A study of the relationship between economic and technical aspects of bitcoin

by

Johan Frederik Kirsten

Submitted in partial fulfilment of the requirements for the degree

Magister Scientiae

in the Department of Mathematics and Applied Mathematics
in the Faculty of Natural and Agricultural Sciences

University of Pretoria
Pretoria

August 2019

SUMMARY

A STUDY OF THE RELATIONSHIP BETWEEN ECONOMIC AND TECHNICAL ASPECTS OF BITCOIN

by

Johan Frederik Kirsten

Supervisor: Prof. E. Maré

Department: Department of Mathematics and Applied Mathematics

University: University of Pretoria

Degree: MSc in Financial Engineering

Keywords: bitcoin; cryptocurrency; stochastic price model; arbitrage trade; sovereign cryptocurrency; money service business

This study investigates the cryptocurrency called bitcoin. A cryptocurrency is a type of currency that depends on cryptography to issue new units instead of depending on government decree like fiat currencies. The study will first explain some of the technical details that make bitcoin work. This is necessary to lay groundwork to get to the actual aim of the study, namely investigating the economic aspects of bitcoin.

The study will evaluate bitcoin, and other cryptocurrencies, along with fiat currencies against certain definitions. In the process it will introduce a new subclass of cryptocurrency - the sovereign cryptocurrency. Bitcoin's implied monetary policy will also be discussed, as well as the problems it creates for central banks.

A hypothesis on the behaviour of the bitcoin price will be explained and research will be provided to support the acceptance of the hypothesis. Using this hypothesis, a stochastic pricing model for bitcoin will be derived. Arbitrage trading strategies will also be provided that explain certain price constraints that operate in the bitcoin market.

The dissertation will also introduce a means to improve the anonymity of a user of bitcoin and will reason that improvements such as these and others will increase the use of bitcoin.

Therefore, improvements to anonymity will increase the economic relevance of bitcoin and increase its competitive edge over the traditional banking system.

It will be reasoned, based on the possible problems created by bitcoin's monetary policy, as well as the growth projections implied by the stochastic pricing model, and the increased economic relevance due to improvements in anonymity, that central banks would need to create their own cryptocurrency that conforms to certain requirements – the previously introduced sovereign cryptocurrency.

The study will conclude by explaining the technical changes needed for a fork of bitcoin to become a sovereign cryptocurrency, as well as a mathematical model to control the monetary policy of the sovereign cryptocurrency. As its aim, adaptive monetary policy will have stable prices for the economy using the sovereign cryptocurrency to price its goods and services.

Please note, that while every effort was made to use published references, the field of cryptocurrencies is very young and changing constantly. Thus, most publications on the subject are simply placed on websites on the internet. This is especially true for the work relating to the founding of the field, and the data sources of the operation of the cryptocurrencies. Therefore a lot of the references do refer to websites on the internet.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Central Bank Digital Currency…….. CBDC

Collateralised Debt Obligation…….. CDO

Cumulative Distribution Function…… CDF

Elliptic Curve Cryptography…… ECC

Great Financial Crisis…… GFC

I Owe You…….…… IOU

Modern Monetary Theory……..... MMT

Money Service Business……... MSB

Rivest-Shamir-Adleman…… RSA

Unspent Transaction Output……. UTXO

Proof-of-Work…….. PoW

LIST OF DEFINITIONS

Currency: A system of measurement of economic value

Financial asset: An asset in which the holder of the asset has the contractual right to receive compensation from a counterparty that has the contractual obligation to provide that compensation

Real asset: An asset where the holder of the asset has full control of the asset and there is no counter party

Commodity: A class of real assets that are fungible and can be bought and sold in a market

Money: Any currency that fulfils the functions of money, which include serving as a unit of account, a means of exchange and a store of value.

Unit of account: The prices of goods and service of a country are priced in the currency

Means of exchange: The currency is used in the sale and purchase of goods and services

Store of value: The value of the currency in relation to the goods and services of the country is stable

Cryptocurrency: A type of currency that depends on cryptography to secure its value instead of depending on government decree like fiat currencies

Blockchain: The database used to store the transactions of a cryptocurrency and comprises a chain of blocks linked by the hash of each block

Proof-of-Work: A system used by a cryptocurrency to ensure the integrity of its blockchain and requires a certain amount of work be performed to generate a cryptographic proof that proves the work was done.

Stablecoin: A cryptocurrency that has a stable exchange rate to a government issued currency

Difficulty: A measure used to determine a target value for the hash of the block and is an indication of the amount of processing power used by a PoW cryptocurrency system

Price-difficulty ratio: The ratio of the market price of a PoW cryptocurrency to the difficulty of the PoW cryptocurrency

NOMENCLATURE

The capitalisation of the word bitcoin was standardised throughout this dissertation to use small capitalisation. This is in line with the trend to use small capitalisation for services that are used as utilities, such as electricity, internet and payment system such as bitcoin. Also as bitcoin is a payment system, its unit of account also needs to be written using small capitalisation.

REFERENCING STYLE

Regarding the number of references, the Vancouver style of referencing is used.

DECLARATION

I, the undersigned, declare that the dissertation, which I hereby submit for the degree Magister Scientiae at the University of Pretoria, is my own work and has not previously been submitted by me for a degree at this or any other tertiary institution.

ETHICS STATEMENT

The author, whose name appears on the title page of this dissertation, has obtained, for the research described in this work, the applicable research ethics approval.

The author declares that he has observed the ethical standards required in terms of the University of Pretoria's Code of Ethics for Researchers and the Policy guidelines for responsible research.

Signature

Johan Kirsten

June 2019

CONTENTS

CHAPTER 1: INTRODUCTION

Bitcoin is a new type of currency, called a cryptocurrency, which allows a holder to trade it for goods and services with parties they have never met, apart from contact through the internet. The system that supports its transactions operates completely outside of the traditional banking system. As such it has the potential to revolutionise the financial system of the world completely.

Specifically, bitcoin is a distributed virtual currency that can be traded between parties without a prior trust relationship. Distributed, in this instance, means that its components are spread all over the world, there is no centralised authority that controls it, and it does not have a single point of failure. The term virtual indicates that it is entirely run on and stored using computers.

Traditionally the banking system has been used as a trusted middle man to send money between parties that have no prior trust relationship. The fact that bitcoin can facilitate exchange between two parties with no prior trust relationship means that it is in direct competition with the banking system as a payment system.

Due to the revolutionary nature of bitcoin and its implications for the banking system, the aim of this dissertation was to obtain a clearer understanding of bitcoin, especially some of its economic aspects. In the process of obtaining a better understanding of bitcoin a stochastic model was developed and researched. This dissertation will derive and explain this stochastic model, and the supporting research.

Among the implications of this model is that bitcoin still has significant growth potential in real value. The problem is that no one knows at which point it will stop growing. It might already have peaked, or it might reach a market capitalisation that rivals that of the dollar. If bitcoin reaches a market capitalisation in excess of several trillion dollars it will be large enough to create competition for the existing financial system and it could create significant economic problems. There is only so much economic activity in the world. If the proposed model is right and bitcoin is able to grow to such a size without being in a bubble it could cause large price swings in the fiat currencies of the world as the fiat currencies and bitcoin would compete for the same economic output.

Another problem is bitcoins ability to provide some form of anonymity that the traditional banking system cannot provide. Currently the anonymity that bitcoin provides is not complete and can be broken by state institutions. As an example of possible improvements

to anonymity, the dissertation will introduce a system that can be implemented within bitcoin that will improve anonymity. Improvements like these and others that will be referenced will make the case that bitcoin will be able to have economic appeal that the traditional banking system is not able to provide due to regulation.

Central banks therefore cannot afford to ignore bitcoin. Either it grows too large to ignore or innovation starts to make it possible for shadow economies to grow that are outside of the control of central banks.

Fiat currencies might not be up to the task of stopping bitcoin's growth. It might be necessary to create a central bank digital currency (CBDC). A CBDC must be able to provide the advantages of bitcoin, to be effective competition for bitcoin, and the advantages of fiat currencies, to be acceptable to central banks.

The objectives of this dissertation are:

1. Understand the technical details of bitcoin
2. Review the economic nature of bitcoin
3. Investigate limits on the price of bitcoin
4. Research a stochastic model for the price of bitcoin
5. Create a system that can improve the anonymity of bitcoin
6. Design a cryptocurrency that can be adopted by governments

Before getting to the results of this investigation, the dissertation will first start by examining the environment that created bitcoin in an effort to create a better understanding of it. Further, the dissertation will attempt to explain how bitcoin works which will allow better understanding of bitcoin, without getting into too much technical detail.

The dissertation will investigate bitcoin as an economic entity, specifically its economic classification as opposed to that of fiat currencies, and introduce sovereign cryptocurrencies as a concept. An estimation of the GDP of the bitcoin economy will also be provided.

Then the dissertation will explore the price of bitcoin. Constraints on the price will be derived using arbitrage trades. The dissertation will then derive and explain the hypothesis that the price-difficulty ratio of bitcoin is modelled by a lognormal distribution. The aforementioned difficulty is a measure of the strength and size of the processing network that underlies bitcoin. Research will be provided that supports this hypothesis. Based on

this hypothesis the dissertation will derive and explain a model for the price of bitcoin that is similar to the stochastic model for stock prices, except that the drift is determined by the growth in difficulty.

An innovative system, called anonymous atomic swaps, that can be included in bitcoin that will allow users more anonymity will be developed and explained. The improvement will be mainly of academic interest as it would not only require changes to bitcoin but also mass adoption for it to be effective. Other work that is currently in development, which will provide practical improvements to the anonymity of bitcoin users, will be discussed. These improvements use a slightly different public key encryption system than the current system used by bitcoin. But these changes will allow users of bitcoin perfect anonymity, without any of the problems associated with anonymous atomic swaps, and must not be ignored by authorities.

During this investigation into bitcoin a possible candidate CBDC was also developed. The candidate CBDC developed is called a sovereign cryptocurrency and has an adaptive monetary policy. This sovereign cryptocurrency will have features that extend on those of bitcoin, such as allowing for the efficient measurement of GDP, the growth in GDP, velocity, and inflation. Mechanisms that allow the monetary base of the sovereign cryptocurrency to expand or contract will also be explained. Finally, a mathematical model for the control of the monetary base of the sovereign cryptocurrency will be discussed.

Fig. 1 below shows the dependencies of the chapters in the event that the reader only wants to read certain chapters.

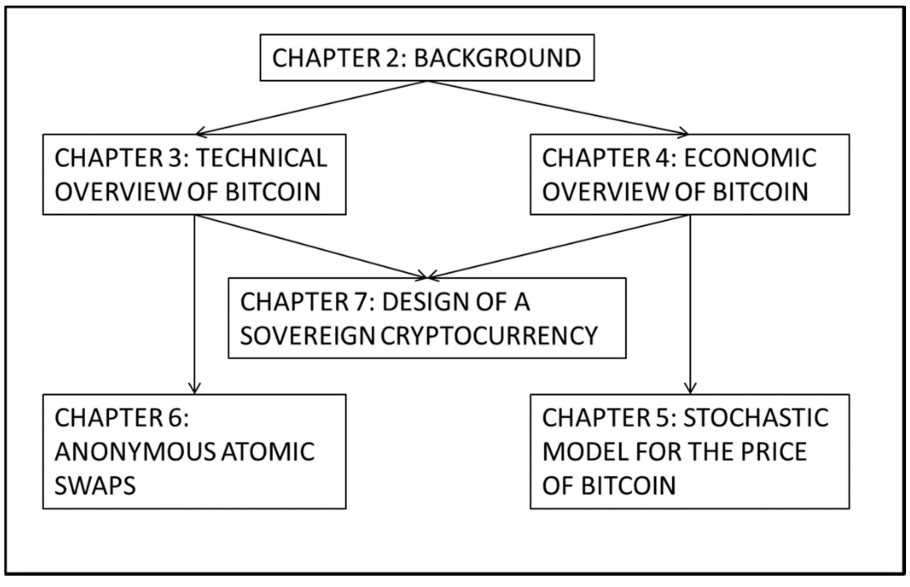

Figure 1. Dependancies of chapters

CHAPTER 2: BACKGROUND

Before the bitcoin protocol was developed, there were other proposals that would eventually help by providing the building blocks for bitcoin. The first of these was the ecash protocols of David Chaum [1,2].

Later proposals, which included Wei Dai's b-money [3] and Nick Szabo's bit gold [5], provided the means to create distributed digital scarcity. Specifically b-money publicly announced the transactions so that a trusted party was not needed.

In order for there to consensus on the sequence of events, a type of peer-to-peer timestamp system was necessary. This was developed by Adam Back in Hashcash [4]. Adam Back had created a proof-of-work (PoW) scheme that was later incorporated by Hal Finney [6] into the reusable proof of work (RPOW).

Bitcoin built on these innovations and as such was the culmination of work by different individuals.

Bitcoin itself was invented and created by an individual or group calling themselves Satoshi Nakamoto and introduced in [7]. The true identity of Satoshi Nakamoto is still unknown to this day. They launched bitcoin on 3 January 2009. This was happening at the height of the Great Financial Crisis (GFC). Satoshi Nakamoto recorded within the first block of data in the bitcoin ledger – the blockchain – the message: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” This is in reference to the main article of the Times on 3 January 2009. At the time the Chancellor of the Bank of England was about to give a second bailout to banks that had run into trouble during the GFC.

Numerous reasons have been mentioned as to what caused the GFC of 2008 as discussed in [8, 9, 10, 11, 12]. These include the obvious reasons such as the housing crisis to the more subtle reasons such as too little regulation. A lot of these reasons have been addressed over the course of the past 10 years. However, there is one fundamental reason for the GFC that has not been addressed and it goes to the heart of the matter and the financial system: the nature of financial assets.

Financial assets by their nature are IOUs. There are two parties to a financial asset: the party that has the contractual right to receive compensation from the party that has the contractual obligation to provide that compensation. The inherent risk with financial assets

is counterparty default risk, the risk that the obliged party will default on its obligation to provide compensation leaving the party that has the contractual right without any compensation.

It was this counterparty risk that was inherently the underlying problem that led to the GFC. At the height of the GFC the Collateralised Debt Obligation (CDO) in which banks invested started to default. These investments became known as toxic assets. Once these started to default, the bank holding them lost its investment. This problem spread to banks that did not even invest in the CDOs but invested in the troubled banks.

The spreading of a financial crisis like this is called contagion and was investigated for the GFC by Baur [13]. The risk of contagion, which is also called systemic risk, is defined as the risk that a financial crisis at one, or more, bank spreads to other banks and other financial institutions and eventually to the entire financial system. Contagion is a problem inherent in financial assets.

At the start of the GFC the investment bank Lehman Brothers went bankrupt. That meant that another financial institution that held a financial asset with Lehman Brothers as the counterparty lost their investment. This placed other financial institutions at risk of collapse.

The fear of capital loss eventually stopped banks from lending to each other, causing the entire financial system to start shutting down. That is when the governments started to step in and provide bailouts.

It is against this backdrop that bitcoin came into existence, when Satoshi Nakamoto published the seminal paper [7] on bitcoin, and bitcoin became functional in January 2009. . Bitcoin as a currency carries no counterparty risk because it is not a financial asset. The next chapters will explain this in greater detail and better define the economic nature of bitcoin.

CHAPTER 3: TECHNICAL OVERVIEW OF BITCOIN

Due to the technical nature of bitcoin, certain concepts must be understood before attempting to understand its economic nature. This chapter will discuss the components of the bitcoin network and the emergent behaviour of the network due to the implementation of the bitcoin protocol.

The majority of the details in this chapter were obtained from Antonopoulos [14]. If further details on the technical nature of bitcoin are required, please refer to Antonopoulos [14] and many of the references contained therein. A paper that also gives an overview of bitcoin for a non-technical audience is Böhme et al [15].

3.1 COMPONENTS OF THE BITCOIN NETWORK

The bitcoin network is a network of peers. That is, each node in the network has equal status in the functioning of the network. For this network to function the nodes of the network need to support the following four functions:

1. Storing the blockchain;
2. Mining;
3. Routing; and
4. Allow users, using wallets, to exchange bitcoins.

A node does not need to support all four functions. Some nodes only support a single function from the list and are called lightweight nodes. Other nodes, called full nodes, support all four functions.

3.1.1 Blockchain

Bitcoin transactions are stored in a database called a blockchain. This is effectively a ledger that stores which bitcoin can be spent by which account. A transaction entry into this database moves control of an amount of bitcoin from one account to another account. The blockchain itself is stored as multiple copies on computers all over the world and can therefore be described as a distributed transaction database. The copies are kept in

synchronisation, without need of a central authority, through the bitcoin protocol that creates what is called emergent consensus. This concept will be explained later in this chapter, but first the structure of the blockchain will be explained in more detail.

The blockchain derives its name from the fact that it is made up of a chain of blocks. Each block contains a number of transactions and each block is linked to a previous block to form a chain all the way back to the genesis block – the first block created by Satoshi Nakamoto on 3 Jan 2009.

Fig. 2 below shows an object graph of a block.

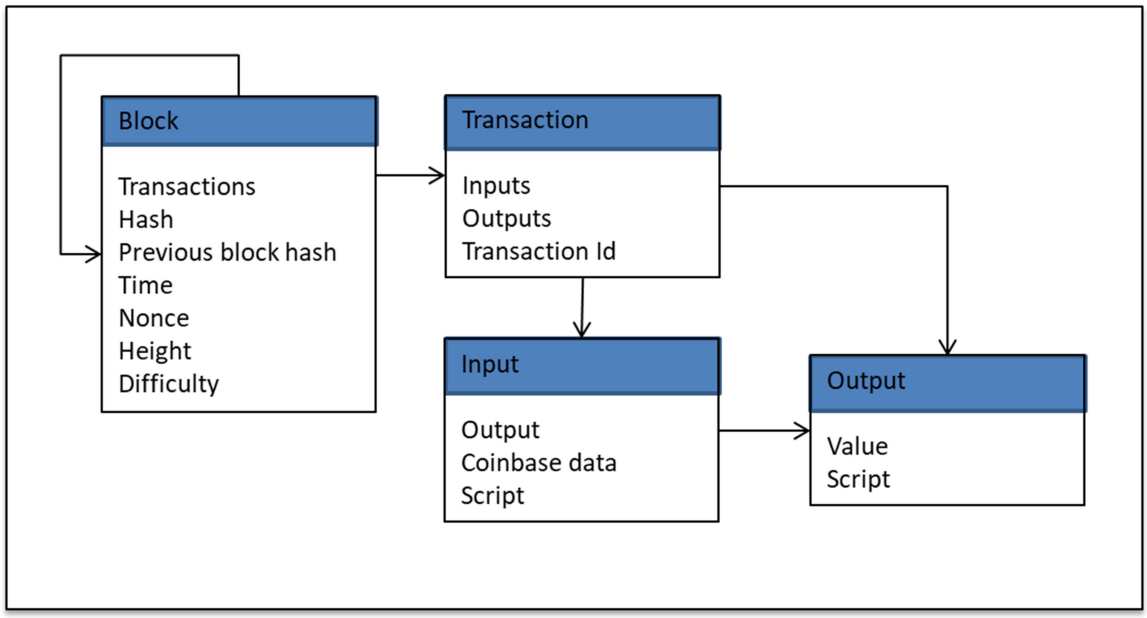

Figure 2. The object graph of a block

3.1.1.1 Block

As can be seen from Fig. 2, a block consists of transactions and transactions consist of inputs and outputs. Each input of a transaction also references an output of a previous transaction that is being spent by the input. Each block also references a previous block.

The block can be identified by its hash, which is generated by computing the hash of the entire block. For those unfamiliar with hash functions, the hash function summarises the entire block into a string of finite length called the hash. It is not possible to recover the block contents from the hash, but the hash is a unique identifier of the block contents. Haber [16] describes more about using a hash function to time stamp an electronic document, like the block.

The hash function used by bitcoin is the SHA-256 hash function, which is part of a family of hash functions, SHA-2, developed by the US government and patented by Lilly Glenn [17].

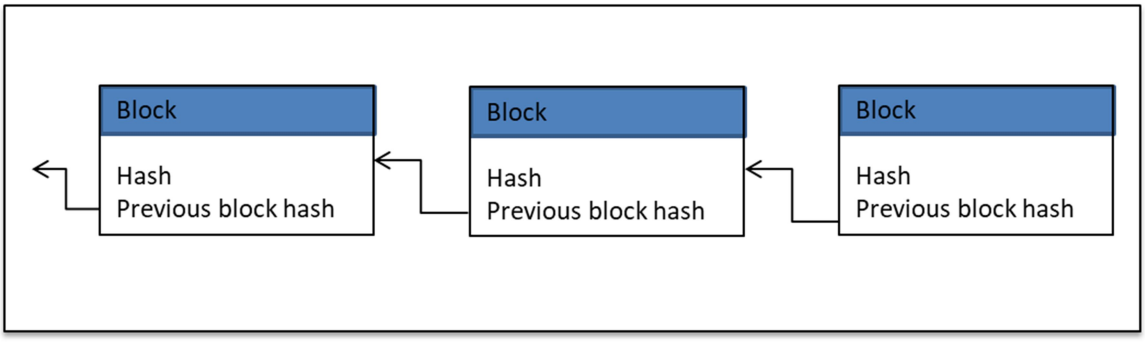

Figure 3. Chain of blocks

The blockchain is formed by each block referencing the hash of the previous block, as shown in Fig. 3. This previous block hash (which references the previous block) is also included in the calculation of hash of the current block. This makes the hash of a block dependent on the hash (and the contents) of the previous block. This creates a chain of hash values, with the hash of each block dependent on the hash (and therefore the contents) of the previous block. This means that any change to the content of any previous block would change its hash and therefore the hash of any subsequent blocks. This is an important point as it will be shown later on when emergent consensus is discussed.

The time field in the block specifies the time at which the block was mined. The height field in the block specifies the integer index of the block in the blockchain. The first block, the genesis block, has a height of one. Each block in the blockchain increments the height with one from the height of the previous block as it gets added to the blockchain.

The nonce and difficulty fields in the block are relevant to the mining process and will be discussed in detail later on. A nonce is simply a field that can contain any value and by changing it the result of the hash of the block is changed. The difficulty is a field that is used to determine a target value for the hash of the block.

3.1.1.2 Cryptographic puzzle

The bitcoins in the blockchain are stored in the value field of each output. It should be noted that there are no account numbers in the output, or even the input. This is because it is stored in the script field. The script field of an output actually contains a small program

that creates what is called a cryptographic puzzle. For an amount of bitcoin stored in an output to be spendable, the solution of the cryptographic puzzle must be presented by the script in an input that references the output, as shown in Fig. 4.

