UNIVERSITEIT•STELLENBOSCH•UNIVERSITY

jou kennisvennoot • your knowledge partner

Determining the Intrinsic Value of Cryptocurrencies

by

David Timothy Rodwell and Robert Cronjé

Assignment presented at the University of Stellenbosch in partial fulfilment of the requirements for the degree of

Honours of Commerce

Department of Statistics and Actuarial Science
University of Stellenbosch
Private Bag X1, 7602 Matieland, South Africa

Supervisor: C. J. van der Merwe

December 2018

DECLARATION

We, the undersigned, hereby declare that the work contained in this assignment is our original work and that we have not previously in its entirety or in part submitted it at any university for a degree.

Signature: .....

D.T. Rodwell

Date: .....

Signature: .....

R. Cronjé

Date: .....

Chapter 1

ABSTRACT

One of the products of the digital age is cryptocurrencies. The introduction of the concept of a cryptocurrency, namely Bitcoin, was presented in 2008, through a research paper proposing the idea of a peer-to-peer electronic payment system. Many variants of Bitcoin have since then been created and introduced into the market, all possessing varying functionality and value. The literature available so far, on valuing bitcoin and cryptocurrencies in general, is extensively consulted to determine the best possible valuation technique.

This research paper investigates whether cryptocurrencies possess any intrinsic value through a cost of production valuation technique. Within the cost of production framework a model for bitcoin and altcoins is presented. The model output is determined to be consistent as a lower-bound value for the market price, by plotting the model price against the market price. In addition, a Granger causality test is conducted through a multivariate auto-regressive model to determine whether the model price causes the market price, in essence providing evidence for the case that the cost of production is a coherent means to determine the intrinsic value.

The Granger test yields inconclusive results, for a number of reasons outlined in this paper. The feasibility of the models presented, thus have little statistical backing. However, the output produced by the model in most cases still acted as a lower bound with convergence occurring after the renowned 2017 bubble.

Key words: Cryptocurrency, Bitcoin, altcoin, intrinsic value, cost of production

Chapter 2

OPSOMMING

Een van die produkte van die digitale era is kriptovaluta. Die bekendstelling van die konsep van 'n kriptovaluta, naamlik Bitcoin, is in 2008 voorgestel deur middel van navorsing wat die idee van 'n eweknie elektroniese betalingstelsel voorstel. Baie variante van Bitcoin is sedertdien geskep en aan die mark voorgestel, wat almal wisselende funksionaliteite en waardes het. Die literatuur wat tot dusver beskikbaar is, oor die waarde van bitcoin en kriptovaluta word breedvoerig in die algemeen geraadpleeg om die beste moontlike waardasie tegniek te bepaal.

Hierdie navorsingsdokument ondersoek of kriptovaluta enige intrinsieke waarde het deur middle van ân koste van produksie waardasie tegniek. Binne die koste van produksie raamwerk word 'n model vir bitcoin en altcoins voorgestel. Die model uitvoer is bepaal om konsekwent te wees as 'n laer-gebonde waarde vir die markprys, deur die modelprys teen die markprys te vergelyk. Daarbenewens word 'n Granger-kousaliteitstoets uitgevoer deur 'n meerveranderlike outo-regressiewe model om vas te stel of die modelprys die markprys veroorsaak, wat in wese bewyse lewer vir die saak dat die produksiekoste 'n samehangende manier is om die intrinsieke waarde te bepaal.

Die Granger-toets lewer onoortuigende resultate vir 'n aantal redes wat in hierdie dokument uiteengesit word. Die haalbaarheid van die modelle wat aangebied word, het dus min statistiese steuning. Die uitset wat deur die model vervaardig word, het egter steeds in die meeste gevalle gehandel as 'n laer grens met konvergensie wat plaasgevind het na die bekende 2017-borrel.

CONTENTS

DECLARATION ii

1 ABSTRACT iii

2 OPSOMMING iv

CONTENTS v

LIST OF TABLES viii

LIST OF FIGURES viii

3 INTRODUCTION 1

3.1 Introduction . . . 1

3.2 Problem Statement . . . 2

3.2.1 Research Problem . . . 2

3.2.2 Research Question . . . 2

3.2.3 Summary of key concepts . . . 2

3.3 Summary . . . 5

4 LITERATURE REVIEW 6

4.1 Introduction . . . 6

4.2 Cryptocurrencies . . . 6

4.2.1 Altcoins . . . 6

4.2.2 Tokens . . . 7

4.3 Bitcoin . . . 7

4.3.1 Blockchain . . . 7

4.3.2 Block Structure . . . 8

4.3.2.1 The Block Header . . . 8

4.3.3 Mining Process . . . 9
4.3.3.1 Proof-of-Work . . . 10
4.3.3.2 Difficulty . . . 10
4.4 Valuation Models . . . 11
4.4.1 Cryptocurrencies Valued as Money . . . 11
4.4.2 Cryptocurrencies Valued as Commodities . . . 12
4.4.3 Cost of Production Models for Cryptocurrencies . . . 13
4.5 Summary . . . 16

5 METHODOLOGY 17
5.1 Introduction . . . 17
5.2 Cost of Production Model . . . 18
5.2.1 Bitcoin Model . . . 18
5.2.2 Altcoins . . . 19
5.3 Cost of Production Inputs . . . 19
5.3.1 Block Reward . . . 20
5.3.2 Difficulty . . . 20
5.3.3 Hash Rate . . . 21
5.3.4 Network Hash Rate . . . 21
5.3.5 Block Time . . . 21
5.3.6 Electricity Cost . . . 21
5.3.7 Energy Efficiency . . . 22
5.4 Intrinsic Value Analysis . . . 22
5.5 Summary . . . 23

6 RESULTS 24
6.1 Introduction . . . 24
6.2 Valuation Analysis . . . 24
6.2.1 ETH . . . 25
6.2.2 XMR . . . 27
6.2.3 LTC . . . 30
6.2.4 Graph Inference . . . 32
6.3 Statistical Analysis . . . 33
6.4 Summary . . . 34

7 SUMMARY, CONCLUSION AND RECOMMENDATIONS 35

7.1 Introduction 35
7.2 Shortcomings 35
7.2.1 Data 35
7.2.2 Statistical Analysis 36
7.3 Summary and Findings 36
7.4 Further Research and Recommendations 37
7.5 Conclusion 37

REFERENCES **39**

LIST OF TABLES

4.1 Summary of altcoins 7
4.2 Structure of a Block Header 8
5.1 Hash rate inputs 21

LIST OF FIGURES

4.1 Example of the Merkle Hash 9
6.1 Model Price and Market Price of ethereum vs Time 25
6.2 Inputs for ethereum 26
6.3 The relationship between the price in USD against the intrinsic value of monero 27
6.4 Inputs for monero 28
6.5 The relationship between the price in USD against the intrinsic value of litecoin 30
6.6 Inputs for litecoin 31
6.7 The market price and model price for various coins over 30 days 32
6.8 The market price and model price for various coins 33

CHAPTER 3

INTRODUCTION

3.1 Introduction

The cryptocurrency markets have had some spectacular growth, as well as some devastating crashes. Introduced to the world in 2008 (Nakamoto, 2008), this new peer-to-peer platform for electronic payments, has gathered widespread media attention. Consequently, many investors have found interest in cryptocurrencies like bitcoin (BTC), ethereum (ETH), litecoin (LTC) and many, many more. The purpose of this research paper is to investigate whether these digital currencies have any intrinsic value and if so, how one would model the true price of such a technology.

Opinions on this topic are very contrasting, with some believing in the value of the technology while others brush it off as some sort of phase. To get to the heart of the problem of estimating the intrinsic value of cryptocurrencies, one first needs a full understanding of the technology itself. With a complete background and history of the technology one will begin to understand the initial intention of the technology as well as the many other uses cryptocurrencies have to offer.

The supply of coins is driven by computing power by dedicated coin mining machines and those selling their coins. The stark increases in demand, that have been recently seen due to the heightened media attention, is why there has been major increases in the prices. This has led many to declare that there is a bubble in cryptocurrency markets. This is an interesting claim, since it implies that the market values of cryptocurrencies are trading above their intrinsic values.

Whether they believe that the intrinsic value is zero or anything else, there is little research on determining the intrinsic value of cryptocurrencies. One may be tempted to model cryptocurrencies as currency, however one will soon notice that the endeavour is far more complex than that. Cryptocurrencies are a completely unique asset class and one should treat it as such. The models in determining the true value of the technology, are distinct from those of other investment instruments.

3.2 Problem Statement

3.2.1 Research Problem

The cryptocurrency markets, and the bitcoin market in particular, has seen their market capitalisation soar especially during 2017. Subsequently the markets have dropped considerably in value. This drop has not all together discredited cryptocurrencies since they still trade in healthy secondary markets and their supply is still driven by dedicated miners. If there is any inherent intrinsic value to cryptocurrencies, then there should exist some underlying factors that may contribute to this value. The problem is therefore to determine what the underlying factors are that contribute to a coin's price and to see if it is possible to produce a model that estimates the intrinsic value of the coin.

3.2.2 Research Question

As such, the research question can be formulated as follows: can one estimate the intrinsic value of cryptocurrencies? Furthermore, if an intrinsic value can be estimated, how would this value be modelled?

3.2.3 Summary of key concepts

In order to discuss the various factors revolving around modeling intrinsic value with regards to cryptocurrencies, the reader needs to familiarise themselve with a few fundamental concepts. Some of these concepts is summarised below, and the remaining concepts is addressed in the chapter 4 under the literature review. In this paper the **intrinsic value** is based off Moore (1922), where he defines intrinsic value as the value of an object which is only based on it's non-relational properties. These non-relational properties are those which can be formed without reference to another object.

The first concept which must be understood is that of the nature of a cryptocurrency and how it can be defined. **Cryptocurrency** can be described as a decentralised digital currency, which is measured in coin units that are divisible to a certain amount. Most cryptocurrencies utilise blockchain technology in a peer-to-peer network to keep the integrity of the asset secure. There exists many types, and they are open-source in nature. Some having varying features and some being copies of already existing coins. The most popular of these coins is **Bitcoin**[1]. Bitcoin can be summarised as an electronic peer-to-peer (P2P) decentrailised payment system based on cryptocurrency (Nakamoto, 2008).

A concept often discussed alongside cryptocurrency is that of blockchain. **Blockchain** can be seen as the underlying structure of cryptocurrency. It can be expressed as a real-time publicly distributed ledger of the

[1]In this paper the capitalised Bitcoin refers to the cryptocurrency system while. In bitcoin refers to the cryptocurrency coin

various transactions from the Bitcoin system, where there is no single entity which controls or owns the data (Crosby, Nachiappan, Pattanayak, Verma and Kalyanaraman, 2016). Furthermore, no exisiting information can be removed unless agreed upon by the majority of the network, which in essence causes the blockchain to be self-regulating. Crosby *et al.* (2016) further explains this point by making an analogy, where one man will be more tempted to steal a cookie jar if alone rather than in a crowded marketplace. A blockchain is comprised out of a chronologically ordered collection of blocks. In this instance, a block is defined as data structure which stores information about the cryptocurrency being used, such as the difficulty, a reference to the most recent completed block and the time-stamp for the current block. A block also contains a list of approximately 500 completed transactions (Mwale, 2016). The **Difficulty variable** is an exogenous measure of how computationally intensive it is to find a new block which generates a hash under a certain threshold (Hayes, 2017). Throughout this paper the difficulty is denoted as δ.

The method that cryptocurrencies use to keep the integrity of the system is through a **Proof-of-Work** system, where a Proof-of-Work is used to prevent attackers to introduce invalid transactions into the blockchain. This is done through using either a time or resource consuming algorithm. Hashcash is Bitcoin's Proof-of-Work system, where the block header is hashed through a hashing algorithm to meet certain difficulty requirements (Back, 2002). This hashing algorithm has a very low probability of success rate which makes the process time and resource intensive. It is important to note that the reward for validating transactions will only be granted upon producing a valid Proof-of-Work. In other words, a miner which successfully obtains the "correct" hash will be rewarded for the effort of going through the process of mining. The concept of what is a "correct" hash is defined in chapter 4.

