain technology could be utilised to decrease fraud resulting from the integrity of any asset. As the integrity of the asset is maintained by various nodes, counterfeiting, double spending or document alternations are minimised.

- Consensus process: Resulting from the size of the Bitcoin blockchain the computing power required to launch an attack would be very high and are therefore regarded as impractical (Condos *et al.,* 2016*).* The attackers would need to introduce the fraudulent transaction, ensure that a block is published from the generated transaction through solving a mathematical puzzle, and subsequently compete against the 'good' nodes to generate further blocks to ensure the network accepts the transaction and the block as valid. The fact that the blockchain is linked cryptographically makes the processing of fraudulent transactions even more difficult (Crosby *et al.,* 2016).

- Immutability: Each transaction is broadcasted to the entire network, which then validates and records the transaction in blocks. After a block is added to the blockchain, it cannot be modified and falsification is difficult. No block (entry) can be deleted or reversed once it has been added to the chain and is stored in the distributed network (Abeyratne & Monfared, 2016; Wilson, 2016). Therefore, blockchain is very effective in the prevention of objective information fraud, for example loan application fraud, where fraudulent information is fact-based. (Chai & Zhu, 2016).

Table 5.1 Matrix of the blockchain technology characteristics mapped to the significant risks identified and control objectives achieved through the technology

	SIGNIFICANT RISKS IDENTIFIED						CONTROL OBJECTIVES			
Blockchain characteristic	**Trust**		**Double-spending**	**Repudiation**		**Theft (fraud)**	**Completeness**	**Accuracy**	**Validity**	**Integrity (including Privacy)**
Sub-categories if risks identified	Reliability	Authenticity	Fraud	Discrepancies	Un-authorised transactions					
Level 1: Transaction encryption										
• Cryptographic hashing				X		X			X	X
• Digital signatures (Asymmetric cryptography)		X	X	X	X				X	X
Level 1: Verification of transactions										
• Broadcasted to network – peer-to-peer network	X	X							X	
• Validation/Verification process (Decentralised)	X	X			X	X			X	

Blockchain characteristic	Trust		Double-spending	Repudiation		Theft (fraud)	Completeness	Accuracy	Validity	Integrity (including Privacy)
Sub-categories if risks identified	Reliability	Authenticity	Fraud	Discrepancies	Un-authorised transactions	Theft				
Level 2: Blockchain block content										
- Previous block header hash		X	X			X			X	
- Immutability of blocks			X	X	X	X			X	X
- Timestamping			X	X					X	
Level 3: The block generation process										
- Proof of work		X	X						X	
Level 4:Broadcasting of block										
- Decentralised public network		X				X			X	X

Blockchain characteristic	**Trust**		**Double-spending**	**Repudiation**		**Theft (fraud)**	**Completeness**	**Accuracy**	**Validity**	**Integrity (including Privacy)**
Sub-categories if risks identified	Reliability	Authenticity	Fraud	Discrepancies	Un-authorised transactions	Theft				
Level 5: Transaction validation										
Network participants approving and validating transactions		X			X				X	
Level 6: Maintenance										
Blockchain maintenance - block is added to the chain (distributed ledgers)	X	X	X			X			X	X

Source: (Author’s own construct)

5.3 Remaining and additional risks of the blockchain technology

The blockchain technology is a breakthrough technology with many possible applications in financial as well as non-financial sector. Even though the blockchain application addresses many risks, there are still additional risks which users need to take into consideration when adopting the technology (Crosby *et al.*, 2016).

The additional risks, identified through mapping performed in step 3 and other risks identified during research performed in step 1.2, were grouped together to provide a list of additional risks users need to consider before implementing the blockchain technology.

5.3.1 Underlying costs

The consensus mechanism, POW, which is utilised in the Bitcoin system to verify transactions, results in relatively high costs. These costs are caused by electricity and hardware charges to solve the mathematical problem during the validation process (Decker & Wattenhofer, 2013; Levin, 2017).

With the implementation of the blockchain system, entities will face challenges such as translating existing manual or paper-based documents into blockchain format (data needs to be in a digital form), which might be time-consuming and costly (Crosby *et al.,* 2016). Furthermore, even if computer-based systems are utilised, they might be old and outdated, and will need to be upgraded before they would be compatible to the blockchain system (McLean & Deane-Johns, 2016).

