

https://dspace.org/

An overview of blockchain technology in the South African financial industry

Maboe, Realeboga

2018

https://hdl.handle.net/10539/28592

Maboe, Realeboga Rebecca, (2018) An overview of blockchain technology in the South African financial industry, University of the Witwatersrand, Johannesburg, https://hdl.handle.net/10539/28592

Downloaded from a DSpace repository. https://dspace.org/

An Overview of Blockchain Technology in the South African Financial Industry

Realeboga Maboe

Student number: 350954

Thesis submitted in fulfilment of the requirements for the degree of

Master of Management in Finance and Investment

FACULTY OF COMMERCE LAW AND MANAGEMENT

WITS BUSINESS SCHOOL

UNIVERSITY OF THE WITWATERSRAND

Supervisor: Dr Blessing Mudavanhu

October 2018

DECLARATION

I, Realeboga Maboe, declare that the research work reported in this dissertation is my own, except where otherwise indicated and acknowledged. It is submitted for the degree of Master of Management in Finance and Investment at the University of Witwatersrand, Johannesburg, South Africa. This thesis has not, either in whole or in part, been submitted for a degree or diploma to any other universities.

	5 October 2018
Signature of student	Date

ABSTRACT

Blockchain, the new kid on the block, has the potential ability to change the way data are handled in the financial industry giving it a disruptive nature worthy of being explored and understood. However, not much is known and understood about these applications in the world, let alone in the South African landscape. The introduction of new financial innovations with the promise of being disruptive in nature always bring a sense of uncertainty and concern about the impact this new technology will have on the current way of doing things.

Due to its highly technical nature, Blockchain is yet to be fully understood by many who stand to benefit from adopting it. Apart from understanding how it works, its application is paramount to possibly bringing innovative changes to the financial sector. The mandate is to attempt to fully unpack the nature of the phenomenon with relation to financial innovation and to see the process by which it evolves or is experienced.

The purpose of this study is to provide an exploratory literature review of the full nature of Blockchain technology and bitcoin and investigate how the innovation evolved and is being experienced in South Africa. This will be done through looking at secondary sources with focus on the application it has as a new financial innovation within the financial industry in South Africa. This is still in the process of being done and begs the question of whether bitcoin is an important disruptive financial innovation which is here to stay in South Africa or not. The exploration aims to prepare a theoretical and practical basis for future studies.

Keywords: Bitcoin, Cryptocurrency, South Africa, Financial Innovation and Blockchain

TABLE OF CONTENTS

DECLARATION 1

ABSTRACT 2

LIST OF FIGURES 5

LIST OF TABLES 5

1. INTRODUCTION 6

1.1 Purpose 6

1.2 Problem Statement 7

1.3 Purpose of the Study 7

1.4 Research Question 7

2. LITERATURE REVIEW 9

2.1 What is Financial Innovation? 9

2.1.1 Financial Innovation Defined 9

2.1.2 FinTech 10

2.1 3 The Purpose of Financial Innovation 11

2.1.4 Success Factors 11

2.1.5 Brief Overview of History 12

2.1.6 Some Pros and Cons 14

2.2 The Different Types and Applications of Financial Innovation 16

2.3 The Drivers of Financial Innovation 19

2.4 The Future of Financial Innovation 20

2.5 Conclusion 21

3 BLOCKCHAIN UNPACKED 22

3.1 Overview of Blockchain 22

3.2 What is Blockchain? 24

3.2.1 Is Bitcoin a Form of Currency? 26

3.3 Where does it come from? 33

3.4 How it Works 33

3.4.1 Types of Blockchain (Access Control and Authorisation) 33

3.4.2 Data Structure 35

3.4.3 Ways to Obtain Bitcoin: Mining and Transactions 38

3.4.4 Consensus Algorithms 41

3.5 Players in the Blockchain Ecosystem 44

3.6 So What? 45
3.7 Some Advantages 45
3.8 Some Challenges 46
3.9 Conclusion 51
4 BLOCKCHAIN USE CASES 53
4.1 Overview of Potential Blockchain Uses 53
4.2 Conclusion 59
5 CONCLUSION 60
6 REFERENCES 62

LIST OF FIGURES

Figure 1: Financial innovations in the last 1000 years. Source: Ramakrishnan & Perumal (2008)..... 12
Figure 2: Financial innovations in the last 50 years. Source: Ramakrishnan & Perumal (2008)..... 13
Figure 3: Recent developments in the South African banking market. Source: Camarate & Brickmann (2018)..... 14
Figure 4: Price of Bitcoin in South African Rands (Coin Gecko, 2018) 31
Figure 5: Price of USD in South African Rands (South African Reserve Bank, 2018) 32
Figure 6: Price of USD in Bitcoin (Gold Price, 2018)..... 32
Figure 7: Bitcoin volatility time series charts (Buy Bitcoin Worldwide, 2018)..... 33
Figure 8: Blockchain contracts (Deloitte, 2017)..... 34
Figure 9: A chain of digital signatures (Deepika & Kuar, 2017) 37
Figure 10: An overview of how the transferring of Bitcoin works (Bistarelli & Santini, 2017)..... 41

LIST OF TABLES

Table 1: Top 10 Cryptocurrencies, as at 17 June 2017 (CoinMarketCap, 2017)..... 25

1. INTRODUCTION

1.1 Purpose

For the past few years, there has been a new term being thrown around in the financial world. A term which has raised eyebrows, caused concern and even excited those who heard it. Cryptocurrency. A word which is a combination of cryptography and currency. But what is this strange term, where does it come from and why do we even care? This has been a topic which has transcended disciplines ranging from economics and finance to engineering and computer science, where it all started. Maese (2014) put it well stating how cryptocurrencies are "a financial and technological innovation that integrates existing concepts about money, accounting, networks and remittances in one holistic invention".

This new phenomenon was not all that met the eye. There was a more powerful underlying technology driving cryptocurrency: Blockchain. Blockchain has been defined by the authors of Blockchain Revolution Don and Alex Tapscott as “an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value” (Storyful, 2017). Deloitte (2017) called Blockchain “a technology that allows people who don’t know each other to trust a shared record of events”.

The technology has been rising to the occasion for the past two to three years by shaking the world of financial innovation just as the first ATM did in the 1970s, if not by a greater degree. Blockchain has the potential ability to change the way data are handled across almost all industries giving it a disruptive nature worthy of being explored and understood. However, not much is known and understood about these applications in the world, let alone in the South African landscape, even more so in the financial industry.

It all started in 1998 when Wei Dai created the concept of "b-money" in a publication, an electronic money system which could be distributed and was anonymous. Nick Szabo followed suit with the creation of "Bit Gold". Similar to Bitcoin and other cryptocurrencies, it too was also an electronic currency system which needed the inclusion of proof-of-work with cryptographically published solutions (Sharma, Nisar, & Raina, 2017). Bitcoin was the first of the cryptocurrencies to be created by a group of people or person with the pseudonym Satoshi Nakamoto in 2008 (Vejacka, 2014). Nakamoto published a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" a year before Bitcoin was created.

A digital medium of exchange, bitcoin is based on cryptography where we find a decentralised, secure system for economic transactions (Vejacka, 2014). It is a combination of cryptography and virtual electronic money. The uniqueness of bitcoin comes from its self-regulating nature, where no third party, be it government or institutions, have any control over the system. This is completely opposite to fiat money which is mainly controlled by central banks. The system

allows users to control their own accounts on their own computer or mobile phone, eliminating the need for a bank. Nigam (2016) mentioned that one of the commonalities regarding electronic payment systems is the existence of trusted third parties who process transactions. This is not the case with bitcoin, testing the boundaries of trust. It has, however, been shown that the complexity of the system makes it tamperproof and very secure to use (Sharma, Nisar, & Raina, 2017).

As an ever-evolving country, South Africa has also jumped onto the bandwagon of using Blockchain and even more so of adopting bitcoin. However, to understand this technology, one needs to delve into the theory of financial innovation.

1.2 Problem Statement

The introduction of new technology with the promise of being disruptive in nature always brings a sense of uncertainty and concern about the impact that this new technology will have on the current way of doing things. In a world where financial innovation is slowly becoming the norm, it is increasingly important to understand these new innovations with regard to the greater financial industry and some of their potential results. Blockchain has stirred the world with its introduction in 2008. Due to its highly technical nature, Blockchain is yet to be fully understood by many who stand to benefit from adopting it. The recent need for organisations across the world to gain insight on what Blockchain is has been rapidly increasing, with South Africa not being an exception. Apart from understanding how it works, its application is paramount to possibly bringing innovative changes to the banking sector. The mandate is now to attempt to fully unpack the nature of the phenomenon with relation to financial innovation and see the process by which it evolves or is experienced. This is still in the process of being done and begs the question of what the future with Blockchain will look like in South Africa. This remains a very contentious issue.

1.3 Purpose of the Study

The purpose of this study is to provide an exploration of the full nature of Blockchain technology and bitcoin and investigate how the innovation evolved and is being experienced in South Africa. This will be done through looking at secondary sources with focus on the application it has as a new financial innovation within the financial industry in South Africa.

1.4 Research Question

In fulfilling the purpose of this study a few research questions will be the focus:

a) What is the full nature of this financial innovation- Blockchain and bitcoin?
b) What is the process by which Blockchain evolves or is being experienced?

c) How will this financial innovation shape the South African financial landscape in future- is Bitcoin an important disruptive financial innovation which is here to stay in South Africa?

This paper is an exploratory literature review which derives insights, trends and gaps from literature review and desk (more so online) research of current business press papers, professional and academic reports, literature from journals, blog commentaries, company web pages pertaining to Blockchain technology with bitcoin used to explain the technology's most well-known application in finance (Nowinski & Kozma, 2017). In this way, the paper is aimed to prepare a theoretical and practical basis for future studies.

Due to Blockchain's immaturity, the sole use of journal articles would have limited the scope of the paper. To expand the needed knowledge, other secondary sources were employed in an exploratory manner including topic related magazines, blogs, professional consulting companies, conference papers and reputable newspapers for their reports. The need for these extra resources was to expand on what journals have already cited as use cases for the technology as well as to ensure that the most up-to-date information around the ever-changing technology was cited.

The paper will be structured as follows: Chapter 2 will look at a literature review around the theory of financial innovation then Chapter 3 will expand on literature about Blockchain and bitcoin. Chapter 4 will explore some of the available use cases followed by Chapter 5 which will conclude and offer some recommendations for further studies.

2. LITERATURE REVIEW

"You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990s"

– Blythe Masters, former JP Morgan Chase CFO

There are a multitude of research papers which have been attempting to address the issue of financial innovation. Many of the recent ones have mainly focused on how financial innovation was a contributor to the global financial crisis of 2008. There are many financial innovations, but in this research, we carefully examine bitcoin which is a new instrument in the financial markets. In order to understand this new innovation, it was important to understand what financial innovation is as a starting point.

Bitcoin and its counterpart, Blockchain can be regarded as financial innovations as per definitions in literature which will be examined in this chapter.

2.1 What is Financial Innovation?

1s Bitcoin an important disruptive financial innovation which is here to stay in South Africa? This is a question which this paper is attempting to explore. However, in order to delve deeper into understanding and answering this question, it is important to first understand what financial innovation is and how it ties in with bitcoin.

We are living in the information age where information is power and financial innovations often come with technological advancements which make information fast and easily accessible like the likes of internet banking and the ATM. Innovation is an important business process enabling effective competition in business (Ramakrishnan & Perumal, 2008.

2.1.1 Financial Innovation Defined

Financial innovation has many definitions, with each author attempting to refine the definition according to their needs. There is yet to be a consensus to the meaning of financial innovation as will be shown in this section.

One of the earliest definitions of financial innovation was by Schumpeter (1934) as cited by Basarir and Sarihan (2017) who defined innovation as: "the implementation of a new or significantly improved product (good or service), or process, a new marketing method, or a new organisational method in business practices, workplace organisation or external relations". The authors further went on to look at the determinants of financial innovation and attempted to provide basic information about measuring financial innovation through reviewing other works on the subject, along with a statistical analysis using data of the interaction of banks in Turkey with financial innovation.

Ben-Horim and Silber (1977) defined financial innovation as any new innovation within the product or process space which warrants patent protection. Salampasis and Menntion, (2013) went deeper by defining financial innovation as the link between sustainable development and the financial sector. They have stated that financial innovation "embraces changes in the offerings of banks, insurance companies, investment funds and other financial service firms, as well as modifications to internal structures and processes, managerial practices, new ways of interacting with customers and distribution channels".

Financial innovation is about understanding the needs of the customer and being different from the competition. Personal offerings are created, with focus on the customer if it is within the bounds of regulation and any other constraints. It is evolving to gear up for the future, it is about choices and prioritisation (Salampasis & Menntion, 2013). This is further explained by how it popularises new financial instruments as well as financial technologies, institutions and markets. It is a combination of advances in technology for improved access to information, means of payment, trading along with that of emerging new financial services and instruments. Lewis and Mizen (2000) are cited as associating financial innovation with what customers require over time, changing requirements of suppliers, policy and environmental conditions along with technology.

Anther view noted by the author for some narrower definitions which hold more for product innovations (which is not so much our focus) include being a completely new solution or a combination of a traditional financial instrument where new elements are incorporated to improve the instruments liquidity and increasing potential applications. The product can substitute a traditional financial instrument by improving the finances of the business employing the new product. The product should be able to be used irrespective of which segment of the financial market it is used in and can be used in new financial processes or strategies that mainly use this new product.

Lastly, financial innovation describes any form of change in the scope, scale and delivery of financial services.

2.1.2 FinTech

Schindler (2017) attempted to answer why "FinTech" (financial technology) is happening right now as well as why it is getting more attention than what traditional innovation usually receives. These questions are answered by introducing the concept of the "depth" of innovation and show that the greater the impact innovation has to transform financial services, the deeper the innovation. The author defined depth by splitting it into surface innovations, genuine innovations and foundational innovations. The fundamental nature of products and services does not change in surface innovations. Genuine innovations, on the other hand, change the fundamentals such as with credit default swaps which allowed investors to hedge and value credit default risk of a company for the first time. Lastly, foundational innovations go as deep as changing the

infrastructure and parts of the financial system. This occurs very rarely and includes the creation of the banking system and banks.

Evidence of the high interest in FinTech in South Africa is seen by the creation of an innovation policy framework to be implemented in 2019 (Intergovernmental Fintech Working Group, 2018).

FinTech has the potential to remove market inefficiencies in the future. The exponential growth in technologies including Blockchain, distributed ledgers, cloud computing, big data, application programming interfaces and emerging alternative internet-enabled platforms show what the future has in store for the financial system. Some of these platforms are growing at rates which are becoming too big to ignore (Intergovernmental Fintech Working Group, 2018).

2.1 3 The Purpose of Financial Innovation

Financial innovation's aim is to reduce the cost of offering different services and products by the financial system and make them more available to clients for improved quality for long-run sustainable growth. This aim helps define financial innovation as a new thing which reduces risk and costs or provides an improved service or product or instrument to better meet the demands of participants.

Financial innovation's main purpose is to introduce financial intermediation where it would not have happened before, for example the option hedge funds gave endowments and pension funds to rival the once traditional options of stocks, bonds and cash. Access to credit, increased choice and lowered costs have been the fruit of financial innovation.

Innovation shapes human society at different levels, most of which still needs to be researched to see what its social value is. Financial innovations which change the core function of the financial sector (moving of funds from surplus to lack at a rewarding level) create value, often by making credit more readily available (Johnson & Kwak, 2011). As mentioned by other authors, financial innovation is often used to maximise firm profits and for protecting market participants from risks which arise from unfair transactions.

2.1.4 Success Factors

Those who create these innovations, always hope that they will succeed. Since innovation is not costless, a systematic approach is needed for innovation and not the trial and error approach which some innovators have primitively been using. In order to have a sense of what successful implementation of financial innovations looks like, a measuring method is needed. It is common that most innovators innovate for increased profits, so ceterus parabis, a successful innovation ought to show directly or at least be correlated to the coveted profits. Another proxy for success which can be used is measuring the popularity of the innovation. An example for using popularity as a yard stick is if trading volume is used to measure popularity of a new security.

Factors which can affect success, as mentioned by Flood (1992), are finding insight in the demands of potential users and finding whether there already exists a potential substitute to rival

the innovation. Unfortunately, it is nearly impossible to codify all the elements of a successful innovation into a collection of rules.

Aligned with the success of financial innovation is its diffusion. It is found that the faster the diffusion, the more immediate the impact is, resulting in a higher social return on the initial investment. Financial innovation depends upon innovation users and customers for diffusion and how the pay-offs will impact the innovators and society as a whole.

2.1.5 Brief Overview of History

The South African financial system finds its roots in the discovery of diamonds and gold. Their discovery and the growing mining industry transformed the economy of the country. Diamonds in South Africa were discovered in the 1830s. The consolidation of the diamond mines saw the humble beginnings of the financial system in South Africa, entrenching the imperial banks and introducing the development of publicly listed companies and a growing stock market. The first merchant bank in the country was created by one of the major mining-finance houses, Anglo American Corporation in the 1960s (Mckenzie, 2016).

The chronicles of innovation can be organised to show the history of finance, globally as shown in figure 1 and 2 below.