In addition to Proof-of-Work there is a Proof-of-Stake protocol. This method of verifying transactions was introduced after the Proof-of-Work protocol. The rise of the Proof-of-Stake protocol was due to the large energy consumption that was being used in producing a valid Proof-of-Work. The difference between the traditional Proof-of-Work and the Proof-of-Stake protocol is that the hashing algorithm is performed in a smaller range where a miner will only be allowed to generate one hash per unspent wallet-output per second, in contrast to the unlimited range presented in the Proof-of-Work protocol and hence less energy intensive (King and Nadal, 2017).

A valid Proof-of-Work is produced through cryptocurrency mining. This is the process where previous transactions are collected and validated. The process continues until either a valid Proof-of-Work is produced or a new block is produced by a different miner which is then added to the existing blockchain (Mwale, 2016). Once the new block is added the process is repeated. The reward for successfully mining a bitcoin

block currently stands at 12.5 BTC and is expected to halve by 31st May 2020. One crucial concept to grasp in a Proof-of-Work setting is **Hashing Algorithms**. However, in order to understand a hashing algorithm it is essential to acknowledge what a hash function is. In cryptography a cryptographic hash function h is formally defined as $h : \{0,1\}^* \rightarrow \{0,1\}^n$ where $^* \in \mathbb{Z} \geq 1$. The function states that any arbitrary length binary string produces an output of n bits of binary strings, this output value is also sometimes referred to as the hashed value. In order for a function to be classified as a hash function it must satisfy the following requirements as described by Rogaway and Shrimpton (2004):

The function must be preimage-resistant. For a given hashed value it is computationally infeasible to find an arbitrary length input which hashes to the same hashed value, i.e. for a given y it is impossible for find an unknown input x such that $h(x) \rightarrow y$. It is necessary in cryptography that when a message, or in this case a hashed value is computed, that the original input cannot be discerned. Secondly, the function must be second-preimage resistant which means that it is computationally infeasible to find a second input to generate the same hashed value, i.e. for a given x to find a x^* such that $x \neq x^*$ then $h(x) \neq h(x^*)$. This ensures that two unique strings will not produce the same hashed value. Lastly, the function must possess the characteristic of collision resistance which means that it must computationally infeasible to find any two inputs x, x^* which produces the same hashed value. It is important to note that collision resistance implies second-preimage resistance but the reverse implication does not hold.

The purpose of hashing algorithms in the case of cryptocurrency is to be used as a medium for verifying transactions and to prevent hackers from duplicating blocks or creating artificial transactions. An analogy can be made where these hashing algorithms can be compared to the protocols banks use to prevent money counterfeiting (printing notes on special paper, introducing a watermark etc.). These algorithms usually make use of one way compression functions. These functions are less resource intensive to compute but are extremely difficult to invert. In cryptocurrency the Merkle Dåmgard construction is widely used since it takes an arbitrary length input and compresses it to a fixed length output using a variety of these one way compression functions (Bitcoin Wiki, 2018*b*). More information on the Merkle Dåmgard structure is given in chapter 4.

A **Mining Rig** is the actual machine that is used to produce the cryptocurrency. These can range from a personal computer to a dedicated "set-ups" that are solely used for producing cryptocurrencies. The usage of the terms "rigs", "machines" and "mining hardware" is used interchangeably, simply meaning the physical collection of components that allows one to mine for a coin. The process of mining only reaps rewards probabilisticaly. In order for miners to obtain a steady stream of income during the process of mining, instead of waiting months to 'hit the jackpot', they can join **mining pools**. Mining pools act as a collective group of miners, each contributing to solving the hashing algorithm the way they had done before. If a miner in

a pool is successful in mining a block the rewards for that block is shared among the pool and distributed in accordance with mining contribution or in some similar fashion. This way members of the pool receive income more regularly, although in smaller quantities.

Since the introduction of bitcoin in 2008, there has been much development in hardware technology. This is known as **the evolution of mining hardware**. Initially bitcoin was mined using only the central processing unit (CPU) as the processor. One's personal computer, however, runs many tasks in the background and is therefore not very efficient. Many soon realised that using graphics processing units (GPUs), instead was much more efficient at mining since these machines have a more dedicated nature. The need for more dedicated machines grew and the development in processing technology surpassed that which is expected under Moore's Law[2]. Field-programmable gate array's (FPGA) were found to much better at dedicated tasks such as mining, and the technology quickly developed to application specific integrated circuits (ASIC), rendering FPGA in the case of mining for bitcoin, obsolete. ASIC's are currently the most efficient technology available for mining cryptocurrencies such as bitcoin (Hayes, 2017).

ASIC's are essentially integrated circuits that are designed to do one specific function very efficiently. In the bitcoin case, the ASICs are designed to hash the SHA-256d mining algorithm. These machines act as an additional processor to the computer host, that solely performs the hashing algorithm and can only be used for its dedicated task. It must be noted that certain cryptocurrencies cannot be mined for using ASIC machines, since their hashing algorithm differs to that of bitcoin. Certain hashing algorithms are much more robust than the SHA-256d algorithm that bitcoin employs, which makes them "ASIC-proof". This means that there are no dedicated machines available to mine for them. Therefore, for coins that employ "ASIC-proof" hashing algorithms, they are at the stage in their evolution of mining hardware where the most efficient processors are GPU's.

3.3 Summary

In the fourth chapter a detailed literature review is presented where various concepts is given to understand the context of the valuation of the intrinsic value of crytocurrencies. The concepts involve block structure and valuation models which have been implemented in order to capture the nature of cryptocurrencies and their unique financial facets. In the fifth chapter the methodology for valuing the cryptocurrencies is presented where the methodology of Hayes (2018) is modified in order to accommodate altcoins. In the sixth chapter these results are discussed and is summarised. In chapter seven shortcomings of the methodology and areas for further research is presented.

[2]Moore's Law states that the number of transistors in a dense integrated circuit doubles about every two years. Which roughly translates to: the processing power of a machine will double every two years, and the costs thereof will remain approximately the same

CHAPTER 4

LITERATURE REVIEW

4.1 Introduction

This chapter is split into three sections. The first section is a detailed discussion of the different types of cryptocurrencies, followed by a more focused approach to Bitcoin and its mining infrastructure. The third section will provide possible valuation methods and discuss the relevance of these models to bitcoin and other cryptocurrencies.

4.2 Cryptocurrencies

As of June 2018 there were 1586 different cryptocurrencies[1] that are widely used and dedicated to different purposes ranging from enhancing anonymity in transactions to lowering the transaction costs of high volume exchanges. Cryptocurrencies are split into two main categories namely, altcoins and Tokens (Arsov, 2018).

4.2.1 Altcoins

Altcoin is an abbreviation for "alternative coin". The majority of these coins were a fork[2] made in attempt to share in the gains of Bitcoin (Dolce, 2017*b*), most of these coins are either no longer in use or used as a speculative investment instrument. The manner in which altcoins differ from Bitcoin is achieved through mainly two methods. The first is by employing a different Proof-of-Work algorithm. Bitcoin uses Hashcash with a SHA-256 hashing algorithm as its foundation to produce a Proof-of-Work (Back, 2002). In an example of the altcoin litecoin, the SHA-256 hashing algorithm is replaced with the Scrypt algorithm. Usually the altcoin hashing algorithms are a combination of multiple hashing algorithms. The combination of which

[1] Obtained on the 22nd August 2018 at `https://coinmarketcap.com/all/views/all/`

[2] A software fork is occurs when minor changes are made to an existing programming protocol. In the Bitcoin setting these changes result in a split of the original blockchain (Dolce, 2017*a*).

is either done in series (X11) or parallel (Myraid algorithm). Additionally, a few altcoins also introduce a Proof-of-Stake system as opposed to Proof-of-Work (Bitcoin Wiki, 2017).

Table 4.1: Summary of altcoins

Comparison of altcoins with Bitcoin				
Name	**Symbol**	**Deflationary**	**Hashing Algorithm**	**Created**
Bitcoin	BTC	Yes	SHA-256	2009
Ethereum	ETH	Yes	Ethash	2015
Dash	DASH	Yes	X11	2014
Litecoin	LTC	Yes	Scrypt	2011
Monero	XMR	No	CryptoNight	2014

Deflationary cryptocurrencies are coins which have a fixed supply. Furthermore, the protocols of these hashing algorithms are beyond the scope of this research paper and is left for further reading.

4.2.2 Tokens

Blockchain protocol tokens or tokens, is a unit of value which is sold through an initial coin offering (ICO) in order to generate liquidity in a cryptocurrency or to produce revenue for further development of the network (Batiz-Benet *et al.*, 2017). These ICOs are unregulated and are only backed by the business idea and profit incentives, however ICOs raised 3.5 billion USD in 2017 alone. This large amount of capital raised lead to the creation of many decentralised communities (Shroff and Venkataraman, 2012) with ethereum and Bitcoin being notable examples. These tokens can be used within the blockchain ecosystem as a medium of exchange for goods and services (Bitcoin Wiki, 2018*c*). Within this paper, the valuation models presented is primarily focused on determining the intrinsic value of cryptocurrencies. The valuation of these tokens as defined above is left as an area for further research.

4.3 Bitcoin

This section will provide a background to the original Bitcoin infrastructure. Since most altcoins are forks of the Bitcoin, it is critical to first establish an understanding of concepts related to blockchain technology, the Bitcoin block structure, and the inputs and processes involved in the mining algorithm.

4.3.1 Blockchain

The blockchain can be considered as a publicly distributed ledger of all Bitcoin transactions which has been agreed upon by the majority (51 %) of participants within the network (Crosby *et al.*, 2016). The transaction data is stored in data structures known as blocks. These blocks are then arranged chronologically, with the

most recent block addition containing the latest validated transactions. This technology was implemented to combat the double spending problem[3]. The manner in which the double spending problem is overcome is through public-key cryptography. The application of blockchain in the Bitcoin infrastructure resulted in decentralisation transactions, since all available information is publicly available with no central authority required to verify transactions.

4.3.2 Block Structure

The structure of a block can be split into a block header and body. The block header plays an essential role in the mining process since it is the only part of the block which is used in producing a valid Proof-of-Work. In the case of Bitcoin the body is mainly composed of a list of transactions and is on average 1500 times larger than the header (Mwale, 2016). The body structure is similarly structured for altcoins which incorporates blockchain.

4.3.2.1 The Block Header

The block header consists of the following components: A version counter, the previous block header hash, a time counter, the nonce, the nBit variable and the Merkle root hash.

Table 4.2: Structure of a Block Header

Component	Description and Function
Version Counter	The version counter indicates what validation procedures to follow, version 4 is the most recent release as of June 2018.
Previous Block Hash	The previous block header hash, is used to relate the current blocks position within the blockchain.
Time Counter	A time counter, indicates the amount of time elapsed since the miner started hashing the header. A constraint imposed upon the time counter is that is must be greater than median of the previous 11 blocks.
Nonce	The nonce, which functions as an unique counter. The nonce allows for multiple hashes to be produced when applying the SHA-256 hashing algorithm.
nBits Variable	The nBits variable, which is indicates the number of leading zeros that must be achieved in order to produce a valid Proof-of-Work. Another way or stating this is that the nBits ensures that the target threshold is reached. The target threshold is a 256-bit integer, since the nBit is only 32 bits a conversion is necessary.
Merkle Root Hash	Explained in detail below

Source: (Bitcoin Wiki, 2015)

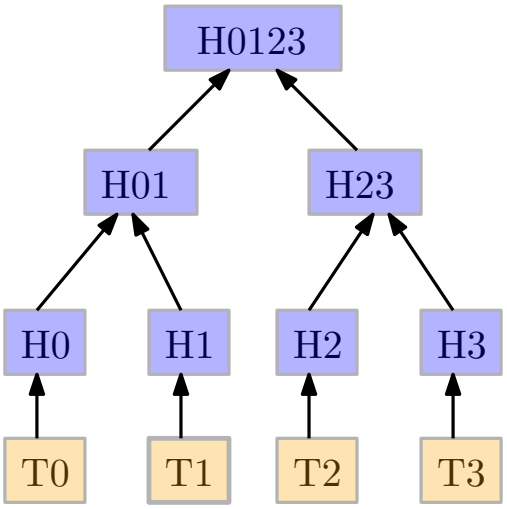
Merkle root hash

The final component is the Merkle root hash. This hash is as a result of the Merkle-Damgård construction which uses one-way compression functions. Now suppose that $\mathcal{H}$ is a family of hash functions where h :

[3]This occurs when a single unit of currency is used twice within the same transaction (Spending the same coin twice).