Redundancy, as discussed above, could be beneficial to users but on the other hand, this redundancy results in increased costs; furthermore, nodes require computers with increased processing power to be able to maintain a copy of the entire blockchain (Ammous, 2016). It is therefore regarded as an additional risk for potential users as the underlying costs could increase to an extent that the blockchain application is not economically feasible any longer.

5.3.2 Completeness and accuracy

Completeness and accuracy of digital records is not addressed through the blockchain system. Only the authenticity, validity and integrity are addressed when the transacting parties are confirmed, the time and date of the transaction, and the content of the record when it is submitted (Condos *et al.,* 2016).

5.3.3 Fraud and security

As noted by Chai and Zhu (2016), all types of fraud are not addressed through the blockchain application. As previously discussed, the integrity of records is addressed through blockchain being a distributed, public ledger which results in records being saved on multiple computers. Furthermore, the updating of records is dependent on the POW consensus system, resulting in fraudsters not easily being able to change records already recorded on the system.

Even though fraud, based on objective information, for example loan applications which are fact-based, is sufficiently addressed through the blockchain system, the problem of fraud still remains. This is applicable to subject information fraud, for example rating fraud where the fraudulent information is not easily verified as the ratings are based on subjectivity and cannot be verified by the system (Chai & Zhu, 2016). However, this risk is mitigated through the fact that the blockchain system only allows accounts to be created based on valid identities. In traditional systems, one person could control and create multiple accounts, which increased the problem of subjective information fraud, as multiple fraudulent ratings could be submitted. In blockchain, even though the ratings cannot be confirmed, the number of fraudulent ratings is limited, since the number of users created by fraudsters is limited.

With this technology innovation there are also new types of attacks on the system as described below. These attacks are not yet understood and are thus less mitigated than attacks occurring in conventional database architecture (Lorenz *et al.*, 2016).

The following attacks are discussed in more detail below: 51% attack, identity theft, money laundering, and hacking (Xu Xu, 2016).

- **The 51% attack**
  The 51% attack occurs when a single node dominates the verification and approval of transactions on the network by having significantly more computational power than the rest of the nodes in the network. Thus, the 51% attack results in the specific node having more than half of the network's processing power and consequently the ability to outpace the rest of the nodes in the network. The node will be able to manipulate the blockchain through including fraudulent transactions or double-spending digital assets, for example. This risk specifically exists in blockchains with smaller networks (Swan, 2015).

- Identity theft

  One of the characteristics of the blockchain network is privacy. The security of digital assets is, however, dependent on the safeguarding of the private key (Xu Xu, 2016). As explained in chapter three, the private key is required to exchange digital assets, but if a node's private key is stolen it cannot be recovered. Consequently, all the digital assets held by the node will be stolen and it is highly unlikely that the thief will be identifiable. Thus, identify theft in the blockchain environment could most likely be more devastating than identity theft in the offline world.

  For example, in the case of credit card companies, risks are controlled by central authorities who safeguard transactions, detect suspicious activities and assist in finding thieves. Furthermore, the current cryptography standards are not entirely uncrackable (Swan, 2015). With the development of quantum computing, it is not impossible for cryptographic keys to be cracked quickly, demolishing the foundation of blockchain technology (Crosby *et al.*, 2016).

- Illegal activities

  Since the blockchain technology is not yet regulated it might become a possible avenue for illegal activities. Furthermore, Bitcoins might be used for money laundering activities (Xu Xu, 2016; Crosby *et al.*, 2016).

- System hacking

  The records stored in the blockchain are very difficult to alter or change, but the programming codes and systems utilised to implement the technology are not very difficult to access (Xu Xu, 2016).

5.3.4 Scalability

Scalability of the blockchain system is a challenge because the system has a consensus-based validation system and the ledger is continuously replicated, resulting in the increased amount of stored data. Therefore high-speed or high-volume transactions, real-time capturing and storing of large volumes of data are problematic on the blockchain system (Lorenz *et al.*, 2016).

With the increase of transactions, the blockchain becomes large. With each node storing all transactions on the blockchain for validation purposes, the scalability of the blockchain is limited (Sompolinsky & Zohar, 2013). Furthermore, the Bitcoin blockchain is only able to process more or less seven transactions per second which results from the restrictions of block sizes and the time interval utilised in the block generation process (Nakamoto, 2008), which cannot fulfil the requirement of processing millions of transactions in real-time fashion (Zheng *et al*., 2016).