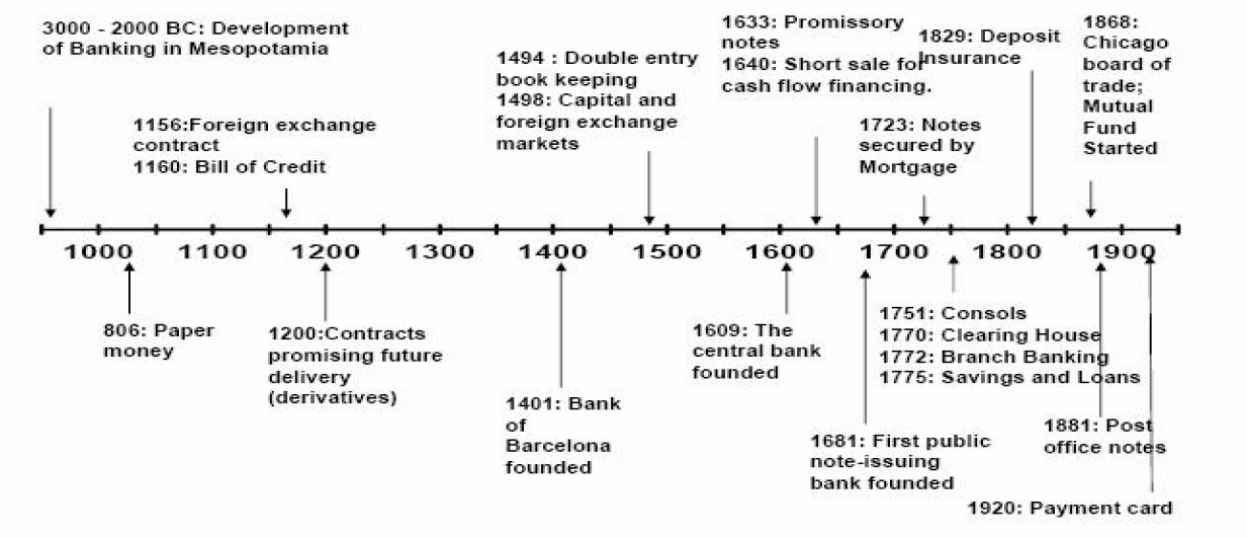


Figure 1: Financial innovations in the last 1000 years. Source: Ramakrishnan & Perumal (2008)

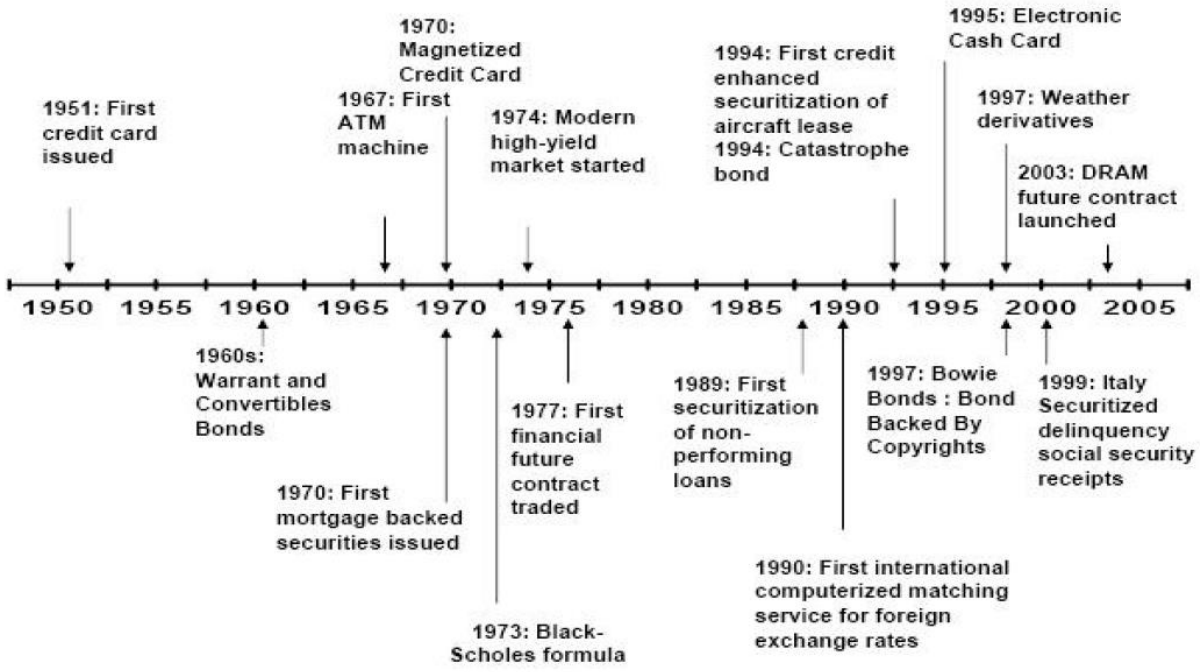


Figure 2: Financial innovations in the last 50 years. Source: Ramakrishnan & Perumal (2008)

The beginnings of financial innovation can be traced as far back as the first use of money in exchange for goods and services thousands of years ago. One can note that after the 1970s, the rate of innovation quickened with focus on new legal instruments (from deregulation and financial liberalisation) and institutional changes. Technical innovation (such as the introduction of ATMs) had taken a back seat at this stage. The mid-1990s saw in increasing role of the internet, mobile phones, personal computers and other new forms of digital services (Dabrowski, 2017).

From cheque books to cash and now to business ecosystems and lifestyle solutions, banking has been evolving. The level of agility of banks has been increasing as they have their minds set on using innovative technology to improve clients' lives. Fintech (financial technology) has become the norm for banks as they fight to remain relevant in an ecosystem which is no longer solely closed off to financial institutions (Alkema & Chen, 2016).

To bring it home, even South Africa saw some financial innovations coming from our local financial services. One is able to see some of the progress made over the last two decades. It is important to note that South African banks are dynamic and relatively well capitalised and that they constantly pursue banking practices which are innovative. It is safe to say that the banking sector in South Africa is one of the most sophisticated worldwide and already encourages world-class innovations in its products and services. Even with this being the case, Blockchain

innovation research in South Africa, as with other economies globally, is still in its infancy (Intergovernmental Fintech Working Group, 2018).

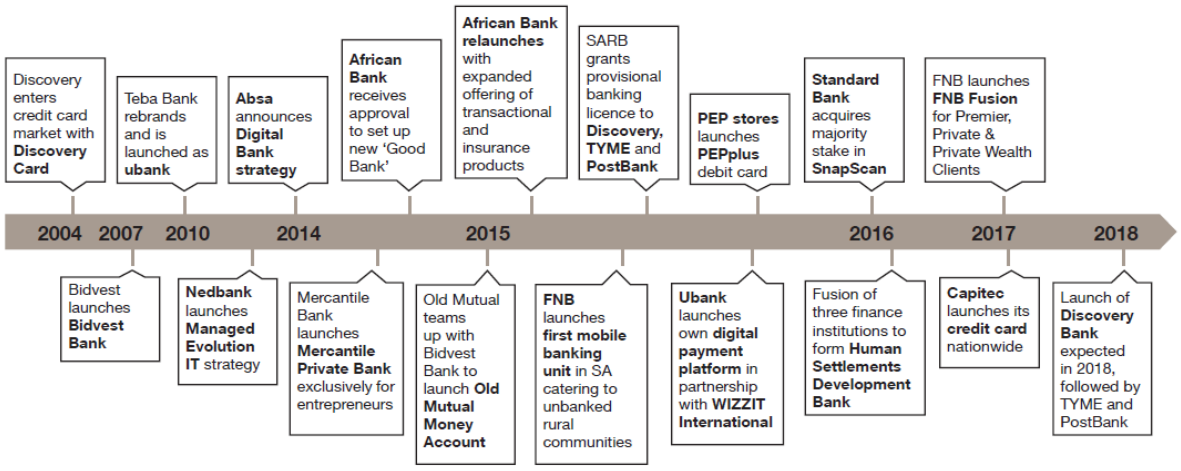


Figure 3: Recent developments in the South African banking market. Source: Camarate & Brickmann (2018)

Recent trends in financial innovation and their meaning for the financial sector were investigated by Dabrowki (2017) with a focus of their effect on monetary policy. To our knowledge, no other similar research has been done in South Africa around financial innovation, apart from looking at it regarding monetary policy.

One of the trends which have been occurring in the South African banking landscape has been the appearance of digital solutions offering low-cost models for operations which have been providing better customer experiences (Camarate & Brickmann, 2018).

Other examples of progress include African Bank's drive to offer a fully digital transaction bank. Commonwealth Bank of Australia's subsidiary, TymeDigital, is gearing to offer customers access to funds through mobile phones. The offering of banking solutions geared towards the various taxi associations, could disrupt banking as it is a R40-billion industry requiring funding which is now offered at high rates by traditional banks (Camarate & Brickmann, 2018).

Banking will always be needed, but the traditional meaning of banking is fast moving to accommodate tech savvy, flexible, price sensitive millennials and other who prefer all their needs met via their smartphone (Alkema & Chen, 2016).

2.1.6 Some Pros and Cons

Bara et al (2016) touched on the double-edged nature of financial innovation, having a "good" and "bad" side. Financial innovation of the right kind assists banks to invest in technologies that ensure that they fulfil their intermediary roles and in doing so drive growth. It reduces costs and improves capital productivity. One can see the effects of financial innovation through its positive impact on the economy through creating jobs and thus personal income being used to buy goods

and services which grow the economy. This shows how innovation and job creation are positively related. Some literature has shown that there is a positive correlation between financial innovation and economic growth, although the growth rates to this effect are yet to be researched in South Africa. Bara et al (2016) went on to attempt to empirically study this relationship in the SADC region using Autoregressive Distributed Lag Model and found a weak positive relationship. The positive side of it includes venture capital opportunities and equity crowdfunding which is still in its infancy and overall global welfare (Mendes-Da Silva, 2015).

One result of financial innovation is economic freedom which is the level in which institutions can guarantee not being affected by coercion from government, production constraints, distribution or the consuming of goods and services beyond the extent needed for citizens to maintain and protect liberty itself. Advances in data processing and telecommunications have pushed financial innovation which has now changed bank offerings and their production processes. Frame and White (2014) mention multiple studies which have shown the positive view of financial innovation.

Financial innovation, like everything else in finance, has been found to have a "dark side" such as increasingly complex transactions and products. Apart from what research shows is the case with the global crisis of 2008, it also includes industries experiencing higher growth volatility. The financial crisis has been cited as being instigated by financial innovation, which can be argued was the reason cryptocurrencies were created in the first place (Sukamulja & Sikora, 2018). Product innovations seen in the past decade have been collateralised debt obligations (CDO), negative-amortisation, credit default swaps, synthetic CDOs and many more. These were the accused culprits for the financial crisis, depending on which fence you sit on.

The financial crisis has raised concerns around trusting banks. Blockchain is leveraging off this insecurity to gather momentum. Emerging market banks cannot do without innovation. Millions of unbanked new entrants who need new ways of doing business have created a market which cannot be ignored by traditional financial institutions. The disruptive pace needs the network effect to continue its momentum (Alkema & Chen, 2016).

With a lack of innovation in an economy, businesses opt for cost cutting methods for short term financial gains, with retrenchments being one of the leading ways to cut costs for firms (Hausman & Johnston, 2014).

The one other dark side of financial innovation to be considered is how it is able to undermine poverty reduction, especially in a developing country like South Africa, where financial activity and development increases but the effect can be open markets which can increase the gap between the poor and the rich, effectively harming the poor (Buckley, Arner, & Panton, 2014).

Some products arguably increase asymmetric information issues, increasing moral hazard. There have been studies (including Idun and Aboagye cited by Bara et al (2016)) which have shown a

negative relationship between financial innovation and economic growth in the long-run but a positive one in the short-run in Ghana.

One of the challenges brought on by financial innovation is how it has made it more difficult to interpret financial data since the sensitivity of data is more likely to be changed by financial innovation. This causes a profound effect on the operation and structure of the financial system. There is an element of trial and error involved in implementing financial innovation, where failures can be costly where innovations have been diffused widely (Frame & White, 2014).

Competition is created by technological innovation in business. When this goes wrong through being exploited and applied to financial systems, we have seen failed financial strategies on an enormous scale. The scale of financial fraud is exacerbated by technological innovation in financial techniques and the internet (Betz & Khalil, 2011).

2.2 The Different Types and Applications of Financial Innovation

Financial innovation is used to complete incomplete markets, respond to regulations and taxes, stimulated by technological shocks, minimize costs, look at solving agency concerns and information asymmetries and responding to risk and globalization (Ramakrishnan & Perumal, 2008).

In further understanding what financial innovation is and some of its uses, this section surveyed literatures pertaining to several specific financial innovations that have appeared over the past 30 years or so that were specifically driven by technological change.

Some of the greatest needs in the African financial system are mobile money transfers, financial inclusion and improving remittances which in turn will generate increased economic activity. All three can be and are being solved using financial innovation which can be differentiated by dividing them into radical and incremental where radical innovations includes updates to risk management by including new risks.

A few scholars, amongst them Basarir and Sarihan (2017), have grouped innovation types into process, product, organisational and marketing. Sukamulja and Sikora (2018) further expanded these groupings into five classifications: new financial markets (insurance derivatives), new financial intermediaries (venture capital funds), new financial services (e-banking or e-trading), new financial instruments, and new financial techniques (leverage buy-out and Value at Risk).

To further show the lack of consensus in definitions in the financial innovation world around financial innovation, another classification which is aligned with the other previously mentioned authors is by Blach (2011) who citied J. Schumpeter. Schumpeter grouped various innovations through technological means as being: (a) new methods of production, (b) new products, (c) new sources of supply of raw materials, (d) the opening of new markets, (e) new methods of management and (f) new business structures and organisational forms. The OECD went on to use Schumpeter's work to develop four innovation groups namely marketing, process, product and business organisation (which are the exact groupings found by Basarir and Sarihan (2017)).

These developments are only seen as innovations if they are seen as new for the organisation or group implementing them, whether previously known by the market or not.

Another view of categorising financial innovations mentioned by the author are (a) process innovations, (b) product innovations and lastly (c) innovations which enable risk-shifting (Blach, 2011).

Blach (2011) noted that there are various groupings which in turn perform various functions, which should also be classified. They mapped the functions of these innovations to those of the financial system assuming that the very nature of innovation is to increase efficiencies in the financial systems enabling it to perform its functions.

There are six core functions alluded to by the author and they are:

a) Risk management,
b) Aggregating of resources,
c) Combating issues with incentives due to agency relationships and asymmetric information,
d) Using price information to make financial decisions,
e) Economic resource transfer across industries and borders,
f) Trade facilitation through settling and clearing of payments.

These functions form the core of the financial system with the main role of the system being moving funds from surplus to areas of deficit. For this to occur, certain qualities are needed including efficiencies, integrity, transparency, reliability, liquidity and innovativeness. The two qualities which stand out for this paper are transparency (how transactions are concluded, and their information shared) and efficiency (where transactions can be made with the lowest costs possible and all participants have the same access to information that matters to their decisions).

Contrary to Ben-Horim and Silber (1977) who focused on discussing product innovation, this paper will focus on process innovations (as named as a classification of financial innovation by Blach (2011)). Of the types of innovations, bitcoin can be found to fit in with “process innovation”. Innovation in the process section of the banking world mainly refers to advances in how clients access their accounts and any new ways of making payments for meeting the customer needs for ease and convenience.

Some process innovations in financial system in the past few decades have now become the norm; these include variations of derivatives, funding mechanisms (such as private equity and venture capital), credit offerings and payment options. The application of FinTech is wide ranging from delivery channels, electronic payments, peer-to-peer lending, automated advice and cybersecurity to name a few (Intergovernmental Fintech Working Group, 2018).

i. ATM

Automatic Teller Machines (ATMs) have been cited as been one of the biggest innovations in the financial world. Introduced in the early 1970s with relatively fast diffusion in the 1980s, they forever changed access of accounts by customers by creating 24/7 access to all.

ATMs came about in an attempt to alleviate the pressure of ending business hours in Europe along with restrictions to expand branches in the US. It took about 18 years for their implementation from the time the idea was generated and had a host of innovators collaborating to make it how it has come to be known today (Arthur, 2017).

ii. Debit Cards

The cards used in early ATMs transformed into the now widely used debit cards which have the added functionality of being able to make payments at a point-of-sale. Seen as "pay now" instruments linked to cheque accounts, debit cards require a pin to access the users' information instantaneously be it online, at an ATM or at a point of sale. Research around debit cards is focused on the probability of users taking it up (demand side research). Frame and White (2014) looked at these papers and their results.

iii. Online Banking

Online banking saw its creation from the need for remote access. It all started with telephones then moved to personal computers and now to mobile phones. Online banking has allowed customers not only to know what is going on in their accounts but also to make payments and transfer money as they pleased. The creation and adoption of the internet in the late 1990s made commercial banks take up this technology and by 2012 over 90 percent of commercial banks offered online banking to their clients. Frame and White (2014) also looked at the literature around online banking and found that the focus was on attempting to understand what determines bank adoption and how it affected the banks' performance and some demand side studies.

iv. Payment Options and Providers

Payments have seen a host of disruptions in the past few years. In the payments or money transfer realm, the likes of Shoprites Money Transfer enable remittances to be sent from South Africa to other African countries.

PayFast, a payment provider in South Africa, already has 30 000 online websites which use bitcoin as a means of payment. Johannesburg has seen innovative Blockchain work being done, with start-ups based in Sandton at the Alphacode workspace, working on solutions for a virtual stock exchange to be based in the Maldives. Apart from Blockchain, the likes of PayPal and SnapScan have been launched. Banks benefit with these innovations by partnering with them, for example Standard bank with SnapScan in 2013 and First National Bank with PayPal in 2010. UnionPay, China's sole domestic bank card organisation, has partnered with Barclays Africa in 2016 (Alkema & Chen, 2016).

v. Blockchain in the Form of Bitcoin

The creation of cryptocurrency and a digitised system could be the new "ATM" of financial innovation. This technology will be fully unpacked in the next chapter.

2.3 The Drivers of Financial Innovation

Certain factors can be heralded for contributing to innovative success as found by Hausman and Johnston (2014) to curb the relatively low levels of current innovation. It is known that to foster a competitive environment, innovation is key. Global competition has been cited as a factor which affects financial innovation along with financial system integration.

A brief look at these factors is important in understanding whether blockchain and bitcoin will be successful in South Africa (if we strip away some of the challenges that first need to be overcome by the country) by avoiding these factors which account for poor levels of innovation.

The three main factors mentioned by the authors are funding, education and competitive factors:

a) Funding

Capital is needed to ensure that there is consistent research being done in the field of financial innovation. Although not only focused on government providing the funding for this research, financial institutions have brought it onto themselves to also invest in research not only for themselves but for the industry at large. Other parties have also been involved in financial innovation research ranging from research groups, universities, incubators, focus groups and other private players.

b) Education

It is imperative that the next generation of innovators are groomed to take over. Training, be it in formal educational institutions or on the job, needs to be on par with the innovation we hope to have in future. The educational system will need to be changed to adopt to changes in technology.

c) Competitive factor

Globalisation and increased competition have put pressure on firm profitability. The need to be the best has made the rate of innovation needed higher than ever before. This has caused adoption of innovation to also increase, for example the radio reached 50 million users in 38 years as compared to television taking 13 years, four years for the internet and three years for the iPod and just a year for Facebook. Business needs to constantly be innovating to remain relevant.

Wall (2014) found regulation and technology to be the two main drivers of innovation, especially in looking at the future of financial innovation. Financial services work in a highly regulated environment. These restrictions have pushed them to innovate to overcome these restrictions to reduce regulation cost. This was said to be the case in the financial crisis where prudential

regulation was circumvented by financial innovation creating riskier banks. This broke down old rules and helped increase competition, although to the detriment of the whole financial system of the world. Technology has always been one of the biggest drivers to innovation. With the invention of the ATM in the 1960s, the evolution of banking has never been the same. The likes of debit cards, smart cards and automatic bill paying has improved the customer experience in ways never thought of being possible. Data manipulation is now made easier by advances in information technology, and now statistical models are being employed for risk management and complex valuation formulas.

Ramakrishnan (2015) has noted competition and regulation as the two basic financial innovation drivers resulting from barriers faced by financial institutions in attempting to reach their financial goals. He concluded that it takes an element of risk taking and creativity to be innovative. He also agreed that financial innovation occurs as a result of the need of greater profits thus searching for new ways to increase these profits.

2.4 The Future of Financial Innovation

The rapid speed of innovation in the technological space is set to change the financial industry and financial services if it continues at this innovative pace. This can be attributed to being due to globalisation, economic growth, deregulation and even more so due to the advances which have been made in Information and Communication Technology. The increases in innovation will be the case even more so if we do not experience another financial stability shock, financial innovation will see its importance grow over the next several years. One can already see the trajectory of the financial service within the next two or so decades where exclusively online service renderings will be the norm, where brick and mortar banks will have disappeared on a large scale and electronic payments and transfers will be more developed. The future of financial innovation sees our ability to process, obtain and store information advancing, piggy backing off further information technology advancements.

This bring to question whether current financial institutions will survive this exponential increase in competition, where new non-banking entrants have been shaking up the industry. The lack of legacy infrastructure issues such as those found in the banking sector allows new player to enter the market at lower costs to customers using technology (Camarate & Brickmann, 2018). The entry of non-banks to now offer banking solutions to customers has been on the rise. These non-banks enter the market with little or no risk but with limits to what they can offer due to regulation. It is currently unheard of to allow non-financial newcomers to one day completely take over the market due to the need for certain practices to be regulated, but it is guaranteed that the current business model employed by traditional financial institutions will look completely different in the coming years (Dabrowski, 2017).