$\{0,1\}^{n+t} \rightarrow \{0,1\}^n$, and $t > 0$ then $h \in \mathcal{H}$ is known as a compression function. For example, a one-way compression function may take two arbitrary length inputs and produce one hashed value. The Merkle-Damgård transformation of h is defined as $MD_h : \{0,1\}^* \rightarrow \{0,1\}^n$. These transformations are used in generating the Merkle root hash as illustrated by 4.1.

Figure 4.1: Example of the Merkle Hash



T0, T1, T2 and T3 represents the transaction block IDs. These transaction block IDs are generated when a transaction is made. These tranaction block IDs are then hashed through one-way compression functions to obtain H0, H1, H2 and H3 respectively. These hashes are then hashed again pairwise, using one-way compression functions until the final hashed value is formed (in this case H0123), this final hashed value is known as the Merkle root hash. This root ensures that the integrity of the transactions remain and cannot be modified, unless the block header is changed, since if any of the values T0, T1, T2 or T3 is changed to say T4, then the subsequent H0, H1, H2, H3 will produce a different hash value. Thereafter, once all the pairwise hashing is completed the final hash value produced will differ from the previous final hashed value H0123 (Coron *et al.*, 2005). Furthermore, the structure allows verifying transactions to be less resource intensive. For example in figure 4.1 if the user wanted to check if T1 was included in a block, instead of downloading the whole blockchain to verify, the only values the user would need is H23 and H0.

4.3.3 Mining Process

In a trustless currency system such as Bitcoin, a new method of verifying transactions had to be developed. Any user may choose to verify transactions to add a new block to the existing blockchain. These users are known as miners and the process to verify transactions subsequently been coined the term mining (Kroll *et al.*, 2013). For the network to recognise a new valid block has been created the miner must produce a Proof-of-Work. Once a valid Proof-of-Work is produced, the user is then rewarded with 12.5 BTC as of June

2018. This amount is not fixed and is halved every 4 years which when can be estimated to every 210 000 blocks mined (Nakamoto, 2008). Once a block is appended to the blockchain it is then broadcasted to the network. This reward acts an incentive for mining, which in turn improves the integrity of the system since more transactions are being verified by more users. Antonopoulos (2014) explains that if two different blocks are mined at the same time, each miner attempts to extend the blockchain that corresponds to the chain which demonstrates the greatest Proof-of-Work, as known as the longest chain.

4.3.3.1 Proof-of-Work

As mentioned above, Bitcoins' Proof-of-Work is derived from the Hashcash protocol. This Proof-of-Work uses the block header to generate a hash which must meet certain requirements. Mwale (2016) formally describes the Proof-of-Work protocol, as a miner M computers a hash of the block header H such that the target difficulty T is met. In other words if V is the hashed value of H then the leading number of zeros of the hashed value V must be,

$$\text{Leading number of zeroes}\,(V) \geq T \tag{4.1}$$

It is important to note that H is a function of the following,

$$H = H\,(H_{t-1}, n_t, MD_h) \tag{4.2}$$

Where H_{t-1} is the previous block header, MD_h is the Merkle root hash and n_t is the nonce. In this function the variables MD_h and H_{t-1} are fixed due to its definition. Hence, if the difficulty requirement is not met, the nonce is incremented such that $n_{t+1} = n_t + 1 \quad , t = 0, 1, \ldots, 2,147,483,647$ with the initial nonce $n_0 = 0$ and a new hash is generated until the difficulty requirement is met. Since the nonce is a 32-bit number, the amount of iterations may reach the max number (2,147,483,647) allocated to a 32-bit integer. In this instance, the block header is updated and a new Merkle root is obtained and the nonce value is reset to zero (Back, 2002).

4.3.3.2 Difficulty

The difficulty target ensures that a Bitcoin block is generated every 10 minutes (Bitcoin Wiki, 2018*a*). This is to ensure that the mining is not dominated by a few players with superior computational power. The way Bitcoin adjusts the difficulty target is the following. It firstly calculates the time to find the last 2016 blocks and compares it to the expected time of 20,160 minutes (keeping in mind an expected block every 10 minutes is to be maintained). The ratio between the two is then calculated and is multiplied to the current difficulty target and consequently, an upward or downward adjustment is made (Antonopoulos, 2014).

4.4 Valuation Models

To find the true value of any cryptocurrency one first needs to identify which asset category it falls into. As the name suggest one can view cryptocurrencies as currencies, for which the coin in question will need to meet the criteria of money (Yermack, 2013). The usage of digital currencies as hedging instruments much like commodities (Dyhrberg, 2016) and the similarities of the money supply of bitcoin to that of gold indicates that the asset can be valued in an analogous way. The mining process for Proof-of-Work coins are inherently resource intensive and therefore a lower bound minimum price based on the cost of production can be determined or approximated and is independent of any expectation of future returns (Garcia, Tessone, Mavrodiev and Perony, 2014). Therefore, there exist a vast array of methods for valuing cryptocurrencies, some of which are more suitable than others. The suitability of the models is investigated in this section.

4.4.1 Cryptocurrencies Valued as Money

Economist argue that money has three main characteristics: medium of exchange, store of value and unit of account (Yermack, 2013). To investigate whether cryptocurrencies meet these criteria, bitcoin is considered, since it is the most successful cryptocurrency to date. Yermack (2013) argues that bitcoin meets the criteria of medium of exchange, since many online merchants seem to accept it as a form of payment, however it fails the latter two criteria. Security related problems, such as hacking attacks and thefts undermines bitcoin as a store of value.

Van Alstyne (2014) counters this by giving examples of how centralised currencies are not immune to these problems either. Although Cryptocurrency exchanges have been victims to major hacks amounting to losses of millions of Dollars, hacking fraud has also affected banks with losses due to theft of similar or greater magnitudes. He further argues that bitcoin can act better than credit cards at detecting fraud, due to the public ledger in Bitcoin's block-chain structure.

As a unit of account, bitcoin fails since it has high number of leading zeros (confusing buyers and sellers), exhibits very high time series volatility, and trades for different prices on different exchanges without possibility of arbitrage says Yermack (2013). Volatility, however, cannot alone be the reason for why bitcoin cannot function as a currency, only why risk averters would avoid it (Van Alstyne, 2014). Van Alstyne (2014) gives an example of how people use volatile derivatives as medium of exchange store of value and unit of account all the time. He also explains that money can be anything as long as people trade with it, keep it as wealth and they measure it in prices, regardless of the number of leading zeros.

Bull Jenssen (2014) describes bitcoin as a digital commodity money and compares it to commodity money in general. Like commodity monies, bitcoin can only be obtained in two ways: using resources to mine or exchanging assets or goods for the currency. Bull Jenssen (2014) further gives examples of commodity money

and argues that the Proof-of-Work of bitcoin in the mining process gives it its intrinsic value, much like the cost of acquiring commodities contributes to its value.

Yermack (2013) and Van Alstyne (2014) both make compelling, yet contradictory arguments regarding Bitcoin's use as money. The points made by both individuals is useful in determining the usefulness of any cryptocurrencies as money. Some currencies may overcome the obstacles faced by bitcoin and may be considered as money and may therefore be valued as a currency.

4.4.2 Cryptocurrencies Valued as Commodities

Grant (2018) quotes former Federal Reserve Governer Randy Krozner: "I think the best way to think about what are called cryptocurrencies is really to say it's crypto assets." Koszner says this is because they are not used much like a currency and mainly as a speculative asset, much like gold. A minority of participants use cryptocurrencies such as bitcoin as a medium of exchange or a unit of account according to Krozner.

Cryptocurrencies and gold have many similarities (Dyhrberg, 2016). Bitcoin, for example, is structured so that the rate at which it is supplied resembles the rate at which Gold is mined[4]. Both bitcoin and gold derive its intrinsic value from the fact that it is resource intensive to supply and that they have scarcity. They both are not backed by any central authority or nationality (Dyhrberg, 2016). Differences between gold and bitcoin do exist, for example gold used to be used as a medium of exchange during the Gold backed era but has since been abandoned due to liquidity issues. It is most commonly used today as a store of value, whereas bitcoin may function as both a medium of exchange and a store of value (Dyhrberg, 2016).

Dyhrberg (2016) warns that bitcoin (and other cryptocurrencies) may face the same liquidity issues that gold faced. This is due to the fact that there is a limit on the money supply of bitcoin, which can have adverse effects if the user base is to increase significantly. Another reason is that the verification of transactions of bitcoin can take some time (sometimes an hour), which also negatively affects liquidity.

In principle bitcoin can be used as a currency, but in practice this does not seem to be the case Yermack (2013). Dyhrberg (2016) concludes that, as a hedging instrument, bitcoin is something between that of gold and the dollar. Hayes (2017) believes that cryptocurrencies have virtual intrinsic value which cannot be directly compared with the tangible intrinsic value of gold.

[4]hence the term mining.

4.4.3 Cost of Production Models for Cryptocurrencies

Garcia *et al.* (2014) argues that the intrinsic value of bitcoin equals at least the cost of producing it. That is, a lower bound, which is independent from any subjective assessment of future returns. They obtain the estimate by expressing the difficulty as the number SHA-256 hashes required on average to mine one bitcoin. They then use an approximation of the power requirements of the most efficient mining hardware per Mh/s (hash rate). An approximation of average electricity costs is then used to determine the cost of mining. It must however be noted that since their paper was published much advancement has been made in the mining of bitcoin i.e the evolution of mining hardware.

Hayes (2017) expands on the paper by Garcia *et al.* (2014) by providing a holistic framework for a cost of production model to value bitcoin. He bases his argument on the mining profitability of bitcoins and the opportunity cost of not mining for altcoins. That is an individual would undertake mining if the marginal cost of production were less than or equal to the marginal product. The work produced by Hayes (2017) is very useful in determining the intrinsic value of cryptocurrencies and is discussed in some detail and is the subject of the rest of the chapter.

Hayes (2017) does warn that the market value of bitcoin may be very different from the lower bound estimate, after all the market price of bitcoin is determined through supply and demand. This does not take anything away from the usefulness of obtaining such an estimate since it forms part of the objective pricing of the cryptocurrency; whereas the subjective elements, which are difficult to quantify, may be another component in determining the price. Hayes (2017) makes the following assertion: "The more aggregate computational power employed in mining for a cryptocurrency, the higher the value." One of the reasons for this is that mining also serves to verify transactions therefore the more mining power contributed to a specific cryptocurrency the greater its general acceptance. Aggregate mining power thus serves as a proxy for overall use and acceptance. The difficulty can serve as an indirect proxy for the aggregate computational power, since the more network power employed the greater the difficulty becomes.

A second reason he gives is based on the mining profitability of the cryptocurrency. A rational miner is motivated by profit and would only undertake mining if the marginal cost of production were less than or equal to the marginal product. This would incentivise miners to mine only coins they deem profitable and thus would lower the aggregate computational power for a cryptocurrency if they chose to mine for an alternative altcoin (Hayes, 2017).

The methodology employed to prove these assertions are based on least-squares multiple regression. He first states the assumptions and performs the regression analysis to test five hypotheses. The paper by Hayes (2017) can be consulted for specifics of the regression analysis. The following hypothesis were found to be significant:

1. The amount of mining (computational) power devoted to finding a 'coin' is positively correlated to altcoin value.

2. The rate of 'coins' found per minute is negatively correlated to altcoin value.

3. Altcoins based on the scrypt algorithm will be more valuable than SHA-256d, all else equal

The following hypotheses were not supported by the analysis:

1. The percentage of coins mined thus far compared to that which is left to be mined before the total money supply is reached is positively correlated to altcoin value.

2. The longevity of the cryptocurrency is positively related to altcoin value.

To check the possibility of whether the causality of the first significant hypothesis is true or perhaps reversed, Hayes (2017) employs a Granger causality test to see if the computational power is indeed the cause for the price and not the other way around. His results indicate that the causality is strongly one-directional where aggregate hashing power is a causal factor in determining altcoin price.