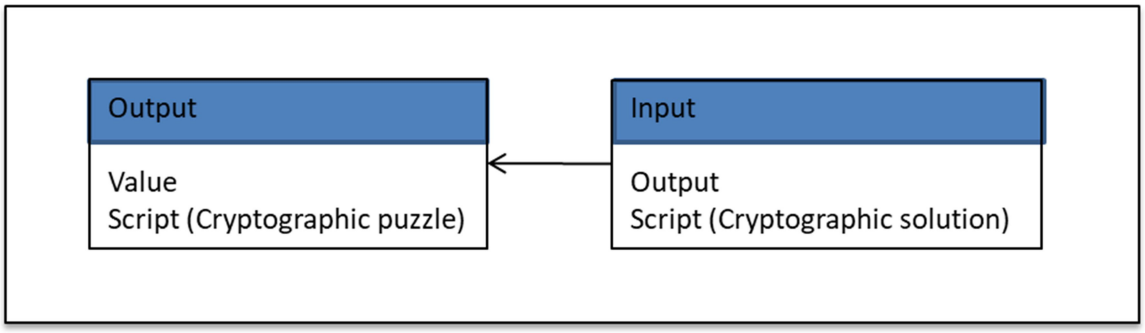

Figure 4. Input and output pair within a transaction

To create the cryptographic puzzles and solutions stored in the script fields of the outputs and inputs respectively, public key cryptography is used. In public key cryptography, a key is split into a public and private key. This public and private key pair is associated with an address, which is the address of the account. The public key is made available to the public, while the private key is kept secret by the owner of the account. It is an aspect of public key cryptography that the private key is not derivable from the public key or the account address.

The cryptosystem used by bitcoin for the public key cryptography is called elliptic curve cryptography (ECC) as described in Koblitz [18] and Miller [19]. It uses points on a curve and projections from one point to another point to do the encryption. It improves on traditional cryptosystems, such as Rivest-Shamir-Adleman (RSA), by having smaller keys and therefore is harder to break and uses fewer resources to implement. This last point is important for use on limited devices such as mobile devices.

To create a cryptographic puzzle for an account, the public key related to the account address is used. Only the owner of the secret private key for that account and public key is able to generate the cryptographic solution that will solve the cryptographic puzzle. This allows the owner of the account to spend the bitcoins stored in an output that is locked by a cryptographic puzzle only the owner can unlock.

3.1.1.3 Transactions

To better understand the structure of the transactions of the blockchain it is easiest to imagine the transactions as a graph where each node in the graph is a transaction, as shown in Fig. 5. The inputs and the outputs of transactions form the links of the transaction graph, with the input of a transaction referencing the output of a previous transaction. This is why the transaction ID is required on the transaction. The transaction ID of the transaction identifies the transaction itself. This transaction ID is used by the inputs of a transaction to reference the outputs of other transactions.

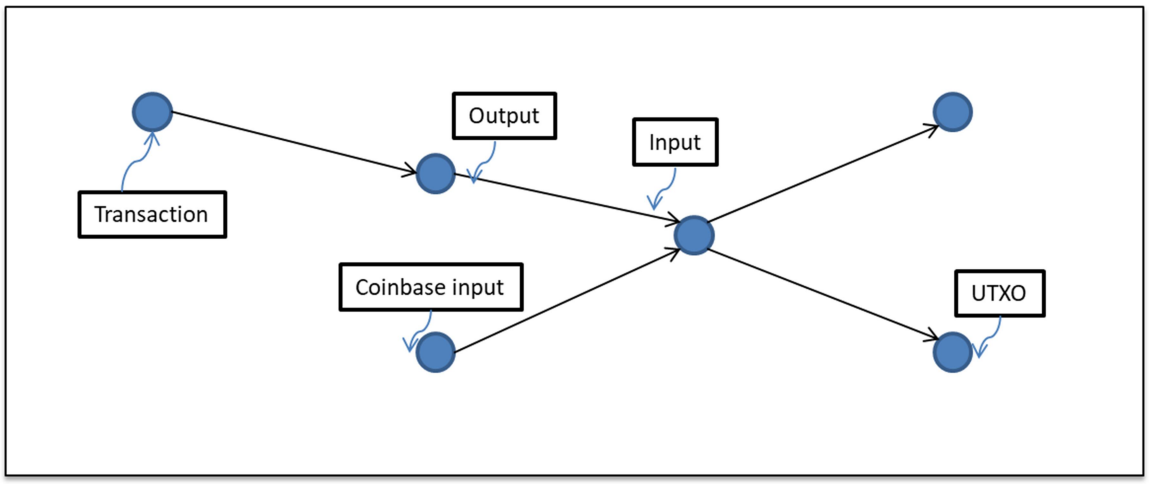

Figure 5. Transactions as a graph of nodes

The bitcoin protocol requires that each output be spent in its entirety. In other words an output can only be referenced by a single input. All of the inputs of a transaction together reference all of the outputs spent by the transaction. The sum of the values stored in these outputs is the total amount spent by the transaction. The list of outputs of the transaction determines which accounts receive how much of the total amount.

To spend a specific amount a user of the bitcoin network must construct a transaction that has enough inputs to cover the specified amount. This means a transaction will always have one or more inputs.

The total amount spent by a transaction is also usually larger than the amount that a user wants to spend. In this case an extra output is added to the transaction that contains the change the user will receive when spending. This output will send the change amount back to the spending user's account address.

The input transactions of the transaction graph contain coinbase inputs instead of normal inputs. These coinbase inputs differ from other normal inputs in two ways:

1. Coinbase inputs have a value stored in the coinbase field; and
2. Coinbase inputs do not reference a previous output as normal inputs do.

A block is only allowed to have a single coinbase input. It is used by the miner to create new bitcoins and credit its account with these bitcoins. It is also used to credit the miner's account with the fees earned for including the transactions in the mined block.

The outputs of the transaction graph are transactions, whose outputs have not been spent, i.e., these outputs are not referenced by other inputs. These are called Unspent Transaction Outputs (UTXO). The sum of the values of these UTXO equals all of the spendable bitcoin in existence.

3.1.2 Wallets

A wallet is an application that runs on a computer, such as a server, laptop or smart phone, which provides a user with:

1. The means to check the balance in accounts managed by the wallet; and
2. The means to create bitcoin transactions and transmit these transactions to the bitcoin network;

The wallet does not store any bitcoin. The bitcoin values are stored in the UXTO in the blockchain which is stored in nodes across the world. The wallet only stores the public and private keys associated with the accounts that are managed by the wallet. These public and private keys are those mentioned previously and are used to create and solve the cryptographic puzzles used in transactions created by the wallet.

A wallet typically is able to hold multiple accounts, and a user may have multiple wallets. It is relatively easy for a user using one of their wallets to generate a new account. The user is not required to register any personal details to create the account. This makes it difficult to ascertain the identity of the holder of any bitcoin account.

3.1.3 Routing

Once a transaction is created by a wallet it is transmitted to the network by the wallet. The wallet connects to one or more nodes and transmits the transaction. The rest of the network finds out about this transaction because the nodes on the network immediately forward any received transaction to its list of peers. In this manner the transaction cascades through the network, hopping from node to node in a process called routing.

3.1.4 Mining

Routing does not actually add the transactions to the blockchain. This is the responsibility of the miners that collect the transactions into blocks. The miner performs a predetermined calculation on the block called mining. Once the mining process gets the block to pass a set of predetermined rules, the block is said to be mined and the miner transmits the block to the rest of the network. If the rest of the network agrees that the block passes the rules, the block is accepted as the next block in the blockchain. This process is then repeated to find the next block through the mining process.

This section will discuss the steps involved in mining in greater detail and the functions of the mining process within the bitcoin network.

3.1.4.1 Mining steps

In order for a miner to successfully mine a block it performs the following steps:

1. Validate collected transactions against the current blockchain to ensure the transactions are valid transactions;
2. Combine the transactions into a candidate block;
3. Choose a random value to put into the nonce field of the block and calculates the hash of the block;
4. Check if the calculated hash is lower in value than a calculated target, and if not the process is repeated from step three using a new nonce;

This process is repeated until the calculated hash is lower than the calculated target, or until another miner provides a block that has a calculated hash that is lower than the target.

3.1.4.1.1 Validation of transactions

Each transaction received by a miner, or any routing node for that matter, is always compared to a list of validation rules. There are a lot of rules that a transaction must comply with in order for it to be accepted, but the most important requirements are:

1. The transaction must not double spend; and
2. Each input of the transaction must have a cryptographic solution that solves the cryptographic puzzle of the output referenced by the input.

Together these requirements ensure that a transaction only spends bitcoins it has a right to spend and that it does not double spend bitcoin.

The first of these checks involves making sure that the each output referenced by each input in the transaction has not already been referenced by a previous accepted transaction's inputs. As mentioned previously an output may only be referenced by a single input, thus preventing double spend.

The second of these checks involves combined the cryptographic solution of each input with the cryptographic puzzle of its referenced output and validating that the solution solves the puzzle.

3.1.4.1.2 Combine transactions into candidate block

The collection of accepted transactions is called the mempool. These are transactions that are valid but have not been included in a mined block. When a miner is ready to begin mining a block it selects a number of transactions from the mempool and constructs a candidate block. A candidate block is a block that has not been mined.

The miner typically selects those transactions with the highest transaction fee. The transaction fee for a transaction is calculated as the difference between the spendable bitcoin referenced by the inputs and the total bitcoin of the transaction's outputs. The bigger this difference is, the higher the transaction fee. The higher the transaction fee, the quicker a transaction will be included in a candidate block.

3.1.4.1.3 Setting the nonce and calculating the hash

The mining process involves calculating the hash of the block. An aspect of calculating the hash of a block is that changing even a single bit in the block will result in a completely different hash being calculated. This allows the miner to change the nonce field to different values and to each time calculate a different hash.

It is not possible to specify the hash and then calculate the nonce required to generate the specified hash. The calculation of a hash is a one directional operation. This is a very important aspect of calculating a hash. It ensures that the miner must do repeated calculations if it must obtain a hash that must meet certain requirements, such as those in the next step.

3.1.4.1.4 Comparing the hash to the target

The bitcoin protocol (the set of rules that the bitcoin network operate on) requires that any block hash must have a value lower than a calculated target for it to be accepted as the next block of the blockchain.

The target is calculated as the inverse of the difficulty specified in the difficulty field of the block. The miner is not allowed to decide independently on a difficulty. The difficulty is calculated on the data contained in the blockchain that all the other nodes in the network have a copy of.

For a certain difficulty (and therefore target) a mining network with certain strength will mine a block at a rate that fluctuates but has a certain average. This is because the calculation of the hash and it being below the target is a random event. It is not possible to predict if the next calculated hash will be below the target. The miner will have to randomly guess the nonce and try each one in a brute force method to find a hash that is below the target. Once it finds this hash the candidate block is said to be mined. The miner transmits this mined block to the rest of the network and it becomes part of the blockchain. But the time taken to find this hash, called block time, is therefore not certain and is different for each block. But over a fixed stretch of time a certain average block time can be calculated.

If the strength of the mining network increases, blocks will be mined at a faster rate. By increasing (or decreasing) the difficulty at certain intervals, to keep up with increases (or decreases) in mining network strength, the average block time can be kept around a certain

prescribed amount. For the bitcoin network this desired block time is 10 minutes. The difficulty is therefore effectively a measure of the processing strength of the mining network.

The fact that a miner is able to provide a block with a hash that is lower than the target is proof that the miner expended energy (and therefore spent money) in finding the hash. This proof is called Proof-of-Work (PoW). As it will be shown later PoW is an important requirement in the consensus on the state of the blockchain that emerges from the bitcoin network, and is called emergent consensus.

It is possible to calculate the average time for a miner to find a block. This will be necessary in the chapter of the pricing model of bitcoin.

The hash is a 256 bit value and the target is some value below the max hash value. Therefore the probability of a block having a hash below the target is

$$p_h = \frac{T}{2^{256}}, \tag{1}$$

where

p_h is the probability of a single hash being below target

T is the target.

In the bitcoin protocol, difficulty is defined as

$$D = \frac{T_{max}}{T}, \tag{2}$$

where

D is the difficulty

T is the target

T_{max} is a constant equal to 2^{224}.

Substituting Equation 2 into 1 yields the probability that a hash, using difficulty D, is a valid hash,

$$p_h = \frac{1}{2^{32} \cdot D}. \tag{3}$$

Then

$$p = \frac{H}{2^{32} \cdot D}, \quad (4)$$

where p is the probability of obtaining a valid hash within a second using a piece of mining equipment that is able to perform H hashes per second.

Therefore the expected time to find a valid hash is

$$t_m = \frac{2^{32} \cdot D}{H}, \quad (5)$$

where

Tm is the average time for a miner to mine a block

D is the difficulty

H is the hashing power of mining equipment in hashes per second.

3.1.4.2 Functions of mining

The mining component of the bitcoin network performs three very important functions:

1. Injects bitcoin into circulation when it sells bitcoins to pay for its expenses; and
2. Provides the PoW required for emergent consensus; and
3. Removes bitcoin from circulation because it charges a transaction fee for the rendering of its services.

These functions are at the core of the functioning of the bitcoin network. It is these functions that allow for the emergent aspects bitcoin such as emergent consensus, the redundancy of trust and the price of bitcoin as it will be shown in a later chapter.

3.2 EMERGENT CONCENSUS

Emergent consensus is the property of the bitcoin network that the distributed copies of the blockchain converge to the exact replicas of each other due to the rules of the bitcoin network (the bitcoin protocol). Emergent consensus is important to the bitcoin network because the redundancy of trust created by the bitcoin network relies on consensus to emerge so that the blockchain can be relied on as a record of who owns/controls which bitcoins.

This emergent consensus is dependent on the following four actions that are taken by different nodes within the bitcoin network:

1. Validating and routing a transactions received from wallets;
2. Mining of blocks using the process describe previously;
3. Validating and routing of the mined blocks; and
4. Selection rules to determine which sequence of blocks to select in case of forks in the chain.

This section will discuss how each of these steps helps to create emergent consensus.

3.2.1 Validating and routing transactions

As discussed previously the network nodes can support a routing function that first validates and then forwards the valid transactions it receives. This function ensures that only valid transactions are processed by the network. Please refer to the previous section for a more detailed explanation on what constitutes a valid transaction.

For consensus to emerge the transactions that are included must be valid transactions otherwise the blockchain cannot be trusted to reflect a true state of who owns/controls which bitcoins.

3.2.2 Mining of blocks

The mining process is described in detail in the section 3.1.4. In this process the miner that mines the block is rewarded with bitcoins. To remove the incentive to cheat at the process, the miner must prove they have done work to produce the mined block. This is the role of the PoW in the form of creating a hash that is lower than the target.

Thus PoW ensures that valid blocks are generated and were not simply generated by the miner in order to enrich themselves with bitcoin.

3.2.3 Validating and routing of mined blocks

Once a miner mines a block it transmits it to the rest of the network. Each node that receives a new block will first validate the block to verify that the PoW is present. Valid mined blocks are then routed to the peers of the node. In this manner only valid mined blocks propagate through the network. Once a node validate and routes a new mined block it will add it to its blockchain.

3.2.4 Selection of chain

It is possible for two miners to create valid mined blocks at approximately the same time. Each of these blocks will propagate through the network and each node of the network will receive the two blocks in a different sequence. This creates a problem for consensus to emerge.

To overcome this problem, each node forks the current chain and adds each of the two new blocks to each own blockchain. Each miner then decides against which one of the two blocks to link their next candidate block. Once a miner mines a new block it will transmit it to the network, extending one of the two forks with an extra block. At this point the fork in the blockchain can be resolved by each node using a rule in the bitcoin protocol that states the longer leg (in terms of PoW) of a fork is the correct leg to use, i.e. which leg produced more PoW.

The result is that the shorter leg is abandoned by each node in the network so that all of them have the same copy of the blockchain. Thus consensus has emerged.

This competition between two legs after a fork will continue until one leg is longer than the other. Typically the length of the longer leg in the chain is no more than three blocks, but typically only two. Thus typically two blocks are found at the same time, after which a new block is found that resolves the fork.

The reason this rule is used, is that the length of the leg after the fork determines the amount of mining network processing power was used to generate the leg. The longer the leg, the more processing power was used to generate it. That is, the majority of the processing power of the network gets to decide which leg is the correct leg to follow.

Effectively the length of the leg can be seen as the network voting using its processing power on which leg to use.

The problem with this rule is that if more than 50% of the processing power falls under control of a single miner, they would be able to control which leg of a fork to follow. This is called a 51% attack.

This would allow a miner to do things like double spend or exclude certain addresses from spending on the network. It does not give the miner the ability to spend someone else's bitcoins. This is only possible if the privacy of the private key is compromised.

As the bitcoin mining network gets larger the probability of a 51% attack diminishes, because the investment required to launch such an attack becomes prohibitively expensive. Instead it makes more economic sense to simply mine and collect the fees and rewards.

Thus through emergent consensus the user of the network is able to trust the reliable functioning without needing to trust the participants in the network.

CHAPTER 4: ECONOMIC OVERVIEW OF BITCOIN

This chapter reviews the economic nature of cryptocurrencies in general and bitcoin in particular. Specifically the economic nature of cryptocurrencies is evaluated against certain definitions and sovereign cryptocurrencies are introduced at the hand of these definitions. The value of cryptocurrencies is then discussed, showing that if a cryptocurrency's blockchain has value then the cryptocurrency should have value. Finally, bitcoin's monetary policy is discussed as well as the problems that would be created if bitcoin grows large enough or is adopted by an economy.

4.1 ECONOMIC NATURE OF CRYPTOCURRENCIES

4.1.1 Definitions

In general assets can be divided into real assets and financial assets. Real assets (which could also be called holding assets) are assets in which the holder of the asset controls the asset and all advantages to holding the asset accrue to the holder of the asset. An example of a real asset is a house.

Financial assets are assets in which the holder of the asset has the contractual right to receive compensation from a counterparty that has the contractual obligation to provide that compensation. An example of a financial asset is a bond.

With real assets there is no counterparty, while with financial assets there is counterparty. Therefore financial assets carry the risk of counterparty default which is not present in real assets. This explanation of real and financial assets was obtained from Wray [20].

Another definition that is relevant in the evaluation of cryptocurrencies is commodities. A commodity is a class of real assets that are fungible and can be bought and sold in a market. Fungible means that one instance of the commodity is indistinguishable from another instance of the same commodity. An example of a commodity is gold. This definition of a commodity is taken from [21].

The final measure that bitcoin will be evaluated against is the functions of money. A currency functions as money if it is a store of value, a unit of account and a medium of

exchange. A store of value means that its value in relation to the goods and services of the country is stable; therefore a person can hold the currency and expect to buy the same goods and services with it tomorrow as they can today. A unit of account means that the price of goods and service are priced in the currency. A medium of exchange means it is used in the sale and purchase of goods and services. These functions of money are described in Wray [20].

4.1.2 Fiat currencies

Traditional currencies are called fiat currencies, meaning that they derive their value because they are decreed the currency of a country by the country's government. Effectively the government guarantees to accept the fiat currency it issues as payment for tax liabilities. Thus, a country's fiat currency is an IOU of the government and therefore a financial asset. Because a country's fiat currency is fungible and can be exchanged in markets it is also a commodity.

It has been shown by the economic theory called Modern Monetary Theory (MMT) that the acceptance by a government of its own issued currency in payment of tax liabilities will cause the currency to be used by its citizens to price and trade goods and services in that currency. More details on MMT can be obtained from Wray [20].

In other words, because the government accepts its fiat currency in payment of taxes, there will always be demand for the currency and the result is that goods and services in the country is priced and exchanged in terms of the currency. So long as a country's fiat currency also has a stable value in the markets and little inflation, due to good monetary and fiscal policies, it will act as a store of value. Therefore, given good monetary and fiscal policies, a country's fiat currency will comply with the definition of being money.

4.1.3 Cryptocurrencies

Cryptocurrency is any currency that uses cryptographic proofs and procedures to facilitate the exchange of the currency. This includes bitcoin. Because there is no single counterparty involved in holding a unit of cryptocurrency, it fulfils the definition of being a

real asset. The counterparty risk has been replaced with a price and liquidity risk. Note that it is possible for the owner of bitcoin to transfer bitcoin to a custodian for safe storage. In that case the custodian then holds the bitcoin as real asset, and the owner holds a financial asset against the custodian which owes the owner the bitcoin.

Bitcoin also fulfils the definition of being a commodity. Two bitcoins cannot be distinguished and can be traded on exchanges for other cryptocurrencies or for fiat currencies.

Currently no cryptocurrency can be classified as money. Due to the wild price fluctuations of cryptocurrencies, they do not store value very well. Also, while bitcoin can be used to pay for goods and services and is therefore a medium of exchange, those goods and services are priced in terms of a fiat currency, usually dollars. Therefore no cryptocurrency has been established as a unit of account.

4.1.4 Sovereign cryptocurrencies

Following from the previous definitions, the biggest differences between cryptocurrencies such as bitcoin and fiat currencies such as the dollar are:

1. Fiat currencies are financial assets and cryptocurrencies are real assets; and
2. Currently most fiat currencies can be classified as money, while no cryptocurrencies can currently be classified as money.

Applying Modern Monetary Theory to cryptocurrencies implies that for a cryptocurrency to be acceptable as unit of account it would need to be accepted as payment for tax liabilities. The problem would then be that the cryptocurrency's price, as seen in its exchange rate and the price of goods and services would still fluctuate wildly. To be a good store of value, a cryptocurrency would also need an adaptive monetary policy that adjusts to the changes in the economy of the country. An adaptive monetary policy in this context means a monetary policy that adapts to its economic environment. This is opposed to the rigid monetary policy employed by cryptocurrencies, such as bitcoin, that increases the supply of bitcoin at a predictable rate.

But these differences, acceptance as payment of tax and an adaptive monetary policy, can be resolved with a sovereign cryptocurrency. A sovereign cryptocurrency is defined as any

cryptocurrency that is accepted in payment of the tax liabilities of a government and with a proper adaptive monetary policy would become money.

The only difference between fiat currencies and sovereign cryptocurrencies is that sovereign cryptocurrencies are real assets while fiat currencies are financial assets. Sovereign cryptocurrencies therefore directly challenges the notion that money must be a financial asset.

At present central banks are not investigating the implementation of their currencies as a cryptocurrency. Most initiatives by central banks to use cryptocurrencies involve projects such as the South Africa Reserve Bank project Khokha [22]. These initiatives involve testing the use of cryptocurrencies for interbank payments using private blockchains. In contrast to this a sovereign cryptocurrency is built on a public blockchain.

A variation on the idea of a sovereign cryptocurrency is the concept of Central Bank Digital Currency (CBDC), such as those described by Bech et al [23]. A CBDC is a currency that is controlled by the central bank with all the retail banks effectively becoming full reserve banks. With a CBDC the central bank directly controls the creation of money, as opposed to the fractional reserve banking system creating money by way of issuing of loans. A sovereign cryptocurrency is therefore a CBDC that uses blockchain technology. Recently the South African Reserve Bank has shown interest in creating a CBDC [24].

Very little data and research are available on CBDC because at present no monetary system uses it. The Bank of England has done a study of CBDC that uses modelling in Barrdear [25]. But very little insight was provided of the potential effect in introducing a CBDC on the retail banking system. In Switzerland there was a recent referendum to ask the citizens if they want to introduce a CBDC [26]. The initiative, if implemented might even have used blockchain technology. The initiative failed at the polls, with only about 25% of the voters supporting the initiative. Even the central bank of Switzerland opposed the initiative.

The biggest problem seems to be the public's willingness to give total control of the money supply to the central bank. Giving too much control of your money over to a central authority would create an authority that is more powerful than the president of a country and would possibly become highly politicised. Such a central monetary authority could potentially have the power to tax at will or reward political allies. The reason people trust

that central bank with discretionary monetary policy is because the independent banking system exists and is not politicised.