Financial innovation is projected by Daborwski (2017) to continue to revolutionise the financial sector as it has been doing for the past half century, but at a faster rate and with more sophistication. What the future needs is for increased simplification and transparency- lessons

learnt from the financial crisis. The argument then is whether innovation by non-banks is a good idea or not. Wall (2014) makes a case for it on condition that enhancing competition is its primary consequence.

Apart from the new non-banking players, we see "disintermediation" where the middleman (mediators, brokers) is fast increasing and big implications for financial transactions might be seen. The Khatoon and Fiyazi (2016) looked at financial innovations which have a glimpse of what the future with disintermediation will look like touching on mobile payment systems and cryptocurrency sidechaining; it is a phenomenon worth keeping an eye on since even traditional banks play an intermediation role which might now be at risk of one day completely disappearing (in its traditional sense).

2.5 Conclusion

The discussed authors have shown how financial innovation can generally be defined using a narrow approach or broad approach. The narrow approach encompasses any new developments which are completely new, combinations of traditional instruments with new elements, any existing instruments being applied in a new way etc. The broad approach includes any new developments for every element found in the financial system (regulators, instruments, institutions and markets) (Blach, 2011).

One thing is for sure, financial innovation cannot be stopped for as long as finance and money still serve human life. Another crucial question is how FinTech will shape the financial landscape going forward. Regulation is a forerunner in literature for driving financial innovation as players try find ways to circumvent the laws without breaking them in order to maximise their profitability, increase market share and meet the ever-changing needs of their customers.

It is important to constantly seek to balance the globalisation of finance while improving the benefits yet minimising risks. Understanding the foundations of financial innovation can open avenues to understand this.

The research regarding the features and definitions of financial innovation are not necessarily new. As new innovations enter the financial world, it will be interesting to see how financial innovation evolves.

3 BLOCKCHAIN UNPACKED

"In future, it might seem just as strange to say that I am trusting a third-party institution with my interests as to say that I am using an abacus today"

- Gavin Wood- Ethereum Co-Founder

3.1 Overview of Blockchain

One of the financial innovations developed after the financial crisis was the rise of digital currency also called cryptocurrency. Khatoon and Fiyazi (2016) touched on cryptocurrency sidechaining in their paper which looked at financial innovations which showed a glimpse of what the future with disintermediation will look like. Vora (2015) concluded to note that cryptocurrencies are a welcomed development in the financial field. Of the types of innovations, cryptocurrency can be found to fit in with "process innovation". Innovation in the process section of the banking world mainly refers to advances in how clients access their accounts and any new ways of making payments for meeting the customer needs for ease and convenience. The focus will be on bitcoin and Blockchain which covers the "making of payments" or transactions element of process innovation.

Cryptocurrency along with Blockchain, its underlying technology, have been the talk of the town for the past few years since it became public in 2008. Many have applauded the Blockchain technology as one of the top technological innovations seen in the 21st century. It is only in recent years where it is being discovered that it transcends its main use for managing transactions within the financial world. This technology has unlocked the potential to not only disrupt but reshape a plethora of sectors, above and beyond its economic benefits, with focus on consumer-to-consumer interactions. The revolution of the internet is small in comparison with what can come out of Blockchain in terms of its transformative power. Blockchain not only uses the internet but allows one to transact (Kloete, 2017). Blockchain has often been referred to as the "trust machine", after the low levels of trust in the banking sector arose after the financial crisis of 2008. Even with these current breakthroughs, many practitioners and researchers struggle to conceptualise the true potential of Blockchain.

Blockchain has been described by Swan (2007) as an "append-only tamper-resistant database". The terms distributed ledger technology and Blockchain are sometimes used interchangeably. The general form is described by the term distributed ledger whereas Blockchain is the specific form. The key features of a distributed ledger include being updated by a consensus mechanism, the leaving of a tamper-proof historic audit trail, having a shared network database of transactions and having a unique cryptographic signature for each record with timestamps.

There were a few drivers one can speculate on around why this technology was developed. One of these drivers was a response to the ever-increasing fall in confidence in the soundness of

government-backed 'fiat' money (Shah, 2013). Other drivers which have pushed for the adoption of Blockchain include the need for cybersecurity. With credit card fraud and other similar instances where customer data is compromised, the need for cybersecurity is high. The needed level of trust is placed on a network system which is computationally smart instead of the traditional third parties. Another already mentioned driver was the 2008 financial crisis which saw the need of trust in the financial world needing to be restored.

Bitcoin is defined by dictionary.com as "a type of digital currency that uses state-of-the-art cryptography which can be issued in any fractional denomination and has a decentralized distribution system". Cryptocurrency, the umbrella under which Bitcoin falls, on the other hand was defined as "a digital currency or decentralized system of exchange that uses advanced cryptography for security" by dictionary.com. Cryptocurrency is a combination of cryptography and currency where cryptography is similar to the art of writing in code or cypher where data can be stored or transmitted in any form allowing it to only be read and processed by its intended users.

The recent surge in the popularity of bitcoin has garnered the attention of business professionals and academics alike unlike any other cryptocurrency. However, most of the discussions about bitcoin have been confined to computer science literature or the blogosphere with almost no academic research devoted to the economics of bitcoin.

In so far as research is concerned, many of the current literature continue to focus on use case analyses and dissecting the proof of concept prototypes. Fields such as computer science and mostly finance have been the focal point thus far in trying to understand this technology. Blockchain should never be looked at as a standalone product but rather as one which complements other products and services. Some applications for the Blockchain technology are applied to supply chains and public administration. The most well-known and first application of Blockchain was with cryptocurrencies with bitcoin being the most popular.

Blockchain will not only affect technological use but relationships and the way parties interact ranging from individuals to organisations, to business-to-business interactions, the transparency of processes and data, and, finally, it will spread to productive levels of the economy and change its sustainability. One example is seen with the many electronic sites popping up to facilitate the trade of other cryptocurrencies with bitcoin; liquidity and conversion rates have increased (Deepika & Kuar, 2017).

The heralded Blockchain technology differs in its packaging. Many independent Blockchains have been introduced in recent years but none are yet to reach the large scale seen with bitcoin. These other Blockchains offer different benefits ranging from improved data capabilities, faster speed and new consensus mechanisms. Blockchain tokens have introduced a new asset class, although currently still seen as high risk by investors. It is argued that cryptocurrencies such as bitcoin perpetuate the perception of high risk due to volatile prices. Investors have noted

cryptocurrencies price movement's non-correlation to traditional assets, making them ideal for investment diversification. Their high level of liquidity and accessibility is a bonus.

With the Blockchain Africa conference held in March 2018 in Johannesburg, it is without a shadow of doubt that South Africa will be one of the African market leaders around the development of Blockchain. This gave more reason to focus on the technology in South Africa by looking at it through the lens of what has already been done across the world. The concept of peer-to-peer or even business-to-business is revolutionary (Kloete, 2017). The man on the street will be able to contribute to the economy in ways which they have never been allowed to before. In a country where the majority of the economy is controlled by a few, this has the potential to be a game changer in the spreading and accumulation of wealth going forward.

3.2 What is Blockchain?

Many have had their stab at describing what Blockchain is. Tapscott and Tapscott have defined it as “an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value”. Some enthusiasts have called it the new internet which is a distributed ledger which works as a "consensus of replicated, shared and synchronised digital data spread across multiple locations globally, without a central administration or data storage" (Nihilent Technologies, 2017). According to the Bank of England, Blockchain is “a technology that allows people who don’t know each other to trust a shared record of events” (Garfinkle, 2017).

To explain how Blockchain operates, the focus will be on bitcoin since Blockchain forms the backbone as it is the underlying technology powering bitcoin. This technology can be thought of as working like email. It can be used by anyone, yet not a single company oversees it (Garfinkle, 2017).

The programmable nature of Blockchain allows for instructions to be embedded into blocks. Instructions such as “if” this “then” do that “else” do this make it possible for transactions or other actions to be executed when certain rules are followed (Deloitte, 2017). It allows for verified transactions to become permanent, secure, verifiable and irreversible on the Blockchain. 120,000 transactions on average are added to the Blockchain every day and Bitcoin is now actively traded against 30 global currencies (Cheung, Roca, & Su, 2015).

Bitcoin falls under one of the many applications of Blockchain, it being the first application. But what is bitcoin? Bitcoin is an open source project created using the proof-of-concept principle allowing transactions to be processed securely by a decentralised peer to peer network. This new financial innovation brought with it solutions to traditional payment disadvantages including double spending or chargebacks. Transactions are pseudonymous and not anonymous since the bitcoin addresses are pseudonyms for real users (Bistarelli & Santini, 2017). Double spending and chargebacks were averted through using signed encryption keys reducing fraud risk

experienced by merchants. As a recent technology, it unfortunately did not get spared malicious attacks coming in the form of end user targeted attacks, data breaches and even government sponsored regulation (Heid, 2017).

Digital currency is a medium of exchange that is stored electronically in a series of bits (0s and 1s) stored in a computer file. Importantly, this includes national fiat currency stored electronically in a bank account. Under this broad definition, over 95 percent of the world's currency in circulation is stored in digital rather than physical (i.e., cash) form. (Desjardins 2015). Bitcoin falls under a broad spectrum of virtual currencies which are a subset of digital currency that is not issued by a central bank or public authority nor attached to a fiat currency, i.e., currency that a government declares to be legal tender (Pisa & Juden, 2017).

Rank	Name	US$ Market Cap	US$ Price	Circulating Supply
1	Bitcoin	43 630 891 619	2660.98	16 396 550 BTC
2	Ethereum	34 736 739 597	375.25	92 569 593 ETH
3	Ripple	10 215 346 626	0.26	38 290 271 363 XRP
4	Litecoin	2 428 105 598	47.06	51 592 007 LTC
5	Ethereum Classic	1 950 098 114	21.04	92 694 964 ETC
6	NEM	1 848 834 000	0.20	8 999 999 999 XEM
7	Dash	1 295 180 283	175078	7 368 399 DASH
8	IOTA	1 177 470 178	0.42	2 779 530 283 MIOTA
9	Bithares	888 444 894	0.34	2 596 160 000 BTS
10	Stratis	766 295 675	7.79	98 428 282 STRAT

Table 1: Top 10 Cryptocurrencies, as at 17 June 2017 (CoinMarketCap, 2017)

The table above shows other cryptocurrencies which use Blockchain as their backbone. As many as approximately 300 cryptocurrencies have been created to date. Bitcoin had exceeded a total value of $42 billion as at 6 July 2017. This is only slightly below the market capitalisation of Ford Motor Company (Fernández-Villaverde, 2017).

Bitcoin uses cryptography. Through a clever combination of cryptography and game theory, the bitcoin Blockchain could be used by any participant in the network to cheaply verify and settle transactions in the cryptocurrency world (Catalini & Gans, 2017). The business dictionary defines cryptography as a

> "discipline or techniques employed in protecting integrity or secrecy of electronic messages by converting them into unreadable (cipher text) form. Only the use of a secret key can convert the cipher text back into human readable (clear text) form. Cryptography software and/or hardware devices use mathematical formulas (algorithms) to change text from one form to another."

The first block, a "genesis" block is encrypted. Anything can be encrypted. For bitcoin, it was a quote from the Financial Times. This quote was embedded in the block's binary data: "The Times 3 January 2009, Chancellor on brink of second bailout for banks". This formed the basis of the hash brought into the first transaction (Serapiglia, Serapiglia, & McIntyre, 2015).

Ambil et al (2017) mentioned immutability, no double spending and cryptographic strength to be what is needed for Blockchain systems to be ideal. Authors believe that Blockchain will eliminate fraud and ensure quicker delivery of trade. Issues which it can solve range from transaction forgery, to censorship transactions and transaction reversals.

Many have claimed that the bitcoin phenomenon is a bubble which is bound to burst at any moment. Others are convinced that it is a Ponzi scheme. Development Bank of Singapore has called bitcoin a Ponzi scheme (Das, 2017). The authors went through an econometric study to find the existence of bubbles in the bitcoin market. The technique used is robust in bubble detection and was created by Phillips, Shi and Yu in 2013.Three major bubbles were found for the period of 2011 to 2013 (Cheung, Roca, & Su, 2015).

Acknowledged by Quiggin (2013) to be a pure bubble, Bitcoin has never been able to run away from that stigma. The author compares bitcoin to the wrath of the 18th century South Sea Bubble as being a company which carries out an undertaking of great advantage, but with nobody knowing what it is. Apart from bubbles, bitcoin is also said to outmatch Ponzi schemes and describes the currency as being parallel to the fictitious dotcom company imagined in Garry Trudeau's Doonesbury, whose only product was its own stock. The author further argues that bitcoin in fact has no source of value due to the computing power involved in mining disappearing the moment it runs. This computing power cannot be reused in anyway. The moment the cryptocurrency stops being accepted in exchange for goods and services, the value will drop to zero. An adjunct lecturer in Public Policy at Harvard, Chris Robert has also added to say that media speculation has increased the bubble status of bitcoin (Shah, 2013).

Bitcoin is thought to not have an intrinsic value as all it is a computer programme. Its value seems to stem from its speculative value. Due to its speculative nature, bubbles are bound to follow it. Cheung et al (2015) confirmed claims of the existence and burst of bubbles in the Bitcoin market.

3.2.1 Is Bitcoin a Form of Currency?

The end of the bartering system came with the minting of shiny metals into coins. Fair trade was promoted by this coinage which had established value. The move to paper money was an add-on to coins and the rise of national currency was born. It first was backed by previous metal; however, the gold standard has been a thing of the past for ages. The first form of currency technology came in the form of print technology. The next wave of change came when the introduction of plastic came in the form of banking cards, especially for credit (Hurlbert &

Bojanova, 2014). Could digital currency be the next wave in the evolution of money? Nakamoto (2008), the creator of bitcoin defines an electronic coin as "a chain of digital signatures".

Before delving into whether bitcoin is money or not, it is important to remember that in essence our fiat or "normal" money is also just tokens. These tokens take a digital form or are symbolic and take metallic (coins) or paper form. Perceived value of currencies such as the Euro was constructed over hundreds of years, where history involving culture and politics played an important role. The US dollar on the other hand is valued using network effects since millions agree on its value and the currency is used in the real economy. Getting to a point where currency is accepted does not happen overnight. Various parties are involved ranging from government to central banks, institutions and commercial banks (Brett, 2016).

Money was defined by the Merriam-Webster dictionary as "something generally accepted as a medium of exchange, a measure of value, or a means of payment". As per the definition of money by economists, these conditions are what it will take for cryptocurrency to be seen as "money". A medium of exchange, a unit of account, a store of value; bitcoin to some extent meets these three criteria for money (Nigam, 2016). Bitcoin surely stores some form of value and is used as a means of payment for goods and services. Generally accepted value is deemed by societal views and acceptance of symbols of worth. An appropriate example is of how money was sent around using telegraphs by the Western Union in 1871 (Maese, 2014). Virtual currency is thus not a crazy and new idea after all.

There have been a few debates amongst economists about whether virtual currencies contain the core features of money. Many institutions have had their say with the U.S internal Revenue Service (IRS) seeing virtual currencies more as property rather than a currency. The IRS felt that capital gains taxes must be paid on it, making it more an asset (a store of value), but is seen to not have any intrinsic value. The future of virtual currencies lies in its ability to gain traction for usage and acceptance for payment by users. The U.S had less than one percent of its population either own or having owned this technology. The major differentiator between the demand for virtual currencies and fiat/sovereign currencies is their opportunity costs. Nominal interest rate is the cost involved in holding fiat money whereas for virtual currency it is its exchange (or principal) risk due to the floating exchange rate with a fiat currency (Schuh & Shy, 2016).

Bitcoin is not confined to a geographical or political environment meaning it has no real economy to establish its dominance. Until recently, very few companies priced their goods and services in cryptocurrencies (as a unit of account). Bitcoin is also still not seen as a means of exchange by most vendors. This does not strip away its potential to become a currency, although it is yet to garner support to be a fully-fledged currency. For this reason, few governments have put bitcoin in the box of "digital asset" as opposed to being seen as a currency. Many have argued that bitcoin works like gold in this sense. What can be concluded without any opposition is that indeed bitcoin (i) is a digital coin with the capability of being moved around between different players, (ii) bitcoin can be exchanged for some of the major currencies, now even

including the South African rand, meaning it has market value to a certain extent and (iii) it is randomly used in exchange for goods and services, even though this is not yet the norm and the occurrences are far in between (Brett, 2016).

What is seen as one the greatest hurdles for virtual money is it not being legal tender due to not being backed by a government. The lack of monetary policy ability and tax revenue is also another sore point. Apart from competing with fiat money, cryptocurrencies also have the burden of competing among themselves. Bitcoin is privileged to have a first-movers advantage to the other coins. The second-mover advantage is all the subsequent coins have at their disposal to become a success in the long run. The costs of switching are lower for bitcoin than the other coins (Luther, 2016).

3.2.1.1 Medium of Exchange

Contrary to popular belief, some retailers, merchants and even financial institutions have braved the unknown and have been some of the first to accept cryptocurrency as legal tender (a store of value). The first to step out into the water was a computer programmer, Laszlo Hanyecz, from Florida USA who purchased two pizzas for 10 000 bitcoin (BTC) on 22 May 2010, which equated to $6.36 million on 1st July 2014 (Nigam, 2016). The virtual currency has since then seen by others buying and selling products in exchange for cryptocurrency. The likes of Overrstock.com (a US online retailer), WordPress and other conglomerates from Dell to Universal Store at Microsoft have joined the wagon. Donations are now permissible using bitcoin at Wikipedia since Google can calculate the conversion rate while PayPal processes the payment. Recently, eateries such as Subway and desktop gaming platforms such as Stream have also joined in accepting bitcoin for payment; web documentation company, The Internet Archive, have also joined the movement. Some financial institutions including international giant Deutsche Bank have also started looking into Blockchain technology for payments (Deepika & Kuar, 2017). In South Africa, major retailer Pick n Pay allowed bitcoin to be used as a trial run in 2017.

Taran et al (2015) looked at a few incidences where bitcoin was used as a means of exchange. In as much as some governments have blatantly banned the use of cryptocurrency, more specifically bitcoin, there are some private businesses which actively use it. Institutions like the University of Nicosia in Cyprus accepts bitcoin as tuition fee. Gambling sites (for example Online Casino, Casino PeerBet and SatoshiDice) also accept bitcoin. Stores such as Bitcoinshop.us offers tangible products in exchange for bitcoin. Products range from watches to air conditioners; although delivery is restricted only to the Unites States. Memory Dealers offers equipment for personal computers such as memory cards and other electronics. It is one of the few stores which have used bitcoin since its inception. CoinSpot has helped bitcoin users by offering a listing of local merchants accepting bitcoin. Some of their clients include Keystone Pet Place and Java Nomad which delivers fresh coffee beans straight from Bali. CoinSpot also has Persian Shoes in its books, a store which offers handmade shoes and bags from Iran.

It is interesting to note that countries with a strong currency are more open to supporting cryptocurrency whereas the weaker less stable currencies, like China's yuan, try to ban it. Australia fully supports and uses bitcoin. A community in Launceston has begun building a closed economic system using bitcoin. Other countries which are not too weary of cryptocurrency include the United States, Bulgaria and Singapore.

One can buy property in London using bitcoin and book at a hotel in Russia's St. Petersburg. Air Baltic is happy for users to make bookings using bitcoin and Expedia allows hotel bookings.

The authors note that it is important to note the difference between payment systems (like PayPal) and actual currencies. Payment systems entail having rules, procedures and technical infrastructure facilitating the transferring of costs from one party to another.

Recent developments saw a French bank partnering with Bitcoin Central for them to be registered as a Payment Services Provider (PSP) under the European Union law. This will see Bitcoin Central being able to offer what financial institutions can from debit cards to account insurance and other banking services to Bitcoiners. Even the likes of American economist Ben Bernanke see the potential of bitcoin being a long-term investment (Dewi & Soekarno, 2014).