The second significant hypothesis takes into account the block reward and the time required to mine a block. It amounts to the faster the rate of unit formation the lower the price, which is an extension of the law diminishing marginal utility. The idea here is that scarcity will drive the value of the cryptocurrency, so if a coin is structured so that it creates an abundance of units in rapid succession, this would diminish the value of that coin. The regression analysis found that the "rate" of coins mined did negatively influence the price.

Scrypt algorithms are much more robust than SHA-256d algorithms, since the algorithm was created to improve upon the SHA-256d. Scrypt coins thus require more computing power per unit than it's SHA-256d counterpart. This *relative hardness*[5] will cause the scrypt coin to be worth more, if all else is equal.

Hayes (2017) gives reasons for why the other hypothesis did not prove to be significant and his work can be consulted for more details. He removes these insignificant parameters from his regression analysis and runs the analysis again. The following is inferred from the adjusted model:

1. A 1% increase in aggregate Gh/s (hash rate) output, will increase the price by approximately 0.69%.

2. A 1% increase in coins produced per minute, will reduce the price by approximately 0.98%.

3. given that the altcoin uses the scrypt protocol, the price will be higher by approximately 7.46% compared to its SHA-256 counterpart, all else equal.

[5]The relative hardness pertains to how computationally complex the hashing algorithm is when producing a hashed value.

The model employed is extremely useful in determining the value drivers of cryptocurrencies, especially Bitcoin. Hayes (2017) shows that more than 84% of the value formation of a cryptocurrency can be explained by the following three variables: computational power employed, rate of coin production and relative hardness of the mining algorithm. "This suggests that relative rates of production for given level of mining effort are paramount. For a given level of hashpower, increasing the difficulty will yield less units, and thus the relative cost of production" (Hayes, 2017). Furthermore the total money supply is not a determinant in the price but rather the rate of production.

During the writing of this paper Adam S. Hayes released a paper in July 2018. In this paper, he back-tests the marginal cost of production model to the value of bitcoin. The technique that Hayes (2018) employed was to fit a Vector Autoregression (VAR) model to the log differenced time series. He does this so that he can perform a Granger test, which normally tests temporal causality, he instead uses it to evaluate the post-hoc predictive power of the cost of production pricing model.
Hayes (2018) tests the following two hypothesis

H_{01}: The market price does not "cause" the model price
H_{02}: The model price does not "cause" the market price

The results given by Hayes (2018) reveal that H_{01} cannot be rejected. This is what is to be expected since the market price should not be the cause for the model price. H_{02} is strongly rejected, which confirms that the model price does indeed cause the market price. This lends credibility for the cost of production model presented by Hayes (2017).

His findings are remarkable. Not only does he find evidence for bitcoins intrinsic value he also draws conclusions about the flaws of other bitcoin valuing techniques. He indicates that valuing bitcoin as a traditional financial asset (such as money) and attempting to value bitcoin due to exogenous factors is misguided. He suggests that although bubbles may appear in bitcoin markets like those experienced in 2017, that the value of the coin converges to the marginal cost of production value (Hayes, 2018). During periods of excess demand (e.g. a price bubble) the price of bitcoin will not collapse to zero but rather to the model value, either by the difficulty adjusting upwards, or the market price decreasing, or both to resolve the discrepancy (Hayes, 2018).

4.5 Summary

The valuation technique that is most suitable to estimating the intrinsic value of cryptocurrencies is a cost of production model. This relies on the economic theory that the marginal cost of production must equal the marginal utility for any one miner. Other valuation techniques, such as viewing cryptocurrencies as money may be inappropriate on the account that they mostly fail the requirement properties of money. The mining process for cryptocurrencies is inherently resource intensive and therefore there are costs involved with the supply of cryptocurrencies. The analysis for bitcoin has been performed by Hayes (2018). A similar approach is implemented in the next chapter, applied to the altcoins monero, litecoin and ethereum in particular.

CHAPTER 5

METHODOLOGY

5.1 Introduction

Hayes (2017) presents a basic framework for determining a marginal cost of production model for altcoins. The output of this model represents the supposed intrinsic value of the altcoin and possibly a lower market value bound. Hayes (2018) performs a VAR back-test to determine whether this model does in fact confer to a intrinsic value for bitcoin specifically.
In this chapter the VAR testing framework that Hayes (2018) employed is presented as well as the marginal cost of production model Hayes (2017) provides. The same technique Hayes (2018) uses to back-test bitcoin is used to back-test the values of altcoins. However some modifications are needed for the cost of production model to be applicable to other altcoins.

The following assumptions are made:

- Each miner has perfect mobility of capital. That is, they are able to switch mining from one altcoin to another without enduring any additional costs for doing so. All that is needed is to change some of the software settings to dedicate mining to another coin. There is a slight flaw in this assumption in the sense that ASIC machines which are essentially the only way to mine for bitcoin profitably (at the time of this paper), cannot be used to mine for some of the hardier algorithms. This consideration will be made when calculating the prices of altcoins that use the Scrypt or other protocols.
- Each miner is endowed with the most efficient mining hardware available for that altcoin. Although an important consideration when deciding whether the undertaking of mining is profitable or not if one does not own a machine, it will be considered a sunk cost. This is done to consolidate the fact that the model under consideration is indeed a lower bound value.
- Internet fees are considered negligible. Internet fees pale in comparison to electricity costs.

- All other costs, such as monitors, CPU, motherboard, etc. can be ignored and considered sunk costs like the mining hardware itself.

5.2 Cost of Production Model

Within this section two production models is presented. Firstly, a model for coins that are based off the SHA-256 (Bitcoin) and Scrypt (litecoin) hashing algorithms and thereafter a model for altcoins where the process of mining is applicable. The rationale around why only mining coins are considered is that the cost of production model is partly focused on the expenses incurred in the mining process.

5.2.1 Bitcoin Model

The model is defined in terms of bitcoin as follows,

$$IV = \frac{Expense/Day}{BTC/Day} \tag{5.1}$$

where

$$Expense/Day = (\rho/1000) \cdot (\$/KwH \cdot W/Gh/s \cdot hr/day) \tag{5.2}$$

where ρ is the hashing power expressed in Gigahashes per second (Gh/s) and $\$/KwH$, $W/Gh/s$, hr/day is the electricity cost of 1 Kilowatt expressed in terms of 1 dollar, the amount of Watts consumed per Gigahashes a second and how many hours mining a day respectively.

$$BTC/Day = \left(\beta \cdot \frac{\rho}{\delta}\right) \cdot \theta \tag{5.3}$$

where β denotes the block reward, δ notes the difficulty expressed in Gigahashes per block (Gh/Block), ρ is the hashing power expressed in Gigahashes per second (Gh/s) and θ a constant fixed at 0.00002012 . This constant θ is the product of the normalised probability of mining a block with a single hash together with the number of seconds in a day. The θ parameter can be defined as follows

$$\theta = \frac{86,400}{2^{32}} = 0.00002012 \tag{5.4}$$

where $86,400$ is the number of seconds per day and $\frac{1}{2^{32}}$ is the probability of a successful hash being generated. This probability is only applicable to the Bitcoin and Scrypt case due to the structure of the hashing algorithms. Therefore, the BTC/Day expression can be interpreted as the theoretical amount of bitcoins mined per day multiplied by the probability of successfully mining a block in a day. Although the units in the parameter ρ will cancel in (5.1), it is simpler to calculate the expressions (5.2) and (5.3) individually then to calculate their quotient.

5.2.2 Altcoins

The reason why a modified model is presented for altcoins is due to the hashing protocols of altcoins. Since most modern coins have been adjusted to be "ASIC proof" hence, the parameter of $W/Gh/s$ is not feasible and will cause altcoins the intrinsic value expression to produce abnormal results. These abnormal results can be attributed to $W/Gh/s$ being particularly large for altcoins where, in particular, low-hash rates are produced with standard consumer graphic cards or CPU's. This causes the denominator to be small and subsequently resulting in the IV being abnormally large. Furthermore, the hashing protocols for altcoins imply that the previous constant θ will not be feasible since the probability of producing a hash to mine a block is significantly more complex to solve analytically. The proposed Altcoin model is defined as follows,

$$IV = \frac{Expense/Day}{Altcoin/Day} \tag{5.5}$$

where

$$Altcoin/Day = \frac{\phi \cdot \beta \cdot \xi}{\Phi} \tag{5.6}$$

where, ϕ is the hash rate expressed in megahashes per second[1] (Mh/s), β denotes the block reward as used in (5.3), ξ is defined as the total blocks mined per day in the network and Φ is the overall network hashrate measured in (Mh/s). The ratio of $\frac{\phi}{\Phi}$ can be described as a proxy for the probability to successfully mine a block per second. The Expense per day is then defined as

$$Expense/Day = \$/KwH \cdot Watts \cdot hr/day \tag{5.7}$$

where, $\$/KwH$ and hr/day is denoted the same as in (5.2) and $Watts$ is the reported Watt usage of the mining equipment.

For Scrypt hashing algorithms, (5.3) will remain unchanged although not strictly earning bitcoins. Since the hashing algorithm is similarly structured to the SHA-256 hashing algorithm, the θ parameter will still be viable. However, (5.2) is modified to (5.6) due to some alterations in the hashing algorithm causing it to be slightly more memory intensive. Thus in turn, causing the algorithm to be more "ASIC proof", skewing the energy efficiency parameter. Hence, in summary, the model for coins which use the Scrypt hashing algorithm, the $Expense/Day$ expression is modified to the altcoin case. Furthermore, the BTC/Day expression is used but in this case the result is in litecoins per day.

5.3 Cost of Production Inputs

During the process of mining a large amount of computational power is required to produce a valid Proof-of-Work, which is used to verify that the block produced is correct. Electricity is one of the biggest costs

[1]The unit of hash rate may be adjusted for simplicity when working with difference altcoins. However, if an unit adjustment is made to the hash rate, the same adjustment must be applied to the network hash rate.

in mining for cryptocurrencies. Any rational miner will only consider mining for an altcoin if they deem it profitable. The profitability of mining is therefore dependent on the region and the specific electricity costs of that region. This is an important consideration to make when using the model provided by Hayes (2017) to obtain a intrinsic value for cryptocurrencies. The electricity cost being one of the most important externalities for mining a coin, to value an altcoin one also needs information about the internalities of the coins structure at the time of calculation.
Some of the internalities that are present in Hayes model presented above are the following:

- β block reward
- ρ hash rate produced by a miner (Gh/s)
- δ the difficulty (expressed in units of GH/block)

These are inherent to the coin that is mined for and will differ for each altcoin.

The internalities for the altcoin model are different:

- β block reward
- ϕ hash rate produced by a miner (Mh/s)
- Φ network hashrate
- ξ total blocks mined per day

These variables will differ for each altcoin.

5.3.1 Block Reward

The block reward data is readily available for coins that have a larger market capilisation than other minor coins. This usually remains constant for longer periods of time compared to difficulty which adjusts on a more frequent basis. However, in the case of monero there is a block reward emission formula which exponentially decreases over time, the emission formula based off the Cryptonight hashing algorithm (Saberhagen, 2013). The block reward data is collected using the website `https://bitinfocharts.com/`.

5.3.2 Difficulty

The difficulty of mining for an altcoin is readily available on most online exchanges and some websites[2]. The difficulty of a block is updated on a regular basis, and this value will need to be the correct value for the time of the calculation.

[2] An example of such a website is `www.bitinfochart.com`

5.3.3 Hash Rate

The hashpower produced by a miner is a difficult value to estimate. This is because each miner in effect contributes varying amounts of computing power. The miner that contributes the most power will have the highest probability of success; however the successful miner does not always have the most powerful machine. The average hashpower is almost impossible to calculate for a specific coin since each miner will have different combination of hardware dedicated to mining for this reason a strong assumption is made to fix the hash rate for the analysis of altcoins. These initial estimates is obtained through a reputable mining calculator which attempts to approximate an average miners hardware.

Table 5.1: Hash rate inputs

Coin	Value	Source
Ethereum	108 Mh/s	`https://www.coinwarz.com/calculators/ethereum-mining-calculator`
Monero	2800 H/s	`https://www.coinwarz.com/calculators/monero-mining-calculator`
Litecoin	580 Mh/s	`https://www.coinwarz.com/calculators/litecoin-mining-calculator`

5.3.4 Network Hash Rate

The network hash rate is the cumulative mining power within the network for a particular coin. The network hash rate values for each altcoin is obtained through `www.bitinfochart.com`. The value is updated constantly with time between updates usually ranging between 2 and 5 minutes depending on the platform being used.