Sovereign cryptocurrencies can actually help solve this problem, while at the same time to allow central banks to have the necessary control over the money supply. A sovereign cryptocurrency would allow a central bank to relinquish enough control over monetary policy to a deterministic monetary policy implemented within the code of the sovereign cryptocurrency while retaining enough control to manage the money supply effectively.

The unanswered question is what the effect of a sovereign cryptocurrency would be on the fractional reserve banking system. MacDonald et al [27] argues that blockchains compete directly with banks to decentralize transactions, and Raskin et al [28] argues that a sovereign digital currency will remove the need for public to keep deposits at retail banks. In short, a holder of a sovereign cryptocurrency would not need a bank to store and exchange his holdings, and without deposits banks would not be able to make loans. The only way to get an answer to this question would be to implement a sovereign cryptocurrency.

It might be that either a central bank must use the existing discretionary monetary policy with an independent fractional reserve banking system, or, if it switches over to a sovereign cryptocurrency, have an environment with:

1. A adaptive monetary policy implemented in a sovereign cryptocurrency; and
2. A banking system that does not rely on fractional reserve lending, but possibly custodian services and mining, and is therefore much smaller.

4.2 THE VALUE OF CRYPTOCURRENCIES

Cryptocurrencies have become something to pay attention to. It represents a technology that will not go away and has certain real world applications that are of value. These include:

1. Easy flow of capital across borders, as cryptocurrencies reduce the cost and legal hurdles of sending the cryptocurrency to another country; and
2. Storing the hash of document in a cryptocurrency transaction allows documents to be stored safely in the knowledge that any modification will be detectable by comparing the hash in the blockchain to the hash of the document.

It has been widely recognised that there is value/advantages in the blockchain technology that underpins the functioning of cryptocurrencies such a bitcoin to deliver these services. The ability to make trust redundant amongst transacting parties makes the blockchain technology valuable.

What is not widely understood is that any blockchain based system requires a cryptocurrency for its proper functioning. Without a cryptocurrency malicious parties would be able to overwhelm the blockchain system without consequence. As a result of the cryptocurrency component of a blockchain it requires the payment of money to perform transactions on the blockchain. This limits any attempts to overwhelm a blockchain system. The payment of fees in the cryptocurrency of the blockchain also compensates the miners for the work done in processing transactions.

Therefore, if blockchain has value/advantage, its cryptocurrency must have value. Because bitcoin has the largest, most established and most valuable blockchain, stating that bitcoin does not have value, is like saying the banks, and the payment system it upholds, have value, but the money transmitted by these banks does not. It is a clear contradiction.

The value of a cryptocurrency is also related to the cost of energy, due to PoW. Because of the PoW, the mining network expends energy and spends money to put a cryptocurrency in circulation. As it will be shown in chapter 5 this insight can be used to derive a stochastic model for a cryptocurrency.

4.3 MONETARY POLICY OF BITCOIN

Each time a block of bitcoin is mined, the miner receives a predetermined reward in the coinbase transaction. This reward halves each four years. This results in bitcoins entering circulation at a predictable exponential decaying rate. This is effectively the monetary policy of bitcoin. It is predetermined and rigid, and therefore does not adapt to changes in the economy. In fact, Vidal-Tomás et al [29] shows that bitcoin is not affected by monetary policy news.

This could create a problem if bitcoin grows to challenge the fiat currencies of the world. It is a possibility, however much one might deem it unlikely, for bitcoin to grow to a size that it is competitive with fiat currencies for world economic output. If, under such pressure, fiat currencies collapse and people start using bitcoin, bitcoin's rigid monetary policy could cause problems.

In the event that bitcoin does become a major currency and because bitcoin's monetary policy does not adapt to the economy that transacts using bitcoin, the prices of goods and services priced in bitcoin could swing wildly. This could create very big swings in the GDP of an economy that prices goods and services in bitcoin.

To address this potential problem this dissertation will describe the sovereign cryptocurrencies that provides the economic advantages of cryptocurrencies by introducing the advantages of fiat currencies.

4.4 ESTIMATING THE GDP OF THE BITCOIN ECONOMY

In order to assess the bitcoin economy, the only available source of information was used: the blockchain. Data on the blockchain is publicly available and can be found at the website www.blockchain.info.

To properly assess the size of the bitcoin economy, a distinction needs to be made between bitcoin transactions of a capital nature and those for goods and services, which would make up the GDP of the bitcoin economy. The reason for this is that the GDP of an economy is the annual transactions of goods and services that are conducted in the denominated currency of the economy.

The bitcoin economy was investigated for the period of December 2016 to December 2017. Unfortunately due to the rapid growth of technologies such as the Lightning Network, this estimation becomes difficult to perform on more recent data.

The estimation was determined by subtracting the total daily bitcoin transactions that originate from bitcoin exchanges (which represents the capital flows), from the total daily bitcoin transactions (which is all the daily transactions). The data for the capital flows was obtained from [30] and the data for the daily transactions was obtained from [31].

A 30-day moving average is applied to smooth the Fig to make trends more visible, thereby obtaining an estimation of the daily transactions of goods and services in bitcoin. This moving average of daily transactions is multiplied by 365 to obtain an estimate for the annual GDP of the bitcoin economy. The resulting graph is shown in Fig 6 (amounts denoted in USD millions). Note that these figures likely still contain capital flows between persons that did not use an exchange to transact. These transactions include the exchange of bitcoin for a traditional currency through an informal channel such as meeting in person.

Unfortunately it is not possible to estimate the size of these transactions. As such, this is not an accurate estimation, but does give an indication of the order of size of the bitcoin economy and the behaviour of its growth and contraction.

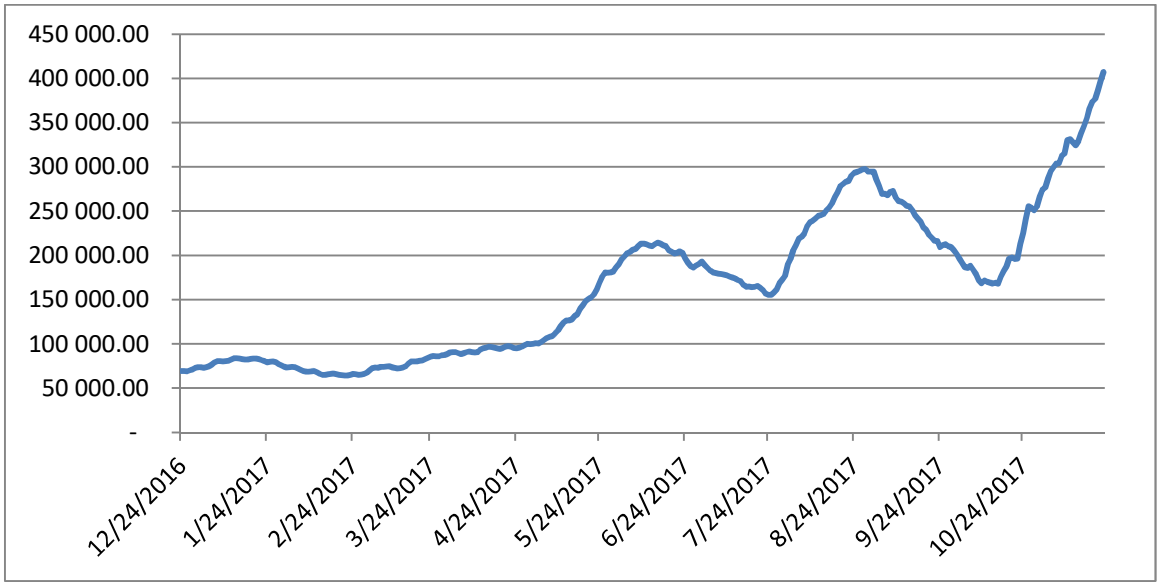

Figure 6. Estimation of the GDP of the bitcoin economy

Fig 6 shows that, if the bitcoin economy remains stable, it has a GDP of USD 400 billion. This estimate would place the bitcoin economy among the top 40 countries in the world.

The month-on-month growth of the bitcoin economy was calculated and is shown in Fig 7.

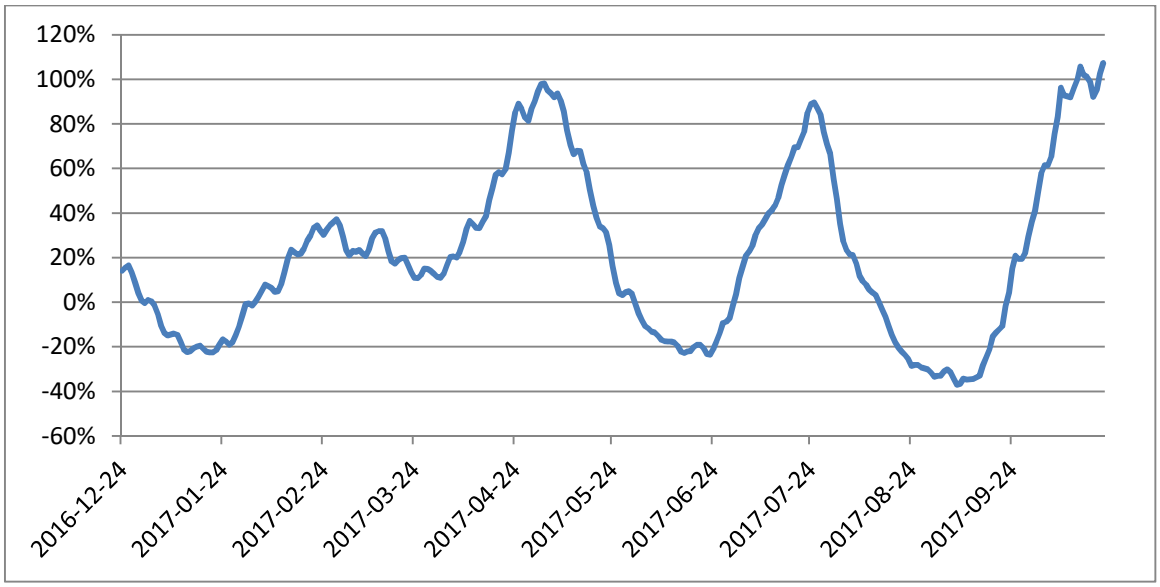

Figure 7. Month-on-month growth of the bitcoin economy

The graph above shows that the bitcoin economy grows in cycles. It contracts and then expands, which is expected from an economy based on a money supply that is not

expanded and contracted in order to protect the economy against recessions. The average growth of the GDP is about 50% per month for the period under investigation.

For an alternative analysis of the bitcoin economy that analysis the relationship of accounts and groups accounts, please see Tasca et al [32].

CHAPTER 5: STOCHASTIC MODEL FOR THE PRICE OF BITCOIN

Very little work has been done on models for the market price of bitcoin. One researcher that has attempted an answer is Hayes [33, 34, 35]. In Hayes [33] a regression model is first built to determine which possible factors help determine the price. Hayes [33] also derives a deterministic model using the assumption that the cost of production is the fair price of bitcoin due to the competitive nature of the bitcoin miners and that miners will stop mining below the stated cost of production.

The problem with the approach taken in Hayes [33] is that the cost of financing the mining equipment is not taken into consideration. This dissertation will show that the price point at which the miners stop mining is, due to the cost of financing, much lower than the production cost of bitcoin. As such, the model in Hayes [33] does not reflect the fair price of bitcoin. Rather than develop a deterministic model, like the model in Hayes [33], this chapter will attempt to derive a stochastic model for the price of bitcoin.

The chapter will introduce a constraint on the price of bitcoin using arbitrage trading strategies. This will result in the development of the production cost of bitcoin, which defines a ceiling above which arbitrage profits using certain trades becomes possible.

This chapter continues by investigating the following hypothesis: the price-difficulty ratio of a PoW based cryptocurrency over a certain period is modelled by a lognormal distribution. Research will be provided that supports the acceptance of the hypothesis.

Accepting this hypothesis, reasoning will be given to show that the price-difficulty can be modelled using the same stochastic model as that used for stock prices. Reasoning that the returns in the price-difficulty is equal to the sum of returns due to the growth of the difficulty (μ_d) and the returns of the price; and assuming that μ_ρ is negligible based on the same data used to show that the price-difficulty ratio is lognormal; the stochastic model for the price of bitcoin will be derived.

The stochastic model for the price of bitcoin is effectively the same stochastic model used for the price of stocks, except that the drift is replaced by the growth in difficulty (as used by the bitcoin network), and is therefore a Markov process

This is in contrast to the model developed for the price of bitcoin by Schilling et al [36]. In Schilling et al [36] it is shown that, given certain assumptions, the price of bitcoin is a martingale. The difference between that model and this model is that this model implies the growth of the difficulty drives the price of bitcoin. This implies that more work should be done to investigate the growth of difficulty. One possible way these two models can be reconciled is if it can be shown that the difficulty is also a martingale.

5.1 CONSTRAINTS ON THE PRICE OF BITCOIN

This section explores the limits to the bitcoin price using arbitrage trading strategies.

5.1.1 Production cost of bitcoin

The production cost of bitcoin is that price at which an arbitrage opportunity is present if bitcoin trades above it.

This section explains an quasi-arbitrage trading strategy (some operational risks preclude pure risk free arbitrage) that can be employed if the price of bitcoin is above the production cost of bitcoin. The production cost of bitcoin is calculated as the ratio of total expense of operating the mining equipment to the bitcoin earned in the same time period. The trade requires the arbitrageur to obtain a loan to pay for the mining equipment and then operate the equipment to earn bitcoins which are then sold at the elevated price.

Effectively the mining of bitcoin makes the miner naturally long on bitcoin and short on dollars. The sale of the bitcoin is a transaction that is short on bitcoin and long on dollars. The two positions cancel each other out and the profit is the difference between the market price and the cost of mining bitcoin.

As more miners sell at the elevated price or open short positions in the future market, it forces the price down until it reaches the production cost of bitcoin.

Define

$$E_e = C_e \cdot H \cdot Q_h, \tag{6}$$

where:

E_e is the expense due to electricity in dollars per second

C_e is the cost of electricity used by mining equipment in dollars per kW-s

H is the hashing power of the mining equipment in hashes per second

Q_h is the power consumption of mining equipment in kW per hashes per second.

The other cost is the instalment of the loan per second. Define

$$E_l = \frac{r \cdot C_h \cdot H}{365 \cdot 24 \cdot 60 \cdot 60 \cdot (1 - e^{-r \cdot T})}, \tag{7}$$

where:

E_l is the loan repayment per second

C_h is the cost of capital of the mining equipment per hashes per second

H is the hashing power of the mining equipment in hashes per second

r is the interest rate of the loan

T is the duration of the loan.

Define the total cost of mining per second as

$$E_m = E_e + E_l. \tag{8}$$

To determine the amount of bitcoin earned per second from mining, Equation 5 derived earlier is needed:

$$t_m = \frac{2^{32} \cdot D}{H}, \tag{9}$$

where:

t_m is the average time to mine a block in seconds

D is the current difficulty used by the network

H is the hashing power of the mining equipment in hashes per second.

Each block gives the miner a reward of R bitcoins, so the average bitcoins earned per second is

$$B = \frac{R \cdot H}{2^{32} \cdot D}, \tag{10}$$

where

B is the average bitcoin earned per second

R is the reward of bitcoin per block.

Defining

$$D = D_0 e^{\mu_d \cdot t}\,, \tag{11}$$

where:

D_0 is the difficulty at time t = 0

μ_d is the growth of difficulty

t is time

gives

$$B = \frac{R \cdot H}{2^{32} \cdot D_0} e^{-\mu_d \cdot t}. \tag{12}$$

Therefore, defining the production cost of bitcoin as

$$P_c = \frac{E_m}{B}, \tag{13}$$

then

$$P_c = \frac{E_e + E_l}{B} \tag{14}$$

and therefore

$$P_c = \frac{C_e \cdot H \cdot Q_h + \frac{r \cdot C_h \cdot H}{365 \cdot 24 \cdot 60 \cdot 60 \cdot \left(1 - e^{-r \cdot T}\right)}}{\frac{R \cdot H}{2^{32} \cdot D_0} e^{-\mu_d \cdot t}}. \tag{15}$$

Cancelling out H and rearranging gives

$$P_c = \frac{C_e \cdot Q_h + \frac{r \cdot C_h}{365 \cdot 24 \cdot 60 \cdot 60 \cdot \left(1 - e^{-r \cdot T}\right)}}{R} 2^{32} \cdot D_0 e^{\mu_d \cdot t}. \tag{16}$$

Defining

$$P_{c0} = \frac{C_e \cdot Q_h + \frac{r \cdot C_h}{365 \cdot 24 \cdot 60 \cdot 60 \cdot \left(1 - e^{-r \cdot T}\right)}}{R} 2^{32} \cdot D_0, \tag{17}$$

gives

$$P_c = P_{c0} e^{\mu_d \cdot t}. \tag{18}$$

Defining the electricity cost as

$$P_e = \frac{E_e}{B} \tag{19}$$

and the finance cost as

$$P_l = \frac{E_l}{B}, \tag{20}$$

it follows that

$$P_e = P_{e0} e^{\mu_d \cdot t}, \tag{21}$$

where

$$P_{e0} = \frac{C_e \cdot Q_h}{R} 2^{32} \cdot D_0, \tag{22}$$

and

$$P_l = P_{l0} e^{\mu_d \cdot t}, \tag{23}$$

where

$$P_{l0} = \frac{r \cdot C_h \cdot R}{365 \cdot 24 \cdot 60 \cdot 60 \cdot (1 - e^{-r \cdot T})} 2^{32} \cdot D_0. \tag{24}$$

5.1.2 Example

Using the Antminer S9 as an example, P_{c0} is calculated using Equation 23 and the amounts specified in Table 1. The difficulty is the difficulty of the network on 2 September 2018. The reward was calculated as the 12.5 BTC block reward plus an estimated 2.5 BTC in transaction fees. The values used for the mining equipment was obtained from [37] on 12 June 2018. An earlier date for the hardware is used because it takes a few months from ordering to delivery.

	Value	Unit
Hash power	1.4E+13	Hash/second
Difficulty	6727225469722	

Reward per block	15	BTC
Interest	3	%
Loan duration	1	Year
Cost of miner	837	USD
Cost of electricity	0.12	USD/kWh
Power	1.3	kW

Table 1. Values used in the estimation of current production cost of bitcoin

The result of the calculation is a value of \$9,668.85 for P_{c0}. This can be broken down into P_{e0} = \$5,962.10 due to the cost of electricity and P_{l0} = \$3,706.75 due to the finance cost.

The price of bitcoin, as on 2 September 2018, is \$7,220.00/BTC. This is lower than the production cost of bitcoin, and therefore the miner is not making a profit. But it is still above the electricity cost. This makes sense because above \$9,668.85 there is an quasi-arbitrage opportunity and short positions will enter the market if the price of bitcoin goes too far above this.

At this level it still makes sense for the miner to mine, due to the fact that the loan must be repaid.

If the price is below the production cost of bitcoin and still mines the loss is

$$L = P_c - P, \tag{25}$$

where

L is the loss

P_c is the production cost of bitcoin

P is the market price of bitcoin.

If the miner stops mining the loss is the cost of financing, because this is not optional. The second hand market for mining equipment is not strong due to the fast depreciation in the value of the equipment.

The miner would want to have the minimum loss, therefore

$$L = MIN(P_c - P, P_f), \tag{26}$$

where

L is the loss

P_c is the production cost of bitcoin

P is the price of bitcoin

P_f is the financing cost of the equipment.

This can be rearranged to yield

$$L = MIN(P_e - P, 0) + P_f \, . \tag{27}$$

Therefore only when the price of bitcoin falls below the electricity cost should a miner stop mining. So, if the price of bitcoin falls below, $5,962.10, it will start to make more sense for the miner to stop mining.

The interesting thing is the price of bitcoin has recently moved below the electricity cost, causing the difficulty to start to decrease. Therefore the cost of electricity does not provide a floor for the price of bitcoin. This is because bitcoins cannot be converted back into electricity. It is a one way process.

The same is not true about prices above the production cost of bitcoin. The risks involved in mining bitcoin are not as high as they are for other commodities. Agricultural and mined commodities have various risks that are of a significant nature. Bitcoin on the other hand has very little risk involved. Apart from interruption of electricity and breakdown of a miner, there is very little risk. This means that profit above the production cost has more in common with arbitrage profits than it does with economic profits. Therefore the presence of the production cost of bitcoin does place a ceiling on the price of bitcoin. The question then becomes, why did bitcoin trade at such astronomic heights as above $18,000.00 in December 2018?

One possible reason is the futures market. Once it became possible to short bitcoin, the market might have crashed and kept falling because the price was above the electricity cost as per Equation 27.

5.2 THE PRICE-DIFFICULTY RATIO

5.2.1 Hypothesis

The bitcoin network can be modelled as company where miners are equity holders and bitcoins are promissory notes issued by the company. The company redeems these promissory notes as payment for rendering the service of transferring ownership of these promissory notes. It is the requirement by the bitcoin network that its services are remunerated in bitcoin by the bitcoin network, and this is what gives the bitcoins their inherent value. Each equity holder can decide to sell their earned bitcoins thereby issuing dividends, or reinvest those earnings in additional mining equipment.

As more miners join the network the equity gets diluted at the same rate. Given that mining revenue in bitcoin is relatively stable, this means that bitcoin revenue gets smaller at the same rate. Assume all the miners' expenses are in some fiat currency, such as dollars, and are fixed in that fiat currency for a given installation. These expenses would include:

1. Electricity;
2. Rent; and
3. Salaries.

Also, assume the miners' target is to have a stable fiat currency income, such as dollar income. Given these two assumptions the miners will require that the price of bitcoin in dollars must grow at the rate at which the mining network is growing.

This model implies that if the price of bitcoin in dollars is too low, the miners are less willing to sell (issue) bitcoin (bonds) and more willing to save them, and if the price is high the miners are more willing to sell (issue) bitcoin (bonds) and less willing to save them. If the miners implement a trading strategy to stabilise their dollar income, then upwards price pressure will occur for prices lower than their target price and downwards price pressure will occur for prices higher than their target price. This target price will differ between miners, but its average will always change at the same rate as the rate at which the strength of the mining network changes.

Assuming this average target price is the breakeven price for miners, this implies a bitcoin price-breakeven price ratio should exhibit a return to mean behaviour. This has been suggested by Fundstrat's Tom Lee [38].

The problem with this is that average breakeven point is very difficult to estimate for the entire network. There are too many unknown variables requiring too many assumptions.

One would have to determine the breakeven price for different categories of miners, each with different inputs, and then determine that weighting for each category.

This dissertation suggests that one should rather use the bitcoin price-difficulty ratio. As explained in the technical overview of bitcoin, the difficulty is a proxy for the strength of the bitcoin network. Because bitcoin revenue is relatively stable, the bitcoin revenue for every miner is inversely dependent on difficulty. Therefore the bitcoin price-difficulty ratio is a proxy for the bitcoin price-bitcoin revenue product and therefore proxy for dollar revenue of the miner.

As previously argued that miners would aim for stable dollar revenue, this implies the bitcoin price-difficulty ratio over a specified period should be modelled by a stochastic distribution. This implies the following hypothesises:

The price-difficulty ratio of a PoW cryptocurrency over a certain period is modelled by a lognormal distribution.