A further concern resulting from the fact that all the nodes have a copy of all the transactions in the ledger is the possibility that the ledger might grow faster than the number of network nodes (Ammous, 2016). If the blockchain wants to increase the volume of transactions, the blocks size will need to increase, resulting in more computational power to add a block to the blockchain, resulting in fewer nodes adding to the network and subsequently a more centralised network.

Skudnov (2012) notes that one of the reasons why the blockchain is not scalable is that without improvements to the Bitcoin protocol, a normal desktop computer, for example, will not have sufficient power to process a transaction because of the size of the blockchain. Furthermore, when transacting on the blockchain for the first time, the process of downloading the existing blockchain and validating before executing the first transaction could be time-consuming and increases continuously as the number of blocks in the chain expands (Crosby *et al.*, 2016).

5.3.5 Privacy

Even though privacy is preserved through public keys in the blockchain system, transactional privacy cannot be guaranteed since the values of all transactions and the balances for all public keys are publicly visible (Kosba, Miller, Shi & Wen, 2016).

5.3.6 Government regulations

Regulatory compliance: Blockchains with their own currency, such as Bitcoin, are not regulated and not controlled by the Reserve Bank. Therefore, transactions are cleared when they are valid or blocked if not valid and the process cannot be overridden by regulators. Subsequently the application of blockchain in highly regulated professions such as law or finance, where currencies other than Bitcoin, which are regulated, are involved, might cause regulatory problems and legal complications. Furthermore, blockchain operates online and across jurisdictions with different regulatory rules which will further complicate matters in ensuring compliance with all rules (Ammous, 2016).

5.3.7 Quantum computing

As the blockchain technology is based on the fact that a single party cannot resolve the mathematical problem resulting from a lack of computer power, the future Quantum computers might pose a problem. These computers might be able to crack the cryptographic keys easily which would cause the whole system to be inefficient. However, the keys could possibly be made stronger through encryption techniques to ensure that they cannot be cracked.

5.3.8 Understanding by users

A relatively high level of technical understanding is required to utilise the technology (Srisukvattananan, 2016). A lack of understanding could lead to inadequate technical skills resulting in risks not being correctly identified, defined and measured (McLean & Deane-Johns, 2016).

5.3.9 Irreversibility of transactions

One of the characteristics of the blockchain technology is that blocks that have been added to the blockchain and subsequent blocks that are added to the validated blocks cannot be altered without reperforming the validation process of the block and all subsequent blocks. With this benefit which ensures integrity of transactions there is also a limitation of irreversibility and a lack of customisation. With traditional payment systems, human or software errors are easily reversed and corrected by intermediaries. This is not an option on the blockchain system (Ammous, 2016).

5.3.10 Trust

Although one of the characteristics of the blockchain is a trustless payment system, the system is not completely trustless as the users are still exposed to risk in their use of the blockchain technology. The ‘remaining’ trust factor for the blockchain technology is the blockchain software and the third parties who record information about the external world on the blockchain. The blockchain removes the trust for a single specific third party to maintain a ledger. For example, if a user accesses a blockchain through an intermediary, such as a digital currency exchange, they trust the intermediary. Therefore if the intermediary's system fails, then the user may lose control of their assets on the blockchain (Harz, 2017).

5.3.11 Timing errors

In the Bitcoin blockchain, each block contains, amongst other things, a list of transactions and a timestamp which indicate the approximate time when the block was created (refer to chapter three). The timestamp of the block allows the system to regulate the production of Bitcoins and generate proof of the chronological order of the transactions which address the possible double-spending problem, as discussed earlier in this chapter. Because the blockchain technology is so reliant on timestamps, it is very important that the 'timers' of the nodes in the network, which keep track of the network time, are functioning properly to prevent timestamp errors. Yet, even when the counters are working, there is still a risk of a possible attack. Attackers can slow down or speed up a node's network time counter by connecting as multiple peer nodes and reporting inaccurate timestamps (Culubas, 2011).