3.2.1.2 Measure of Value (Store of Value)

Lately, Bloomberg and Thomas Reuters have started reporting bitcoin prices. A few venture capitalists are willing to invest in cryptocurrency firms as the developer community continues to grow (Raymaekers, 2014). This shows the value seen in bitcoin.

Hayes (2014) empirically investigated the sources of value for cryptocurrencies and found that the rate of unit production (negatively correlated to altcoin value), the algorithm (altcoins using scrypt are more valuable than the SHA-256 ones) used and the aggregate computational power used during mining of coins (positively correlated to altcoin value) are the three main factors. Hayes (2014) cites Yermack (2013) by stating that cryptocurrencies have intrinsic money, which other authors dispute. The author acknowledges that this intrinsic value differs greatly from that found in tangible assets such as gold.

Due to not being redeemable from an agent, bitcoin, according to Dwyer (2014) lacks the property of having a store of value. The resources used to create a bitcoin are seen as sunk costs.

Perceived value of bitcoin and other cryptocurrencies seems to be dependent on their specialised use among certain communities and is an ongoing process which is developing as more parties enter this market (Brett, 2016).

3.2.1.3 Volatility

Bitcoin has been blamed for very high volatility, which has negatively affected how it has been seen as a currency. It was found that there exists "pump and dump schemes". These schemes are a form of fraud where the price of bitcoin is artificially inflated using positive statements, causing the sale of the coins to be at higher prices than when they we bought. Vejacka (2014)

touched on some of the aspects of cryptocurrencies including investigating the volatility seen in cryptocurrencies and comparing them with those of other fiat currencies, indices and commodities. The volatility measure used was the standard deviation of all percentage price changes available for data from July 2010 to May 2014. A second volatility measure was implored. The Average True Range (ATR) was designed and used with daily prices and commodities in mind. ATR attempts to adjust for the "missing" volatility where the greatest of the three is used:

a) Current high price minus current low price in the given period
b) Absolute value of the current high price minus the previous period close price
c) Absolute value of the current low price minus the previous close price

The downside is that ATR values are incomparable. However, the author overcame this challenge by using ATR percentages instead. The formula was as follows

$$ATR_t = \frac{ATR_{t-1} \times (n-1) + TR_t}{n}$$

where n was the moving average period and TR was the true range in t given day.

The results showed that indeed cryptocurrencies are highly volatile when compared to commodities, stocks and other currencies.

Many others have had doubts around cryptocurrency due to its assumed extreme volatility. Smith (2016) investigated this hypothesis of high volatility by looking at it from a different angle to previous authors. The author's argument stated that it is inappropriate to treat Bitcoin prices themselves as nominal exchange rates. Since it holds if one considers Bitcoin to behave more like a commodity such as gold as opposed to currency per say. Smith (2016) showed how the behaviour of nominal exchange rates is implied by relative bitcoin prices. The results showed the highly cointegrated nature of the implied nominal exchange rate with nominal exchange rate as determined in fiat foreign currency exchange markets. He used the dollar-euro, dollar-Australian dollar and dollar-pound rates with daily data from 1st September 2011 to 31st January 2014. The methodology used was the Vector Error Correction model for determining the relationship between market and implied exchange rates. For completeness, Smith (2016) also investigated gold-implied exchange rates to find that indeed Bitcoin behaves like the commodity gold.

Risk and return on bitcoin has been a burning issue for some investors. Dewi and Soekarno (2014) investigated this relationship and compared bitcoin's performance with other investments such as gold and stock index in Indonesia. The authors used the optimum portfolio formula along with risk, return and performance evaluation to find results. They found that bitcoin is only great for short-term period investments and for risk seekers.

Three risks are associated with investing in bitcoin. The first is price fluctuation, then there is the risk of other virtual currencies. The third is the lack of guarantee; since there is no central

government backing virtual currencies, no agency or institution is available for the people to put their trust in.

Since July 2010, bitcoin has been traded against the US dollar and the rate of growth for the number of transactions have been remarkable and exponential with a compound annual growth rate of 265% from August 2010 to August 2014 (Nigam, 2016).

In comparing the difference between the levels of volatility of the rand to bitcoin against the rand to the dollar, the first two figures below show the higher levels of volatility experienced between the rand and bitcoin. The volatility between the rand and bitcoin was measured to be at 60163 over a period of 14 months (January 2017 to March 2018). Comparing it to that between the rand and USD of 0.6066 seems ridiculous. This is one of the reasons cryptocurrency is not easily seen as a currency. It violates being a "store of value". For completeness, it was also interesting to look at the volatility (the area shaded in blue) of bitcoin when compared to USD in the third figure. It too proved to be highly volatile as shown by figure four.

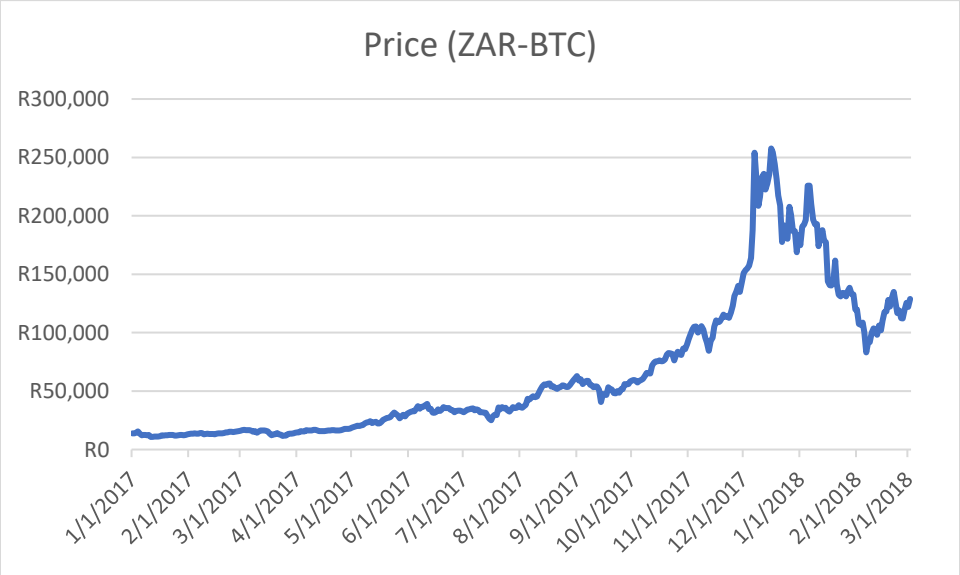


Figure 4: Price of Bitcoin in South African Rands (Coin Gecko, 2018)

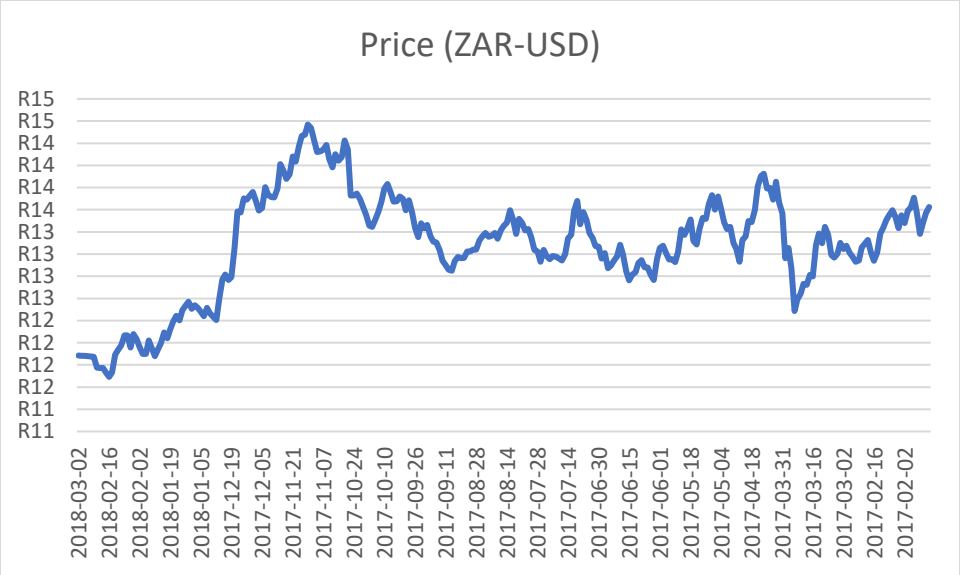


Figure 5: Price of USD in South African Rands (South African Reserve Bank, 2018)

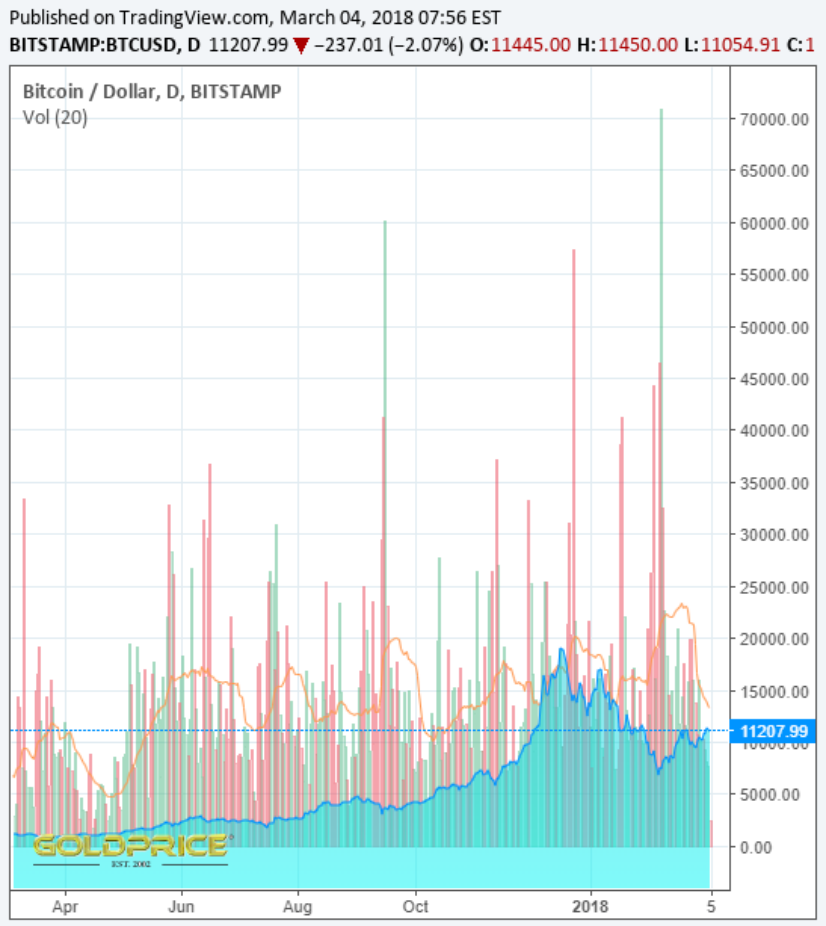


Figure 6: Price of USD in Bitcoin (Gold Price, 2018)



Figure 7: Bitcoin volatility time series charts (Buy Bitcoin Worldwide, 2018)

3.3 Where does it come from?

Bitcoin was the first of the cryptocurrencies to be created by a group of people or person with the pseudonym Satoshi Nakamoto in 2008 (Vejacka, 2014). Nakamoto published a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" a year before bitcoin was created. The past few years after it was unleashed for the world to see, other cryptocurrencies were created. There are a few bitcoin exchanges in South Africa including Singapore's BitEx and South Africa's ice^{3}x (Anderson, 2016). Other bitcoin exchanges in South Africa include Luno, GeoPay, BitSure, Chankura (Copley, 2017). Nakamoto gave Gavin Andresen reign over bitcoin. Andresen is the chief scientist at the Bitcoin Foundation. Although Andresen has oversight, ownership is governed by the use of open-source software and the open protocol (Dwyer, 2014).

Bitcoin later saw automatic teller machines being introduced around the world for ease of access and to complement the existence of exchanges. Johannesburg and Cape Town were the first two African cities to receive a Bitcoin ATM (Automated Teller Machine) in May 2014. It is however a tedious exercise to use the ATM for the first time. New users are requested to provide supporting documents such as the need to submit a telephone number for activation and notifications, government ID, palm scan, and current photo via the ATM's webcam (Saewitz, 2017).

3.4 How it Works

In trying to understand what Blockchain is, it is of importance to understand *how* it works as this is the most complex element to Blockchain. Its functioning was explored by using its application to cryptocurrency, more so in how Blockchain was applied to bitcoin.

3.4.1 Types of Blockchain (Access Control and Authorisation)

Blockchain is the backend database maintaining an openly distributed system. Transactions are validated without requiring a third party, and there is never any downtime and transactions

cannot be reversed. Transparency is maintained through it being public. Every transaction ever made can be traced and scrutinised.

Blockchain can be distinguished by two factors- access control and authorisation. Access control refers to access to the actual data on the Blockchain as either consortium, public or private. As it describes, public Blockchain is accessible to everyone where data can be seen by the public and consensus is also open to the public. For a consortium Blockchain, only pre-selected nodes can form part of the consensus process. Private Blockchains have nodes from one specific organisation which are considered for the consensus process. One should note that private Blockchains lean towards being centralised networks while public Blockchains being fully decentralised. Authorisation speaks to Blockchain being either permissioned or permission-less. To attain these factors, rules and certain measurements need to be decided on and are then embedded to become smart contracts (Ambili, Sindhu, & Sethumadhavan, 2017). Private Blockchains are usually found in corporate intranets, government departments and industry consortia since these users have credentials and are known.

Participants in private Blockchain networks are known a priori and are given permission to update the ledger. Participants are not limited as to where they come from, they may come from the same organisation or from different organisations within an industry sector. Some private relations are then governed by formal contracts, informal arrangements or confidentiality agreements. The figure below shows an example of what would occur if a contract is entered into within the Blockchain (Deloitte, 2017).

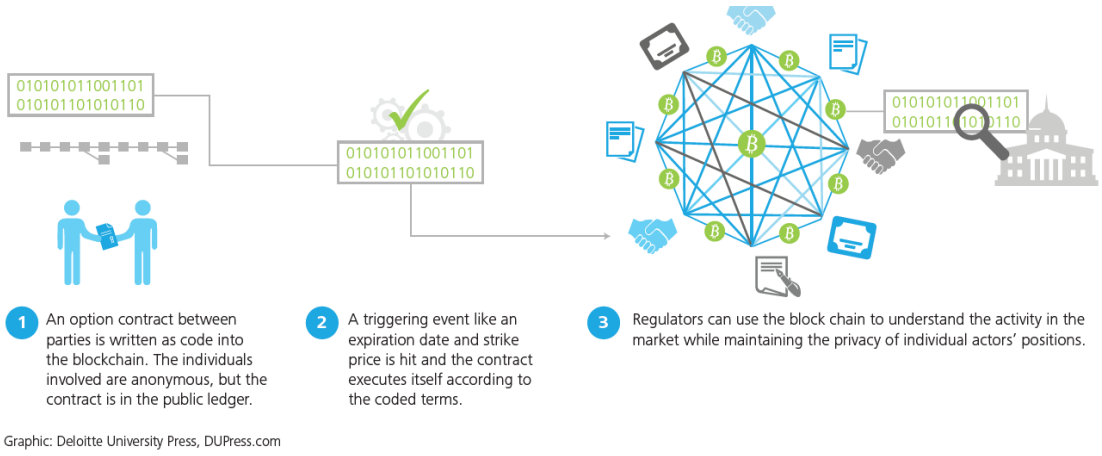


Figure 8: Blockchain contracts (Deloitte, 2017)

There often exists an imaginary line between public and permissioned Blockchains. One generally sees that Blockchains which are permission-less are public while the permissioned are private. Users tend to think that they are forced to choose one model or the other. However, both public and private models are powerful offering distinctly significant effects on financial services. Permissioned ledgers spark conversations around "how do we use this technology to perform an existing business process faster, at a higher level of accuracy and with fewer

resources?" This level of efficiency brings in value to a business even though the underlying business model remains the same. The story around public ledgers incites conversations around "how do we use this technology to completely disrupt an industry?" The natural answer is through the automation and distribution of currently centralised functions (Champion de Crespigny, 2016).

3.4.2 Data Structure

3.4.2.1 Blocks

Bitcoin allows each participant a secure way to manipulate the Blockchain ledger using cryptography without the use of a central authority. One of the basic features of Blockchain is the block. A block is made up of a block body and block header where the block header includes the block version (showing the block validation rules), Merkle tree root hash (shows the hash value of all transactions in the block), timestamp, nBits (the target threshold of a valid block hash), nonce (with a size of 4 bytes, it usually starts with zeros, increasing as the number of hashes increase per calculation), parent block hash (a 256 bit hash value pointing to the previous block) (Zheng et al, 2017).

One of the greatest features Blockchain has to offer is being immutable. All transactions can be verified, cleared and kept safely in storage in the form of a block within minutes or seconds. Blocks, once verified, are linked to preceding blocks to form a chain (see under: "Ways to obtain Cryptocurrency: Mining and Transactions"). This is done by having permanent timestamps and storing the exchange of value ensuring that the ledger cannot be altered (Tapscott & Tapscott, 2017). The updating of the Blockchain network is sequential.

3.4.2.2 Digital Signatures (Keys) and Hashes

The digital signature comes in two parts: the private key and public key. The private key as the name entails is the confidential portion used to sign for the transactions. Each digitally signed transaction gets broadcasted to the entire network. Two phases occur during the digital signing. The signing phase happens first where the sender encrypts their data using a private key and sends it to the receiver. The next stage is the verification phase where the receiver uses the sender's public key to validate the value sent. This enables the receiver to check if the data had been tampered with or not. The most common digital signature is called the elliptic curve digital signature algorithm (ECDSA) (Zheng et al ,2017). To explain how the ECDSA works, it is important to first explain what a hash and nonce are. A hash is an "alphanumeric string resulting from coding data with a cryptographic so-called hash function" while a nonce is "a number unique to the block" (Nowinski & Kozma, 2017). A hash is easier understood as "transformation of the original information" (Dwyer, 2014).

The origins of the ECDSA were explored by Olorunfemi et al (2007). The authors cited its beginnings to elliptic curve cryptosystems which were first suggested by Miller and Kobkitz in the mid-1980s. These two managed to replace modular arithmetic with elliptic curves thus improving how public-key cryptosystems worked. This meant having shorter key lengths and

thus needing less memory and bandwidth in executing using the public keys. The Elliptic Curve Digital Signature Algorithm allows a 512-bit public key to be obtained from a private key (256-bit random number). The elliptic curve crypto-algorithm is called the secp256k1. The production of the public key hash is done by using SHA256 and RIPEMD160 hashing algorithms (see under: "Ways to obtain Bitcoin: Mining and Transactions"). Base58Check encoding is used to encode the public key for generating the Bitcoin address. Time stamps on the Blockchain show the time the block was added. The hash value of the current and previous block become the input for the next block. The previous and next block are "chained" with each other since the hashes are connected (one hash is used to create another), increasing the integrity of the data. There is a link between the time stamp of a block and the hash of each block, allowing verification to occur for the validity of a transaction at any point in time.