5.2.2 Methodology

The price-difficulty ratio was investigated for four of the six largest cryptocurrencies (by market capitalisation). These four cryptocurrencies were selected because they use PoW and therefore have a difficulty time series. These four cryptocurrencies include bitcoin, ethereum, bitcoin cash and litecoin.

Each of the time series for the price of bitcoin [39], ethereum [41], bitcoin cash [43] and litecoin [45] was collected. Each of the time series for the difficulty of bitcoin [40], ethereum [42], bitcoin cash [44] and litecoin [46] was also collected. The difficulty data for bitcoin cash and litecoin were not available for download, but was embedded in the page that was downloaded. The time span for each series is given in the appropriate sections on each cryptocurrency.

To retrieve the data from [44] the following javascript was run on the page using the console function on Chrome:

```
var s = ""; for (i = 0; i < 307; i++) s = s + new Date(d.getValue(i, 0)).toISOString().substring(0, 10) + "," + d.getValue(i, 1) + "\r\n"; s.toString();
```

To retrieve the data from [46] the following javascript was run on the page using the console function on Chrome:

```
var s = ""; for (i = 0; i < 2432; i++) s = s + new Date(d.getValue(i, 0)).toISOString().substring(0, 10) + "," + d.getValue(i, 1) + "\r\n"; s.toString();
```

The price time series values and the difficulty time series values were paired by matching dates. In the event that one time series extended further into the past than the other time series, the start date of the shorter time series was used.

Some of the time series' for difficulty did not have a difficulty value for certain dates and the corresponding price values were then deleted from the price time series. These were only a small amount of cases (less than five in each case) and therefore should not impact the final result.

To obtain the price-difficulty ratio time series the price was divided by the difficulty for each price-difficulty pair and a price-difficulty ratio was obtained for each date. A graph of the time series was created and a histogram for that time series was also created.

A lognormal distribution was fitted to each of the price-difficulty histograms, by calculating the mean and the standard deviation of the series created by taking the natural logarithm of the price-difficulty ratio time series values. To assess the goodness of fit of the lognormal distribution against the data three graphs were generated.

A graph was created that plots the pdf of the fitted lognormal distribution against the price-difficulty histogram. A graph was also created that plots the CDF of the fitted lognormal distribution against that cumulative price-difficulty histogram. A Q-Q plot was created that plots the CDF of the fitted lognormal distribution against the cumulative price-difficulty histogram.

5.2.3 Results

The results obtained from the previously described method for each of the cryptocurrencies is discussed below.

5.2.3.1 Bitcoin

Fig. 8 shows the plot of the price-difficulty ratio over time. The time series starts on 4 June 2016 and ends on 3 June 2018.

Figure 8. Price-difficulty ratio for bitcoin

Fig. 9 shows the histogram of the price-difficulty ratio for the same period.

Figure 9. Histogram of price-difficulty ratio for bitcoin

The distribution has a peak with a large cluster of the data points and then tapers of as the ratio increases.

The first two moments for the natural logarithm of the price-difficulty time series is given in Table 2:

Moment	ln(Price-Difficulty)
Average	1.178
Standard deviation	0.369

Table 2. First two moments for the natural logarithm of the bitcoin price-difficulty ratio

The pdf of the fitted lognormal distribution as described in the methodology is shown in Fig. 10, along with the price-difficulty histogram as a line graph.

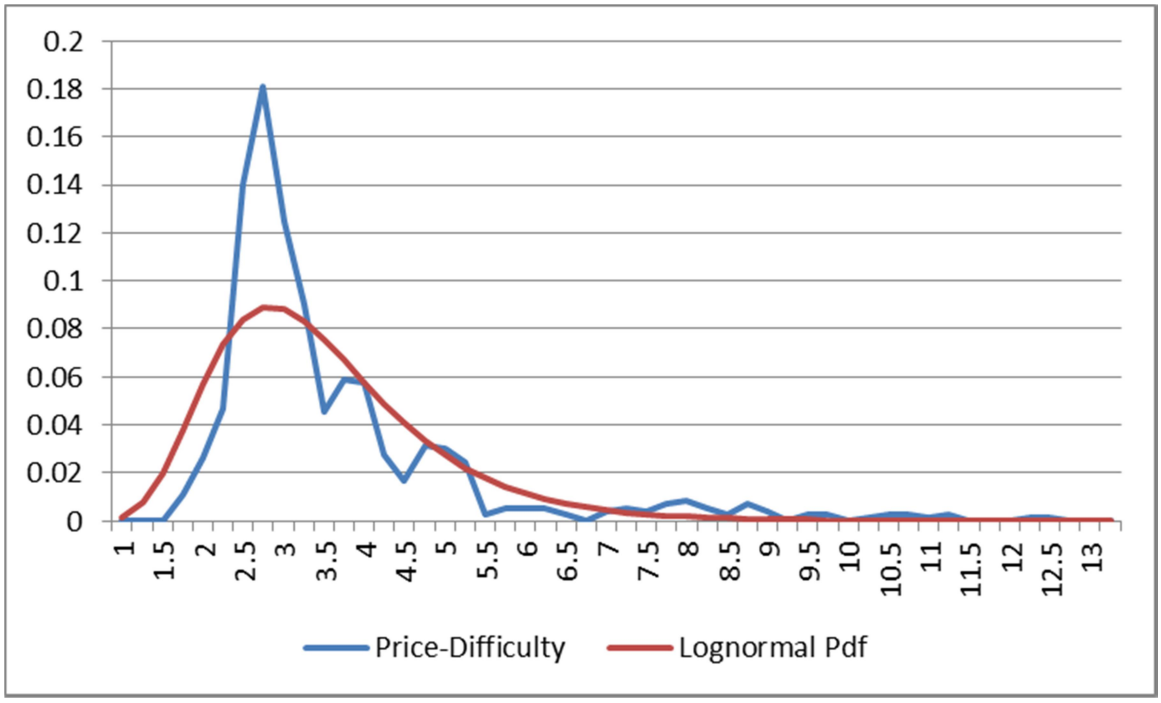

Figure 10. Lognormal pdf fitted to bitcoin price-difficulty ratio

The CDF of the fitted lognormal distribution is shown in Fig. 11, along with the cumulative price-difficulty histogram as a line graph.

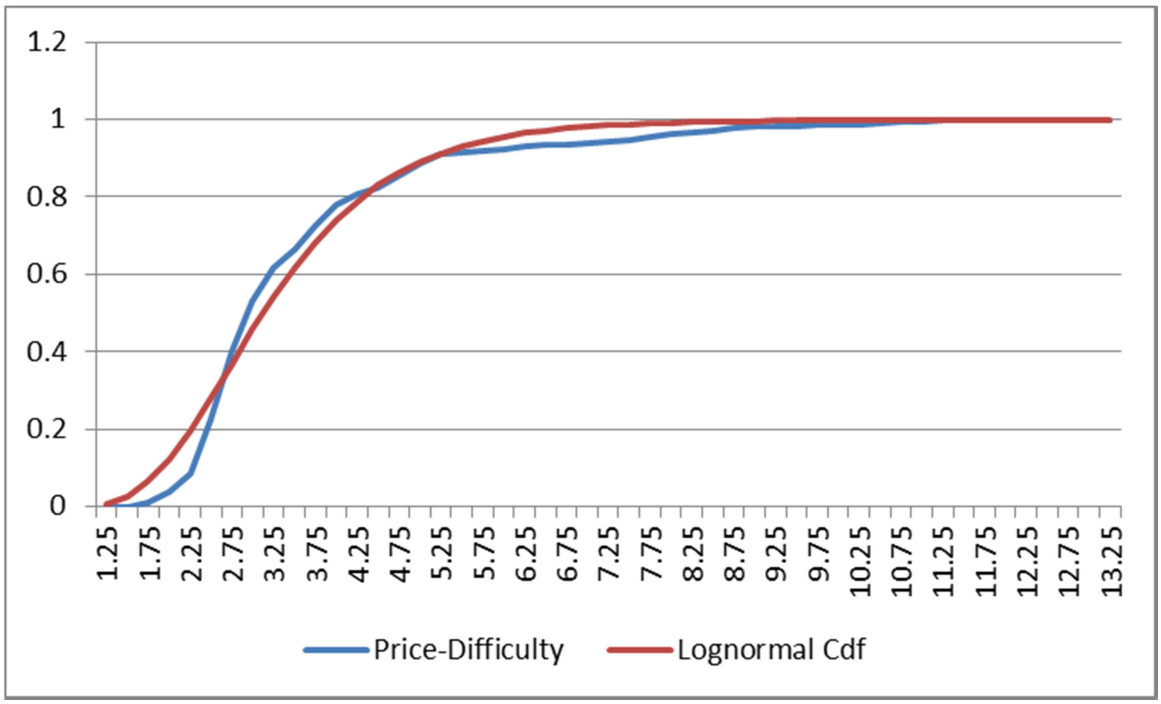

Figure 11. Lognormal CDF fitted to bitcoin price-difficulty ratio

The Q-Q plot of the CDF of the fitted lognormal distribution plotted against the cumulative price-difficulty histogram is shown in Fig. 12. The R-Squared for the linear fit in Fig. 12 is 0.988.

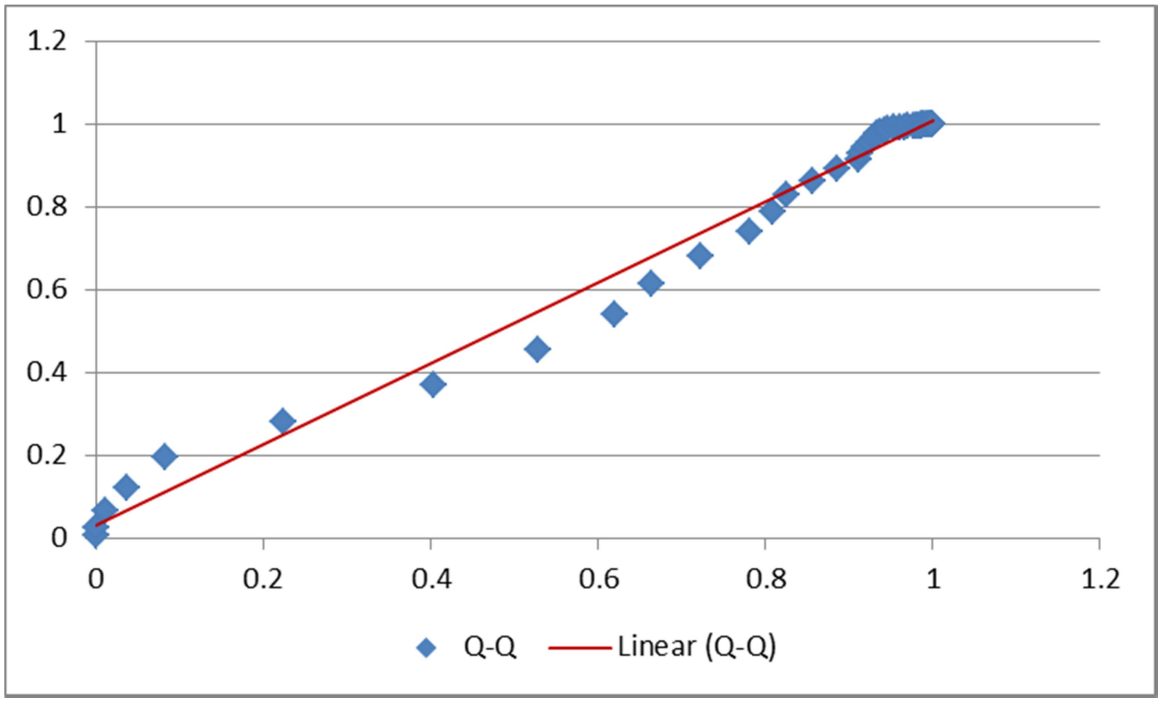

Figure 12. Q-Q plot of bitcoin price-difficulty ratio

These graphs and the value of R-Squared provide strong evidence to support the use of a lognormal distribution to describe the stochastic process that drives the price-difficulty ratio of bitcoin.

5.2.3.2 Ethereum

Fig. 13 shows the plot of the price-difficulty ratio over time. The time series starts on 8 August 2015 and ends on 3 June 2018.

Figure 13. Price-difficulty ratio for ethereum

From this graph the price-difficulty ratio looks like it could have a stationary mean and standard deviation if modelled using a lognormal distribution.

Fig. 14 shows the histogram of the price-difficulty ratio.

Figure 14. Histogram of price-difficulty ratio for ethereum

As before the data series does not go below zero; it has a peak with a large cluster of the data points and then tapers of as the ration increases. This also looks very much like a lognormal distribution.

The first two moments for the natural logarithm of the price-difficulty time series is given in Table 3:

Moment	**ln(Price-Difficulty)**
Average	-1.631
Standard deviation	0.515

Table 3. First two moments for the natural logarithm of the ethereum price-difficulty ratio

The pdf of the fitted lognormal distribution as described in the methodology is shown in Fig. 15, along with the price-difficulty histogram as a line graph.

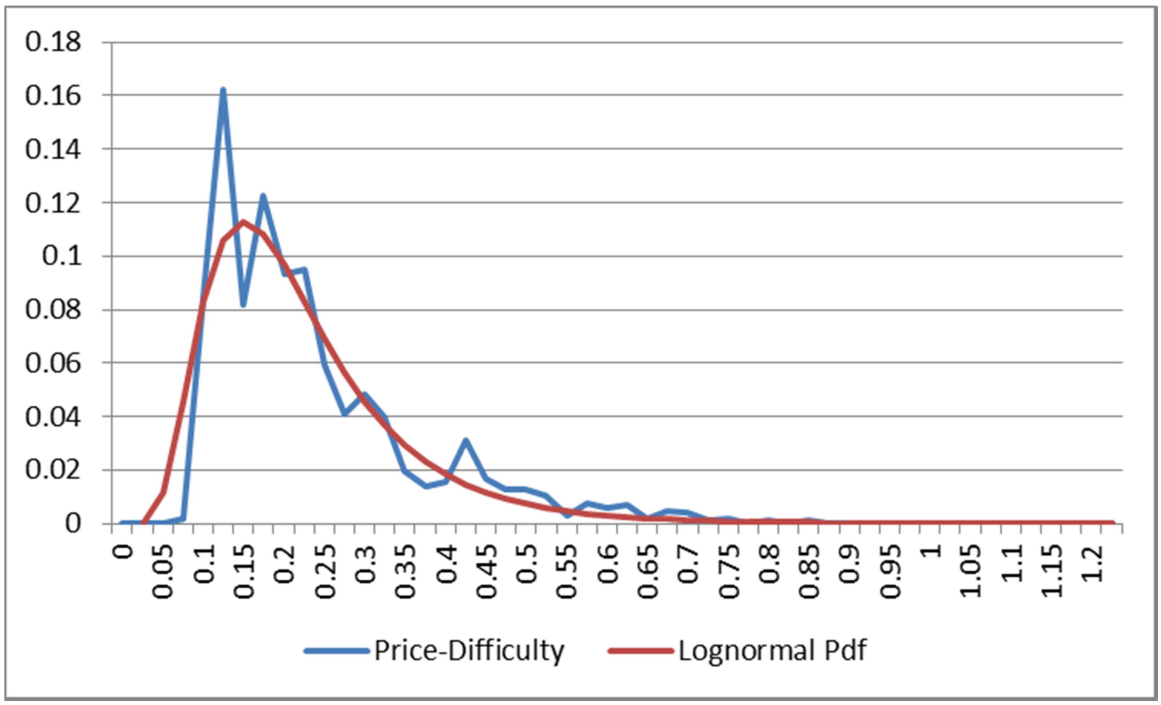

Figure 15. Lognormal pdf fitted to ethereum price-difficulty ratio

The CDF of the fitted lognormal distribution is shown in Fig. 16, along with the cumulative price-difficulty histogram as a line graph.

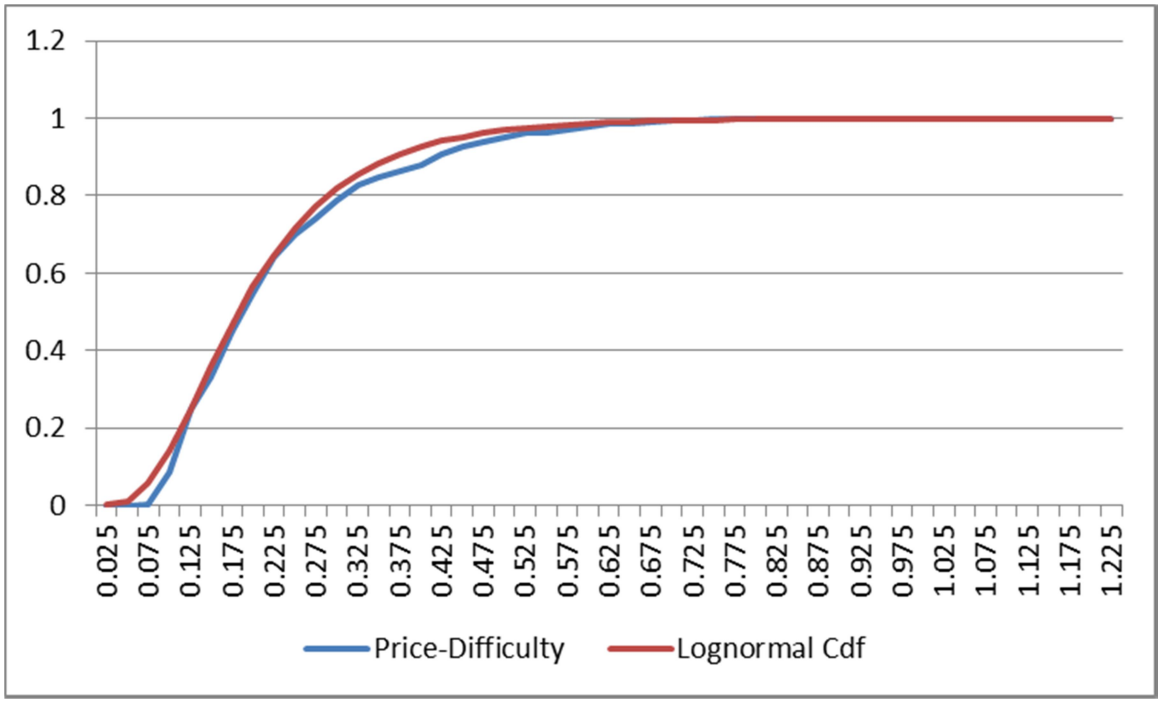

Figure 16. Lognormal CDF fitted to ethereum price-difficulty ratio

The Q-Q plot of the CDF of the fitted lognormal distribution plotted against the cumulative price-difficulty histogram is shown in Fig. 17. The R-Squared for the linear fit in Fig. 17 is 0.997.

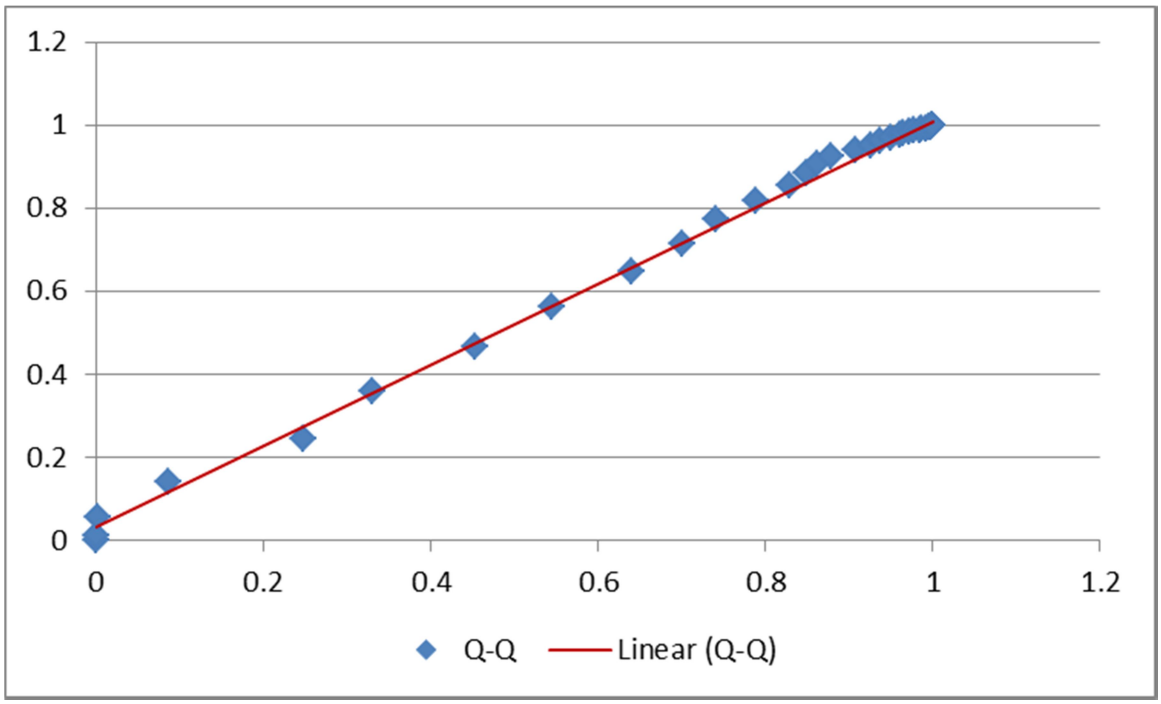

Figure 17. Q-Q plot of ethereum price-difficulty ratio

These graphs and the value of R-Squared provide strong evidence to support the use of a lognormal distribution to describe the stochastic process that drives the price-difficulty ratio of ethereum.

5.2.3.3 Bitcoin cash

Fig. 18 shows the plot of the price-difficulty ratio over time. The time series starts on 2 August 2017 and ends on 2 June 2018.

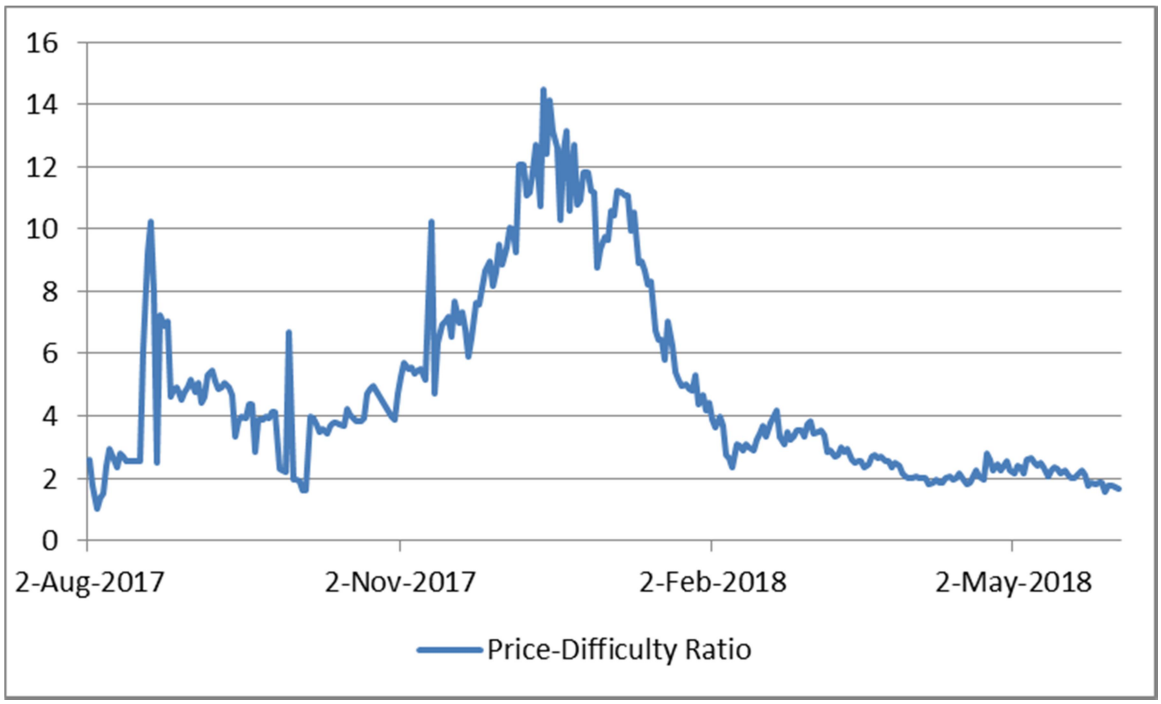

Figure 18. Price-difficulty ratio for bitcoin cash

From this graph the price-difficulty ratio looks like it could have a stationary mean and standard deviation if modelled using a lognormal distribution.