5.3.12 Private key management by users

Key management is a risk since this is an important part in any system which is reliant on cryptography. It includes the generation, exchange, storage, use and replacement of keys, which is a difficult process. Users need to ensure that multiple keys are simultaneously accessible and resistant to digital theft and loss. How to achieve effective key management, including system policy, user training, organisational and departmental interactions and coordination between these elements, remains an unresolved problem (Eskandari, Barrera, Stobert & Clark, 2015). Furthermore, private keys still need to be managed as they are vulnerable to loss or open to theft. For example, Bitcoin software manages several private keys by storing them on a node's local storage in a file or database. A file containing private keys can be read by any application with access to the user's application folder. Attackers could use this to obtain immediate access to the transaction records. Furthermore, users need to be careful not to share their Bitcoin application folder intentionally and they must also be cautious about the possibility of physical theft when using portable computers or smartphones (Eskandari *et al*., 2015).

5.3.13 Throughput

In 2016 the Bitcoin network could process seven transactions per second. Other transaction processing networks, for example VISA, processed 2 000 transactions per second. Therefore the throughput of the Blockchain network will need to be improved to ensure that the increased frequency of transactions can be handled in future (Yli-Huumo *et al*., 2016).

5.3.14 Latency

Currently, as discussed earlier, the average time of generating a block is 10 minutes. The time creation of a block is to ensure that efficient security is achieved and to ensure that the time spent on generating a block outweighs the cost of a double-spending attack. Completing a transaction through VISA will only take a few seconds, which is a major advantage compared to blockchain (Yli-Huumo *et al.*, 2016).

5.4 Conclusion

The blockchain technology characteristics can be utilised as a control mechanism to successfully address the significant risks identified with the exchange of digital assets. The technology is seen as a revolutionary innovation, resulting from the fact that the underlying characteristics of the technology have various applications in various industries that could potentially change the way risks are currently addressed and systems are currently operated.

However, with the implementation of any new technology there are always additional risks that users need to consider, as summarised in section 5.3. The appropriateness of the implementation of the blockchain technology should therefore be carefully weighed up, taking all areas into consideration.

CHAPTER 6. CONCLUSION

Before the introduction of the blockchain technology and its potential to address the risks of digital asset exchange, all digital assets were linked to financial institutions, central banks or central trusted agencies. These trusted third parties are currently responsible for the transaction process and perform the role of a mediator. This results in high transaction costs and time delays in transaction processing.

The blockchain technology can be seen as an exciting but disruptive new technology with the potential of having a major impact on many industries including the financial sector. Bitcoin, which was the application which first introduced the underlying technology blockchain, introduced a system for electronic transaction without relying on trust provided by third parties.

The first objective of this research was to identify the risks present with the exchange of digital assets, as discussed in chapter three. The most significant inherent risks identified were repudiation, lack of trust, double-spending and theft (including fraud). These risks formed the basis of this study.

Next, a literature review was performed. This literature review, presented in chapter four, included an explanation of the blockchain technology and how blockchain technology is applied in the Bitcoin application. Through this review the major characteristics of the blockchain technology were identified. These characteristics were summarised through discussing the various stages of a general exchange of digital asset transaction. The various stages were summarised in levels:

Level 1: Transaction initiation, which consists of the following sublevels:

i) Transaction encryption

ii) Verification of transactions

Level 2: Creation of transactions to form online blocks, which consists of the following sublevels:

i) Blockchain blocks content

ii) Timestamping

Level 3: The block-generation process involves one sublevel, namely:

i) Consensus mechanisms

Level 4: The broadcasting of the block to the entire network

Level 5: Network participants approving and validating transactions

Level 6: The block is added to the blockchain and the digital asset is exchanged. This level involves the following sublevels:

i) Consensus mechanisms
ii) Blockchain maintenance
iii) Blockchain forking

Chapter four also included a summary of the classification of blockchain systems and further advantages of the blockchain technology.

In chapter five the identified characteristics of the blockchain technology were mapped to the identified risks identified in chapter three. This was done by firstly discussing the current traditional manner of addressing the identified risks, followed by discussing how the blockchain technology's potential to address the identified risks, summarised in a quick reference matrix for potential users. The chapter also included a summary of the additional risks potential users need to consider before implementing the blockchain technology.

Since this study did not focus on providing details of possible implementation in the various industries such as the financial sector and the effect thereof on the specific industries, these areas remain available for further research studies

It is therefore concluded that the underlying blockchain technology characteristics have the ability to address significant risks with the exchanging of digital assets, which no previous technologies have had the ability to resolve without human intervention, the use of internal controls or trusted third parties. Furthermore, the matrix provided can be used as a quick guide to identify specific blockchain characteristics and what risks each specific characteristic is addressing and the consequent control objective achieved through addressing these risks.