If any form of modification occurs in the data, there will be a change in the hash value of that block causing the hash of all previous blocks to also change. This is seen as a forged block and will be rejected by the system due to being inconsistent. To avoid such forgery, Blockchain uses a number called a nonce in each block, for security. This nonce needs to be unique and can only be used once to assist in verifying the hash. The hash can be compared to having a unique fingerprint for each block. To produce this fingerprint, the block header (a data set which is pre-determined) is used by a miner (see: “Ways to obtain Bitcoin: Mining and Transactions” for definition of a miner). The block header represents all transactions in the block, as well as time stamps and other fixed data in that time period. For the sake of difficulty, one of the conditions to be met by the miner is for the block hash to be lower than or equal to a number known as a target (to be accepted by the network). This target is a 256-bit number (extremely large) that all bitcoin clients share. The lower the target, the more difficult it is to generate a block. The block hash starts with some number of zeros (according to the level of difficulty) up to a maximum value of a 256-bit number. If a hash is below the target, then a reward is won. The hashes or fingerprints are 64 hexadecimal digits. At present the bitcoin network desires 17 zeros at the start meaning 68 bits must be zeroes (Lee, James, Ejeta, & Kim, 2016). It is important to note that post the maximum number of 21 million bitcoins, miners will no longer get a reward for solving the algorithm (Smith J. , 2016).

The figure below depicts the transfer of Bitcoins using cryptographic methodologies.

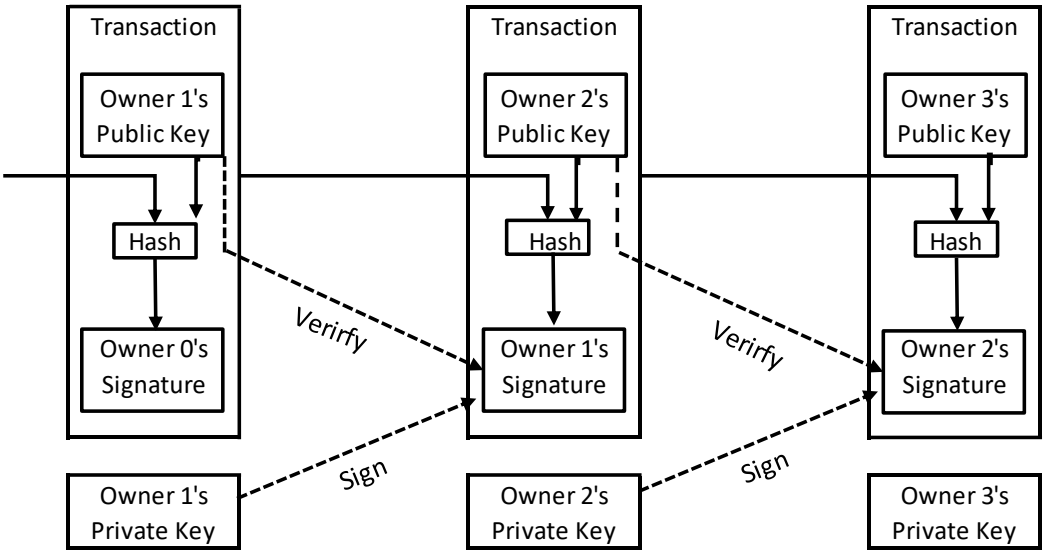


Figure 9: A chain of digital signatures (Deepika & Kuar, 2017)

When a new currency is introduced into the market, it comes with a predetermined amount of cryptocurrency (21 million coins in the case of bitcoin); this is to ensure scarcity. This finite amount of a cryptocurrency is called a "hard cap" and can never be changed once the first coin has been "minted" as this hard cap forms part of the core features and code for most of the cryptocurrencies including bitcoin. Hard caps form part of the factors which determine whether a coin is valued properly or not (Newkirk, 2017). Another interesting argument posed by Woodside (2013) as to why the number 21 million was chosen is due to the creator Satoshi being playful with mathematics as this number is the answer to a geometric series by inputting the initial block reward of 50 coins, having 6 blocks created every hour amounting to one every 10 minutes and the reward for miners being halved every four years meaning very 210 000 blocks. This then gives us the geometric series:

$$210\,000*50*(1/(1-0.5))=21 \text{ million}$$

To date, no one knows the real reason behind having chosen 21 million coins as a cap, all that exists among authors is speculation and theories yet to be proven. The rate of production is set in advance using a specific value and is known publicly. The units are referred to as coins and a peer-to-peer computer network is used for costless transfer of coins. (Vejacka, 2014). For inflation management, the currency is gradually introduced into the market until the maximum cap is hit. Although, once the currency hits its finite cap, hyper-deflation may occur and the reward that was one realised by miners will become eroded as it becomes more difficult to mine (since the level of difficulty increases and the amount of resources needed become too expensive).

Bitcoin block generation works like a sort of lottery, where one fills in the lucky numbers and hopes that they match up. Miners compete to crack the algorithm in turn for a fee of newly minted currency (as a reward). Only a specific hash will be accepted where the first computer to find the correct hash is deemed the winner. As the difficulty of the system increases, it is like the lottery expanding the numbers to choose from, making winning that much more difficult. Mining rigs (a collection of many super computers) have been introduced as the price of bitcoins continued to increase. This has resulted in a higher hash rate. "Hash rate is the unit of measure of processing power for any of the cryptocurrencies. It is the measure of how many hash calculations per second a processor can perform." (Serapiglia, Serapiglia, & McIntyre, 2015). The infrastructure upgrades will continue to occur as prices increase to ensure increasing pay-outs. In the beginning, many used the Bitcoin profits to upgrade their machines and this trend has been continuing, as there is now no other way to remain competitive (Peck, 2013).

If someone from the network tried to spend the same coin, two conflicting transactions will exist in the network. This situation does not exist for long; only one of the two transactions can be accepted. It is the benefit of the node to only work on extending the longest chain, if this is not done, all that effort will have been for naught. With the simultaneous broadcasting of different versions of the next block, nodes will receive the nodes are different times. To ensure that the correct one is used, the node will work on the first one it received and save the other branch just in case it becomes longer. The wallet does not necessarily need to be constantly online for it to be part of a transaction. When the wallet next connects to the network, an up-to-date Blockchain may be requested by the user. (Serapiglia, Serapiglia, & McIntyre, 2015)

3.4.3 Ways to Obtain Bitcoin: Mining and Transactions

There are few options for users to obtain bitcoin. In all methods of obtaining bitcoin digital wallets, which are stored on users' computers or mobile phones, are used to store the coins. The wallet is a software which manages the coins during transactions, just like a traditional wallet with cash inside. The contents of the wallet come standard with a regularly updated file which has a list of all bitcoin transactions ever made (Hurlbert & Bojanova, 2014). Everything on the wallet functions as information does on files. Wallets can be seen as spreadsheets which keep track of the balance (Dwyer, 2014). To begin using the likes of Bitcoin, a wallet will need to first be installed (Nigam, 2016). The wallet is associated with an address for the user and the address is 33 alpha numeric characters. Users are able to have more than one wallet.

The first way to obtain digital currency is through "mining" the currency. A participant first announces their intention to enter the network, where this transaction runs through the network to find a "miner" (someone who verifies transactions by performing complex manipulation to find the solution to the cryptographic problem using a powerful computer). Mining refers to the “computational power to process transactions for a cryptocurrency Blockchain to receive a reward of cryptocurrency for the effort” (Ahamad, Nair, & Varghese, 2013). This computational power comes as either GPU (Graphic Processing Unit) or CPU (Central Processing Unit) processing. A third more advanced level of computational power is the Application Specific

Integrated Circuit (ASIC). ASIC was first publicised in early 2012, costing thousands of US dollars and were hard to find and was "the technological progression of the endgame for Bitcoin" (Peck, 2013). Now ASIC is readily available at reduced cost. CPU is great at doing complex calculations and manipulations to a small data set whereas GPU is better employed on large data set for simple manipulations. The two main actors on the network are the miners and the network; they both facilitate the block chain or the common ledger (Serapiglia, Serapiglia, & McIntyre, 2015).

Each encryption algorithm requires different computational power. The power is used to solve artificial mathematical problems (Vejacka, 2014). The SHA-256 needs mining speeds measured in GH/s while Scrypt mining rates are in KH/s. The CPU, GPU and ASIC are then used to connect to the network and are used for the participation and confirmation process. There is a process of bundling the new coins along with transfer fees for finding a solution for a specific block of transactions. Visa works in exactly the same manner, where at this stage the transactions are approved. The Blockchain is created every 10 minutes for the case of bitcoin.

SHA-256 is a cryptographic hash function and forms part of bitcoin's proof-of-work for confirming transactions. Due to the high cost of mining (due to its rigorous requirements), individual miners tend to join mining pools allowing them to use joint resources and not have to rely on their own "mining farm" (Deepika & Kuar, 2017). SHA-256 uses a more complex encryption than the Scrypt algorithm (which has a shorter hash rate cycle). The initial hash rate was around 7Mhz which a CPU could handle. Mining rigs have caused this rate to now exceed 1.3 Hhash/s post 2010. Apart from the power consumption needed, miners also need to invest in cooling solutions so that their machines do not overheat (Serapiglia, Serapiglia, & McIntyre, 2015).

Blockchain is an open ledge used for book keeping for the system (Sharma, Nisar, & Raina, 2017). In this ledger, the transaction records are stored in "blocks". Once a seller publicly sends through their desire to sell to a buyer, the deal is logged, and deemed either valid or rejected by different nodes (members within the network). A cryptographically protected block is value-added to a chain, linearly after receiving verification. The transactions packed in these blocks need to meet strict cryptographic rules for network verification. The rules ensure that blocks created prior are not altered or modified in any way since if this occurs the subsequent block would be invalid, breaking the system. A new block is appended to old blocks to form a "chain". Nigam (2016) notes that only the longest chain is recognised as representing a consensus by the network. This is done regularly as transactions occur. It allows user computers to all agree on the state of the system (Vejacka, 2014). The ledger is sensitive to slight changes and these can cause discrepancy within the whole network. For example, if 7000 computers form part of the network, all 7000 would need to be infiltrated at the same time for the modification to work. This creates an unbreakable, safe system which enables trust among the users. Amidst all this, various miners are competing to be the first to find solutions. This makes it difficult for the same miner to have created consecutive blocks due to the high competition among miners. The data take copious

amounts of time and are costly due to the mentioned computational requirements. These records are permanently stored in the system (Nigam, 2016). There is an assumption from the side of bitcoin of honestly from its users and so majority voting (and consensus) helps avoid double spending and is used for dispute resolution. Long chains of proof-of-work act as a security mechanism as opposed to the conventional use of central banks which invoke the element of trust for cash and double-spending detection.

The second way for obtaining bitcoin is through the selling of goods and services in exchange for this currency.

The last and most popular way is through buying fiat currency for bitcoin (usually done through exchanges).

In the case of the first and second way of receiving bitcoin, keys are needed. The keys are necessary to open the restricted files which make up the system. The process of sending money involves the sender first encrypting their data using the public key of the receiver. The payments are broadcast digitally for requesting an update to the public ledger. The sender then sends the encrypted data to everyone. Once the receiver receives this data, they decrypt it using their private key (similar in use as an ATM PIN) to view the value of the currency sent (Vejacka, 2014).

The main source of bitcoins still remain the first two mentioned above, but one recent unique way is through ATMs. This can be seen as a subset of using exchanges. Bitcoin has evolved to offering ATM services for bitcoin purchases. This is available in South Africa. The exchange rate used is from any one of the big e-markets where bitcoin can be exchanged for any other cryptocurrency. A low fee is charged for the maintenance of the ATM. This has allowed bitcoin to infiltrate the market at a higher rate than in countries where ATMs do not exist (Vejacka, 2014).

Like anything else with value, bitcoin's value stems from the supply and demand for it.

Below is a simplified view of a Blockchain transaction:

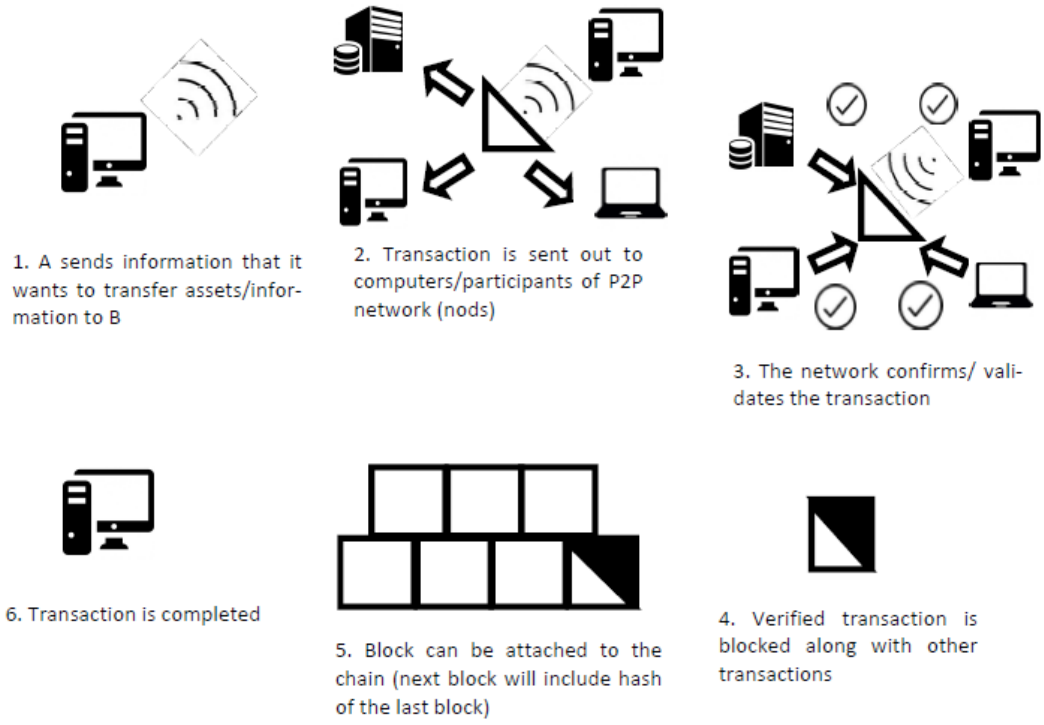


Figure 10: An overview of how the transferring of Bitcoin works (Bistarelli & Santini, 2017)

In short, mining works in this way (and occurs as part of step 3 of the figure above):

(a) The miner collects transactions and verifies them by checking a set of rules according to what the protocol requires for example checking the format. The miner is able to reject the transaction if the sum of the of the output value is less more than the sum of inputs

(b) Once a transaction has been validated, it is added to a block (Bistarelli & Santini, 2017).

3.4.4 Consensus Algorithms

Consensus algorithms are used to come to an agreement on a common value in peer to peer networks. The computer power needed to reach a consensus on the network is incredible.

These algorithms ensure that there is no majority rule from one party when decisions are made. Consensus can be derived by using different methods such as proof of stake, proof of work, leader-based consensus, delegated proof of stake, proprietary distributed ledger, N2N and PBFY and derivatives.

The main purpose for consensus algorithms is to solve the Byzantine generals' problem. In this problem, a group of generals each in charge of a portion of the Byzantine army encircle a city and must come up with a plan of attack for this city and must agree on one plan. The simplest form is when the generals have to choose to either retreat or attack; generals should all agree on either option. Traitors make the decision process more difficult. The Byzantine fault is a fault

which occurs where different users see different symptoms or outcomes. If there is a loss of a system service, a Byzantine failure occurs. Blockchain systems should not tolerate Byzantine faults. The number of traitors need to be less than one third of the users for a system to perform reliably (Ambili, Sindhu, & Sethumadhavan, 2017).

Federated consensus mechanism entails converging overlapping subnets which have been picked to reach an opinion. Proof of validation is responsible for validating transactions and forms blocks called validators which are special nodes. A disadvantage of proof of work is its high energy consumption. Proof of stake solves disadvantage (Ambili, Sindhu, & Sethumadhavan, 2017).

There are a few approaches to reaching a consensus within the Blockchain. Zheng et al (2017) made a summary of the different consensus algorithm options as explained below:

Proof of Work (PoW), which was the first approach, is used with bitcoin. The recording of transactions in a decentralised network needs someone to be selected to do so. Random selection is the easiest way to select someone but comes with vulnerability to attacks. Work in the form of computer calculations needs to be performed by a node for a block to be published by a node. For consensus to occur in PoW, the calculated value using the nonce for obtaining the hash value must be equal to or less than a specific given value. A block is broadcasted by the node which reaches the target value, all the other nodes in the network need to mutually agree to the correctness of the hash value. Once validated by all nodes, the block is appended to every miners' Blockchain. Mining is the PoW process in bitcoin.

Since the network is decentralised, it is normal for there to be simultaneous nodes achieving the target value. When this is the case, branches then form. It is, however, impossible for both these competing forks to end up forming blocks simultaneously. PoW will then only allow the branch which becomes the longest to be the authentic one and only that branch will be allowed to append to the existing blocks while the shorter branch falls away. This process needs a lot of computing power which results in enormous amounts of resources being expensed in the form of electricity.

Within the PoW mechanism, the amount of energy (number of hashes) needed for transaction verification is decided upon by the target difficulty and hashing algorithm. Mining began with the use of Central Processing Units (CPUs) but slowly migrated to the use of Graphic Processing Units (GPUs) which could perform the same function but at a faster rate. The introduction of Application Specific Integrated Circuits (ASICs) came last and came with faster speeds than GPU (Farell, 2015).

Proof of stake (PoS) was created to be the energy-saving cousin to PoW. With PoS, the job of miners is to prove who owns an amount of currency using the account balance of users. This was found to be unfair and it was then decided to use the stake size approach for choosing who gets to append a new block to the Blockchain. There are two programmes which assist with this.

Blackcoin was selected to assist in using randomisation for predicting who will generate the next block. It works by searching for the lowest hash value along with the stake size. The other programme is Peercoin where the older and bigger the set of coins, the more likely it is to be selected for mining the next block. PoS boasts efficiency and less energy usage when compared to PoW.

Practical byzantine fault tolerance (PBFT) tolerates byzantine faults using a replication algorithm. It is able to withstand one out of three "malicious byzantine replicas". Rules are created and in each round a user is selected according to the rules giving them the responsibility to execute a transaction. There are three stages to the process: "pre-prepared, prepared and commit". A two third vote is needed in each phase for moving to the next phase.

Delegated proof of stake (DPOS) is a derivation of PoS where DPOS is a representative of a democratic system. Stakeholders are able to elect who will generate and validate blocks causing the process to be quicker since fewer nodes are involved in validation. Dishonest miners can easily be voted out if the need arises.

Ripple employs subnetworks which are collectively trusted within the larger network. Nodes are then split into server nodes (these form part of the consensus process) and client nodes (purely for fund transfers). There is a Unique Node List in each server which assists in determining the addition of a new transaction to the ledger. If 80 percent of the server nodes are in agreement with the query, the transaction is added to the ledger. The ledger is deemed to be correct only if the percentage of faulty nodes in the server nodes is less than 20 percent.

Another type of consensus algorithm is Tendermint which is a byzantine consensus algorithm. There are three steps to reach a consensus which are repeated every round where an unconfirmed block is broadcasted by a proposer. In the pre-vote step there is the decision by validators whether to broadcast a pre-vote for the proposed block or not. Following this, a node needs a two third vote to broadcast a pre-commit in the pre-commit step. Finally, the block is validated by the nodes and broadcast as a ‘commit’ for that specific block. To become a validator, a user needs to lock their coins and if as a validator you become dishonest, you get punished.

Farell (2015) mentioned the possibility of mixing of PoW and PoS. To overcome the distribution challenge posed by PoS, allowing the distribution and minting of the coins to be executed by a PoW approach solves the issues. After some time, the PoS then takes over creating energy efficiency for the virtual currency.

Three main properties differentiate the various consensus algorithms namely energy saving, node identity management and tolerated power of adversary. To be deemed a good consensus algorithm, one needs to be safe, efficient and convenient.