5.3.5 Block Time

The block time is a measure of the average length of time it takes for the hashing power of the network to successfully mine a block. This information for each altcoin is readily available online[3]. This value is static since it is related to the internal protocols of the particular coin.

5.3.6 Electricity Cost

The main externality mentioned is the electricity costs expressed as:
$\$/KwH$: the dollar price per kilowatt-hour
There are a number of ways that one can estimate the electricity cost input in the model. One consideration is to use the global average, this would assume that mining is done by equal number of parties across the world. This is obviously not a realistic assumption, since miners may be concentrated to some specific regions that dominate the mining environment for a specific altcoin. To obtain a more realistic representation of the cost inputs for miners of an altcoin it may be more accurate to use a cluster weighted average rather

[3]An example of such a website is `www.coingecko.com/en`

than a global average. This would require the determination of where the geographical locations are of the majority of altcoin miners. Then to use these weights in conjunction with the rates in those regions to determine the weighted average, which gives a much better representation of the actual electricity costs incurred by miners dedicating their machines to mine for altcoins. However, the prominence of mining pools cause this calculation to be more complex since the locations of these mining pools are diverse geographically by nature. Hence, for the purpose of this research this amount is fixed at $0.13\$/kWH$ which is the average cost of electricity in the United States of America in 2011 adjusted for inflation to 2018 (Jiang, 2011).

5.3.7 Energy Efficiency

Another externality to consider is the energy efficiency of the hardware used for mining.
$W/Gh/s$: is the energy consumption efficiency of the producer's hardware
Although this is an externality it must be noted that a consideration must be made with respect to what the most efficient machine is available for mining each altcoin. For example, altcoins based on the Scrypt protocol can be most efficiently mined with GPU's whereas bitcoin which uses a less robust algorithm can be mined by ASIC machines which are much more efficient in comparison to GPU's. The energy consumption for each mining machine specification will be compared to the hardware comparison wiki, if available, using an internet archive capturing service[4].

5.4 Intrinsic Value Analysis

A similar methodology is applied, but specifically for the altcoins: ethereum, monero and litecoin. The same Granger test is employed as described below, however adjustments need to be made to the cost of production model so that it is relevant to other altcoins.

A log-difference of both the price and the intrinsic values is taken in order to obtain stationarity to fit the VAR models. The stationarity of these data series is then confirmed by the Dickey-Fuller tests. The number for appropriate lags is then determined by the Akaike's Information Criterion (AIC), Hannan-Quinn Criterion (HQ) and the Schwarz Criterion (SC). Thereafter, the VAR models are fitted and in cases where parameters were statistically insignificant, a restricted VAR model is fitted with a threshold of 2 for the t-value. The VAR models residual series is then tested for white noise by the Portmanteau test. The relevant VAR or restricted VAR models are then tested for causality by performing a Granger test and thus testing the same two hypothesis' that was presented by Haynes (2018). This analysis is performed for the various time series in R with implementation of the `vars`, `TSA` and `urca` packages.

[4] An example of such a service can be found at `https://web.archive.org/`

5.5 Summary

The methodology's employed requires gathering the input variables for the altcoin model presented in this chapter. Data that is specific to each coin under analysis is obtained and is different for each altcoin. These variables are block reward, difficulty and the miner's hash rate. External data (i.e. data not inherent to a specific coin) such as Electricity cost and energy efficiency of mining hardware is also required. Some of the inputs remain constant throughout the analysis, due to the challenge of obtaining relevant data. Graph inference and a statistical analysis is performed in the following chapter.

CHAPTER 6

RESULTS

6.1 Introduction

An assessment of the viability of the cost of production model as an estimate of the intrinsic value of altcoins is performed in this section. The following sections include a comparison of the market price of the altcoin and the estimated intrinsic value under the model. In addition to this, the input variables are also compared, so that the interaction of the variables can be seen on the resulting model price. The graphs are discussed and reasons are given for the anomolies in the data.

6.2 Valuation Analysis

First the data is obtained for the various altcoins and the model price is calculated. This is then plotted against the market price. Inference is performed on these graphs by assessing the anomalies and providing reasons for the movements of the market price and the intrinsic value price.

6.2.1 ETH

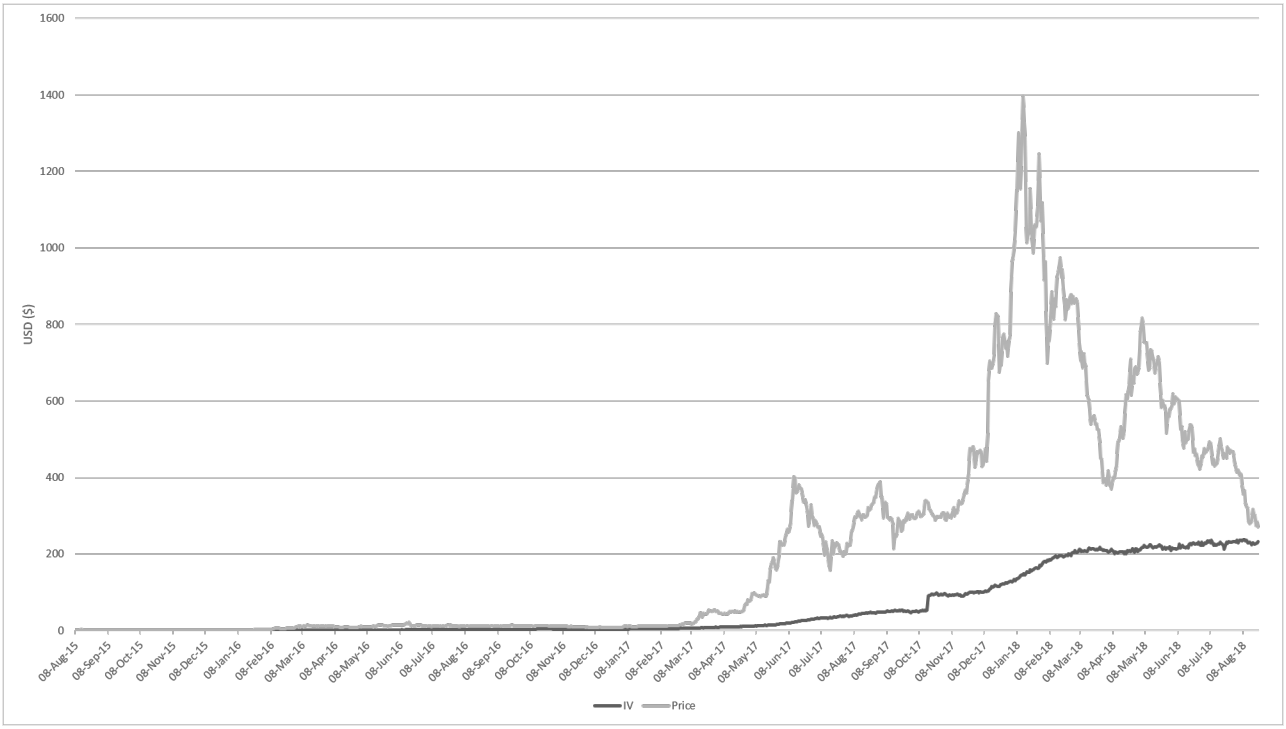
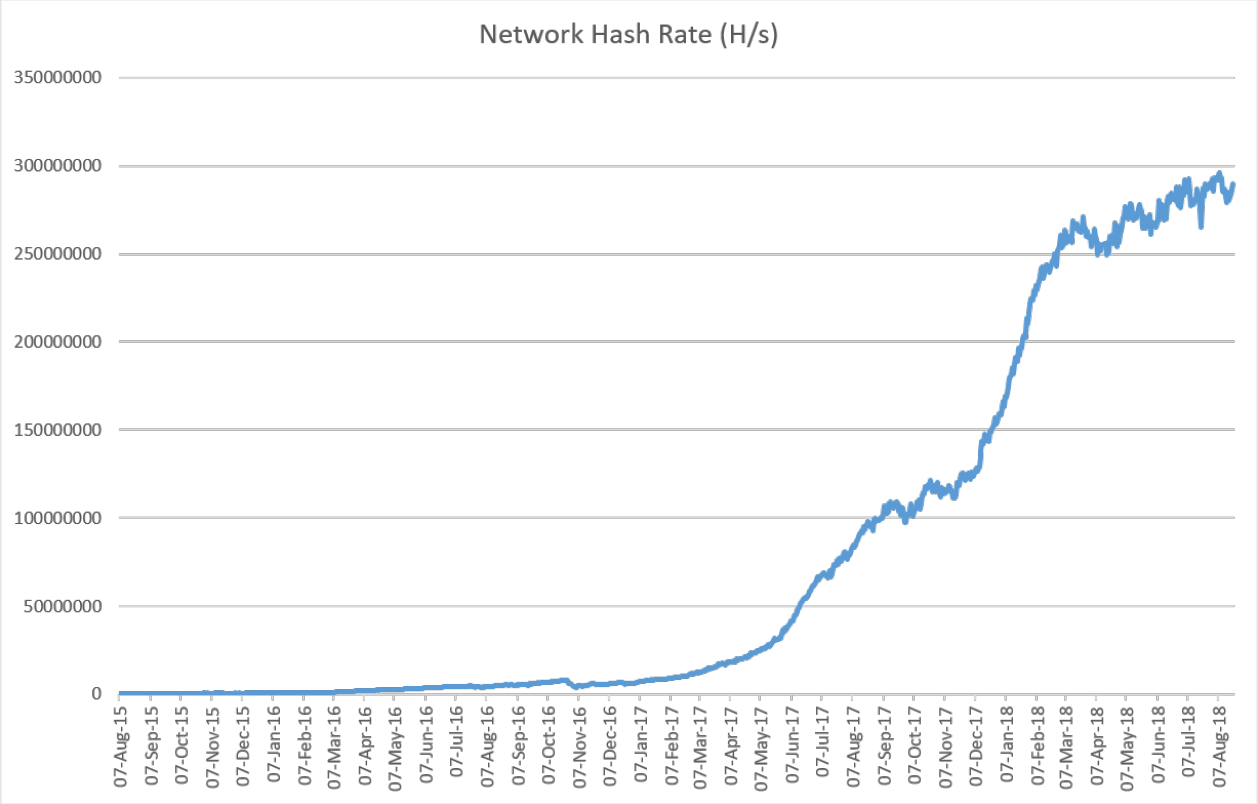
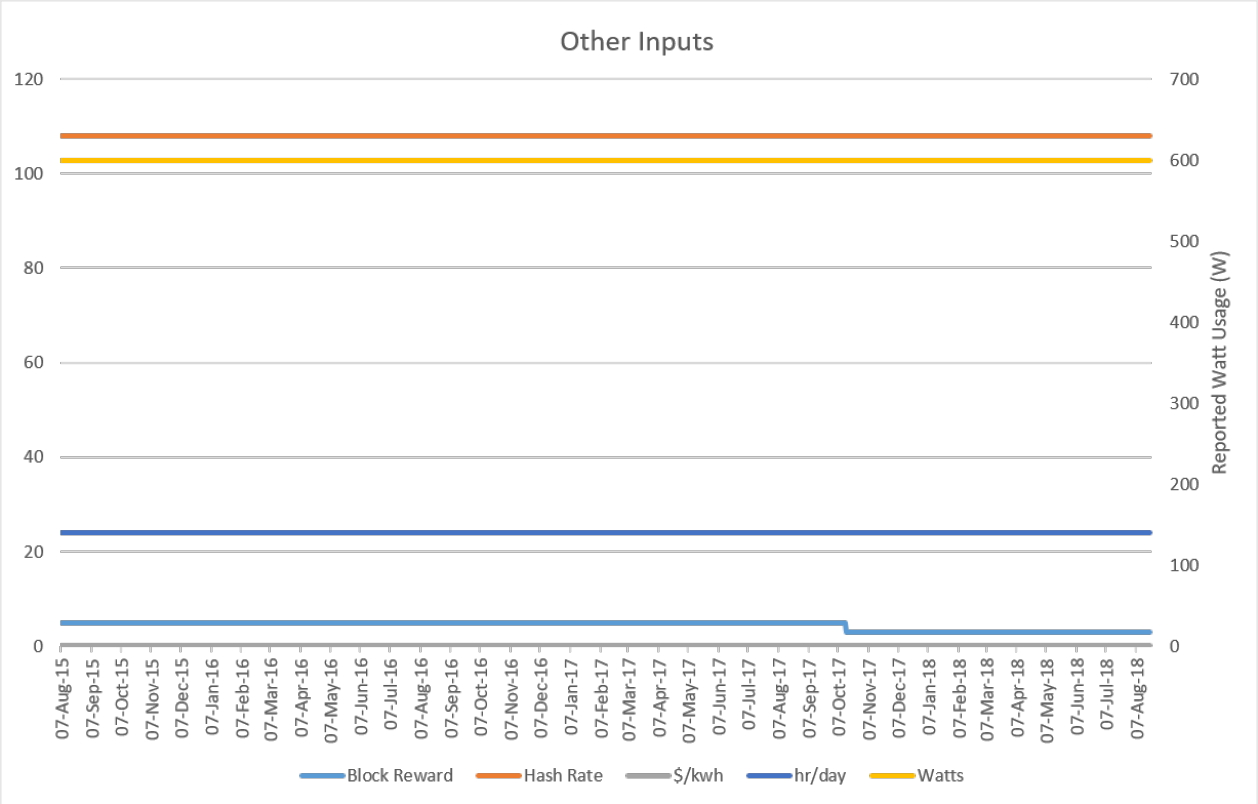