Therefore the matrix can be used by various industries to evaluate whether the blockchain characteristics will address their specific risks and achieve their control objectives. The underlying blockchain technology is a new and an exciting technology innovation. Not only does this technology have the ability to address specific risks with the exchanging of digital assets but it is also expected to have far-reaching possibilities in the financial sector and many other industries in the near future.

LIST OF REFERENCES

Abeyratne, S.A. & Monfared, R.P. 2016. Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology,* 5(9):1-10.

Ali, R., Barrdear, J., Clews, R. & Southgate, J. 2014. Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin 2014, Q3.*

Ammous, S. 2016. *Blockchain technology: What is it good for?* [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832751 [2017, August 15].

Back, A. 2002. *Hashcash – A denial of service counter-measure.* [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf [2017, March 7].

Badev, A. & Chen, M. 2014. Bitcoin: Technical background and data analysis. Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board, Washington, D.C. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544331 [2017, August 7].

Bahga, A. & Madisetti, V.K. 2016. Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications.* [Online]. Available: http://file.scirp.org/pdf/JSEA_2016102814012798.pdf [2016, November 28].

Buterin, V. 2015. *Visions Part 1: The value of blockchain technology.* [Online]. Available: https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/ [2017, June 12].

Butler, R. 2004. B2B suppliers: Addressing the repudiation of orders in an open account system. *Meditari Accountancy Research*, 12(2):21-39.

Cachin, C. 2016. *Architecture of the hyperledger blockchain fabric.* [Online]. Available: https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf [2017, July 15].

Chai, Y. & Zhu, D. 2016. Fraud detections for online businesses: A perspective from blockchain technology. *Financial Innovations,* 2:20. [Online]. Available: https://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0039-4 [2017, February 2].

Chaum, D. & Roijakkers, S. 1990. Unconditionally secure digital signatures. *Crypto '90, Abstracts*:206-214. [Online]. Available: https://link.springer.com/content/pdf/10.1007/3-540-38424-3_15.pdf [2017, May 17].

Christidis, K., Devetsikiotis, M. 2016. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access.* 4: 2292-2303.

Chuen, D. 2015. *Handbook of digital currency*. San Diego: Academic Press. [Online]. Available: https://www.elsevier.com/books/handbook-of-digital-currency/lee-kuo-chuen/978-0-12-802117 [2017, March 2].

CICA, 1998. I*nformation Technology Control Guidelines*, 3rd edition, The Canadian Institute of Chartered Accountants, 1998.

Committee of Sponsoring Organisations of the Treadway Commission, 1992. COSO Report on Internal Control and Integrated Framework [Online]. Available: https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf [2017, May 17].

Conceptual framework of financial reporting. 2010. [Online]. Available: https://www.iasplus.com/en/standards/other/framework [2017, January 20].

Condos, J., Sorrell, W.H. & Donegan, S.L. 2016. *Blockchain technology opportunities and risks.* [Online]. Available: https://www.scribd.com/doc/296118021/Blockchain-Technology-Opportunities-and-Risks [2017, March 22].

Crosby, M., Nachiappan, N Pattanayak, P., Verma, S. & Kalyanaraman, V. 2016. Blockchain technology: Beyond Bitcoin. *Applied Innovation Review,* 2:6-9. [Online]. Available: http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf [2017, January 20].

Culubas, 2011. *Timejacking & Bitcoin.* [Online]. Available: *http://culubas.blogspot.co.za/2011/05/timejacking-bitcoin_802.html* [2017, July 17].

Dang, Q. 2012. Recommendation for applications using approved hash algorithms. *Technical Report, National Institute of Standards and Technology.* [Online]. Available: http://ai2-s2-pdfs.s3.amazonaws.com/6711/6ea5ac79a7f225b8e780fde5f1fb5e93e20f.pdf [2017, April 16].

Decker, C. & Wattenhofer, R. 2013. Information propagation in the Bitcoin network. 13th IEEE International Conference on Peer-to-Peer Computing. 9-13 September 2013.

Duranti, R. & Rogers, C. 2012. Trust in digital records: An increasingly cloudy legal area. *Computer Law & Security Review,* 28:522-531.