3.5 Players in the Blockchain Ecosystem

As it stands, it is looking as though Blockchain will be foundational for institutions, companies and even individuals. There are many players who have started looking at understanding the technology and who will form part of the users on the network. These players were explored by Tapscott and Tapscott (2017) and include:

Venture capitalists: After having started as an exclusive club of crypto insiders, the venture capitalist world fast got its fingers into the crypto-world which expanded beyond just the most influential venture capitalists. Among those who joined the movement, we saw financial institutions like UBS, Visa, Barclays, Goldman Sachs, Deloitte and YSE among others investing in start-ups (and even incubators) which have their sights on Blockchain. It did not stop there as some pension funds have also been making investments in this space. Data given by DeNova (a platform powered by PricewaterhouseCoopers) has found that "funding in Blockchain companies increased 79% year-over-year in 2016 to US$450 million". It has gone to the extent where academics and advisers are being appointed by venture firms such as Digital Currency Group to get to grips of what this technology can do in the venture capital space.

Banks and financial services: Seen as natural adopters to Blockchain, the Global FinTech Report 2017, reported that of the respondents to the survey, 77% of those in the financial sector considered "to adopt Blockchain as part of a production system or process by 2020" (Tapscott & Tapscott, 2017). This was said with the intention of action being taken as we see the likes of Macquarie, Bank of Montreal, CIBC, ING, State Street, BNY Mellon, CIBC, Commerzbank, Commonwealth Bank of Australia, Mizuho Bank, Mitsubishi UFJ Financial Group, RBC, Nordea, Société Générale, UniCredit, TD Bank, Wells Fargo and many others having had already invested in Blockchain and getting the decision makers on board (Tapscott & Tapscott, 2017). The R3 consortium has seen many banks join this consortium and working together to explore and develop the technology for their needs.

Coders and developers: The developer world for Blockchain is unique in that it has no body which has oversight over it. This is per the design of the network. Coders and developers have the option to participate in posting suggested protocol improvements allowing their peers to provide constructive feedback. They can post on online forums, are able to discuss and address any issues or concerns and even test each other's' codes and performing debugging. It is frowned upon by the developer community for one to bypass a peer review while it is highly encouraged to look through others' code for improving one's ideas.

Academics and scholars: The academic world has also been on board in trying to figure out what Blockchain is all about. Institutions in the academic space have been funding research centres and labs in this regard. Some universities including Princeton, New York, Duke and Stanford have even opted to teach Blockchain courses.

Governments, regulators and law enforcement: Central banks across the world have been trying to take the necessary steps to understand Blockchain with their greatest concern being around

regulation and the impact it will have on the country of origin. For example, central banks are each taking different steps to understand this technology. While some governments believe that the first necessary steps lie with strong regulations, others have chosen to take the laissez-faire approach. Some governments have decided to take the "if you cannot beat them join them". Adam Draper (a prolific venture capital) was accurate in stating that “government endorsement creates institutional endorsement, which has value.”

3.6 So What?

It can be agreed upon that the Blockchain technology is still in its infancy, but a lot is expected from it in terms of the value which can be extracted from it. Deloitte (2017) looked at some of the reasons why this paper exists and why the world is going above and beyond to try not only to understand the technology and the process by which this phenomenon evolves and is experienced by its users in the financial world. One of the reasons is how the current way of adding value could be bettered by allowing the use of Blockchain to make it cheaper, faster, transparent and more reliable; the way financial innovation has been creating changes to the financial sector. Using Blockchain's strengths can be optimised by building systems on top of it.

"Fiat money is a currency that is backed up by the promise of a nation or entity that will support the exchange of the physical representation of that money". November 2008 saw fiat money being earnestly challenged then came 2008 and Bitcoin was created (Serapiglia, Serapiglia, & McIntyre, 2015). Nothing would remain the same again.

3.7 Some Advantages

Proponents of Blockchain have highlighted numerous advantages offered by the financial innovation. Various authors have offered some of these advantages and they will be explored in this section. Some of these advantages come as solutions for persistent issues mainly in the financial world where the innovation started.

Third parties are middlemen who currently assist institutions by ensuring the verification of participants' identities, scrutinising the clearing and settlement of transactions and making sure that institutions have a clean bill with their exchange record. Credit card companies and similar companies (which fall under the group of third party agents) have had the online merchant market backed into a corner with no hope of ever being freed from their high fees, limited global freedom in terms of countries allowed by credit card companies for access, complex payment software implementation as well as charge backs (Sharma, Nisar, & Raina, 2017). Now enter bitcoin, a solution that offers lower transaction fees, opens new markets, faster transaction speeds, security and saying goodbye to charge backs. This innovative technology offers online merchants the opportunity to not have third party agents and lower overhead costs. Charge backs will be a thing of the past since transactions cannot be reversed. Another advantage they offer is decreasing uncertainty and increasing levels of trust between parties who would normally not transact with each other. Anderson (2016) added the ability to offer greater transparency as a cherry on top for lowered transaction costs. This opens the world to companies increasing their chance of growth. Fortunately, this comes at reduced cost to institutions using these services. A

classic example is of the 2 percent charge (on average) paid to a credit card company for a single transaction made by merchants. Another cost is of inefficiency levels where transactions must wait three to five working days to clear. (Pisa & Juden, 2017). With cryptocurrencies, no such fees exist.

Bitcoin offers free in-country and cross border transactions where no central body, government or any form of jurisdiction can impose any restrictions to the way funds are sent. Many countries in developing nations face large populations who do not form part of the banking system. With this limitation, the likes of PayPal, Visa and MasterCard are unable to service these regions, whereas bitcoin offers "low cost fast solutions that provide an account to anyone, anywhere, anytime" (Ahamad, Nair, & Varghese, 2013).

Bitcoin offers transactions to not only be quicker, safer and cheaper but also allows users to remain anonymous while bookkeeping is always guaranteed to be correct and cannot be doctored due to not being able to be duplicated (Sharma, Nisar, & Raina, 2017) and (Deepika & Kuar, 2017). Even though transactions are anonymous, there is a high level of transparency (as mentioned by Anderson (2016)) since everyone can see what is on the ledger at any given time. At no point are users requested to give their personal information; this affords the user protection against identity theft (Vejacka, 2014). Nigam (2016) cites payment freedom as one of bitcoin's advantage; the ability to send and receive any amount of money immediately globally at any time with no limitations such as public holidays, imposed limits or borders.

A solution offered by Blockchain technology is in increasing cybersecurity which is also at risk due to third parties having all the data in a centralised place making it a sweet spot for hackers and a single point of failure. Zheng et al (2017) found that structurally, issues of single point of failure are non-existent when Blockchain is employed. Companies are not guaranteed that the third parties they use are in fact trustworthy (Pisa & Juden, 2017). Fortunately, bitcoin transactions are said to be irreversible by Nigam (2016). Fraudsters will have to work that much harder to crack the cryptographic security measures of bitcoin, making the adoption of the technology more appealing to businesses who suffer great losses from fraud (SYSPRO, 2017).

The EY Think Tank (2017) agreed that bitcoin's potential lies in increasing efficiency and its disruptive nature in fields like resource management, for international trade and governance. These fields have been facing high transaction costs made worse by current bottlenecks including corruption, mismanagement and poor infrastructure.

3.8 Some Challenges

Many advantages are yet to be discovered as the financial innovation is slowly being understood. At the time of this paper, the mentioned disadvantages outweighed the advantages, but this is in no way an indication of diminished potential for Blockchain. With this at the back of the reader's mind, the disadvantages will be explored below to further understand some of the limitations of Blockchain and bitcoin.

With the steady increase in the number of sectors which have started adopting the Blockchain technology (beyond the financial industry), there have been some challenges which had reared their ugly head. One size fits all is far from what Blockchain can offer and is about. Modern technologies bring excitement and many discussions about the future, but it is always wise to keep at the back of one's mind that due to being so new, it is still immature and will experience some growing pains with further development being a need for reaching its full potential. An example is the latency that comes with the mechanism which is meant to provide trust to the public Blockchain. Transaction throughput is limited by computation and the consensus mechanism due to needing many (untrusted) participants to agree which takes time. This is, however, not an issue for permissioned Blockchains (Champion de Crespigny, 2016).

The simplest challenge faced by bitcoin is its speed while transacting which needs to be prompt for example while using a vending machine. A customer will not be willing to wait the time it takes for transaction verification (roughly 10 minutes at the time of writing this) to be completed just for a cup of coffee or chocolate (Ambili, Sindhu, & Sethumadhavan, 2017).

One of the greatest challenges faced by this technology as mentioned by Wright (2017) is the rate of adoption as influenced by the thoughts and views of institutions and individuals. It may seem like a brilliant idea to increase transparency but who is to say that those who benefit the most from the current lack of transparency will welcome this new technology. Often business partners and the public are not meant to know certain pieces of information for the benefit of a few. As it turns out, some want it to be kept this way further widening the income gap and limiting opportunities to the few. It is foreseen that it will be individuals and not institutions who will push the implementation of Blockchain technology.

Wright (2017) also noted that the limited number of available software developers with the knowledge to assist implementation of the system impacts the speed of development needed. Training costs are often a deterring factor as developers are found without the necessary skills. Along with training costs, the initial capital costs may also put some firms off. However, as firms start to realise the potential of Blockchain, they may see the high return on investment.

A few other challenges have been mentioned by Pisa and Juden (2017). These include mainly governance and data privacy. A solution for data privacy issues is the use of permissioned networks. These networks are able to limit the number of users with access to a specific ledger. The obligation of financial companies to keep client records confidential make these companies a little concerned with putting all this data on a distributed ledger. This includes having their sensitive trade data remain private. There has been some discomfort conveyed by some users of the network regarding governance. It is not clear as to who in fact enforces, let alone dictates the rules of the system. At present, a 95 percent agreement (as measured by mining power) is required for the Bitcoin Improvement Proposal to be accepted. This has caused slow resolution to issues which need to be fixed by the community around the insufficient block size.

In understanding the governance issue, Tapscott and Tapscott (2017) focused on the issue of maintaining incentives for mass collaboration. The authors found that there is an incentive for miners to maintain the bitcoin infrastructure since if the network crashes, all their hard-earned coins would be worthless or at risk of being lost forever. To deviate slightly, it is important to note the role of miners. It is not to validate transactions since each full node has the capability to do that on its own. Miners, however, provide the preservation of the distribution power which translates to the power to make decisions for block creations, to vote and to mint coins.

It is thus of the utmost importance for making any kind of alterations or upgrades to ensure that is does not cause havoc with the economic incentives to sustain the decentralisation of hard-core miners. Good value should always be able to be extracted from the network from miners for receiving large sums of bitcoin. So be it a small miner who is dispersed geographically or a large mining pool, the competition between the two should be deemed fair with fair remuneration.

The one barrier mentioned by Price Waterhouse Coopers (2016) spoke to the attempt to implement "swarm" principles to resolve conflict. These principles use the collective opinion of all users involved but they are difficult to put to action. Another barrier, of a larger scale, speaks to requirements needed by the regulatory and legal fraternities which Blockchain needs to comply with.

It can be agreed that this technology is still in its infancy with much development needed before full implementation can be seen. Africa at large has an array of challenges ranging from the lack of extensive infrastructure, high instability in the political realm and little to no capitals pools. These are what one would expect to be major hindrances in adopting new technologies to better the continent. However, these very issues create the necessary opportunities for Blockchain technology to grow; unlike in more developed regions. Blockchain might have the perfect position to change African economies and societies.

Tozzi (2017) showed the government instability issues which Blockchain could solve. For the issue of the lack of infrastructure, the author made light of how the technology requires good internet connectivity which is not as stable in most African countries. Another form of government instability is revealed by the lack of investment capital be it for businesses, individuals or government. Blockchain can provide cost-effective and fast access to capital ranging from microloans to that of a government bond.

Apart from other cited disadvantages, some challenges exist which are inherent. The biggest one being the high level of difficulty and complicated nature of this technology (both technically and conceptually). Bitcoin alone has some technical issues which still need to be resolved. The major issue being its scalability causing the community using bitcoin to consider incorporating SegWit2x for the suggested hard fork to be implemented in November 2017.

The common concern with bitcoin is the dark cloud of illegal activity which continues to hang over the technology including assassinations, Ponzi schemes, illegal mining, money laundering,

theft and unlawful gambling. The Silk Road was created in 2011 and is known as the "eBay of drugs". Silk Road 2.0 saw a $2.7 million loss just after inception due to an attack (Hurlbert & Bojanova, 2014). Mt. Gox, one of the biggest bitcoin exchanges in Japan, saw $350 million stolen from its coughers in February 2014 leading to its destruction (Gandal & Halaburda, 2014). The fall of Mt. Gox came from double pay-outs being done from the exchange through attacking the software. Canada's Flexcoin lost $600 000 in a similar incident to Mt. Gox and went under. Mixing services (also known as tumblers) offer the mixing of "clean" money with money from illegal activities mainly in the black market (such as transactions for drugs, weapons, steroids, forged documents, counterfeit currencies, stolen credit card details). These third-party agents interrupt the connection between the two Bitcoin addresses used while transacting (Bistarelli & Santini, 2017). Sheep Marketplace, a market for illegal goods, also saw Bitcoins worth $100 million being stolen from it (Connolly & Kick, 2015).

Due to its anonymous nature, it has been seen to be used for illegal and unethical transactions ranging from human trafficking to tax evasion and drugs (Sharma, Nisar, & Raina, 2017). The black market has been the hardest hit since the level of difficulty to confiscate and arrest criminal activity increases when the black market is mixed with cryptocurrency (Vejacka, 2014).

Zheng et al (2017) also had a stab at identifying some challenges with some solutions:

The biggest stumbling blocks include the above-mentioned security issues as well as scalability. The size limit of a block is 1 MB with it being mined every 10 minutes. Having larger blocks will bring the challenge of needing more storage and slowing down the network. There is a major trade off now between security and block size. Selfish mining would yield better rewards for miners. Here selfish miners collude to not broadcast their mined blocks causing their private branch to be the longest branch (longer than the public branch) and it being used by the network. Honest miners would then have wasted their time and energy mining and appending the public branch. The selfish miners then tend to receive more revenue since they are competing with a smaller pool of other miners. If tempted, miners could hide what they have already mined for gaining future revenue. As the need for this new technology increases, so will the demand for an increase in the number of transactions causing the Blockchain to have to process more data than it was built for. Since each and every node has to store all validated transactions, having to validate an increasing number of transactions is becoming an issue due to block size restrictions. With its ability to handle seven transactions per second, it falls short of the real world need for more transactions.

There have been some suggestions to solve this issue of scalability, split into two main solutions. The one need is for "storage optimisation of Blockchain" as it becomes more difficult for nodes to have full ledger capabilities. One way to assist is for the nodes to either remove or forget old records using an account tree (a certain database which is able to hold the rest of the non-empty addresses). VerSum is another option which allows the outsourcing of the high energy needs by performing the complex calculations on behalf of its clients. The client is guaranteed correctness

since VerSum then compares their output with multiple servers. This, however, introduces a third party which is what the technology is shying away from.

The other solution for easing the issue of scalability is redesigning Blockchain. Bitcoin Next Generation (NG) offers a new design where the block is split into two parts; the part for choosing leaders called the key block, as well as the microblock for storing transactions. Time is then divided into epoches by the protocol. The hashing to generate key blocks is done in each epoche and the generated key makes the node the leader node responsible for the generation of microblocks. With this new version of bitcoin, the longest chain strategy is changed such that the microblocks do not matter (they do not carry any weight) making the sure that the trade-off between network security and block size is addressed.

There has been a concern around privacy (also mentioned by Pisa and Juden (2017)). There is now a way to link IP addresses to user pseudonyms even if the user has a firewall or is behind a Network Address Translation (NAT). Each user uniquely connects to a set of nodes which is identifiable (due to frequent use of the same address). To counter this, the use of mixing is able to offer anonymity to users. This is done by transferring money to multiple output addresses from multiple input addresses. This involves a trusted intermediary to perform the mixing. There lies the risk of the intermediary selling their clients' information for profit. To counter this, Mixcoin has a solution where it encrypts users' requirements (when to transfer and how much) with a private key. Mixcoin offers not only mixing services but has an accountability feature where users advise the service parameters (such as the address of where coins need to be sent to). The same amount is used when mixing with many users transacting at the same time for the anonymity to work. Blindcoin is an improvement on Mixcoin using blind signatures to further separate the input and output address (Maurer, 2016). Unfortunately, theft by intermediaries remains an issue. Another mixing platform is Coinjoin which has a central mixing server which shuffles all the output addresses to prevent theft.

Maurer (2016) showed different mixers using different architectures for mixing coins ranging from peer-to-peer mixing protocols, altcoins and mixing services. Unfortunately, this solution can only help with theft issues but not when coins are “lost”. The various mixers are as follows:

i. CoinSwap encourages transaction through a third party where A first sends coins to B intended to then be further sent to their original intended recipient C who will receive them from B. Transactions can occur even through other altcoins.
ii. CryptoNote introduces a different cryptographic method from that used for Bitcoin. Anonymity is offered for both sender and receiver. This is more a new cryptocurrency than a mixing service which is not susceptible to DoS attacks, but it is not compatible with Bitcoin
iii. Zerocoin, similar to CrytpCoin is also a new cryptocurrency which has extended the Bitcoin technology offering new transaction types where new coins cannot be linked to minting thus creating anonymity.

Apart from mixing, there is another method to assist with combating privacy issues by making transactions anonymous. By using zero-knowledge proof, Zerocoin unlinks payment origin from the transaction making it impossible to create a transaction graph. There is no need for miners to validate transactions using digital signatures since coins are validated if they are part of the list of valid coins. Unfortunately, it still shows amount and where the payment is destined for. Zerocash fixes this by hiding transaction amounts and coin value in user wallets.

Deloitte (2017) had a different view of bitcoin's advantage for lowering transaction costs and its efficiency. The author argued that the network came a high aggregate cost. This argument of inefficiency comes from each node having to perform the same task as every other node for its own copy of the network data in order to attempt being first when coming up with a solution.

By design, there is a finite amount of "coins" available in the network, with the value of each unit being determined by the concept of supply and demand along with constantly changing levels of difficulty needed to mine each coin (Ahamad, Nair, & Varghese, 2013). The actual transaction between accounts is fast and efficient, the difficulty comes in when there is a need to convert currencies from fiat to crypto. This has been one of the deterring factors among merchants, traders and customers for adoption of this new technology. The large demand from Blockchain for storage is also a major issue. It can be over 8GB in size which poses a problem for mobile phone users. Ahamad et al. (2013) suggested considering a third party for storage needs. There is also the case of barriers to those who are not technologically savvy.

Bitcoin is still in its infancy needing more development to occur and remain highly volatile compared to major fiat currencies. There are also far too many to choose from. The volatility makes planning and budgeting nearly impossible for businesses (Vejacka, 2014).

System files stored on users' mobile devices and computers have the risk of being damaged. This results in wallet files being damaged and forever lost (if the wallet file was not backed up by the user) (Vejacka, 2014). These wallets are also high risk for theft from digital predators. It is practically impossible to hedge for any risks associated with cryptocurrencies since the value of Bitcoin does not exhibit any correlation with any fiat currency (Nigam, 2016).

Lastly Varriale (2013) touches on concerns regarding the safety of deposit (particularly after the bail-out of Cypriot depositors). The unwavering concern by regulators has reared its head after 22 Bitcoin companies were subpoenaed. These companies were requested to provide anti-money laundering controls they have put in place along with consumer protection measures and their investment strategies.