Fig. 19 shows the histogram of the price-difficulty ratio.

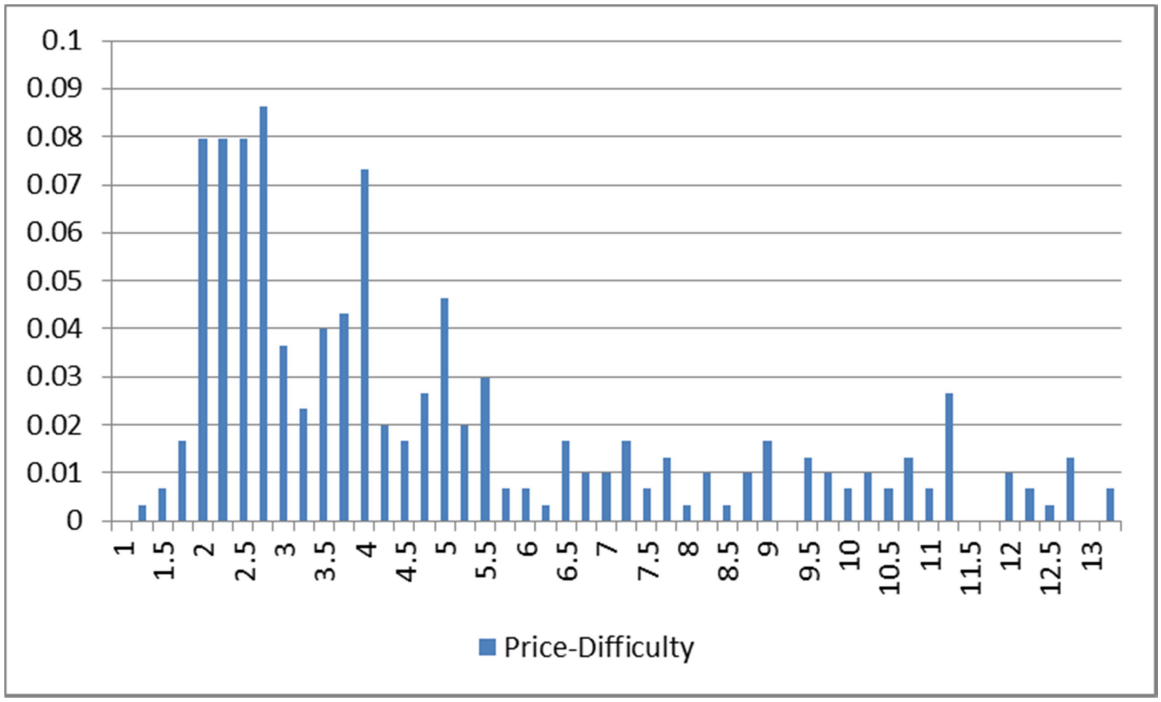

Figure 19. Histogram of price-difficulty ratio for bitcoin cash

As before the data series does not go below zero; it has a peak with a large cluster of the data points and then tapers of as the ration increases. This also looks very much like a lognormal distribution.

The first two moments for the natural logarithm of the price-difficulty time series is given in Table 4:

Moment	ln(Price-Difficulty)
Average	1.389
Standard deviation	0.595

Table 4. First two moments for the natural logarithm of the bitcoin cash price-difficulty ratio

The pdf of the fitted lognormal distribution as described in the methodology is shown in Fig. 20, along with the price-difficulty histogram as a line graph.

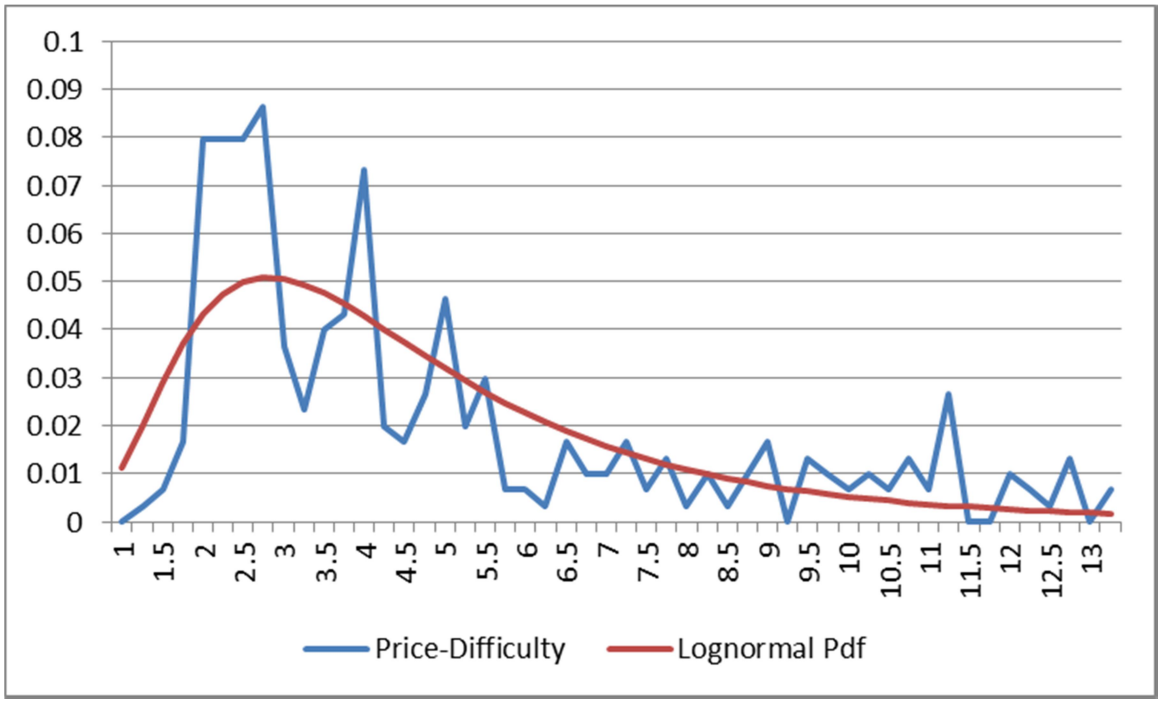

Figure 20. Lognormal pdf fitted to bitcoin cash price-difficulty ratio

The CDF of the fitted lognormal distribution is shown in Fig. 21, along with the cumulative price-difficulty histogram as a line graph.

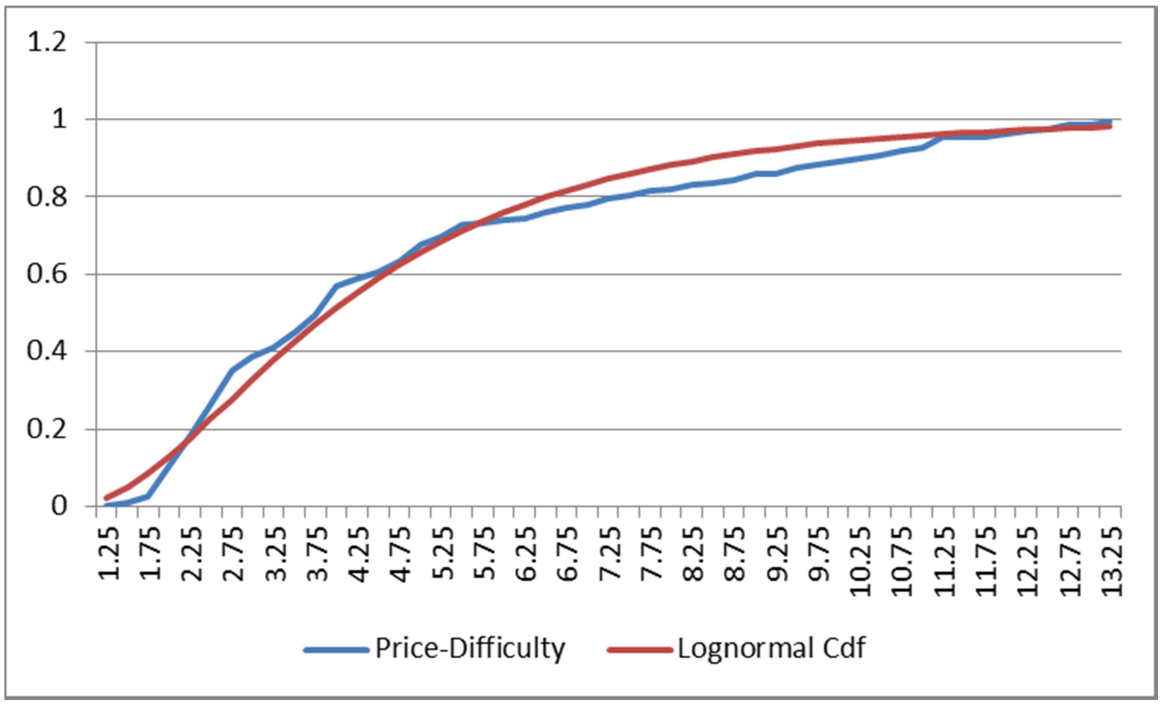

Figure 21. Lognormal CDF fitted to bitcoin cash price-difficulty ratio

The Q-Q plot of the CDF of the fitted lognormal distribution plotted against the cumulative price-difficulty histogram is shown in Fig. 22. The R-Squared for the linear fit in Fig. 22 is 0.985.

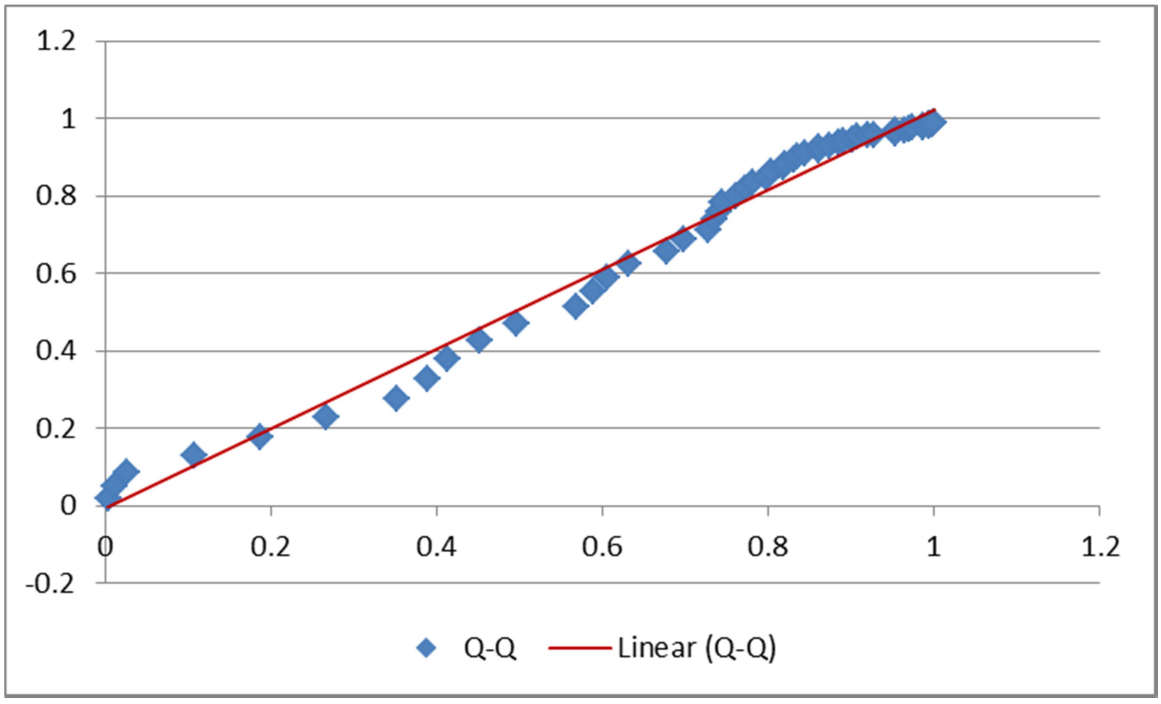

Figure 22. Q-Q plot of bitcoin cash price-difficulty ratio

These graphs and the value of R-Squared provide strong evidence to support the use of a lognormal distribution to describe the stochastic process that drives the price-difficulty ratio of bitcoin cash.

5.2.3.4 Litecoin

Fig. 23 shows the plot of the price-difficulty ratio over time. The time series starts on 28 April 2013 and ends on 2 June 2018.

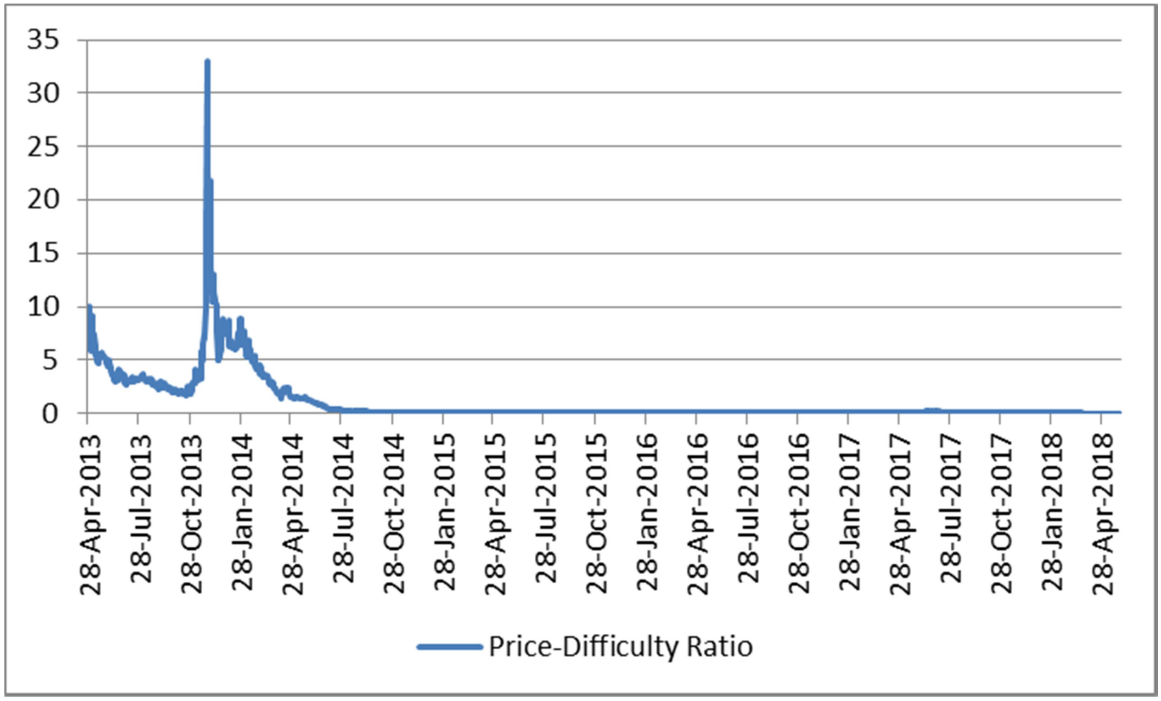

Figure 23. Price-difficulty ratio for litecoin

From this graph the price-difficulty ratio looks much less like it could be modelled using a lognormal distribution than the previous cases.

Fig. 24 shows the histogram of the price-difficulty ratio.

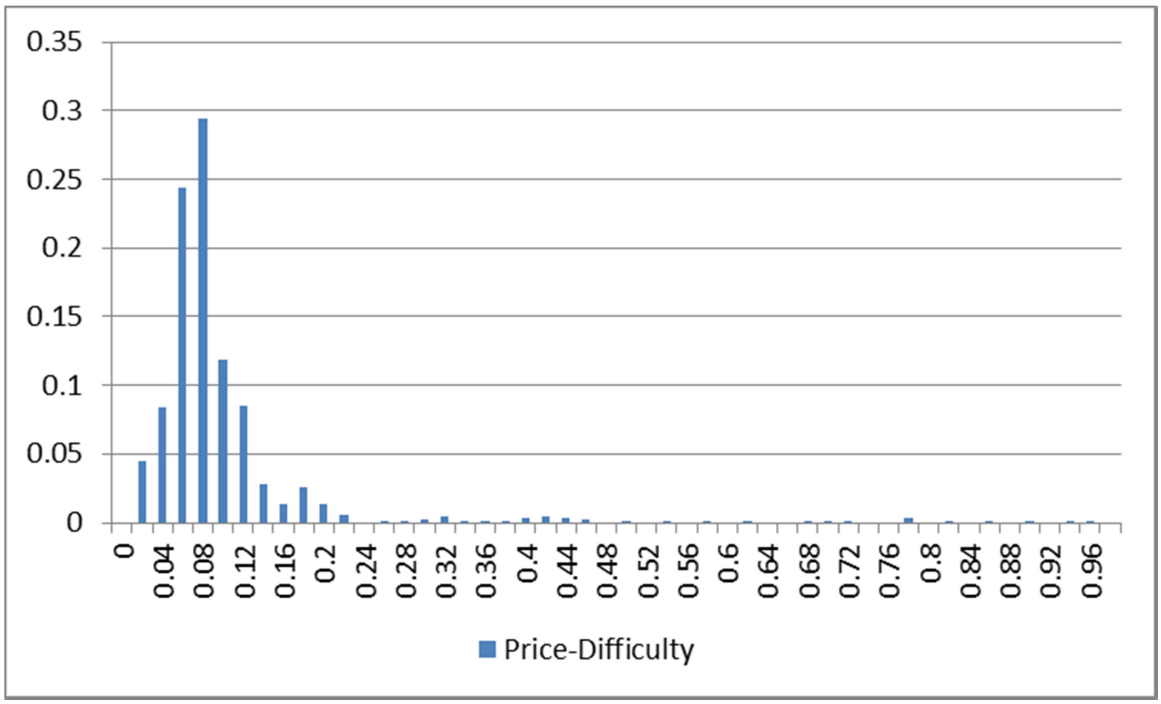

Figure 24. Histogram of price-difficulty ratio for litecoin

As before the data series does not go below zero; it has a peak with a large cluster of the data points and then tapers of as the ration increases. But it does taper of very quickly and might not be best fit with a lognormal distribution.

The first two moments for the natural logarithm of the price-difficulty time series is given in Table 5:

Moment	**ln(Price-Difficulty)**
Average	-1.802
Standard deviation	1.747

Table 5. First two moments for the natural logarithm of the litecoin price-difficulty ratio

The pdf of the fitted lognormal distribution as described in the methodology is shown in Fig. 25, along with the price-difficulty histogram as a line graph.

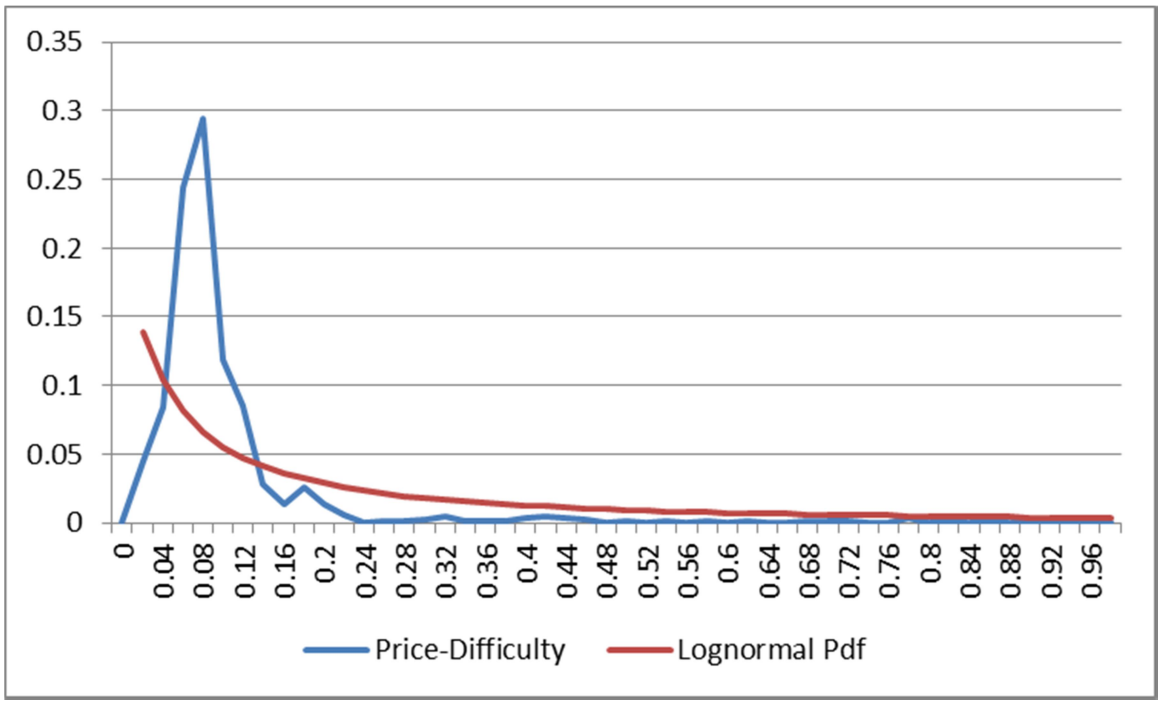

Figure 25. Lognormal pdf fitted to litecoin price-difficulty ratio

The CDF of the fitted lognormal distribution is shown in Fig. 26, along with the cumulative price-difficulty histogram as a line graph.