Figure 6.1: Model Price and Market Price of ethereum vs Time



(a) Ethereum Network Hash Rate



(b) Other Inputs for ethereum

Figure 6.2: Inputs for ethereum

There is little movement present between August 2015 and May 2017, although the IV was consistent as a lower bound. Thereafter, the market price increased rapidly during 2017 due to the increased interest within the cryptocurrency market. Ethereum is often directly compared as an alternative cryptocurrency to bitcoin which resulted in the market price increasing fairly early compared to other altcoins. The slight jump in the IV on the 16th of October is a direct result of the block reward decreasing from 5 ETH to 3 ETH. During early 2018 the IV only increased slightly while being consistently below the market price with the market price ultimately converging to the IV. Thus, in the case of ethereum there are indications that the cost of production model may be viable.

6.2.2 XMR

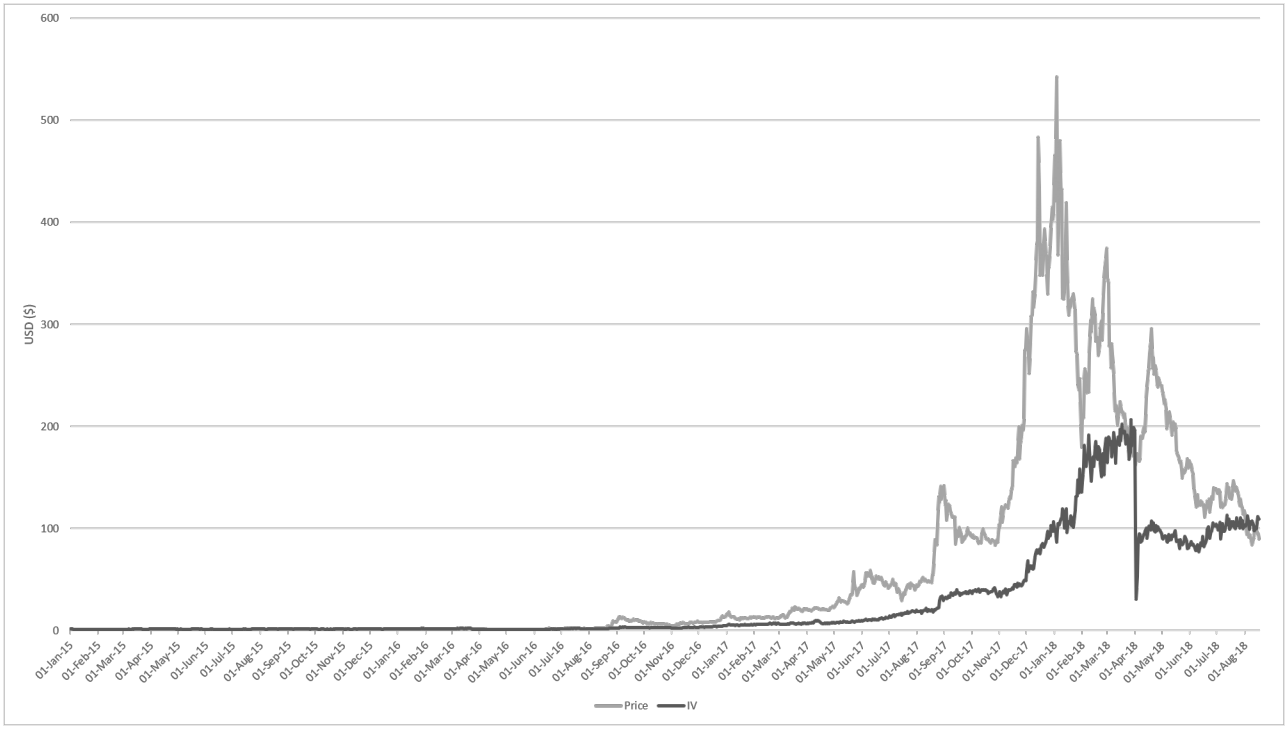
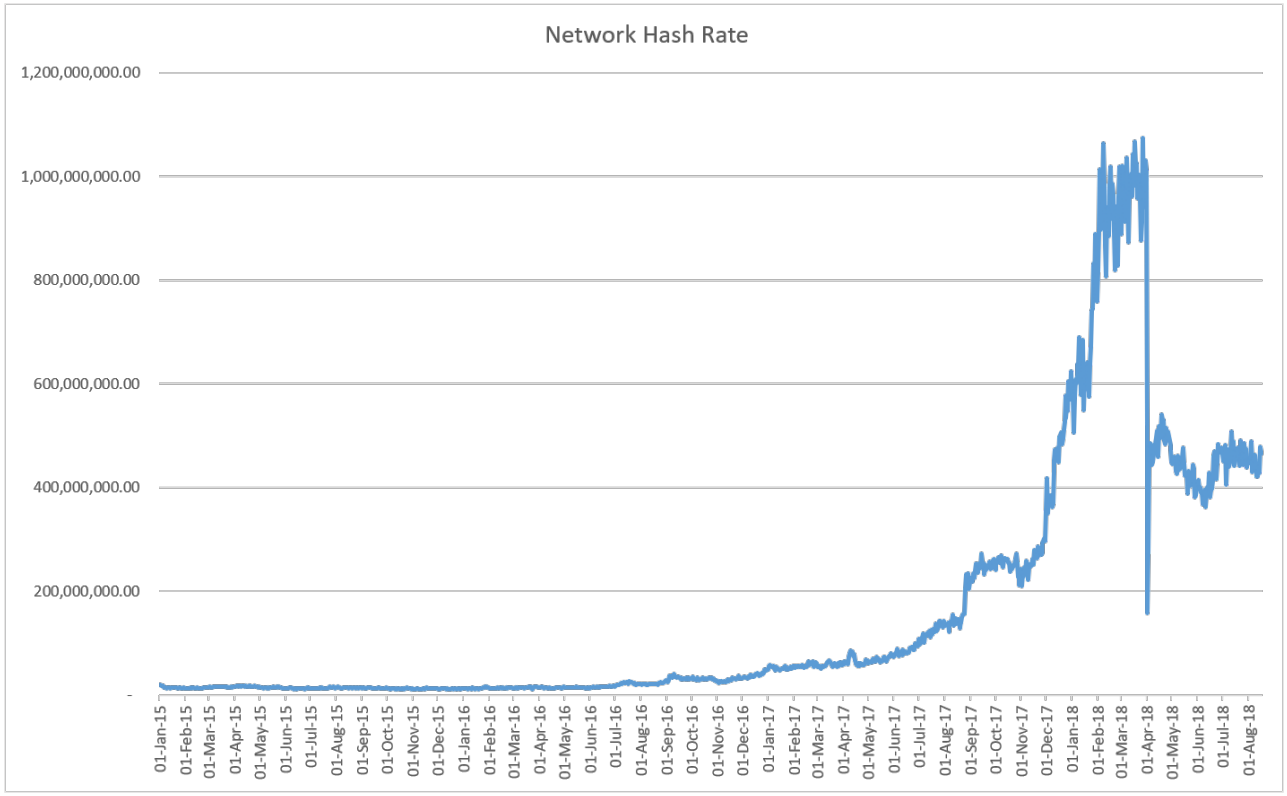
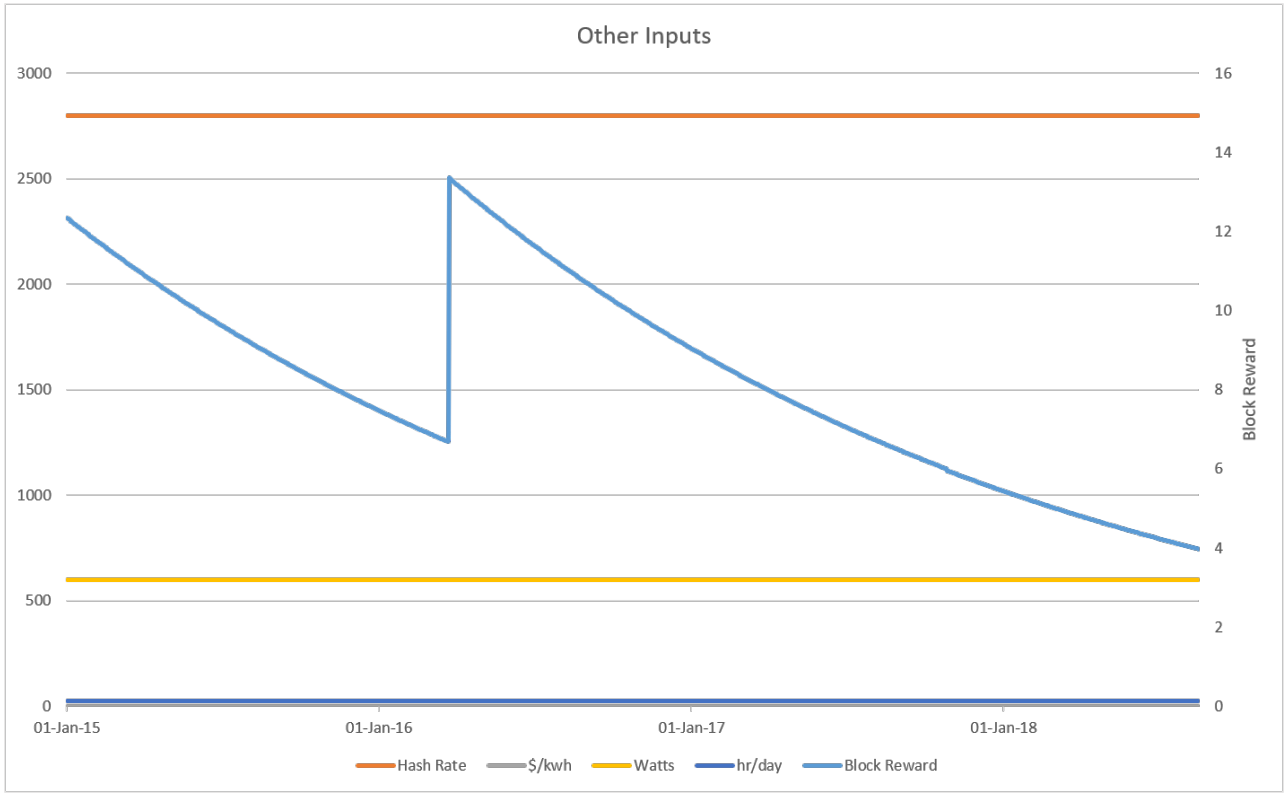


Figure 6.3: The relationship between the price in USD against the intrinsic value of monero



(a) Monero Network Hash Rate



(b) Other Inputs for monero

Figure 6.4: Inputs for monero

From the 1st of January 2015 up until middle September 2016 there was a small difference between the IV and market price for monero with the IV acting consistently as a lower bound. Thereafter, the coin experienced some rapid growth during the 2017 year due to increased investor sentiment. A possible factor for this sentiment was the inherent anonymous functionality of monero. The shape of the IV is somewhat similar to the market price during the 2017 period, although it varies towards the beginning of 2018. It must be noted that even through the rapid growth of monero during 2017 our model was consistent with acting as a lower bound. The sharp decline in the market price as experienced from January to May 2018 can be attributed to the following factors[1],

- The coin was delisted on the 18th of May 2018 from one of the largest exchanges in Japan (Coincheck) due to increased security regulations being introduced
- Various malware mining applications were discovered during this time[2] which hindered investor sentiment to the coin

The hard drop in IV experienced in the beginning of April was due to an ASIC machine for monero being announced and introduced to the market. This deterred miners due to fear of their mining hardware being incompetent, causing the overall network hash rate to drop drastically and subsequently causing the sharp decline of the IV. Shortly thereafter, the Monero team made adjustments to the Proof-of-Work algorithm which resulted in these ASIC machines being redundant. The change to the Proof-of-Work structure was implemented on the 6th of April 2018. This motivated miners, since their existing equipment was again relevant and could compete in the network, causing the overall network hashrate to increase and subsequently resulting in the increase of the IV[3].