3.9 Conclusion

A lot can be learnt from purely understanding how Blockchain and bitcoin work within the realm of financial innovation. This technology shows the multifaceted nature of this innovation which is yet to be seen from other previous financial innovations. Its ability to transcend its original use for financial transactions is testament to the evolution of financial innovation to go beyond just

finance to even more social realms. This makes Blockchain a formidable force to be reckoned with. It seems to have so much to offer and the pioneers of this world have not wasted time in applying some of the benefits Blockchain enthusiasts are eager to explore. Even with the technology's pitfalls, a lot can still be tweaked to create the ultimate financial innovation to forever change the way things are done.

4 BLOCKCHAIN USE CASES

"Bitcoin is better than currency."

- *Bill Gates* (Gaines, 2017)

To get a sense of how this phenomenon is being experienced, the paper will investigate some of the financial innovation's current use cases in this chapter with focus on the financial industry.

4.1 Overview of Potential Blockchain Uses

It has been argued by Pisa and Juden (2017) that while Blockchain-based solutions have the potential to increase output and immensely improve efficiency in certain use cases and more marginally in others, the main challenge in addressing issues does not lie within the scope of technology. The challenges lie in what is hampering Blockchain from reaching its full potential in various spaces.

Two approaches are seen in implementing this technology. External deployment assists in connecting parts of the financial trade system, different entities and banks and providing common frameworks for managing commerce. The second approach is more internal where individual institutions use it to increase efficiencies. Both approaches can be of great significance in the South African space (Wright, 2017).

One of the recent drivers of sustainable economic growth is technological innovation which is has been on the rise due to higher rates of innovation, even more so financial innovation. Innovation has been cited by Pisa and Judan (2017) as a tool to reduce poverty at low cost as well as improve the functioning of the private and public sector. This was just a tip of the ice berg on the vast changes to the way things are done and how the way we think can be influenced by the introduction of new technologies which are explored not only for business profits but for making the world work in a better, sustainable way.

Catalini and Gans (2017) showed how Blockchain challenges the existing revenue models and accumulated knowledge and resources of incumbents, and open opportunities for new approaches to start-up fundraising, the provision of public goods and software protocols, data ownership and licensing, auctions and reputation systems. Silva (2017) added to this by showing how the technology offers faster speeds ranging from minutes to hours as opposed to the three days it takes to settle instruments such as equities, private debt instruments and corporate bonds. Even syndicated loans can see settlement time being cut down to one day as opposed to the usual many days. The most obvious application of Blockchain to the financial world is with auditing which can now be done in real time, making it easier for regulators to dig into corporate records.

With the technology still being in its infancy, there is more to be tested and explored in order to see how much value can be gained from the use of Blockchain and whether it will be adopted into the financial industry. In recent years, we have seen big corporations join the movement in researching the technology with no actual implementation as yet. It will be interesting to see this

technology mature and perhaps become our new norm. Other current developments using the Blockchain technology include contractual agreements, confirmation of identities, registering of property and real-time money payments and transfers. Tapscott and Tapscott (2017) said that similar to the first generation of the internet, Blockchain is being described as the second generation which will not only be disruptive to how business models are seen but will also transform industries.

The disruptive technology seen with the introduction of FinTech (financial technology) has sent shock waves across the financial sector. The rapid growth of the likes of Blockchain and Bitcoin has opened a new gateway for ways to tackle financial exclusion in less-developed countries. This has, however, been slowed down by the lower level of risk that these financial institutions are willing to take; making the adoption of FinTech that more difficult. From anti-money laundering and anti-terrorism laws to increased levels of fraud, having what is seen as high-risk clientele (mainly from low income groups in developing countries), has deterred big financial institutions from wandering into this under-developed terrain. This is a shame since it is in these regions where the most need for fund transfers is found. With the great extent of uncertainty around money transfer technology and the haze around how any form of digital currency (cryptocurrencies included) will be regulated to put these financial giants at ease makes it difficult to envision an efficient cross-border fund transfer system for those who need it the most (Edwards, 2016).

Blockchain (a form of distributed ledger technology) is described as "a network software protocol that enables the secure transfer of money, assets and information via the internet, without the need for a third-party intermediary such as a bank". Can you imagine a world where your credit score is available globally, allowing customers the option to lend from anywhere with competitive interest rates.

The first use case seen by the world powered by Blockchain fell under the world of banking and finance in the form of bitcoin. Swam (2017) looked at four different applications of the Blockchain technology: "digital asset registries, Blockchains as leapfrog technology for global financial inclusion, long-tail personalised economic services and net settlement payment channels". The author argued that the potential risk wold be outweighed by the benefits. The author also mentioned smart assets which are placed on a list and deemed digital assets where these smart assets are easy to verify and transfer due to this digital registration. Some of these assets include land, homes, and vehicles.

It is further said by Wright (2017) how the introduction of smart contracts has the potential to remove the need for lawyers to necessarily be middlemen between clients (Wright, 2017). Syspro (2017) agreed stating that these digital protocols remove the need for any third party such as banks for clearing payments. The existence of smart contracts gives businesses the opportunity to get a say in whether they want to form part of a business bank clientele or not. They do not have to deal with merchant accounts either. Businesses can receive immediate

payment since transactions will be even faster. All that is needed is a good internet connection and a wallet for bitcoin (SYSPRO, 2017). Smart contracts are said to be like known regular contracts (where there exists an agreement between two or more parties with terms and conditions) by Swan (2016). The author notes that the challenge with code-based smart contracts is its automatic execution even when the terms and conditions have been breached by one party.

Smart contracts use an "if-then" method, similar to what is found in a legal contract. The advantage is found where smart contracts can be automatically executed according to the conditions of the smart contract (which must be agreed upon by all parties involved). For transactions which need payment upon receipt of goods such as commodities, once the entry is added to the Blockchain, it can be seen by everyone after which a trigger causes an automatic payment (using cryptocurrency) to the supplier's Blockchain account. The supplier is able to form a digital reputation for future such transactions due to high levels of transparency affording them a much-needed competitive edge (Wright, 2017).

Major challenges faced by smart contracts include being immutable, too secretive and whether they can be enforced by the courts (Nowinski & Kozma, 2017).

FORUS (Free, Open, Real-time, Ubiquitous and Secure) has created its Global Digital Exchange, a "public utility Blockchain and ecosystem solution that will aim to provide a single, global, universal, trusted, user-authentication platform for both mobile and web-based transactions, for the banked and the unbanked". This solution was created by South African engineers and revealed in Johannesburg on the 6th of December 2017. FORUS aims to help in increasing financial inclusion in South Africa (Workman, 2017).

The biggest driver for financial institutions to look towards incorporating Blockchain in their systems is to help reduce transactional banking costs. South African bank ABSA (a subsidiary of Barclays Africa) has joined other global banks (45 other market giants in financial services) in July 2017 to get the R3 Consortium to assist in exploring Blockchain for the financial sector. One can see the positive outlook for Blockchain in South Africa when even the South African Reserve Bank’s governor announced that the Reserve Bank was open to new technologies including Blockchain and other digital currencies. To further give support, South Africa’s Central Securities Depositories (CSDs) Strate signed a Letter of Intent with Russia’s National Settlement Depository (NSD) to partner in finding Blockchain solutions (Campbell R. , 2017).

R3 is a New York based innovation start-up which has formed a consortium and has a coalition of 45 companies (Deloitte, (2017)) which are developing Blockchain for use in the global financial system. Other companies which have joined in developing Blockchain apart from ABSA include Santander, USB, BNY Mellon and Deutsche Bank which have partnered with a Blockchain developer- Clearmatics- to create central bank aimed new digital currency. The R3 consortium along with 15-member banks have started dabbling in smart contracts and have been using them to help process accounts receivable (AR), purchase transactions (or invoice financing

or factoring) and letter of credit (LOC) transactions. These are only in the prototype phase (Ogundeji, 2017).

In view of what the R3 consortium is aiming to achieve, more testing and development is needed before The South African Reserve Bank will recognise and use Blockchain for financial transactions (Anderson, 2016).

With stringent laws around customer information, especially in knowing their identities, the Financial Intelligence Act (FICA), requires all financial institutions to ensure that they verify the identities of all their clients. Banks must be compliant to maintain their banking licenses, but this is a demanding process. Decentralising such a process can assist not only banks but all other institutions needing to verify identities. These institutions can work with South Africa's home affairs department in ensuring data validity and quality. Even medical records can be stored in distributed ledgers (Kloete, 2017).

Know-Your-Customer (KYC) and the Financial Intelligence Centre Act (FICA) are data intensive and take time and resources to be completed by financial institutions. To this effect, it is only natural that the South African Financial Blockchain Consortium -SAFBC- is looking to also explore ways to better manage customer information in a secure way, reducing the need for all the paper work currently involved (Naidoo, 2017).

Exploring KYC is a brilliant example of banks coming together for reaching a common set of standards and best practice when using Blockchain. But why even bother with KYC? There has been a collaborative global fight to prevent financing terrorism and money laundering. However, these initiatives are costly to maintain by individual financial firms. Deloitte (2017) showed that money spent globally on Anti-Money-Laundering (AML) in 2014 amounted to approximately $10 billion. Financial institutions are being required to reduce their costs, but this may be difficult with rising compliance costs. KYC adds to this burden and easily delays transactions (taking up to 50 days to reach satisfactory levels). There is currently duplication of effort among these financial firms further increasing the costs. Introduction of a distributed ledger is only natural as it can automate processes reducing compliance errors. The Blockchain would be able to also remove the duplication of work and allow client details to be updated, encrypted and shared with all network members in near real time. Historical records will be easy to find for ease of verifying compliance audit trails to the regulators. With the large volume of data available to entities, they will be able to spot irregularities and uncover any criminal activity.

Within the world of finance, big stock exchanges ranging from NYSE, Deutsche Börse, the London Stock Exchange and Nasdaq have been looking at Blockchain for their payment needs. The issue of trust has been raised by Nowinski and Kozma (2017) but one should consider how trust is never an issue with the big corporates when it comes to transactions and their security since these big institutions have measures in place such as clearing houses at exchanges to ensure trust. Trust, however, is still to be considered in other transactions such as crowd funded firms. These kinds of companies are forerunners for enjoying the benefits of Blockchain where shares

need to be registered and funds need to be managed along with corporate governance (all business features which need trust and transparency to function).

Lastly, Deloitte (2017) cited how Citi claimed to have built three Blockchains and created its own cryptocurrency, 'Citicoin', to test them. The big bank has also claimed to be the first investment bank to file to obtain the first patent for a securities settlement system using cryptocurrencies.

Bundling of some of these new implementations of Blockchain can see efficiency levels increasing. An example of this would be if identity services, banking services and land registration were to come together and share information.

Another recent application of the Blockchain technology came in the form of Tendermint which was co-founded by Ethan Buchman who called it the "general purpose Blockchain middleware". Tendermint can swap and change between Blockchain applications and protocols allowing programmers the option of choosing their preferred programming language as well as the environment. Buchman further gave Tendermint his stamp of approval by deeming it to meet "the highest standards of security", allowing the network to continue functioning when a third of the nodes randomly fail. It uses proof-of stake as its consensus algorithm. Its ability to be a plug-and-play in terms of replacing other Blockchain softwares' consensus engines, gives it a competitive edge (Tapscott & Tapscott, 2017).

The South African Financial Blockchain Consortium (SAFBC), made up of 22 top industry firms including ABSA, FirstRand, Capitec, Nedbank, Standard Bank and even non-financial institutions such as Bowmans, the University of Cape Town and Maitland, with oversight by the Reserve Bank and the Financial Services Board, have come together to understand Blockchain technology. Farzam Ehsani, SAFBC chairperson put it well saying that "no single company can launch its own proprietary Blockchain that will change the status quo and bring about transformative benefits to the financial system. Collaboration is required." Government and private sector need to come to the table to find a way to move forward and optimise this technology for the greater good of South Africa and its citizens. A domestic standard will be needed across all industries (Naidoo, 2017).

Golix (Zimbabwe's Harare-based trading platform) reached remarkable highs when surpassing the $10 000 mark for Bitcoin in 2017. Some merchants such as importers and car dealerships in Zimbabwe are happy to accept Bitcoin as a means of payment. This has caused Bitcoin to be common in the country's capital. Venezuela is also among some of the countries in the world with a dysfunctional economy which has driven citizens to look for alternative currencies. One can note that monetary policy or political uncertainty are usually the main push factors. The Bitcoin Market Potential Index created by Dr Garrick Hileman, an economic historian from the University of Cambridge has ranked Zimbabwe third, with Argentina and Venezuela ahead of it for having inflation-plagued economies (Monks, 2017).

Sleiman et al (2015) touched on the mostly unknown functionality of Bitcoin. The Bitcoin Blockchain has the "Bitcoin Message Services" embedded in it. This service was created to send and receive information through Bitcoin. For this reason, Bitcoin has a message functionality which can further be explored but remains unused at the present moment (no further developments to it have been done).

South Africa has seen a few pioneers in the Blockchain and cryptocurrency space. Five of these companies are top of mind as shown by Simons (2017). There is Monero which was created in 2014; it brands itself as “secure, private and untraceable”, with accounts and transactions being cryptographically secured.

Civic is a start-up that uses Blockchain to secure identities and prevent fraud. It is able to notify consumers when banks and other institutions access their private data and gives the consumer the option to approve or deny the request. It is currently based in the Silicon Valley but plans to move to Cape Town (as it is owned by a South African).

Luno (formerly known as BitX) is a full-featured cryptocurrency platform with support and functionality options for use with wallets. Luno also offers the major South African banks support in this regard. The offering goes beyond the South African borders with offerings in Malaysia, Kenya, Spain and Nigeria.

A company which enables customers to pay for their electricity bill (when using electricity meters) is Bankymoon. They did their bit for society and delivered these meters to needy schools, allowing anyone around the world to pay for their electricity with cryptocurrency. Bankymoon has been leveraging Bitcoin along with other cryptocurrencies for executing electronic payments and even securities trading. They too have started to find solutions for reaching the unbanked by traditional banks (Tozzi, 2017).

Ekasi-bucks, launched in 2016, is a start-up cryptocurrency firm using Blockchain technology providing customers with wallets, an exchange and point of sale systems. They also offer a loyalty program, consumer analysis systems and inventory management. The company helps bridge the gap by providing the unbanked with banking offerings (they have over 300 000 unbanked clients). They too used Initial Coin Offering (ICO) to raise capital (IT News Africa, 2017).

So far, many of the use cases have been seen in the financial world with the likes of settlements, remittances, claims, transaction of securities, etc. Another use case is in crowd funding and investments to start-ups and artists. Contributors receive dividends as per the smart contract under Swarm (a trial implementation). Other applications include message services and social networking services, providing content on the internet, and decentralised medical services, hotel bookings and academic credentials (Ambili, Sindhu, & Sethumadhavan, 2017).

Edwards (2016) looked at some of the benefits which can be gleaned from the use of digital money and technology which can reduce costs, save time and increase transparency. The article discussed an up and coming player, BitPesa which uses Blockchain as its digital ledger to create a worldwide network of "market -makers". These market-makers can then transparently transact with each other on this database. BitPesa has operations in Nigeria, Kenya, Tanzania, Senegal, Uganda and Democratic Republic of the Congo. Their selling point is their ability to remove the third party (mainly banks) from the transactions while still managing to send remittances; this significantly lowers their transaction costs (to as low as 1-3 percent as well as being faster from the usual duration of a week to a day).

SALT -Secure Automated Lending Technology- is the first "asset-backed" lending platform to allow asset holders who use Blockchain access to liquidity without them having to sell their tokens. To get one-year access with a loan amount of up to $10 000, a SALT coin is purchased for $25. Increasing ones SALT coins gives access to a larger loan amount. Collateral is taken in the form of cryptocurrencies and the traditional periodic instalments are paid for repaying the loan. The system works as with clearinghouses where if the value of the collateral (the cryptocurrency) drops below the margin requirement, a margin call will be sent to the borrower, which needs to be fulfilled otherwise the asset will be is liquidated to cover the remaining part of the loan. Missed payments result in portions of the collateral being liquidated. No credit checks are done on potential borrowers (Hallik, 2017).

4.2 Conclusion

A plethora of case studies around the use of Blockchain and bitcoin as a financial innovation with a lot of potential have been discussed. These examples shed light on the full phenomenon of this innovation making one wonder what else this technology is able to accomplish.

5 CONCLUSION

"One thing that's missing but will soon be developed is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A—the way I can take a $20 bill and hand it over to you, and you may get that without knowing who I am."

— Milton Friedman (1999)

Blockchain…Bitcoin…the future of data storage and data transfer arrived at the world's door in 2008 and is ready to take it by storm. As a new financial innovation, it has had its fair share of teething problems and sceptics but has managed to so far push forward and created a name for itself. Still misunderstood, many have attempted to explore and understand what this technology is about and how it can be used outside its initial use as bitcoin.

Described as a combination of cryptography and currency, cryptocurrency has the potential to be seen as a currency. This potential is being hampered by its high volatility which has it violating being a store of value, an attribute of currency. Bitcoin has a long way to go in being accepted if the regulators come to the party. The technology driving bitcoin is Blockchain, a distributed ledger which has the potential to solve many issues and inefficiencies seen around the world in all industries. This paper has attempted to unpack what Blockchain and bitcoin are: how they work, where they work and what the fuss is about.

The technology has been rising to the occasion for the past two to three years by offering the potential to be applied in the financial industry. Blockchain has the potential ability to change the way data is handled giving it a disruptive nature worthy of being explored and understood. However, not much is known and understood about these applications in the world, let alone in the South African landscape. As an ever-evolving country, South Africa has also jumped onto the bandwagon of using Blockchain and even more so of adopting bitcoin. However, the future of this technology and its uses remains uncertain.

As South Africa gears itself to explore these new ways of doing things, it is with hope that the world (from single individuals to institutions) will take up the challenge in trying to make things work better, mainly so for the improvement of normal lives.

A lot can be learnt from purely understanding how Blockchain and bitcoin work in the context of financial innovations. Although one should note that there is yet to be a consensus to the meaning of financial innovation as shown in the paper. Blockchain and bitcoin seem to have so much to offer and the pioneers of this world have not wasted time in applying some of the benefits Blockchain enthusiasts are eager to explore. Even with the technology's pitfalls, a lot can still be tweaked to create the ultimate financial innovation to forever change the way things are done.

A plethora of use cases have been discussed making one wonder what else this technology is able to accomplish. These applications along with some of the challenges faced have shown the value that can be extracted from using Blockchain. It can be agreed across the board that indeed, Blockchain is yet to change the financial world and is doing so one experiment at a time as development continues to increase. An exciting future awaits us.

The completed mandate was to fully unpack the nature of Blockchain technology and bitcoin with relation to financial innovation and to see the process by which it is evolves or is experienced within the financial industry in South Africa. This has successfully been done by the paper with the help of secondary sources.

With Bitcoin now being tracked by financial institutions, it would be interesting to see what the take up rate of bitcoin is and will be in South Africa. This could be coupled with finding out the rate of diffusion of this financial innovation and measuring its success over a certain period. Factors which can affect success, as mentioned by Flood (1992), are finding insight in the demands of potential users and finding whether there already exists a potential substitute to rival the innovation. Unfortunately, it is nearly impossible to codify all the elements of a successful innovation into a collection of rules. Perhaps focusing only on the success of bitcoin might be valuable.

Another idea at further looking into this topic would be to model the relationship between its inception and its effect on the South Africa's economic growth, similar to the works of Bara et al (2016).

The burning question that remains is whether Blockchain and bitcoin are an important disruptive financial innovation which are here to stay in South Africa?