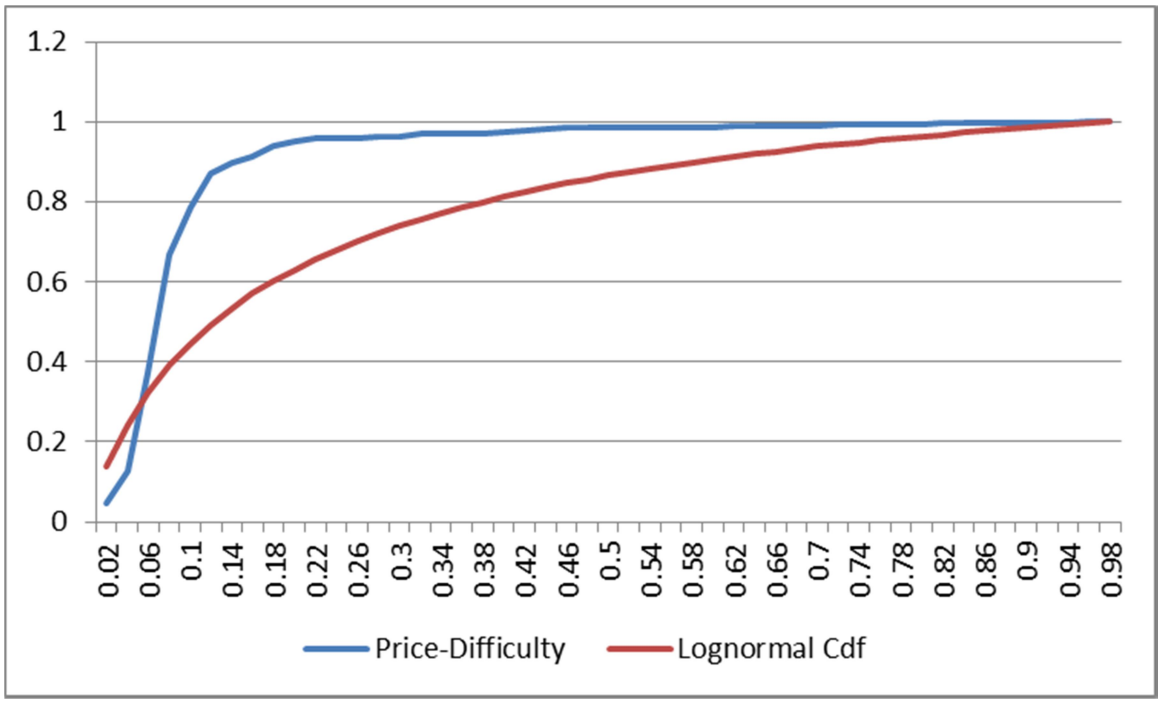

Figure 26. Lognormal CDF fitted to litecoin price-difficulty ratio

The Q-Q plot of the CDF of the fitted lognormal distribution plotted against the cumulative price-difficulty histogram is shown in Fig. 27. The R-Squared for the linear fit in Fig. 27 is 0.680.

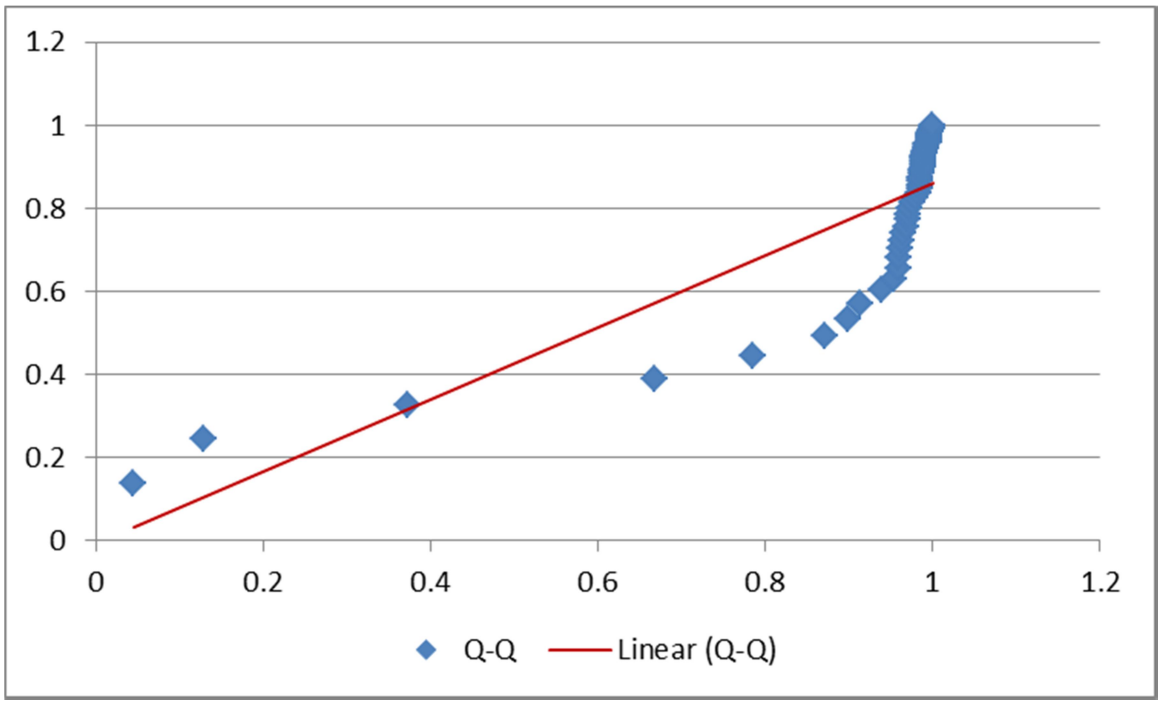

Figure 27. Q-Q plot of litecoin price-difficulty ratio

These graphs and the value of R-Squared do not provide strong evidence that the litecoin price-difficulty ratio is described by a lognormal distribution. A possible reason for this is that litecoin itself has a much smaller market capitalisation than bitcoin. Consequently its price follows that of bitcoin rather than being influenced by its own mining community.

The correlation between the bitcoin price and the litecoin price was calculated to test this possibility. The correlation was determined to be 0.959 which is strong evidence is support of this idea that the litecoin price actually follows the bitcoin price.

5.2.4 Conclusions

The results have shown ample evidence that the price-difficulty ratio of a cryptocurrency that uses PoW can be successfully modelled using a lognormal distribution. The size of the market capitalisation was also shown to be an important restriction. The lognormal distribution only fits the three largest PoW cryptocurrencies. The price of smaller cryptocurrencies seems to be moved by the market, or the larger cryptocurrencies.

5.3 THE STOCHASTIC MODEL

5.3.1 Derivation

To derive a stochastic model for the price of bitcoin, the hypothesis from the previous section that the price-difficulty ratio over a period of time can be modelled using the lognormal distribution is accepted.

Define the returns of the price-difficulty ratio as

$$r = \ln \frac{\rho_i}{\rho_{i-1}}, \tag{28}$$

where:

r is the return

ρ_i is the price-difficulty at time i.

From Equation 28 it follows that r is the sum of two normal distributions and should be modelled by a process that has a normal distribution with mean μ_ρ and standard deviation σ_ρ. The price-difficulty can therefore be modelled using the same stochastic model as that used for stock prices:

$$\frac{d\rho}{\rho} = \mu_\rho \cdot dt + \sigma_\rho \cdot dz, \tag{29}$$

where:

dρ is the change in the price-difficulty ratio

ρ is the price-difficulty ratio

μ_ρ is the mean of the returns of the price-difficulty ratio

dt is the change in time

σ_ρ is the standard deviation of the returns of the price-difficulty ratio

dz is a standard Wiener process.

From the definition of the price-difficulty ratio it follows that

$$\frac{d\rho}{\rho} = \frac{dP}{P} - \frac{dD}{D}, \tag{30}$$

where:

dρ is the change in the price-difficulty ratio

ρ is the price-difficulty ratio

dP is the change in the price of bitcoin

P is the price of bitcoin

dD is the change in the difficulty of bitcoin

D is the difficulty of bitcoin.

Defining

$$\frac{dD}{D} = \mu_d \cdot t \tag{31}$$

yields:

$$\frac{dP}{P} = (\mu_d + \mu_\rho) \cdot dt + \sigma_\rho \cdot dz, \tag{32}$$

where:

dP is the change in the price of bitcoin

P is the price of bitcoin

μ_d is growth of the difficulty

μ_ρ is the mean of the returns of the price-difficulty ratio

dt is the change in time

σ_ρ is the standard deviation in returns of the price-difficulty

dz is a standard Wiener process.

This model can be simplified. Using the data for bitcoin used in the section 5.2, Table 6 contains the first two moments of the natural logarithm of the returns of the price-difficulty ratio and the first two moments of the natural logarithm of the returns of the price.

	ln(Price-Difficulty/Price-Difficulty)	ln(Price/Price)
Average	-0.00065	0.00356
Standard deviation	0.04752	0.04472

Table 6. First two moments for the natural logarithm of the returns of the bitcoin price-difficulty ratio

The average of the daily returns of the price is much larger than the average of the daily returns of the price-difficulty, which implies that μ_d is much larger than μ_ρ. Also σ_ρ can be approximated by σ, the standard deviation of the returns of the price. Therefore Equation 32 can be simplified to

$$\frac{dP}{P} = \mu_d \cdot dt + \sigma \cdot dz \tag{33}$$

This model is the stochastic model for stocks, except that the drift is determined by the growth in difficulty.

5.3.2 Speculative projection

This model implies that opinion regarding the direction of difficulty is extremely important when deciding to invest in a cryptocurrency such as bitcoin. Fig. 28 shows the difficulty for bitcoin over the past two years.

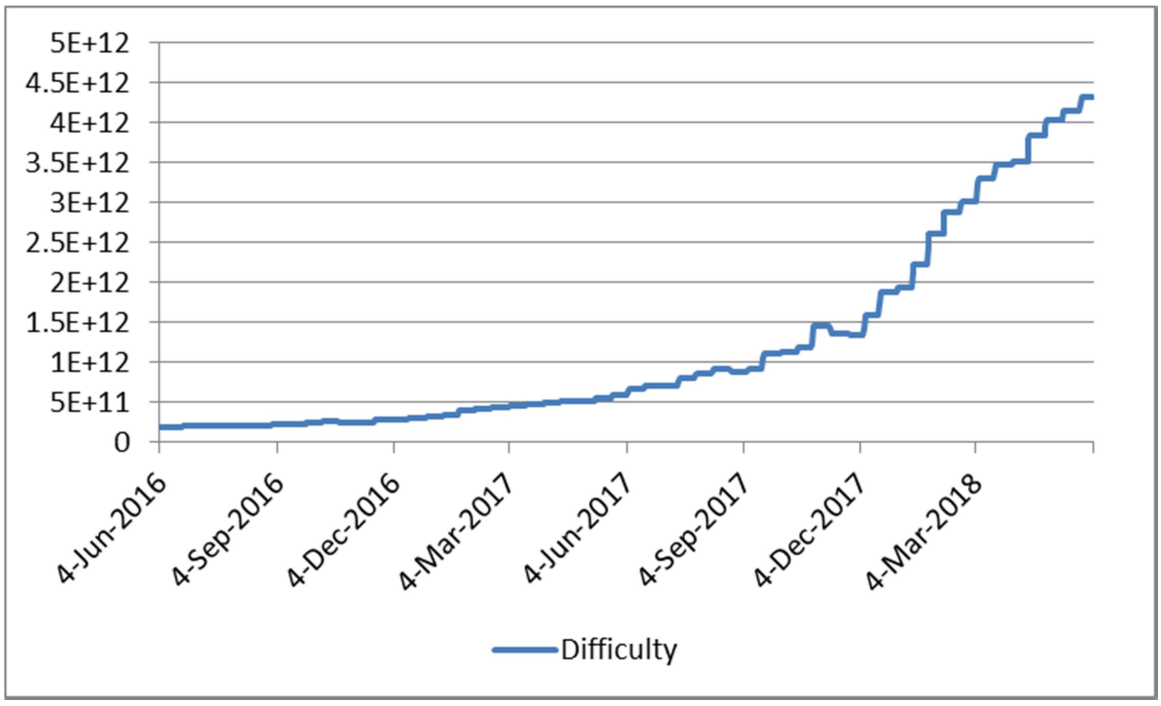

Figure 28. Difficulty for bitcoin

This figure shows that bitcoin has had exponential growth in its difficulty over the past two years. The geometric average for this growth in difficulty is 13.68% per month. In the event that this growth continues, then the expected price for bitcoin will grow from its

present $7,600 to over $ 3.5 million in four years' time giving it a market capitalisation of over $ 60 trillion. At this point in time it is not possible to determine what, if any, restraints will stop the bitcoin network from growing unabated. Only time will tell what will happen with the growth of the network and any projection on the growth of the network is speculation.

What has been shown by Bouri et al [47] and Demir et al [48] is that bitcoin is a hedge against uncertainty. When global uncertainty escalates, bitcoin appreciates. The fact of the matter is that bitcoin was invented after the Great Financial Crisis and we therefore do not know how much bitcoin would appreciate if such a financial crisis were to repeat.

Using the model from the section 5.3.1 a speculative projection can be made for the purposes of example only. The projection is for the price over the next two years, assuming the difficulty continues to grow at the rate of the past two years. Fig. 29 below shows the projections of the price over the next two years using the growth in difficulty to determine the average price and the standard deviation of Table 6 to determine the standard deviation bands. Each projection is a Monte Carlo simulation using the stochastic model. The projection that ends with the lowest price is Model 7 with $31,460.70. The projection that ends with the highest price is model 9 with $733,099.03.

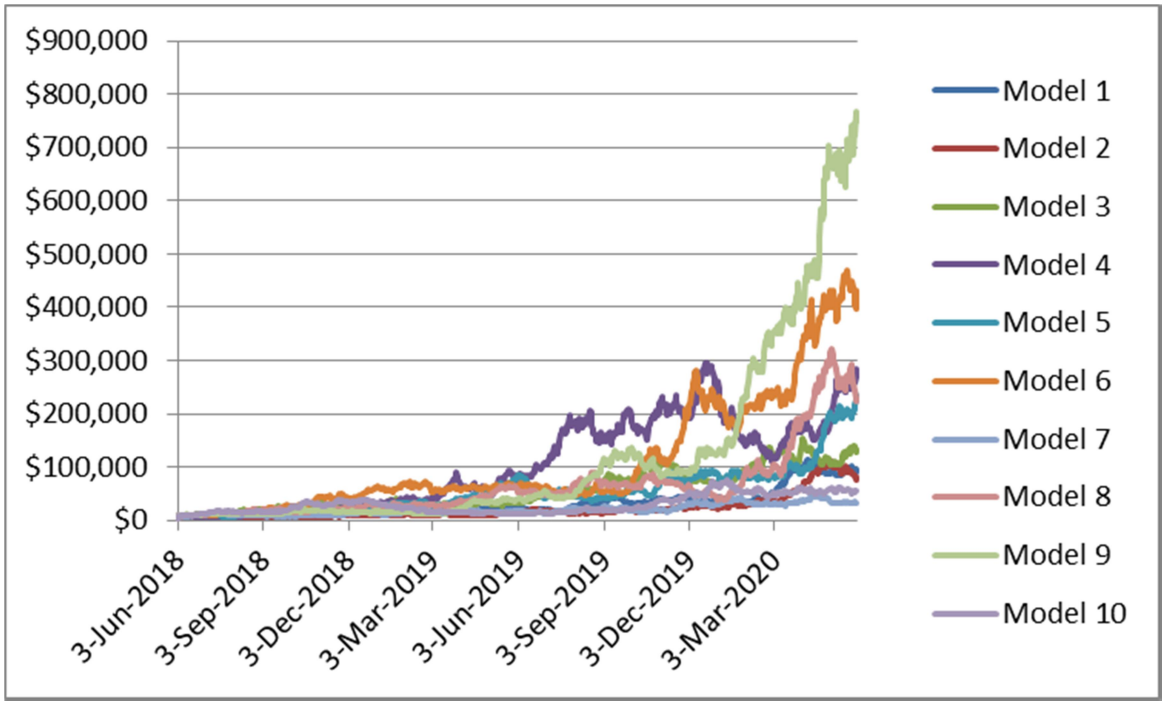

Figure 29. Projections for the price of bitcoin

The problem with this extrapolation is the question where does this end? It surely cannot continue to grow indefinitely. There must be some constraints that will limit this growth.

This example also illustrates the outsized impact of the assumption of the growth of difficulty on the projection of the price of bitcoin. It is therefore important that further research into the growth of difficulty is undertaken, at the very least to reconcile this model with the martingale model developed by Schilling et al [36].

But each of these constraints implies vastly different ceilings on the price of bitcoin. And if bitcoin is able to reach such astronomic height it is imperative that the central banks of the world create competition for bitcoin in the form of a CBDC.

In fact, Hayes [49] argues that cryptocurrencies could disrupt the administration of monetary policy and central banks and move us towards a more algorithmic approach. It was also argued by Kaushik Basu, former Chief Economist of the World Bank, in [50] that the new cryptocurrency Libra [51] could threaten the ability of policymakers to manage monetary environments.

Chapter 7 explains this dissertation's candidate CBDC, the sovereign cryptocurrency, in greater detail. In fact, recently the South African Reserve Bank has shown interest in creating a CBDC [b].

CHAPTER 6: ANONYMOUS ATOMIC SWAPS

Although blockchain technology affords some anonymity to its users, this anonymity can be broken for a network of transacting users if a single account of an individual within that network is linked to that individual's identity. A number of solutions have been proposed but all have different limitations. This chapter introduces a new technique by which a user is able to swap ownership of cryptocurrency coins with another user in an atomic fashion requiring no trust and without publicly linking the legs of the exchanges on the public ledger. To an entity following a trail of cryptocurrency coins, such a swap would end the trail as it would not be obvious which coins the individual being investigated owns after the swap.

The reason this technique is introduced is to show that improvements are possible that improve the anonymity of the user of bitcoin. Currently this technique is not supported by the bitcoin protocol. New techniques are however being developed and implemented in the bitcoin protocol that will provide significant improvements to the anonymity allowed to the bitcoin user. These techniques use Schnorr signatures instead of the normal elliptic key signatures used currently by the bitcoin protocol.

After the anonymous atomic swaps are described the advantages of the technique to use Schnorr signatures will be discussed.

6.1 BACKGROUND

One of the earliest techniques used to obfuscate the ownership of cryptocurrency coins on a blockchain is called tumbling or mixing. It requires that multiple parties give their cryptocurrency coins to a trusted party. This trusted party would then return the cryptocurrency coins to the original owners but using a different account than the original source account. As the accounts are not linked, it is not obvious which trail of cryptocurrency coins to follow in an investigation after a mix.

There are certain drawbacks to this technique. The first, and most important drawback, is that the trusted party might not be trustworthy. They might simply disappear with the cryptocurrency. Or they might keep record of the mix and reveal this to a third party.

Other drawbacks are that the coins from each source must be the same amount. If not, it would be possible to determine ownership of the target accounts by comparing the amounts that were sent into the mix to the amounts sent out of the mix.

A new technique therefore has to resolve the trust issue and provide a mechanism to split the amount being anonymised into different random amounts. The trust issue can be resolved by using atomic swap of cryptocurrency.

Atomic swaps, also referred to as hashed time lock contracts, were first discussed in online discussion forums by Nolan [52]. Since then, open source code has been published that implements two party cross-chain swaps between selected currencies [53, 54].

Basically an atomic swap uses the feature of a blockchain to place conditions on a user's ability to spend the output of a cryptocurrency transaction. Atomic cross-chain swaps are discussed in depth by Herlihy [55].

Suppose Alice wants to exchange alicecoins she owns for the bobcoins that Bob owns, and Bob wants to do the opposite. Alice and Bob do not know each other, much less trust each other. To execute the transaction they can use atomic swaps.

To execute the atomic swap Alice sends alicecoins to Bob. But Alice limits Bob's ability to spend these alicecoins by placing a condition on them being spent.

Alice generates a large random number and computes its hash. This hash is inserted in the conditions of the transaction that sends the alicecoins to Bob. To be able to spend the alicecoins, Bob must provide the secret number that Alice generated to the alicecoin network. The alicecoin network will compare the hash of any number presented by Bob and compare this with the hash Alice encoded in the transaction. If the hashes match, Bob will be able to spend the alicecoins. Without knowing the secret number, Bob is unable to access the alicecoins.

Bob in his turn does a similar transaction. He sends Alice bobcoins and limits Alice's ability to spend them by using the same hash that Alice used in her transaction. But in this case Alice does know the secret number that can be used to spend the bobcoins. Alice therefore supplies the secret number to the bobcoin network, freeing the bobcoins for her to spend.

By watching the bobcoin blockchain, Bob will then be able to see the secret number that Alice used to unlock the bobcoins. He can then use that same secret number to unlock the alicecoins.

In this manner each party received the cryptocurrency coins they desired and neither party had to trust the other.

In the event that neither party used the secret number to unlock the transactions; or Bob did not commit his bobcoins to the transaction, each transaction is encoded with an additional timeout condition. This condition lets the sender of the coins recover the coins after a set amount of time has elapsed.

The problem that atomic swaps have is that the secret number links the two transactions uniquely. If someone is following the alicecoins that Alice owns through the alicecoin blockchain they will see that an atomic swap occurred. They would then just have to scan other blockchains for that same secret number and they will be able to find that she has taken ownership of the bobcoins on the bobcoin blockchain.

The solution to this problem is anonymous atomic swaps. In an anonymous atomic swap, both parties exchange equivalent value in cryptocurrency in an atomic fashion as described above, with the difference that each party uses a different hash generated by a different secret number. The two secret numbers are linked arithmetically to a secret shared only by the two parties.

To achieve this feat a technique called homomorphic hashing is required. Homomorphic hashes can be manipulated arithmetically just as if the secret values they encode are being manipulated. For example, if two numbers, s_1 and s_2, together form a sum z, then the homomorphic hash of each number $h(s_1)$ and $h(s_2)$ can be added together to obtain the hash h(z) of the sum z.

Using this technique Alice would generate two secret numbers, s_1 and s_2, and sends the sum of the two numbers, t, along with the hash of each number, $h(s_1)$ and $h(s_2)$, to Bob. Bob would be able to confirm that the hash of the sum, h(z), is equal to the sum of the hashes, $h(s_1) + h(s_2)$. The t is the secret that only Alice and Bob know. It is never published on any blockchain.

Alice uses the one hash, $h(s_1)$, to send alicecoins to Bob. Because Bob was able to determine that the hashes he has sum to h(z) he is confident that he will be able to

determine s_1 if Alice publishes s_2. Therefore Bob uses the other hash, $h(s_2)$, to send bobcoins to Alice. If Alice recovers her bobcoins with s_2, Bob would be able to use s_2 and t to determine s_1, which enables him to unlock the alicecoins.

An example application of a homomorphic hash in the literature that allows for homomorphic summing of the hashes is by Krohn, et al. [56]. In [56] the hash function used is

$$h(s) = g^s mod\ p \tag{34}$$

The problem with using this hash function is execution time. For the secret, s, to be hard to determine using brute force, the number of bits used for the secret and the hash must be very high, e.g. 256 bits. This implies the secret is a very large number. Raising g to the power of s would take an incredibly long time. This breaks down the usefulness of this hash function, as a hash should be easy to calculate but hard to reverse. In this case one would have to bring down the number of bits used to encode the secret to make it feasible to compute the hash in an acceptable time. But this would make it feasible to mount a brute force attack on the hash.

This paper suggests using a different homomorphic hash function to perform anonymous atomic swaps.

6.2 PROPOSED HASH FUNCTION

Anonymous atomic swaps require a hash function that conforms to the following requirements:

1. The hash function must always give the same hash for the same secret;
2. The hash function must be quick to compute;
3. The hash function must have a large search space to make a brute force attack infeasible; and
4. The secret must be uncorrelated to the computed hash.