During the third quarter of 2018 the market price and IV converged with the market self-correcting towards the IV. This holds consistent with the cost of production model theory.

[1]Read more at `http://globalcoinreport.com/the-fall-of-monero-will-it-recover/`
[2]These malware mining applications injected worms into Android phones
[3]Read more at `https://blockexplorer.com/news/monero-april-2018-hard-fork/`

6.2.3 LTC

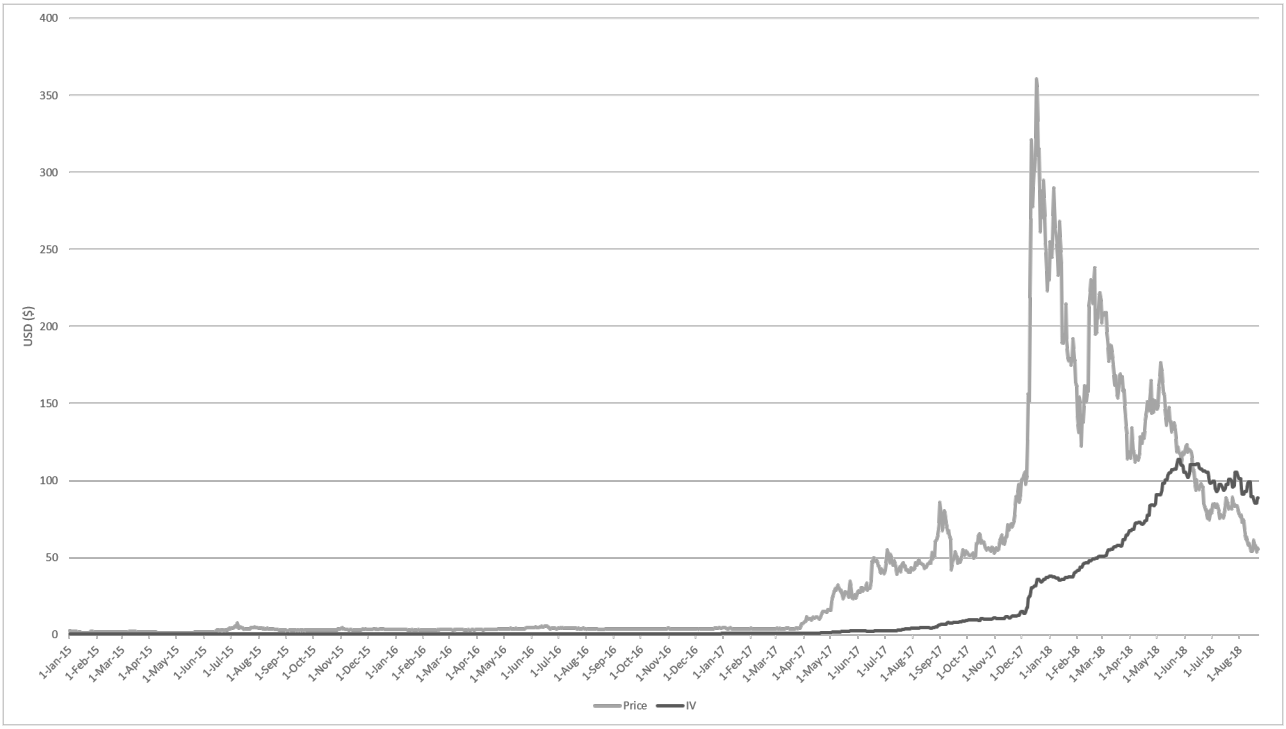
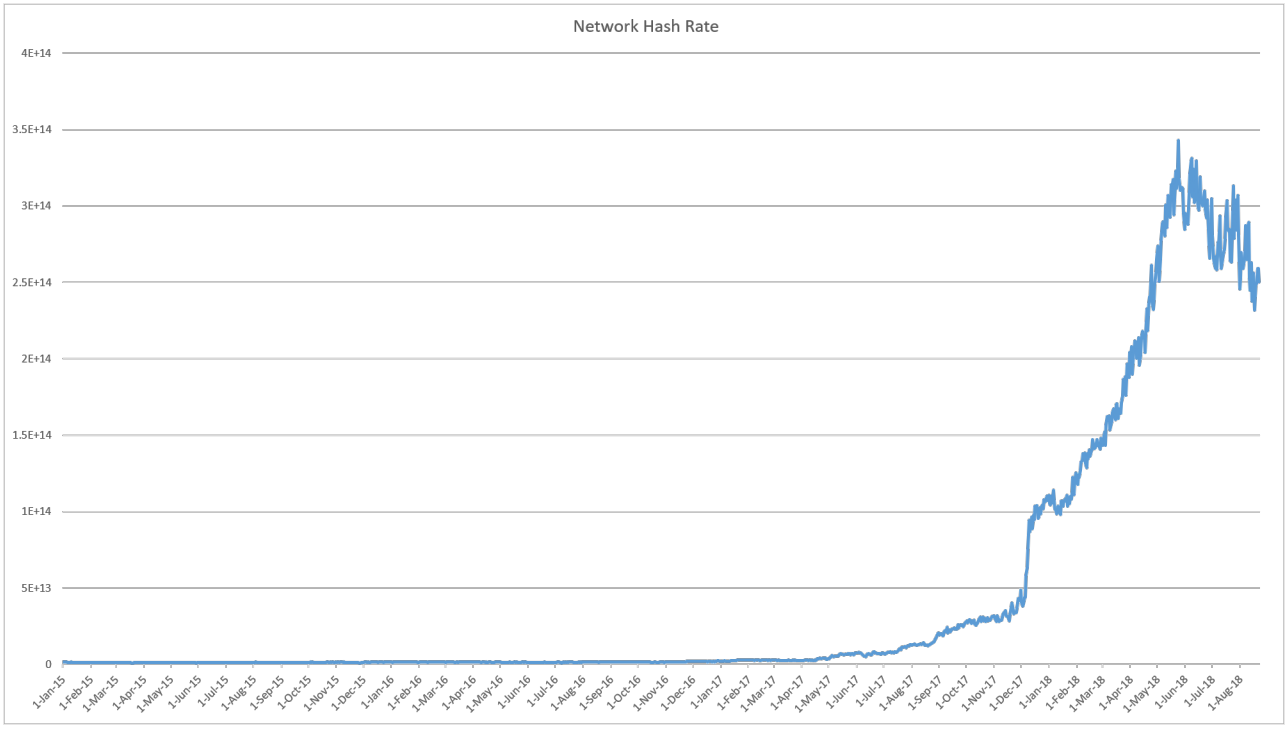
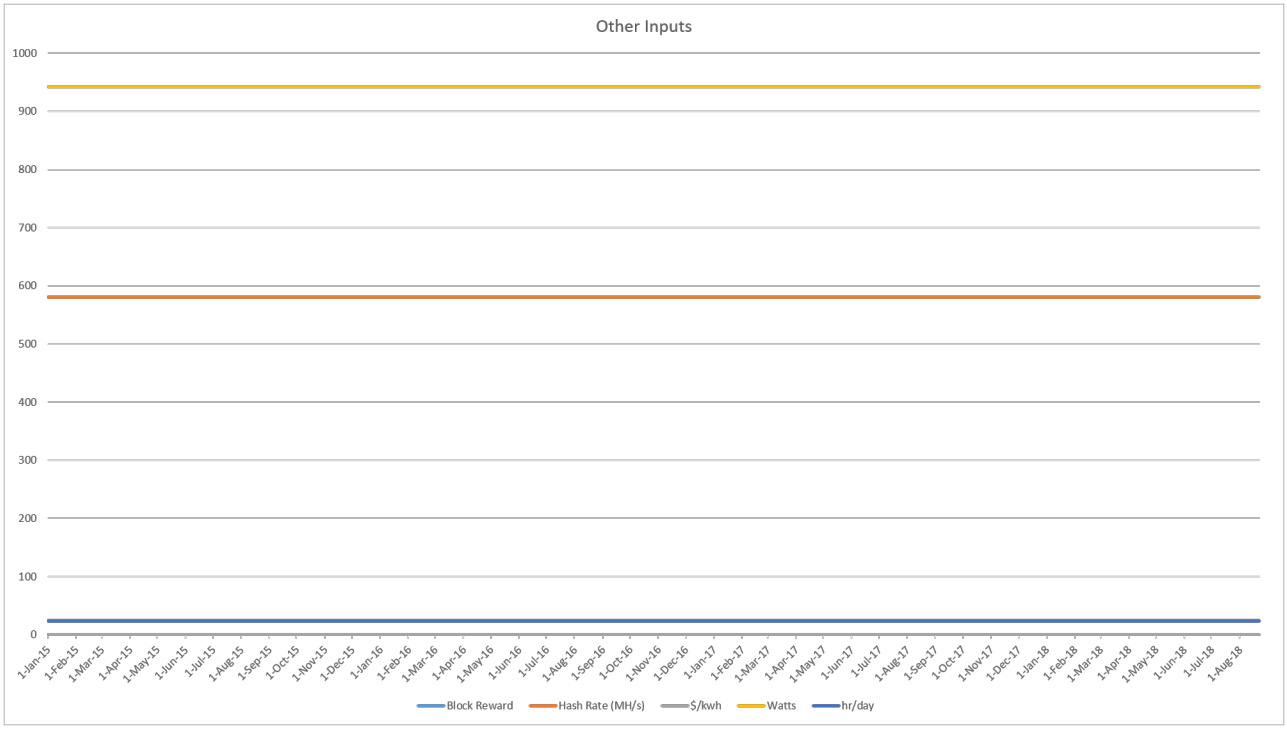


Figure 6.5: The relationship between the price in USD against the intrinsic value of litecoin



(a) Litecoin Network Hash Rate



(b) Other Inputs for litecoin

Figure 6.6: Inputs for litecoin

The IV price and the market price match very closely initially. Only around April 2017 do we see the rise of the value of LTC deviating from the model price. This discrepency can be attributed to large investor sentiment that was evident in crypto markets throughout 2017. This stark increase in demand made mining for coins

very profitable, since the marginal utlity for mining coins during this phase was high. This also created greater competition among miners, with people not only 'jumping on the band wagon' with purchasing coins through exchanges but also entering the supply side market through mining. This is why the IV for LTC also rose in 2017. The difficulty adjusted to keep the rate of supply of litecoin fixed which made mining significantly harder, hence the increase in costs per unit of coin.

Around June 2018, the IV price rises above the market price of LTC. This could mean one of two things. If we assume that our inputs are correct and the cost of production model is a reasonable estimate of the IV of an altcoin, then litecoin is undervalued in comparison to the IV. If our model has inputs that cause the IV to be higher than what it actually is then litecoin may well not be undervalued.