6 REFERENCES

1. Ahamad, S., Nair, M., & Varghese, B. (2013). A Survey on Crypo Currencies. *Association of Computer Electronics and Electrical Engineers*, 42-48.

2. Akhavein, J., Frame, W., & White, L. (2005). The Diffusion of Financial Innovations: An Examination of the Adoption of Small Business Credit Scoring by Large Banking . *Journal of Business Vol. 78 No. 2*, 1-24.

3. Alkema, P., & Chen, J. (2016). *Digital Disruption: New Imperstives for Leadership and Innovation-Perspectives from the Banking Industry.* Johannesburg: University of Pretoria: Gordon Institute of Businss Science.

4. Ambili, K., Sindhu, M., & Sethumadhavan, M. (2017). On Federated and Proof of Validation Based Consensus Algorithms in Blockchain. *IOP Conference Series: Materials Science and Engineering 225 012198* (pp. 1-9). IOP Publishing Ltd.

5. Anderson, M. (2016, November). *African banks warm to blockchain*. Retrieved from The African Report: http://www.theafricareport.com/International/african-banks-warm-to-blockchain.html

6. Bara, A., Mugano, G., & Le Roux, P. (2016). Financial Innovation and Economic Growth in the SADC. *Economic Research Southern Africa*, 1-22.

7. Basarir, C., & Sarihan, A. (2017). Financial Innovation in Turkish Banking Sector and Literature Review. *Research of Financial Economic and Social Studies*, 221-230.

8. Ben-Horim, M., & Silber, W. (1977). Financial Innovation: A Linear Programming Approach. *Journal of Banking and Finance 1*, 277-296.

9. Betz, F., & Khalil, T. (2011). Technology and Financial Innovation. *Internionol Journal of Innovation and Technology Management Vol. 8 No. 1*, 1-25.

10. Bistarelli, S., & Santini, F. (2017). Go with the Flow- Bitcoin- Flow, with Visual Analytics. *ARES 2017* (pp. 1-6). Italy: ARES.

11. Blach, J. (2011). Financial Innovations and their Roles in the Modern Financial System-Identification and Systematization of the Problem . *The Central European Journal of Social Sciences and Humanities Vol. 7 No. 3*, 13-26.

12. Bourji, S. (2017, November 15). *Ethereum Shows Signs of Life as Price Crosses $330*. Retrieved from Hacked: https://hacked.com/ethereum-shows-signs-life-price-crosses-330/

13. Brett, S. (2016). HOw Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance. *United Nations Research Institute for Social Development Working Paper , No. 2016-1*, 1-21.

14. Buckley, R., Arner, D., & Panton, M. (2014). Financial Innovation in East Asia. *Seattle University Law Review Vol. 37 No. 2*, 307-351.

15. Butterworth, B., & Malherbe, S. (1999). The South African Financial Sector: background Research for Seattle Round . *TIPS 1999 Annual Forum*, 1-97.

16. Buy Bitcoin Worldwide. (2018, March 4). *The Bitcoin Volatility Index*. Retrieved from Buy Bitcoin Worldwide: https://www.buybitcoinworldwide.com/volatility-index/

17. Camarate, J., & Brickmann, S. (2018). *The Future of Banking: A South African Perspective.* Johannesburg: PriceWaterhouseCoopers.

18. Campbell, R. (2017, November 24). *African Banks Start to See the Potential of Blockchain*. Retrieved from CCN: https://www.ccn.com/african-banks-start-to-see-the-potential-of-blockchain/

19. Campbell, R. (2017, January 25). *Blockchain Tech Used to Prevent Property Fraud in Africa*. Retrieved from CCN: https://www.ccn.com/blockchain-tech-used-prevent-property-fraud-africa/

20. Catalini, C., & Gans, J. (2017). *Some Simple Economics of the Blockchain.* Toronto: SSRN.

21. Champion de Crespigny, A. (2016). *Blockchain: the hype, the oppotunity and what you should do.* London: Ernest and Young LLP.

22. Cheung, A., Roca, E., & Su, J. (2015). Crypto-currency Bubbles: An Application of the Phillips-Shi-Yu (2013) Methodology on Mt. Gox Bitcoin Prices. *Applied Economics Vol. 47 No. 23*, 2348-2358.

23. Coin Gecko. (2018, March 3). *Bitcoin Price*. Retrieved from Coin Gecko: https://www.coingecko.com/en/price_charts/bitcoin/zar

24. CoinMarketCap. (2017, June 17). *Cryptocurrency Market Capitalizations*. Retrieved from CoinMarketCap: https://coinmarketcap.com/currencies

25. Connolly, A., & Kick, A. (2015). What Differentiates Early Organization Adopters of Bitcoin from Non- Adopters? *Twenty-first Americas Conference on Information Systems* (pp. 1-6). Pueto Rico: Emergent Research Forum Paper.

26. Copley, A. (2017, December 15). *Figures of the Week: Blockchain Opportunities and Challenges in Africa*. Retrieved from Brookings: http://wwww.brookings.edu/blog/africa-in-focus/2017/12/15/figures-of-the-week-blockchain-opportunities-and-challenges-in-africa/

27. Cryptocoincharts. (2017, July 28). *Info*. Retrieved from Cryptocoincharts: http://www.cryptocoincharts.info/coins/info

28. Dabrowski, M. (2017). *Potentia Impact of Financial Innovation on Monetary Policy.* Brussels: European Parliament: Directorate General for Internal Polices.

29. Das, S. (2017, November 15). *Asian Banking Giant DBS Calls Bitcoin a 'Ponzi Scheme'*. Retrieved from CryptoCoinNews: https://www.cryptocoinsnews.com/asian-banking-giant-dbs-calls-bitcoin-ponzi-scheme/

30. Deepika, P., & Kuar, R. (2017). Cryptocurrency: Trends, Perspective and Challenges. *International Journal of Trend in Research and Development Vol. 4 No. 4*, 4-6.

31. Deloitte. (2017). *Blockchain: Enigma. Paradox. Opportunity.* London: Deloitte LLP.

32. Dewi, D., & Soekarno, S. (2014). Alternative Invetsment Evaluation of Bitcoins, Gold and LQ45 Index. *International Conference on Trends in Economics, Humanities and Management*, (pp. 137-141). Pattaya .

33. Dwyer, G. (2014). The Economics of Bitcoin and Similar Private Digital Currencies. *Munich Persoanl RePEc Archive Paper No. 57360*, 1-31.

34. Edwards, S. (2016, December 9). *5 trends affecting the remittance industry*. Retrieved from DevEx: https://www.devex.com/news/5-trends-affecting-the-remittance-industry-89275

35. EY Think Tank. (2017). *How Blockchain can help to tackle Sub-Saharan Africa's challenges*. Retrieved from Ernest and Young: https://betterworkingworld.ey.com/digital/tackling-sub-saharan-africa-s-challenges-with-blockchain

36. Farell, R. (2015). An Analyisis of the Cryptocurrency Industry. *Wharton Research Scholars 130*.

37. Fernández-Villaverde, J. (2017, August 3). *Cryptocurrencies: Some Lessons from Monetary Economics*. Retrieved from Economist's View: http://economistsview.typepad.com/economistsview/2017/08/cryptocurrencies-some-lessons-from-monetary-economics.html

38. Flood, M. (1992). Two Faces of Financial Innovation. *Federal Reserve Bank of St. Louis Review (September/October)*, 3-17.

39. Frame, W., & White, L. (2014). Technological Change, Financial Innovation and Diffussion in Banking. *NYU Working Paper No. 2451/33549*, 1-37.

40. Gaines, R. (2017, November 13). *IF YOU BOUGHT $5 OF BITCOIN 7 YEARS AGO, YOU'D BE $4.4 MILLION RICHER*. Retrieved from Daily News: http://finance.dailynews.ovh/index.html?a=99420&chm_sub6=000b500f72b4849afd98cc79f44b9c8af5&chm_sub7=BizNews.com&chm_DCID=31525197394644118&chm_ZID=7771

41. Gammon, E., & Wigan, D. (2015). Veblen, Bataille and Financial Innovation . *Theory, Culture and Society Vol. 32 No. 4*, 105-131.

42. Gandal, N., & Halaburda, H. (2014). Competition in the Cryptocurrency Market. *Bank of Canada Working Paper No. 2014-33*, 1-29.

43. Garfinkle, C. (2017, October 12). *The Naked Truth about Bitcoin*. Retrieved from Investing for Dummies: http://tradingfordummies.info/the-whole-truth-about-bitcoin/?brand=100610&link=https%3A%2F%2Fspecialfinanceoffers.com%2Flps%2Fbitcoin_v2%2F%3Ffunnelid%3Dfid-1-42-229-0-0-181-1506589943124%26utm_campaign%3DZP_Outbrain_1%26utm_creative%3Dbitcoin_v2%26utm_su

44. Gold Price. (2018, march 4). *Bitcoin Pirce*. Retrieved from Gold Price: https://goldprice.org/cryptocurrency-price/bitcoin-price

45. Goodin, D. (2016, June 21). *Bitcoin rival Ethereum fights for its survival after $50 million heist*. Retrieved from Aer Techinica: https://arstechnica.com/information-technology/2016/06/bitcoin-rival-ethereum-fights-for-its-survival-after-50-million-heist/

46. Hallik, C. (2017, December 13). *SALT – A Technology Bringing New Opportunities?* Retrieved from The Market Mogul: https://themarketmogul.com/salt-crypto-bringing-new-opportunities-key-gates-hell/

47. Hausman, A., & Johnston, W. (2014). he Role of Innovation in Driving the Economy: Lessons from the Global Financial Crisis. *Journal of Business Research Vol. 67 No. 1*, 2720-2726.

48. Heid, A. (2017). *Analysis of the Cryptocurrency Marketplace.* Retrieved from Brave New Coin: htt[s://bravenewcoin.com/assets/Whitepapers/HackMiami-Analysis-of-the-Cryptocurrency-Marketplace.pdf

49. Hilal, K. (2017). *Blockchain technology and Africa's financial revolution*. Retrieved from RedCloud Technologies: https://redcloudtechnology.com/blockchain-technology-africas-financial-revolution/

50. Hull, I. (2016). The Development and Spread of Financial Innovation. *Quantitative Economicss 7*, 613-636.

51. Hurlbert, G., & Bojanova, I. (2014, May/June). Bitcoin: Benefit or Curse? *IT Trends*, pp. 10-15.

52. Intergovernmental Fintech Working Group. (2018). *Fintech Workshop.* Pretoria: Intergovernmental Fintech Working Group.

53. IT News Africa. (2017, July 5). *South Africa: Blockchain startup to service R50 billion Township economy*. Retrieved from IT News Africa: http://www.itnewsafrica.com/2017/07/south-africa-blockchain-startup-to-service-r50-billion-township-economy/

54. Jackson, T. (2017, September 19). *African blockchain moving away from payments narrative*. Retrieved from Disrupt Africa: http://disrupt-africa.com/2017/09/african-blockchain-moving-away-from-payments-narrative/

55. Johnson, S., & Kwak, J. (2011). Is Financial Innovation Good for the Economy? In J. Lerner, & S. Stern, *Innovation Policy and the Economy Volume 12* (pp. 1-5). Chicago: University of Chicago Press.

56. Khatoon, G., & Fiyazi, S. (2016). Financial Innovation that will fuel the Growth of Economy. *International Conference on Recent Developments Emerging Trends in Management Research and Information Science* (pp. 515-520). Krupanidhi: Novitat.

57. Kloete, C. (2017, October 13). *Blockchain technology set to shake up business in Africa*. Retrieved from Engineering News: http://www.engineeringnews.co.za/article/blockchain-technology-set-to-shake-up-business-in-africa-2017-10-13

58. Lee, K., James, J., Ejeta, T., & Kim, H. (2016). Electornic Voting Service using Blockchain. *Journal of Digital Forensics, Security and Law Vol 11 No 2*, 123-136.

59. Lerner, J. (2006). The New New Financial Thing: The Origins of Financial Innovations. *Journal of Financial Economics Vol. 79 No. 2*, 223-255.

60. Luther, W. (2016). Bitcoin and the Future of Digital Payments. *The Independent Review Vol. 20 No. 3*, 397-404.

61. Maese, V. (2014). Divining Regulatory Future of Illegitimate Cryptocurrencies. *Wall Street Lawyer Vol. 18 Issue 5*, 7-10.

62. Maurer, F. (2016). A Survey on Approaches to Anonymity in Bitcoin and Other Cryptocurrencies . *Gesellschaft fur Informatik*, 2145-2150.

63. Mckenzie, R. e. (2016). *Studies in Financial Systems No 15: The South Afican Financial System.* Johannesburg: Financialisation, Economy, Society and Sustainable Development.

64. Mendes-Da Silva, W. (2015). Financial Innovation: An Expanding Research Field . *Journal of Financial Innovation Vol. 1 No. 1*, 1-3.

65. Monks, K. (2017, October 31). *What is fueling Zimbabwe's record-breaking Bitcoin binge?* Retrieved from CNN Africa: http://edition.cnn.com/2017/10/31/africa/zimbabwe-bitcoin-surge/index.html

66. Naidoo, P. (2017 , July 11). *SA takes steps to set up national financial blockchain*. Retrieved from Moneyweb: https://www.moneyweb.co.za/news/tech/sa-takes-steps-to-set-up-national-financial-blockchain/

67. Newkirk, S. (2017, November 15). *There will only ever be 21 million Bitcoins; What is a Coin "Harrd Cap"?* Retrieved from CryptoStache: http://cryptostache.com/2017/11/15/will-ever-21-million-bitcoins-coin-hard-cap/

68. Nigam, A. (2016). Bitcoin: The Futuristic Cryptocurrency for E-commerce Remittances. *International Journal of Languages, Education and Social Sciences Vol. 21 Issue 1*, 1-4.

69. Nihilent Technologies. (2017, March 17). *The Blockchain opportunity*. Retrieved from IT Web: http://www.itweb.co.za/index.php?option=com_content&view=article&id=160508

70. Nowinski, W., & Kozma, M. (2017). How Can Blockchain Technology Disrupt the Existing Business Model? *Entrepreneural Buisness and Economic Review Vol. 5 No. 3*, 173-188.

71. Ogundeji, O. (2017, August 12). *Law Experts: Why Banks Are Scared of Blockchain*. Retrieved from CCN: https://www.ccn.com/banks-scared-blockchain/

72. Peck, M. (2013). The Bicoin Arms Race is on! *IEEE*, 11-13.

73. Pisa, M., & Juden, M. (2017). *Blockchain and Economic Development: Hype vs. Reality.* Washington DC: Center for Global Development.

74. Ramakrishnan, R. (2015, September 27). *Financial Innovation and Regulation.* Retrieved from SSRN: https://ssrn.com/abtract=2336477

75. Ramakrishnan, R., & Perumal, R. (2008). Financial Enginerring and Stakeholder Management. *Bharathidasan University of Trichy: International Conference* (pp. 1-7). Trichy: Bharathidasan University of Trichy.

76. Raymaekers, W. (2014). Cryptocurrency Bitcoin: Disruption, Challenges and Opportunities. *Journal of Payments Strategy & Systems Vol. 9 No. 1*, 30-40.

77. Saewitz, J. (2017, May 21). *Africa to Receive its First Bitcoin ATM*. Retrieved from CCN: https://www.ccn.com/africa-receive-first-bitcoin-atm/

78. Salampasis, D., & Menntion, A. (2013). *Financial Innovation and Sustainable Development.* Luxembourg: Tudor.

79. Schindler, J. (2017). FinTech and Financial Innovation: Drivers and Depth. *Finance and Economics Discussion Series 2017-081*, 1-16.

80. Schuh, S., & Shy, O. (2016, August 30). *U.S Consumers' Adoption and Use of Bitcoin and Other Virtual Currencies.* Retrieved October 2, 2017, from De Nederlandsche Bank: http://www.dnb.nl/en/binaries/Consumers%20VC%20paper_DNB_FINAL_corrected

81. Scott-Briggs, A. (2016, September 17). *10 Blockchain technologies AFfrica*. Retrieved from TechBullion: https://www.techbullion.com/10-blockchain-technologies-africa/

82. Serapiglia, A., Serapiglia, C., & McIntyre, J. (2015). Cryptocurrencies: Core Information Technology and Information System Fundamentals Enabling Currency Without Borders. *Information Systems Education Journal Vol. 13 No. 3*, 43-52.

83. Shah, S. (2013, April 14). *Iterations: How Five Real Economists Think About Bitcoin's Future*. Retrieved from Tech Crunch: https://techcrunch.com/2013/04/14/iterations-how-five-real-economists-think-about-bitcoins-future/

84. Sharma, S., Nisar, N., & Raina, C. (2017). Survey Paper on Cryptocurrency. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology Vol.2 Issue 3*, 307-310.

85. Silva, J. (2017, March 5). *The Economics of Blockchain*. Retrieved from The Market Mogul: https://themarketmogul.com/economics-blockchain/

86. Smith, J. (2016). An Analysis of Bitcoin Exchange Rates. *SSRN No. 2493797*, 1-28 .

87. South African Reserve Bank. (2018, March 2). *Seleceted Historical Exchange and Interest Rates*. Retrieved from South African Reserve Bank: https://www.resbank.co.za/Research/Rates/Pages/SelectedHistoricalExchangeAndInterestRates.aspx

88. Storyful. (2017). *Insights into Blockchain: Opportunities and Challenges across Multiple Industries.* Paris: Capgemini.

89. Sukamulja, S., & Sikora, C. (2018). The New Era of Financial Innovation: The Determinants of Bitcoin's Price . *Journal of Indonesian Economy and Business Vol. 33 No. 1*, 46-64.

90. SYSPRO. (2017, March 24). *Blockchain and the future of finance*. Retrieved from IT Web: http://www.itweb.co.za/index.php?option=com_content&view=article&id=160473&utm_source=Recommended&utm_medium=Web&utm_term=Blockchain&utm_content=Blockchain&utm_campaign=Recommended

91. Tapscott, D., & Tapscott, A. (2017). *Realizing the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies.* Geneva and San Francisco: World Economic Forum.

92. Tozzi, C. (2017, June 15). *Is Africa the next hub for Blockchain Development?* Retrieved from Nasdaq: www.nasdaq.com/article/is-africa-the-next-hub-for-blockchain-development-cm803927

93. van Geffen, N. (2017). *The Sun Exchange named 'best African Blockchain & bitcoin company 2016' at the African fintech awards 2016*. Retrieved from FinTech Africa: https://2017.fintech-africa.com/blog/feed/the-sun-exchange-named-best-african-blockchain-bitcoin-company-2016-at-the-african-fintech-awards-2016

94. Vejacka, M. (2014). Basic Aspects of Cryptocurrencies. *Journal of Economy, Business and Financing Vol. 2 Issue 2*, 75-83.

95. Vora, G. (2015). Cryptocurrencies: Are Disruptive Innovations Here? *Modern Economy 6*, 816-832.

96. Wall, L. (2014). *Two Drivers of Financial Innovation.* Atlanta: Federal Research Bank of Atlanta.

97. Workman, D. (2017, December 6). *FORUS unveils blockchain powered global digital exchange*. Retrieved from IT News Africa: http://www.itnewsafrica.com/2017/12/forus-unveils-blockchain-powered-global-digital-exchange/

98. Wright, B. (2017, August 4). *What is the potential for blockchain in Africa?* Retrieved from IDG Connect: http://www.idgconnect.com/abstract/27673/what-potential-blockchain-africa

99. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus and Future Trends. *IEEE 6th International Congress on Big Data* (pp. 557-564). Honolulu: IEEE Computer Society.