This paper investigates the use of the following function as a homomorphic hash function

$$h(s) = s^n mod\ p, \tag{35}$$

where

$s < p$.

This function is actually a type of pseudorandom number generator, but is used here to hash the secret number s.

This method is deterministic; and for low values of n it is quick to compute, even for large values of s. Even using 256 bit sized secrets it will be quick. This makes it infeasible to use a brute force attack to reverse the hash.

6.3 PROVE HASH IS HOMOMORPHIC

To prove the hash function in 35 is homomorphic, first define

$$h_1 = s_1^n mod\ p\ , \tag{36}$$

$$h_2 = s_2^n mod\ p\ , \tag{37}$$

$$z = s_1^n + s_2^n\ , \tag{38}$$

$$h_z = z\ mod\ p, \tag{39}$$

where

$s_1 \neq s_2$.

To prove Equation 35 is homomorphic, it is necessary to prove

$$(h_1 + h_2) mod\ p = h_z. \tag{40}$$

Use Equation 36 and Equation 37 to obtain

$$(h_1 + h_2) mod\ p \tag{41}$$

$$= (s_1^n mod\ p + s_2^n mod\ p) mod\ p\ .$$

Using the following property of modular arithmetic

$$(a + b) mod\ c \tag{42}$$

$$= (a\ mod\ c + b\ mod\ c) mod\ c\ .$$

Applying this to Equation 41 yields

$$(h_1 + h_2) mod\ p \tag{43}$$

$$= (s_1^n + s_2^n) mod\ p$$

$$= z\ mod\ p\ .$$

which proves

$$(h_1 + h_2) mod\ p = h_z \tag{44}$$

6.4 REVERSING THE HASH

To reverse the hash requires an integer m such that

$$s = h^m mod\ p. \tag{45}$$

Combining this with 36 yields

$$s = s^{n \cdot m} mod\ p. \tag{46}$$

Modifying Euler's theorem,

$$1 = s^{\varphi(p)} mod\ p, \tag{47}$$

so that

$$s = s^{\varphi(p) \cdot t + 1} mod\ p, \tag{48}$$

where t is any integer. Combining this with Equation 46 yields

$$\varphi(p) \cdot t + 1 = n \cdot m. \tag{49}$$

If p is prime then

$$\varphi(p) = p - 1. \tag{50}$$

Using this yields

$$(p - 1) \cdot t + 1 = n \cdot m. \tag{51}$$

If we require

$$(p - 1) mod\ n = 0, \tag{52}$$

then

$$(p - 1) = n \cdot k. \tag{53}$$

Substituting this into Equation 51 yields

$$k \cdot t + \frac{1}{n} = m. \tag{54}$$

Then m will be a fraction and the hash cannot be reversed using this attack.

6.5 COLLISIONS

Each hash can also be a secret. This creates chains of secrets, such as

$$s_2 = s_1^n mod\ p, \tag{55}$$

$$s_3 = s_2^n mod\ p, \tag{56}$$

up to

$$s_{m+1} = s_m^n mod\ p. \tag{57}$$

A chain can have

1. starting points that never recur in the chain;
2. points that transfer from one point to another point; and
3. endless loops.

There can be multiple chains within the same domain.

If there are no collisions then only one point can transfer to another point. This means that two chain paths cannot join. That means that each starting point is also an ending point and it is actually on a loop.

In other words, if there are no collisions, there are only endless loops. That would allow an attacker to apply Equation 45 with an integer m to determine the secret.

This implies that if there are no collisions then a hash is reversible.

If there are collisions, there might be some loops but not everything would be on a loop. Therefore there would not be an integer m that can be used to apply Equation 45. Thus the hash would not be reversible by using Equation 45.

But this does not mean there is no other attack. There might be loops; it's just that the attacker would not know if they are on a loop if the search space is large enough.

6.6 REDUCED SEARCH SPACE

The maximum number of collisions can be determined using Lagrange's Theorem which states: if f(x) is a polynomial of degree n with integer coefficients so that at least one coefficient is not divisible by the prime p, then f(x) ≡ 0 (mod p) has at most n roots modulo p.

Assume we have a collision. This implies

$$h_1 = h_2, \tag{58}$$

in definitions Equation 36 and Equation 37. This implies

$$s_1^n mod\ p = s_2^n mod\ p, \tag{59}$$

$$(s_1^n - s_2^n) = 0\ (mod\ p). \tag{60}$$

Using Lagrange's theorem implies at most n roots, and therefore at most n secrets have the same hash.

Therefore the search space is reduced by a factor 1/n.

6.7 COLLISIONS AND HOMOMORPHIC HASH

The presence of collisions has implications for the homomorphic feature of the proposed hash function. Specifically a hash can have more than one secret. This implies that Equation 40 can have multiple solutions.

If Alice is able to determine two secrets that have the same hash, she can use the one to generate hashes and sums to send to Bob, but use the other secret to unlock the coins Bob sent to her. This will stop Bob from being able to solve Equation 38 correctly and unable to claim his coins. After a time delay Alice will then claim the coins.

This increases the requirement for a large search space. An attacker must not be able to determine any of the secrets that generate the same hash except using brute force.

6.8 LOW CORRELATION

The last requirement for the hash function proposed in 36 is that the correlation between the secret s and its hash value h is very small.

Specifically, this correlation is measured between the vector of all possible s within a range, and the vector of the corresponding hash values for each s.

To measure this for the range 0 ... 2^{16}-1, a prime larger than 2^{16}-1 was generated for p using Maurer's algorithm. The specific value for p was 120097. A value of 3, 7, 5 and 9 was used for n. The results are in Table 7.

N	correlation
3	0.000869
5	-0.003698
7	-0.002891
9	0.000313

Table 7. Correlation between secret and its hash for 16 bit space

The examples used suggest that the correlation for a 16 bit hash function is very low.

The same test was performed for a bit space of 256, but with the same amount of samples and values for n. The samples were chosen at random. The value used for p was 14656571228214736839807814984260904086072221909468537398478314916108106611 7389.

The results are shown in Table 8.

N	correlation
3	0.001038
5	0.003820
7	0.005771
9	-0.000102

Table 8. Correlation between secret and its hash for 256 bit space

The scatter plot was also drawn for the case of n=3 of Table 2 with only 256 random cases. The scatter plot is shown in Fig. 30.

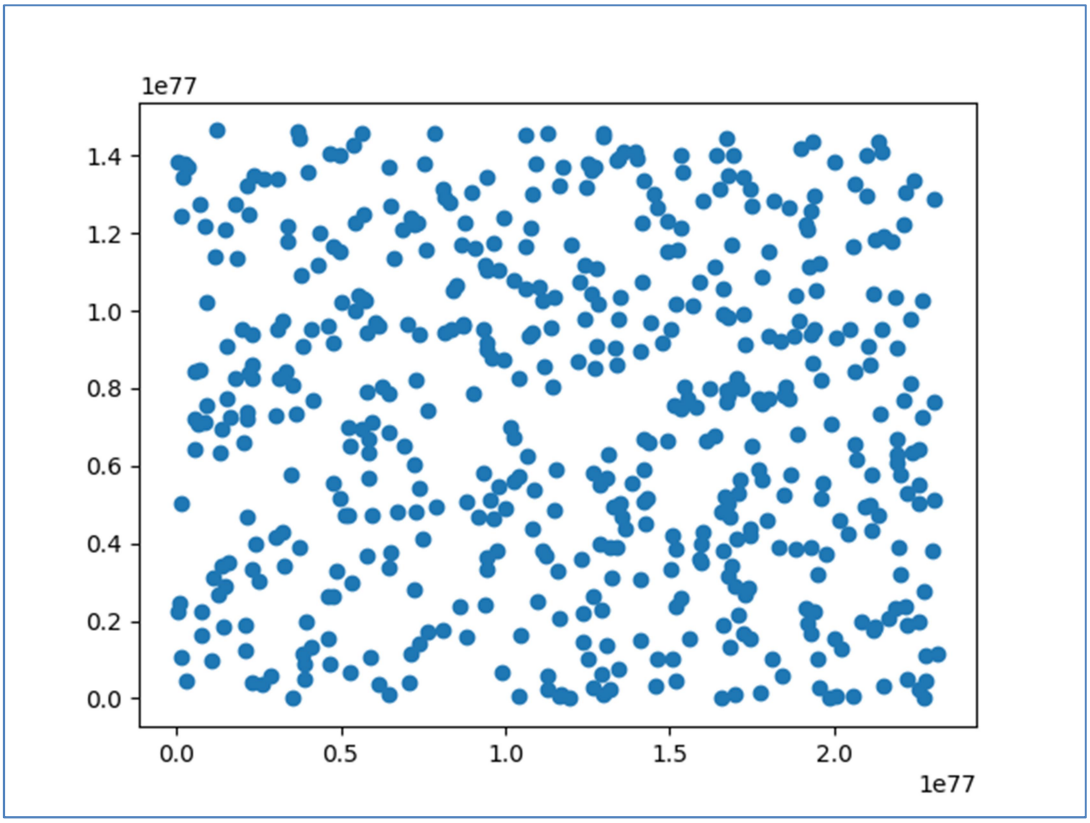

Figure 30. Scatterplot of secret against hash

From this evidence it is clear that the correlation of the proposed hash function in low bit space is very low, and probably also very low in high bit space. Unfortunately it is not possible to perform an exhaustive test for high bit space, as the processing time for exhaustively determining the correlation in high bit space is infeasibly long.

6.9 HEURISTIC ATTACKS

A possible attack would be to try and guess the secrets from the sum. If the sum z is very low or very high, very few secrets will be candidates to generate that sum.

For example, if we use n = 3 and 8 bit representation with p = 257 and the sum is 2, then the secrets must be 1 and 1. The same holds for very high sums. If the sum is 33162750 and the secrets are limited to max 255 then the secrets must both be 255.

This attack can easily be solved by limiting the sums we find acceptable to the range

$$(\tfrac{2}{3} \cdot p)^3 < z < p^3. \quad (61)$$

Another attack would be to try and guess the two secrets from the sum. By using Equation 38 the attacker tries to reduce the search space.

The attacker will have to start with $s_1 = 1$ and solve for

$$c = ceil\left((\mathrm{z} - \mathrm{s}_1^n)^{1/n}, \mathrm{d}\right), \tag{62}$$

where d = 0 indicates the ceil function provides the closest integer higher than its first argument. When d = 1, the value of c is to the closest 0.1 above the first argument of the ceil function.

The error is then

$$e = \mathrm{s}_1^n + c^n - z. \tag{63}$$

The attacker will then have to move through values of s_1 looking for e = 0.

Now observe that

$$b = ceil(10 \cdot a, 0) \tag{64}$$

$$= 10 \cdot ceil(a, 1) \ .$$

That is, we can multiply a by 10 and then ceil to closest integer, or we can ceil to closest 0.1 and then multiply by 10.

Then scale space with x so that

$$s_1' = 10^x s_1, \tag{65}$$

$$z' = 10^{3x} z. \tag{66}$$

Then

$$\mathrm{e} = (\mathrm{s}_1')^n + \left(ceil\left((\mathrm{z}' - (\mathrm{s}_1')^n)^{1/n}, \mathrm{d}\right)\right)^n - \mathrm{z}', \tag{67}$$

$$\mathrm{e} = \left(10^x s_1\right)^n + \left(ceil\left(\left(10^{3x} z - \left(10^x s_1\right)^n\right)^{1/n}, \mathrm{d}\right)\right)^n - 10^{3x} z \ , \tag{68}$$

$$\mathrm{e} = 10^{3x}\left[s_1^n + \left(ceil\left((z - s_1^n)^{1/n}, \mathrm{d}\right)\right)^n - z\right] \ . \tag{69}$$

If we now increase x, the ceil can be approximated by removing it and this then reduces to

$$e = 10^{3x}[s_1^n + z - s_1^n - z], \quad (70)$$

$$e = 10^{3x}0. \quad (71)$$

Therefore e reduces to 0 for all values of s_1 and z if x becomes large enough.

Effectively, as x increases the search space changes from integer space to rational space.

Thus the search for a unique solution to Equation 63 becomes intractable.

Specifically the attacker has to search for s_1 in the range of

$$1 \leq s_1^3 \leq z - 1. \quad (72)$$

Using the range for z in Equation 61, the search space is reduced by most a factor of 2/3.

6.10 MULTI-TRANSACTION SWAPS

At this point it should be clear that there is no limit to the number of transactions that can be linked using anonymous atomic swaps. It is simply a matter of algebra.

If Bob wants Alice to send him the coins using three transactions to three different accounts, and Alice wants Bob to send her the coins using two transactions to two different accounts, it can be achieved using simple linear algebra.

In setting up such a swap, Alice will generate a secret random number for each transaction, five in total. She will also construct a set of linear equations that sum the random numbers in different ways. She must have one less equation than she has secret numbers. She will then send the hashes of the secret numbers, the sum of each equation and the set of equation formulas to Bob. Bob will be able to validate that the equations balance using homomorphic arithmetic, but will not be able to solve the set of linear equations, as he is one equation short of solving all of the unknown secret numbers.

Each of these transactions will have a different amount, but the amounts of Alice's transactions will have to add up to the amounts of Bob's transactions.

As soon as all of the transactions are committed to the blockchain, Alice can start claiming her anonymous coins. As soon as she has claimed the first transaction, Bob will have enough information to start solving the set of equations and can then start claiming his anonymous coins.

6.11 REMARKS

This paper has proposed using hash function that has homomorphic features for use in an anonymous atomic swap. It was shown that the proposed hash function conforms to all the requirements needed of a cryptographic hash function.

To support anonymous atomic swaps, cryptocurrencies needs to support at least the MOD and MUL opcode functions. Alternatively, an opcode that implements the proposed hash function can be added. The value for n and p must also be standardised, so that one swap cannot be distinguished from another swap. To perform the actual swap, current atomic swaps used in distributed exchanges can be modified to make cross-chain atomic swaps anonymous.

But it is not necessary that anonymous atomic swaps also be cross-chain swaps. They can also be on the same blockchain. They would simply swap one set of coins for another in order for the owners to acquire anonymity.

Such a swap would simply be implemented within current wallets. The wallets would broadcast, route and accept swap requests in a peer-to-peer manner.

This would make it relatively easy for owners of cryptocurrencies to acquire anonymity and protect their identity online.

6.12 RELATED WORK

There are several schemes for solving the anonymity problem in cryptocurrencies such as bitcoin, using some sort of mixing technique.

One of the first is CoinJoin, as first proposed by Maxwell [57]. CoinJoin simply mixes the coins of several parties together in one transaction. The first disadvantage of CoinJoin is that it requires preferably many more than two parties to form a transaction together. The second disadvantage is that the outputs of the transaction are linked to the inputs by the transaction and thus using large data processing techniques the identity of the coin owners might be determined after the CoinJoin transaction.

A second technique is called CoinShuffle, as first proposed by Ruffing, et al. [58]. CoinShuffle is similar to CoinJoin in that a single transaction is utilised and multiple

participants are preferred. The difference is that the parties involved use an algorithm to shuffle their destination addresses to increase the difficulty of finding the owner of a particular set of coins sent into the transaction. The disadvantages of CoinJoin are shared by CoinShuffle, except that the shuffle of destination addresses does increase the difficulty of finding the owners after the joining transaction.

One of the most recent techniques is called CoinShuffle++ and was proposed by Ruffing, et al. [59]. It improves upon the CoinShuffle technique mainly by improving its speed to make it more feasible. The disadvantages previously mentioned still remain.

The main advantages of the technique proposed in this paper above these related techniques is that only 2 parties are required in the swap, and that the space of related transactions is the list of all transactions on the blockchain that employ this technique within some arbitrary time window.

A specific disadvantage of the proposed anonymous swaps is that the swap is identifiable as a swap and not a normal transaction. This means that if very few anonymous atomic swaps happen in a certain time frame it is possible to locate possible partners for a swap. A technique developed by Andrew Poelstra and described by Gibson [60] called adaptor signatures, that use Schnorr signatures as described in Schnorr [61], is able to overcome this disadvantage.

Schnorr signatures are homomorphic elliptic curve signatures. This implies that it is possible to perform linear transformations on the signatures to generate new signatures. Adaptor signatures use this property of Schnorr signatures to perform the following types of transactions:

1. Normal transactions;
2. Multi-party transactions;
3. Atomic swaps;

while only storing a single signature in the blockchain. This means that all three of these aforementioned transaction types look exactly the same to any person investigating the blockchain. It is impossible to determine if a single party or multiple parties were involved in signing a transaction. It is also impossible to determine if cryptocurrency was exchanged for goods or whether it was a change of ownership of the cryptocurrency.

Schnorr signatures are in the process of being implemented in the bitcoin protocol. This would allow users to use adaptor signatures. Once this is possible, it will be impossible to track the ownership of bitcoins. This will make bitcoin much more economically attractive and can pose a huge problem for the authorities in regulating the flow of money. It could also allow the uncontrolled growth of a shadow economy. It is problems such as these that make it imperative that governments start to develop their own cryptocurrency.

6.13 ACKNOWLEDGEMENTS

The original idea for using the proposed homomorphic hash for anonymous atomic swaps was developed by the author. All of the content in this chapter was produced by the author. Prior to the inclusion of this chapter in the dissertation the proposed homomorphic hash for anonymous atomic swaps was discussed in a discussion group and inputs were provided by other individuals. A timeline of the development is available at [62]. Specifically, Hamun Davarpanah provided valuable additions. In the discussion [62] Johan Kirsten is user johank and Hamun Davarpanah is user empty[g].

CHAPTER 7: DESIGN OF A SOVEREIGN CRYPTOCURRENCY

Previous chapters have shown that bitcoin could pose a serious threat to the stable functioning of the financial system. Bitcoin has the potential to grow to a size that challenges the world's financial system and competes head on against cryptocurrencies for the economic output of the world.

As mentioned in chapter 5, Hayes [49] argues that cryptocurrencies could disrupt the administration of monetary policy and central banks and move us towards a more algorithmic approach. It was also argued by Kaushik Basu, former Chief Economist of the World Bank, in [50] that the new cryptocurrency Libra [51] could threaten the ability of policymakers to manage monetary environments.

Also, improvements to the bitcoin protocol such as Schnorr signatures could lead to the development of large scale shadow economies that are outside of the control of central banks and authorities. To stop such scenarios, the central banks of the world need to start introducing its own digital currency, the CBDC.

Earlier, an alternative to bitcoin and other cryptocurrencies was introduced, the sovereign cryptocurrency, a candidate CBDC. This cryptocurrency has two properties that distinguish it from other cryptocurrencies:

1. It is accepted as payment for the tax liabilities a citizen has; and
2. It is able to expand and contract the money supply in an orderly fashion.

If a country started using sovereign cryptocurrencies it would provide its population with the advantages of cryptocurrencies and with the advantages of fiat currencies, such as a controlled monetary supply. This would have the potential of limiting bitcoin's growth and would therefore allow central banks to keep control of their monetary supply.

The main disadvantage for a central bank in adopting a sovereign cryptocurrency is the fate of its retail banks, which would be unclear. The difference between a fiat currency and a sovereign cryptocurrency is that the fiat currency is a financial asset and the sovereign cryptocurrency is a real asset. This means that typically a holder of a sovereign cryptocurrency does not need a bank to hold any of the sovereign cryptocurrency. If

bitcoin disrupts the ability of banks to attract deposits, it will disrupt banks' ability to make loans.

This would imply that banks would need to redefine their role in an economy using a sovereign cryptocurrency. They might earn income from mining or they might earn income from acting as a custodian of the sovereign cryptocurrency. In such a case the bank would probably not be allowed by the owners of the sovereign cryptocurrency to lend out its holdings, if current custodian offerings is anything to go by.

A topic related to sovereign cryptocurrencies is the current efforts to establish a viable stablecoin. A stablecoin is a cryptocurrency that has a stable exchange rate to a fiat currency. One of the aspects of a sovereign cryptocurrency is the implication that the exchange rate should be stable. Therefore a sovereign cryptocurrency is by implication a stablecoin.

A stable exchange rate would make a stablecoin a store of value. Some would argue that this would then lead the stablecoin to be accepted as a unit of account and a medium of exchange. Thus the reasoning goes a stablecoin would by its very nature become money. According to this reasoning the instability of cryptocurrency prices are the single biggest hurdle to their widespread adoption.

Examples of existing stablecoin projects include:

1. Seigniorage shares;
2. Tether;
3. MakerDAO;
4. USD Coin; and
5. Basis.

The techniques used by these projects use the following techniques to peg the stablecoin to a fiat currency:

1. Open market operations;
2. Capital reserves; and
3. Interest or dividend payments.

Seigniorage shares [63] use open market operations; Tether [64], MakerDAO [65] and USD Coin [66] use a combination of capital reserves and open market operations; Basis [67] uses open market operations as well as dividend and interest payments.

Basis and Seigniorage shares seem vulnerable to market manipulation, as they do not hold capital to back the peg. The other projects use capital to fix the peg, or they have to attract capital to maintain the peg. These projects' biggest problem seems to be one of scalability.

A discussion on stabilising the price of cryptocurrencies using monetary policy can be found in Iwamura et al [68].

The core of the problem for all these projects is that they target the exchange rate. Central banks do not usually target the exchange rate. Their aim is for stability of prices of goods and services and economic growth. None of these projects uses economics to manipulate the supply of money in the system.

This is not to say it is impossible for private industry to create a viable stablecoin, just that it is a very hard problem to solve without help from a central bank. Even if a stable exchange rate is achieved the problem still remains of gaining people's trust and getting people to actually use it. Governments solve this problem by requiring taxes be paid in its currency.

This section describes the workings of the proposed sovereign cryptocurrency in greater detail. It is not meant to be a final solution, but rather a proposal to further the debate on the subject.

7.1 INITIAL MONETARY BASE AND CHANGING THE MONETARY BASE

A sovereign cryptocurrency would not create its monetary base through the mining network. It would need a more adaptive method to controlling the monetary base. A central bank would most likely pre-mine an initial monetary base, meaning it would start an account it has control over with a pre-set amount of currency. This currency would be sold to any person in exchange for the fiat currency of the country. In this manner the price of the sovereign cryptocurrency would immediately be pegged against the price of the fiat currency.

As economic activity priced in the sovereign cryptocurrency starts to pick up, the central bank would require the ability to modify the amount of currency in circulation to stabilise prices. Traditionally the two main mechanisms open to the central bank are changing short term interest rates and open market activity. By creating a market for the exchange between fiat currency and the sovereign cryptocurrency, a central bank would be able to conduct open market activities.

But a new mechanism would be necessary to change interest rates, because cryptocurrencies are a real asset, it would not necessarily be stored at a bank. To pay the holder of the sovereign cryptocurrency an income on holdings, the structure and rules of the cryptocurrency would need to be modified.

Such a mechanism would need to allow for the addition and removal of cryptocurrency across accounts on a periodic basis. Cryptocurrency can be added using some sort of earnings payment on each account and removed using some sort of taxation on every transaction.

This creates some technical complications that will be addressed in the rest of this section.