Eskandari, S., Barrera D., Stobert E. & Clark J. 2015. *A first look at the usability of Bitcoin key management,* full version. [Online]. Available: https://pdfs.semanticscholar.org/4926/300063d5be4be9a4aa4ec9e812fbcad5072c.pdf [2017, March 15].

Fan, C.I., Huang, V.S.M. & Yu, Y.C. 2013. Computational simulation and risk analysis. *Mathematical & Computer Modelling Special Issue*, 58(1/2):227-237.

Franco, P. 2014. *Understanding Bitcoin: Cryptography, engineering and economics.* John Wiley & Sons. [Online]. Available: https://books.google.co.za/books?hl=en&lr=&id=YHfCBwAAQBAJ&oi=fnd&pg=PA95&dq=Franco+P.+2014.+Understanding+Bitcoin:+Cryptography,+engineering+and+economics.+John+Wiley+%26+Sons%3B+2014.&ots=GLXInYljhS&sig=G1dMLVDFuZQOk8ihaLSe7ib9-Ro#v=onepage&q&f=false [2017, May 16].

Ghosh, A.K. 2001. *E-commerce security and privacy.* Berlin: Kluwer Academic Publishers.

Guo, Y. & Liang, C. 2016. Blockchain application and outlook in the banking industry. *Financial Innovation,* 2:24. [Online]. Available: https://link.springer.com/content/pdf/10.1186%2Fs40854-016-0034-9.pdf [2017, March 18].

Hanley, B.P. 2013. *The false premises and promises of Bitcoin.* [Online]. Available: https://arxiv.org/abs/1312.2048 [2017, March 22].

Harz, D. 2017. *Trust and verifiable computation for smart contracts in permissionless blockchains.* [Online]. Available: http://www.diva-portal.org/smash/get/diva2:1111933/FULLTEXT02.pdf [2017, August 21].

Institute of Directors Southern Africa (IODSA). 2016. King Report on corporate governance for South Africa (King IV). [Online]. Available: http://c.ymcdn.com/sites/www.iodsa.co.za/resource/resmgr/king_iv/King_IV_Report/IoDSA_King_IV_Report_-_WebVe.pdf [2017, March 17].

International Organisation for Standardisation (IS0). 2013. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html [2017, March 17].

International Standard on Auditing 315 (Revised), Identifying and assessing the risks of material misstatement through understanding the entity and its environment, 2014. [Online]. Available: https://www.irba.co.za/upload/2014-IAASB-HANDBOOK-VOLUME-1_0.pdf [2017, June 6].

Janusz, J. Sikorski, J.H. & Markus K. 2016. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Elserivier Applied Energy*, 195:234-246. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0306261917302672 [2017, April 17].

Johnson, D. & Vanstone, S.M.A. 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security,* 1(1): 36-63.

Kakavand, H., De Sevres, N.K. & Chilton, B. 2017. *The Blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies.* [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 [2017, February 8].

Khan, F. 2012. Do Visa and MasterCard own their private network for processing payments? If so, is it very bad idea not to use the Internet instead? [Online]. Available: https://www.quora.com/Do-Visa-and-MasterCard-own-their-private-network-for-processing-payments-If-so-is-it-very-bad-idea-not-to-use-the-Internet-instead [2017, July 14].

Koch, C. & Pieters, G.C. 2017. *Blockchain technology disrupting traditional records systems.* [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2997588 [2017, Augustus 17].

Kosba, A., Miller, A., Shi, E. & Wen, Z. 2016. Hawk: The Blockchain model of cryptography and privacy-preserving smart contracts. 2016 IEEE Symposium on Security and Privacy. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7546538 [2017, July 8].

Lemieux, V.L. 2016. Trusting records, is Blockchain technology the answer? *Records Management Journal,* 26(2):110-139. [Online]. Available: http://www.emeraldinsight.com/doi/pdfplus/10.1108/RMJ-12-2015-0042 [2017, July 21].

Levin, T.M.M. 2017. *Blockchain, the future opportunity for trading progression?* [Online]. Available: http://www.diva-portal.org/smash/get/diva2:1109208/FULLTEXT01.pdf [2017, July 24].

Lewis, A. 2015. *A gentle introduction to immutability of blockchains.* [Online]. Available: https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/ [2017, March 12].

Lim, I.K., Kim, Y.H., Lee, J.G., Lee, J.P., Nam-Gung, H. & Lee, J.K. 2014. The analysis and countermeasures on security breach of Bitcoin. *Computational science and its applications. ICCSA 2014* Vol 8582 of lecture notes in computer science. Springer International Publishing:720-732. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-09147-1_52 [2017, September 5].

Lorenz, J.T., Munstermann B., Higginson M., Olesen P.B., Bohlken N. & Ricciardi V. 2016. Blockchain in insurance – opportunity or threat? *Insurance Practice, McKinsey & Company,* July 2016: 1-9. [Online]. Available: file:///C:/Users/Mari/Downloads/Blockchain-in-insurance-opportunity-or-threat.pdf [2017, March 13].

Loster, P.C. 2005. Managing e-business risks to mitigate loss. *Financial Executive, Risk Management*, 21(5):43-45.

Mak, B. 2012. On the Uses of Authenticity. *The Journal of the Association of Canadian Archivists,* Spring 2012: 1-17.

McLean, S. & Deane-Johns, S. 2016. *Demystifying Blockchain and distributed ledger technology – Hype or hero?* [Online]. Available: https://media2.mofo.com/documents/160405blockchain.pdf [2017, July 27].

Mittal, A. 2017. An analytical study of present positions of Bitcoin. *International Journal of Reserch Granthaalayah.* 5(1): 386-394. [Online]. Available: http://granthaalayah.com/Articles/Vol5Iss1/34_IJRG17_A01_24.pdf [2017, July 27].

Nakamoto, S. 2008. *Bitcoin: A peer-to-peer electronic cash system* [Online]. Available: https://bitcoin.org/bitcoin.pdf [2017, January 21].

Nath, I. 2016. *Data exchange platform to fight insurance fraud on Blockchain*. IEEE 16th International Conference on Data Mining Workshops, 821-825.

O'Dair, M., Beaven, Z., Neilson, D., Osborne, R. & Pacifico, P. 2016. Music On The Blockchain. Technical Report 1, *Blockchain For Creative Industries Research Cluster*, Middlesex University, UK, July 2016.

Pazaitis, A., De Filippi, P. & Kostakis, V. 2017. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. *Elsevier, Technology Forecasting and Social Change,*124:185-204. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0040162517307084 [2017, July 20].

Pilkington, M. 2015. Blockchain technology: Principles and applications. *Research Handbook on Digital Transformations,*edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016, [Online]. Available: SSRN: https://ssrn.com/abstract=2662660 [2017, February 10].

Poelstra, A. 2014. *A Treatise on Altcoins.* [Online]. Available: https://pdfs.semanticscholar.org/5c38/f124040e664cd18a2f61e5dea4231e971d2d.pdf [2017, January 21].

Ratnasingham, P. 1998. The importance of trust in electronic business. *Electronic Business Research: Electronic Networking Application and Policies*, 8(4):313-321.

Reyesa, F.L., Zhangb, J., Royc, R., Andersend, D.F., Whitmoree, A. & Andersend, D.L. 2013. Information strategies to support full information product pricing: The role of trust Luis. *Information Polity,* 18:75-91.

Rogaway, P. & Shrimpton, T. 2004. Cryptographic Hash-Function Basics: Definitions, Implications, and Separations from Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In: Roy B., Meier W. (eds) Fast Software Encryption. FSE . *Lecture Notes in Computer Science*, Vol 3017. Springer, Berlin, Heidelberg.

Rogers, C. 2015. *Virtual authenticity: Authenticity of digital records from theory to practice.* University of British Columbia. [Online]. Available: https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/1.0166169 [2017, July 17].

Romney, M. & Steinbart, P. 2003. Accounting information systems. Prentice Hall, New Jersey.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. & Camerer, C. 1998. Not so different after all: A cross-discipline view of trust. *Academy of Management Review,* 23(3):393-404. [Online]. Available: http://amr.aom.org/content/23/3/393.full.pdf+html [2017, April 18].

Shrier, D., Larossi, J., Sharma, D. & Pentland, A. 2016. Blockchain & transactions, markets and marketplaces. *Massachusetts Institute of Technology, MIT Connection Science*, 2:1-10.

Skudnov, R. 2012. Bitcoin Client, Bachelor's Thesis (UAS) University of Applied Science, Degree Program in information technology. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/47166/Skudnov_Rostislav.pdf
[2017, July 18].

Sompolinsky, Y. & Zohar, A. 2013. *Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains*. [Online]. Available: https://eprint.iacr.org/2013/881 [2017, Jan 18].