7.2 CHANGES TO THE BLOCKCHAIN

To perform effective execution of monetary policy, the most important requirement for a central bank would be the need to know the extent of the economic activity that uses the sovereign cryptocurrency. One method would be for every purchase to store an invoice in the blockchain for that transaction. But reporting an invoice on each transaction represents two problems:

1. It would balloon the size of the blockchain; and
2. People would not report honestly.

Thus instead of inserting invoices in the blockchain it is suggested that the user merely flag a transaction as having paid for goods or services. This protects the user's privacy as the list of goods and services are not made public and a simple flag on each transaction would not increase the size of the blockchain significantly.

But some people would still lie. To improve the quality of the statistics, account addresses can be split into two ranges. The first is for accounts that a seller uses to receive payments. The second is a capital account for the storing of currency. The owner of the account can decide which of these two types of accounts to open and supply to the payer.

The amount of tax for the transaction would also need to be stored in the output. This tax amount would be calculated based on the payment amount. The tax percentage would be calculated using the monetary policy of the sovereign cryptocurrency. A suggested method will be explained later.

The amount paid by the output should not include the tax amount. It should be the excluding tax amount so that the receiving party is not able to spend the tax amount. The tax amount would effectively be removed from circulation.

Part of the mining validation checks would then be for the routing node or the miner to verify that the tax amount is correctly calculated.

7.3 CHANGES TO THE PROTOCOL

It is not possible to charge negative interest rates on cryptocurrencies. The protocol must therefore allow for the removal of currency by adding tax to transactions.

To expand the monetary base, accounts will receive earnings. The protocol of the sovereign cryptocurrency must allow for earnings to be paid to account holders, based on the monetary policy built into the sovereign cryptocurrency and on the balance in the account.

As the main monetary base is pre-mined and additional money is created as interest paid on each account, the miners would not receive the typical block rewards of bitcoin that create currency. The miners would only receive transaction fees.

The code of the sovereign cryptocurrency would predefine certain aspects of the monetary policy, such as:

1. the cycle period over which taxes are collected and earnings are calculated and paid; and
2. The percentage of tax to apply to a transaction amount

The actual percentage amount by which the monetary supply should expand or contract can be specified in a formula or obtained externally by the code. A possible formula for the percentage of expansion of the monetary base will be discussed later in this chapter.

The specific rules that would be added to the bitcoin protocol to create a sovereign cryptocurrency include:

1. At the end of a cycle, an earnings block is required that only has a single earnings transaction; where
    a. An earnings transaction has a single tax input that represents the total of all the tax amounts collected during the current cycle;

b. An earnings transaction also has a single coinbase input that adds or removes currency to allow for the expansion or contraction of the monetary base;
c. An earnings transaction has a single output that specifies the total amount to add to the monetary supply and an effective percentage to apply to each UTXO; and
d. An earnings transaction has a prefixed transaction fee for the miner.

2. If an account has UTXO at the point an earnings transaction is created, it can claim its portion of the earnings by creating a claim transaction that uses the earnings transaction as input and its UTXO to create a new UTXO that includes the currency from the claiming UTXO and the interest from the earnings transaction; and
3. An earnings transaction can be referenced multiple times by different claim transactions, as long as a UTXO that existed before the earnings transaction is used to claim the earnings.

In a PoW cryptocurrency such as the one discussed here an important consideration is the cost of producing a unit of the cryptocurrency. If the cost of production rises to the exchange rate of the currency, mining processing power would not increase.

If this does not allow for a large enough mining processing power, the currency would be vulnerable to attack.

7.4 EXISTING DETERMINISTIC MONETARY POLICIES

In the previous section it was discussed that the central bank would control the amount by which to expand or contract the monetary base. But no specifics were given on how to determine the amount of expansion.

There are existing methods that help central banks determine the interest rate to apply during certain economic conditions. The most famous of these rules is the Taylor rule proposed by Taylor [69]. The problem with using something like the Taylor rule with the sovereign cryptocurrency previously proposed is that the Taylor rule specifies an interest rate. However, the sovereign cryptocurrency requires the central bank to specify the amount of expansion and contraction and the tax percentage. This is not what the Taylor rule was designed for.

The next section discusses the McCallum rule as proposed in McCallum [70] that specifies a monetary policy that states the amount of expansion or contraction of the monetary base, as well as its application within the context of a sovereign cryptocurrency.

7.5 PROPOSED DETERMINISTIC MONETARY POLICY

As discussed in the previous paragraphs, it is not possible to apply a negative interest rate on holdings in an account. To remove supply from the monetary base taxation on transactions is used. If the monetary base has to increase, positive interest rates are applied to the monetary base.

The following formula captures this explicitly

$$e^k \cdot M^k = r^k \cdot M^k - t^k \cdot \sum_j p_j^k \cdot q_j^k \ , \tag{73}$$

where

e^k is the growth in the money supply during cycle k

M^k is the total supply of currency at the beginning of cycle k

r^k is the interest applied during cycle k

t^k is the tax percentage applied to transactions during cycle k

p^k_j is the average price for goods or services j during cycle k

q^k_j is total quantity for goods or services j during cycle k.

If e^k needs to be positive t^k is zero and r^k is equal to e^k. If e^k needs to be negative r^k is zero and t^k is positive. The following equations capture this relationship

$$t^k \cdot \sum_j p_j^k \cdot q_j^k = max[0, -e^k \cdot M^k] \tag{74}$$

and

$$r^k = max[0, e^k]. \tag{75}$$

To determine t^k, if e^k is negative, the cryptocurrency would need to know M_k and e^k and would need to estimate the total transaction volume expected for the next cycle.

This means that e^k must either be specified externally from the blockchain, or a formula would be needed to determine e^k.

One candidate formula for determining e^k is the McCallum rule:

$$e^k = (i^* + g^*) + 0.5[(i^* + g^*) - (i^{k-1} + g^{k-1})] - a^{k-16}, \quad (76)$$

where

e^k is the percentage change in the money supply during quarter k

i^* is desired rate of inflation

g^* is the long run real growth in the economy

i^{k-1} is the measured rate of inflation during the previous quarter

g^{k-1} is the real growth in the economy during the previous quarter

a^{k-16} is the average quarterly increase of the velocity of M over a four-year period from k-16 to k.

Of the parameters, i^* and g^* need to be specified externally, or fixed, in the code of the cryptocurrency. The sum of i^{k-1} and g^{k-1}, as well as a^{k-16}, can be calculated from the blockchain, using transactions that are flagged and that move currency to transaction addresses, excluding tax in the calculation.

CHAPTER 8: CONCLUSION

The aim of this study was to investigate bitcoin, a cryptocurrency, in an effort to better understand its economic nature. The dissertation achieved the following objectives:

1. Understand the technical details of bitcoin
2. Review the economic nature of bitcoin
3. Investigate limits on the price of bitcoin
4. Research a stochastic model for the price of bitcoin
5. Create a system that can improve the anonymity of bitcoin
6. Design a cryptocurrency that can be adopted by governments

Bitcoin's technical nature was investigated with the aim of supporting a better understanding of its economic nature.

Regarding the economic nature of bitcoin, and cryptocurrencies, it was shown that bitcoin can be classified as a real asset and commodity. Meaning that there is no counterparty risk and it is a significant deviation from existing fiat currencies. While investigating the economic nature of the bitcoin economy, an estimation of the GDP of the bitcoin economy was made that placed the bitcoin economy among the top 40 economies of the world.

In the process of investigating the economic nature of bitcoin, a subclass of cryptocurrencies was introduced – the sovereign cryptocurrency – that is able to provide the advantages of cryptocurrencies combined with the advantages of fiat currencies. It was shown that the biggest distinguishing feature of sovereign cryptocurrencies, when compared to cryptocurrencies in general, is that sovereign cryptocurrencies have the potential to be classified as money. This means that sovereign cryptocurrencies would be issued by governments, accepted as payment for tax and the supply controlled by the central bank, while still giving the advantages of a cryptocurrency. They therefore represent a real alternative to fiat currencies.

Once the technical and economic nature of bitcoin was investigated the dissertation turned to the study of the price of bitcoin. Using arbitrage trading strategies it was shown that there are constraints on the price of bitcoin. Specifically the production cost of bitcoin is the ratio of total expense of the miner in mining bitcoin and the bitcoin earned by the miner. Arbitrage opportunities exist if the price of bitcoin is above its production cost, making the production cost the ceiling of the price of bitcoin. Given recent data it was reasoned that a floor to the price of bitcoin does not exist. This is supported by the fact that

it is only possible to convert electricity into bitcoin, but the reverse process is not possible. Bitcoin, once created, cannot be converted into electricity.

The study also developed a hypothesis on the behaviour of the price of bitcoin. Specifically it was hypothesised that the ratio of the price of bitcoin and the difficulty of bitcoin can be modelled with a lognormal distribution. Enough evidence was provided to support the acceptance of the hypothesis.

Based on the accepted hypothesis, a stochastic model for the price of bitcoin was derived. It is like the stochastic model for the price of stocks, except that the drift is replaced with the growth in difficulty used by the bitcoin network.

The dissertation also reasoned that if the anonymity of the users of bitcoin was improved, then the economic appeal of bitcoin will increase. To show that such improvements are possible a technique called anonymous atomic swaps was developed and described. This technique would allow users of bitcoin to improve their level of anonymity. It was explained that the technique is mainly of academic interest as it requires wide adoption to provide any significant anonymity. This problem is solved using Adaptor signatures that depend on Schnorr signatures. Adaptor signatures allow the users of bitcoin to become completely anonymous and present a very real problem for central banks and authorities.

During the study it became apparent that bitcoin, due to its restrictive monetary policy, potential growth and possible improvements to the anonymity of users, bitcoin represents a real problem for the central banks and their ability to effect prudent monetary policy. The study explained specific technical changes that could be made to bitcoin that will allow for the operation by central banks of a sovereign cryptocurrency. A mathematical model for the monetary policy of a sovereign cryptocurrency was derived that would allow central banks to effect prudent monetary policy within the sovereign cryptocurrency, while at the same time making the sovereign cryptocurrency acceptable to the public.

Overall the following contributions were made in this dissertation:

1. A method for the estimation of the GDP of the bitcoin economy
2. A stochastic model for the price of bitcoin
3. A technique for employing anonymous atomic swaps in bitcoin
4. A design for a sovereign cryptocurrency

In the author's view the broader possible "big picture" implications of bitcoin for our world it is that it is actually the culmination of a wave of peer-to-peer technology that started in the 1970's with the development of the Internet Protocol that underlies the entire internet. The dream that was realised with the development of the Internet Protocol was that machines should be able to communicate with each other directly without the need of an intermediary. This lay the foundation of the peer-to-peer paradigm.

This peer-to-peer paradigm is can be thought of as part of a broader move in society away from hierarchical social structures to network social structures. Recently the historian Niall Ferguson [71] wrote a book on the historic struggle between the hierarchical social structure and the network social structure. In the past the hierarchical social structure has been used to implement governments and corporations. It has enjoyed the predominance of power on our planet for centuries. But it has been the network social structure, implemented as family, friendships and peered relations that has caused the changes and the revolutions in our society. Each time it was the network that caused the hierarchy to have to adapt.

Therefore, bitcoin could be thought of as the latest battle front in the battle between the network societal structure and the hierarchical societal structure. But this time it is different. In the past the hierarchical structure always had control of the money. It has always been part and parcel of the trust it engendered in the society in which it exists. But bitcoin allows the network to have its own money by dispensing with the necessity for trust.

This is significant. There have always been bad actors in society. We have used the trust that a hierarchy provides to overcome the problems created by bad actors. But technology now promises us the possibility of an environment that does not need mutual trust. This strikes at the very core of why we need hierarchical structures. Could bitcoin usher in the end of hierarchical structures? Only time will tell. But this does seem like the beginning of a change in the structure in society that will be felt for centuries to come.

Future historians could look back at the development of bitcoin and mark it as the birth of their egalitarian societies. It has already changed the mind of, arguably, the most famous financial historian, Niall Ferguson, as seen in a recent interview by Morris [72].

CHAPTER 9: REFERENCES

[1] Chaum, D. (1983). Blind signatures for untraceable payments. Advances in Cryptology Proceedings of Crypto. 82 (3): 199–203. doi:10.1007/978-1-4757-0602-4_18.

[2] Chaum, D; Fiat, A; Naor M. (1988). Untraceable Electronic Cash. CRYPTO 1988. Lecture Notes in Computer Science, vol 403. Springer, New York, NY

[3] Dai, W. (1998). b-money. Retrieved from http://www.weidai.com/bmoney.txt on 1 November 2018

[4] Back, A. (2002, August 1). Hashcash - a denial of service counter-measure. Retrieved from http://www.hashcash.org/papers/hashcash.pdf on 1 November 2018

[5] Szabo, N. (2005, December). Bit Gold, Retrieved from http://unenumerated.blogspot.com/2005/12/bit-gold.html on 1 November 2018

[6] Finney, H. Reusable Proofs of Work. Retrieved from https://web.archive.org/web/20071222072154/http://rpow.net/ on 1 November 2018

[7] Nakamoto, S. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf on 1 November 2018

[8] Ahamed, L. (2009). Lords of finance. Penguin Press

[9] Fox, J. (2011). The myth of the rational market: A History of Risk, Reward, and Delusion on Wall Street . Harper Business

[10] Patterson, S. (2010). The quants. Crown Publishing Group

[11] Lewis, M. (2010) The big short: Inside the doomsday machine. W. W. Norton & Company

[12] Taibbi, M. (2010) Griftopia. Spiegel & Grau

[13] Baur, D.G. (2012 October). Financial contagion and the real economy. Journal of Banking & Finance. Volume 36, Issue 10, October 2012, Pages 2680-2692

[14] Antonopoulos, A.M. (2017). Mastering Bitcoin: Programming the Open Blockchain. 2nd Edition, O'Reilly, ISBN-13: 978-1491954386

[15] Böhme R., Christin N., Edelman B., Moore T. (Spring 2015) Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives. Vol. 29, No. 2, pp. 213-38

[16] Haber S; Stornetta W.S. (1991). How to time-stamp a digital document, In Journal of Cryptology, vol 3, no 2, pages 99-111

[17] Lilly Glenn, M. (2002, September 5). Device for and method of one-way cryptographic hashing. Retrieved from https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=6829355&KC=&FT=E&locale=en_EP on 1 November 2018

[18] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation. 48 (177): 203–209. doi:10.2307/2007884. JSTOR 2007884.

[19] Miller, V. (1985). Use of elliptic curves in cryptography. CRYPTO. Lecture Notes in Computer Science. 85: 417–426. doi:10.1007/3-540-39799-X_31. ISBN 978-3-540-16463-0.

[20] Wray, L.R. (2012). Modern Money Theory: A Primer on Macroeconomics for Sovereign Monetary Systems. Second Edition, Palgrave Macmillan, ISBN-13: 978-1137539908

[21] Commodity. (2018, November 1). Retrieved from https://en.wikipedia.org/wiki/Commodity on 12 November 2018[22] South African Reserve Bank. (2018, June 5). Project Khokha. Retrieved from https://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/8491/SARB_ProjectKhokha%2020180605.pdf on 1 November 2018

[23] Bech M.L., Garratt R. (September 17, 2017) Central Bank Cryptocurrencies. BIS Quarterly Review September 2017. Downloaded on 7 October 2019 from: https://ssrn.com/abstract=3041906

[24] South African Reserve Bank. (2019, June 6). Retrieved from https://www.resbank.co.za/AboutUs/Departments/FinancialServices/ProcNew/Lists/News%20and%20Publications/Attachments/40/EOI%20MR01-2019-0.pdf on 17 October 2019

[25] Barrdear, J and Kumhof, M. (2016, July). The macroeconomics of central bank issued digital currencies. Retrieved from https://www.bankofengland.co.uk/-

/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies on 1 November 2018

[26] A respectable result for the Sovereign Money Initiative (Vollgeld-initiative). (2018 June 10). Retrieved from https://www.vollgeld-initiative.ch/english on 1 November 2018

[27] MacDonald T.J., Allen D.W.E., Potts J. (2016) Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking. Banking Beyond Banks and Money. New Economic Windows. Springer, Cham

[28] Raskin M., Yermack D. (May 2016) Digital Currencies, Decentralized Ledgers, and the Future of Central Banking. NBER Working Paper No. 22238. Downloaded on 7 October 2019 from: https://www.nber.org/papers/w22238

[29] Vidal-Tomás D., Ibañez A. (December 2018) Semi-strong efficiency of Bitcoin. Finance Research Letters. Volume 27, Pages 259-265

[30] USD Exchange Trade Volume. Retrieved from https://www.blockchain.com/charts/trade-volume on 1 November 2018

[31] Estimated USD Transaction Value. Retrieved from https://www.blockchain.com/charts/estimated-transaction-volume-usd on 1 November 2018

[32] Tasca P., Hayes A., Liu S. (19 March 2018) The evolution of the bitcoin economy: Extracting and analyzing the network of payment relationships. Journal of Risk Finance. ISSN: 1526-5943

[33] Hayes, A. (2015). Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin. MCIS, page 4. AISeL

[34] Hayes A.S. (2019) Bitcoin price and its marginal cost of production: support for a fundamental value. Journal of Applied Economics Letters. Volume 26, Issue 7. Pages 554-560

[345] Hayes A., (March 16, 2015) What Factors Give Cryptocurrencies Their Value: An Empirical Analysis. Downloaded on 7 October 2019 from: https://ssrn.com/abstract=2579445

[36] Schilling, L and Uhlig, H. (2019, May). Some simple bitcoin economics. Retrieved from http://www.nber.org/papers/w24483 on 1 September 2019

[37] Bitmain. (2018, June 12). Retrieved from https://shop.bitmain.com on 12 June 2018

[38] Lee, T. (2018, May 10). Retrieved from https://twitter.com/fundstrat/status/994566148007055361/photo/1 on 1 November 2018

[39] Average USD market price across major bitcoin exchanges. (2018, June 3). Retrieved from https://blockchain.info/charts/market-price?timespan=2years on 3 June 2018

[40] A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners. (2018, June 3). Retrieved from https://blockchain.info/charts/difficulty?timespan=2years on 3 June 2018

[41] Ethereum Price Chart US Dollar (ETH/USD). (2018, June 3). Retrieved from https://www.coingecko.com/en/price_charts/ethereum/usd on 3 June 2018

[42] Ethereum Block Difficulty Growth. (2018, June 3). Retrieved from https://etherscan.io/chart/difficulty on 3 June 2018

[43] Bitcoin Cash (BCH). (2018, June 3). Retrieved from https://www.coingecko.com/en/price_charts/bitcoin-cash/usd on 3 June 2018

[44] Bitcoin Cash Difficulty historical chart. (2018, June 3). Retrieved from https://bitinfocharts.com/comparison/difficulty-bch.html on 3 June 2018

[45] Litecoin (LTC). (2018, June 3). Retrieved from https://www.coingecko.com/en/price_charts/litecoin/usd on 3 June 2018

[46] Litecoin Difficulty historical chart. (2018, June 3). Retrieved from https://bitinfocharts.com/comparison/litecoin-difficulty.html on 3 June 2018

[47] Bouri E., Gupta R., Tiwari A.K., Roubaud D. (November 2017) Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. Finance Research Letters. Volume 23, Pages 87-95

[48] Demir E., Gozgor G., Lau C.K.M., Vigne S.A. (September 2018) Does economic policy uncertainty predict the Bitcoin returns? An empirical investigation. Finance Research Letters. Volume 26, Pages 145-149

[49] Hayes A., (2016) Decentralized Banking: Monetary Technocracy in the Digital Age. Banking Beyond Banks and Money. New Economic Windows. Springer, Cham

[50] Basu, K. (July 27, 2019). Why Policymakers Should Fear Libra Retrieved from https://www.project-syndicate.org/commentary/facebook-libra-inflation-control-problem-by-kaushik-basu-2019-06 on 17 October 2019

[51] An Introduction to Libra. Retrieved from https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf on 17 October 2019[52] Nolan, T. (2016, February 14). Atomic swaps using cut and choose. Retrieved from https://bitcointalk.org/index.php?topic=1364951 on 13 November 2018

[53] Bowe, S. and Hopwood, D. (2017, March 27). Hashed time-locked contract transactions. Retrieved from https://github.com/bitcoin/bips/blob/master/bip-0199.mediawiki on 13 November 2018

[54] DeCred, (2018, March 1). Decred cross-chain atomic swapping. Retrieved from https://github.com/decred/atomicswap on 13 November 2018

[55] Herlihy, M. (2018, January 29). Atomic Cross-Chain Swaps. arXiv preprint arXiv:1801.09515, 2018 - arxiv.org

[56] Krohn M.N.; Freedman M.J.; Mazieres, D. (2004). On-the-Fly Verification of Rateless Erasure Codes for Efficient Content Distribution. IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, ISBN 0-7695-2136-3

[57] Maxwell, G. (2013, August 22). CoinJoin: Bitcoin privacy for the real world. Retrived from https://bitcointalk.org/index.php?topic=279249.0 on 13 November 2018

[58] Ruffing, T.; Moreno-Sanchez, P.; Kate, A. (2014). CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. ESORICS 2014: Computer Security - ESORICS 2014 pp 345-364

[59] Ruffing, T.; Moreno-Sanchez, P.; Kate, A. (2017). P2P Mixing and Unlinkable Bitcoin Transactions. NDSS, 2017

[60] Gibson, A. (2017, October). Flipping the scriptless script on Schnorr. Retrieved from https://joinmarket.me/blog/blog/flipping-the-scriptless-script-on-schnorr/ on 13 November 2018

[61] Schnorr, C.P. (1984, February 24). Retrieved from https://patents.google.com/patent/US4995082A/en on 13 Novemeber 2018

[62] Kirsten, J. (2018, August 30) Retrived from https://bitcointalk.org/index.php?topic=4980960.0 on 13 November 2018

[63] Sams, R. (2015, April 28). A note on cryptocurrency stabilisation: Seigniorage shares. Retrieved from https://github.com/rmsams/stablecoins/blob/master/paper.pdf on 1 November 2018

[64] Tether: Fiat currencies on the bitcoin blockchain. (2016). Retrieved from https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf on 1 November 2018

[65] The Dai stablecoin system. Retrieved from https://makerdao.com/whitepaper/ on 1 November 2018

[66] USD Coin is a US dollar-backed stablecoin. Retrieved from https://www.circle.com/en/usdc on 1 November 2018

[67] Al-Naji, N; Chen, J; Diao, L. (2017, June 20). Basis: A price-stable cryptocurrency with an algorithmic central bank. Retrieved from https://www.basis.io/basis_whitepaper_en.pdf on 1 November 2018

[68] Iwamura M., Kitamura Y., Matsumoto T., Saito K. (October 25, 2014) Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money. Downloaded on 7 October 2019 from: https://ssrn.com/abstract=2519367

[69] Taylor, J.B. (1993). Discretion versus Policy Rules in Practice. Carnegie-Rochester Conference Series on Public Policy, 39, 195–214

[70] McCallum, B.T. (1987). The case for rules in the conduct of monetary policy: a concrete example. Weltwirtschaftliches Archives, 123, 415-429

[71] Ferguson, N. (2018).The Square and the Tower: Networks and Power, from the Freemasons to Facebook. ISBN 0-7352-2291-6

[72] Morris, D.Z. (13 Feb, 2019) Financial Historian Niall Ferguson: a Big Tech Digital Dollar Would Be a Nightmare. Retrieved from https://breakermag.com/financial-historian-niall-ferguson-dives-into-crypto/ on 17 October 2019

CHAPTER 10: INDEX