Srisukvattananan, Y. 2016. Overview of Blockchain and possible use cases in the Thai payment system. B.A. Mathematics & Economics, Wesleyan University, 2016, MBA Tsinghua University. [Online]. Available: https://dspace.mit.edu/handle/1721.1/104513 [2017, July 27].

Stallings, W. 1995. *Network and internetwork security – principles and practice.* Englewood Cliff, New Jersey: Prentice Hall. [Online]. Available: http://wanguolin.github.io/assets/cryptography_and_network_security.pdf
[2017, April 13].

Steinauer, D.D., Wakid, S.A. & Rasberry, S. 1997. Trust and traceability in electronic commerce. *Information Technology Laboratory*, National Institute of Standards and Technology, Gaithersburg, 5(3):118-124.

Stoneburner, G., Goguen, A.Y. & Feringa, A. 2002. Risk management guide for information technology systems. *National Institute of Standards and Technology*. NIST Special Publication 800(30):1-41. [Online]. Available: https://dl.acm.org/citation.cfm?id=2206240 [2017, April 18

Swan, M. 2015. *Blockchain: Blueprint for a New Economy.* O'Reilly Media, Inc. United States of America.

Swanson, T. 2015. *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems.* [Online]. Available: https://pdfs.semanticscholar.org/f3a2/2daa64fc82fcda47e86ac50d555ffc24b8c7.pdf [2017, January 12].

Tak, S., Lee, Y. & Park, E.K. 2003. A software framework for non-repudiation services in electronic commerce based on the Internet. *Microprocessors and Microsystems,* 27:265-276.

Tapscott, D., & Tapscott, A. 2016. The impact of Blockchain goes beyond financial services. *Harvard Business Review.* [Online]. Available: http://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services [2017, January 26].

Vasek, M., Thornton, M. & Moore, T. 2014. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. *Financial Cryptography and Data Security, Vol 8438 of Lecture Notes in Computer Science.* Springer Berlin Heidelberg: 57-71. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-44774-1_5 [2017, September 10].

Velde, F.R. 2013. Bitcoin: A primer, *Chicago Fed Letter*, December 2013 Number 317. [Online]. Available: https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317 [2017, March 10].

Vukolić, M. 2016. The quest for scalable Blockchain fabric: Proof-of-work vs. BFT replication. In: Camenisch J., Kesdoğan D. (eds) *Open Problems in Network Security.* iNetSec 2015. Lecture Notes in Computer Science, Vol 9591. Springer, Cham 112-125.

Wayner, P. 1997. *Digital cash*, 2nd ed. San Diego, CA, USA: Commerce on the Net Academic Press Professional, Inc.

Weber, 1999. *Information Systems Control and Audit*, The University of Queensland, Prentice Hall.

Wilson, S. 2016. How to secure Blockchain technologies. *Constellation Research.* [Online]. Available: https://www.constellationr.com/research/how-secure-blockchain-technologies [2017, April 18].

Windsor, R. 2016. *Re-defining the meaning and scope of digital assets – part 1.* [Online]. Available: http://digitalassetmanagementnews.org/features/re-defining-the-meaning-and-scope-of-digital-assets-part-1/ [2017, June 16].

Wood, G. 2014. Ethereum: a secure decentralised generalised transaction ledger, in Ethereum Project Yellow Paper:1-32. [Online]. Available: http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf [2017, July 14].

Wright, A. & De Filippi, P. 2015. *Decentralised Blockchain Technology and the rise of Lex Cryptographia.* [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [2017, April 17].

Xu Xu, J.J. 2016. Are blockchains immune to all malicious attacks? *Financial Innovation,* 2:25. [Online]. Available: https://link.springer.com/content/pdf/10.1186%2Fs40854-016-0046-5.pdf [2017, August 14].

Yli-Huumo, J., Ko, D., Choi, S., Park, S. & Smolander, K. 2016. *Where is current research on Blockchain technology? –A systematic review.* [Online]. Available: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477 [2017, February 27].

Zheng, Z., Xie, S., Dai, H. & Wang, H. 2016. Blockchain challenges and opportunities: A survey. *Int. J.Web and Grid Services:*1-19.

[Online]. Available: http://inpluslab.sysu.edu.cn/files/blockchain/blockchain.pdf [2017, February 17].