6.2.4 Graph Inference

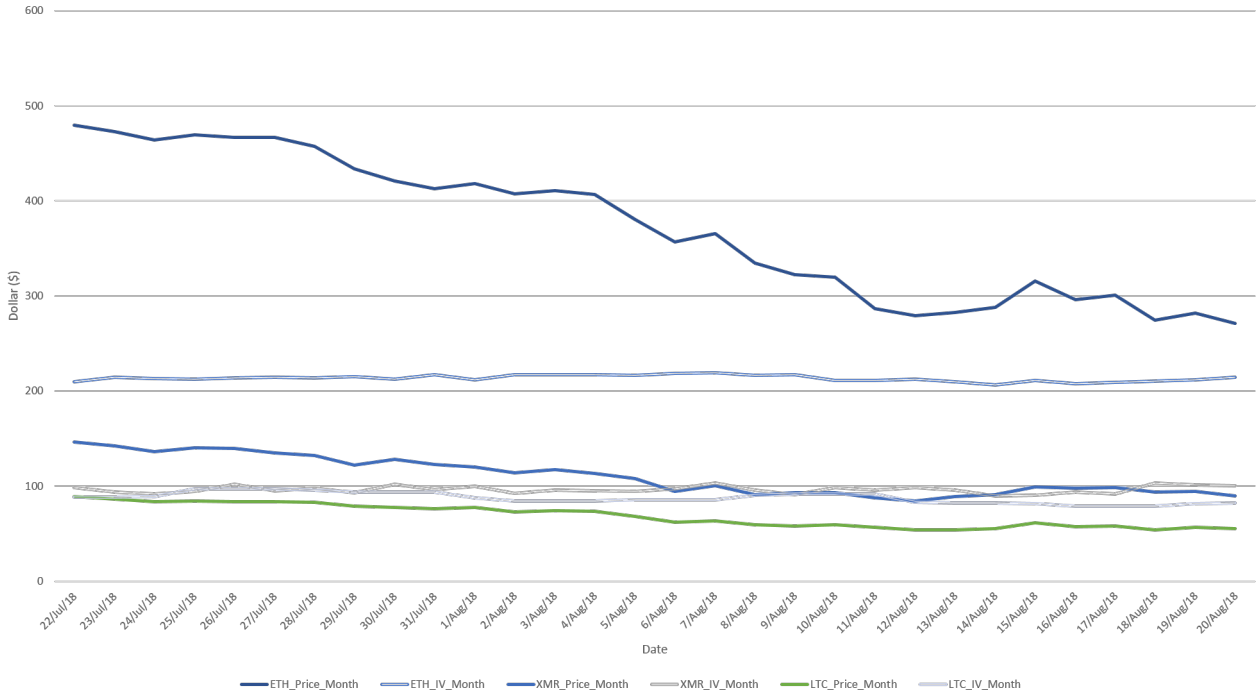


Figure 6.7: The market price and model price for various coins over 30 days

If only a months worth of data is used and compared the market prices with their IV estimates, the data for XMR and ETH indicates that the IV is always lower than the market price. This could support the fact that the model can be used to create a IV lower bound. For litecoin however, the IV is consistently higher than the market price and if the model works and has the right inputs could suggest that LTC was undervalued throughout the month.

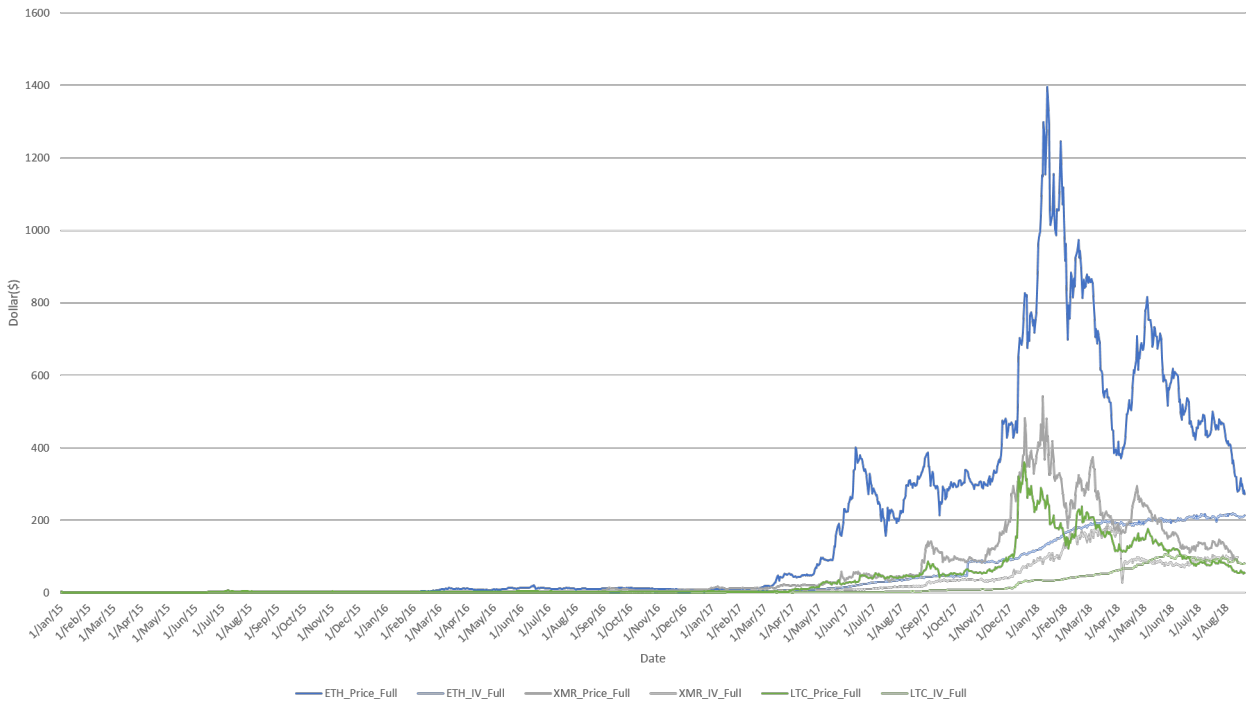


Figure 6.8: The market price and model price for various coins

Using the full time series, one can observe from the above that for most of the time the corresponding IV prices are situated below the market prices. The exception being LTC for which the IV lies below the market price in the most recent data. Although the analysis was done with crude estimates as inputs the model may still serve as a lower bound estimate for the value of the coin.

6.3 Statistical Analysis

A multivariate vector autoregression (VAR) is fitted to the price of the coin and the intrinsic value produced by the model. Thereafter, a Granger analysis is performed to test for temporal causality between the two time series namely, the price of coin and secondly, the intrinsic value produced by the model. This analysis is conducted for ethereum (ETH), monero (XMR) and litecoin (LTC).

This analysis, however, does not produce interpretable results since the VAR model does not produce white noise residuals for any of the altcoins and therefore a Granger test cannot be conducted.

6.4 Summary

The statistical analysis conducted does not yield results that support the altcoin model. This is possibly due to a number of reasons, outlined in the next chapter. The model should not be discarded so quickly, since the inference from the graphs shows that there is credibility for the model to act as a lower bound for the altcoin market price. The market price and model price often move in the same direction and reasons are given as to why the major changes occurred. The constraints of the model is presented in chapter 7, and suggestions are made as to how one can improve the intrinsic value estimate.

CHAPTER 7

SUMMARY, CONCLUSION AND RECOMMENDATIONS

7.1 Introduction

The shortcomings of the statistical analysis in chapter 6 is discussed, and reasons are given as to why this is not feasible. The main issue with this analysis is the data that is required for the model. Suggestions are made on the possibility of resolving these issues as well as suggestions for further areas that warrant research is provided. The overall viability of the model is determined and its interpretability as an intrinsic value model is addressed.

7.2 Shortcomings

As the results suggest, it is inconclusive whether the altcoin model may or may not be an appropriate model for the intrinsic value of the cryptocurrency. This is for a number of reasons, most notably the fact that most altcoins are "ASIC-proof". This makes it especially difficult in obtaining data regarding the most efficient mining machine available and then obtaining a corresponding hash-rate for that specific mining rig and coin. This forced some of the constant assumptions, which may be a crucial determining factor in identifying the intrinsic value price.

7.2.1 Data

A number of constants are assumed in the analysis for the altcoin model. These assumptions are either not suitable in our analysis due to their influence on the model price or because they are approximated as an incorrect constant.

The idea of using mining pools to determine the average hash rate each miner is contributing to the network is flawed. It would make more sense to use a catalogue of mining hardware evolution with the corresponding hash-rate for each coin as an evolutionary time series, instead of fixing the hash-power to the median value. Even this method, however, is flawed for altcoins, since the GPU's used to mine for these altcoins also process background computer tasks and are not as dedicated as their ASIC counterparts. This means that there is too much noise in one's mining rig to determine the specific hash-rate employed for the coin by any one miner. Furthermore, with GPU mining, miners may combine the most optimal graphic cards to increase their hash-rate and in-turn their probability of success, therefore determining the most powerful machine or even assuming that each miner has the most powerful machine is impossible. Another possible way of circumventing this issue is to use the "average network hashrate". The issue with this method is that in the data sources it treats mining pools as a single active miner and aggregates their hash-rate which causes the network average to be higher than what it actually is. This issue is further compounded by not being able to estimate the electricity usage which corresponds to a hashrate produced by an average miner.

The assumption to keep the electricity cost at $13\$/kWH$ may be inappropriate since this is the average electricity cost in USA. The concentration of miners may well not be in this location, which means that some other average value is more appropriate.

7.2.2 Statistical Analysis

None of the altcoins that were tested produced acceptable VAR models. The residuals produced are not white noise. This is attributable to the issues outlined above. Since the VAR models are not suitable the Granger test is meaningless. Although these results are not useful, the altcoin production model may still be feasible in obtaining a crude estimate of the lower bound. The statistical analysis if done in the future may yield positive results, however at this stage the statistical analysis is limited due to data constraints.

7.3 Summary and Findings

Many researchers have attempted to model the price for bitcoin and other altcoins. The methods have varied from currency valuation to commoddity valuation to investor sentiment valuation. The work produced by Hayes (2018) gives major credibility for a cost of production approach to value cryptocurrencies. The marginal cost of production works well for coins such as bitcoin, since they can be mined with dedicated ASIC machines for which the evolution of the hardware and the corrosponding hash-rate is publicly available and easy to obtain. Since altcoins are predominantly mined by GPU rigs, the data is dificulte to obtain. Furthermore, historical data for altcoins such as difficulty, total network hashrates are not always publicly available.

The VAR models did not produce white noise residuals therefore the Granger analysis is not applicable. The evidence for causality is therefore not proven in this paper. However, for the altcoins that were tested feassible estimates for a lower bound value can be inferred from the altcoin model. If in future, the data for altcoins become more readily available, then one may be successful in proving the causality of the model. For certain major events the value of the altcoin model and the market prices seem to move in the same direction, for reasons that can be attributed to the difficulty re-adjustment of the coin itself and the process of mining for that coin. Thus a true intrinsic value can in theory be inferred for this model, given that the input data is correct.

7.4 Further Research and Recommendations

Since the statistical analysis in this paper yields inconclusive results there are many facets to this approach that warrants further research. Namely, getting a better approximate for the mining costs for an average altcoin miner. This would require extensive research into the evolution of GPU mining and their corresponding hash-rates for each altcoin. With the large increase of interest in cryptocurrency, historical data sources may become available in the near future. The increase in availability of historical information may provide an opportunity for the same methodology to be applied and tested.

A better estimate for electricity costs is necessary. This would require one to find the distribution of miners around the world and applying a weighted average to determine the average mining cost.

If one inputs crude estimates for mining hardware and efficiency for non-efficient rigs and the "most" efficient mining rig one may be able to determine a rough interval for where the IV of the coin may lie. It would be a good endeavour to test this in future, so that a range of values for the IV can be determined.

If one decides to proceed with only a crude estimate of the altcoin value, a possible area of further research is to consider the ratio of the market price over the modelled price. This is analogous to a Price-to-Book (P/B) ratio for equities. One could then apply similar investment styles that one would apply to equity portfolio management to cryptocurrency portfolio management.

7.5 Conclusion

A cost of production model, although feasible for bitcoin, is at this stage, unlikely to be feasible for altcoins. The difficulty in obtaining relevant data and the noise in the hash rate data makes fitting a model to the time series particularly difficult and thus no causality can be proved. This does not however mean that the altcoin model is not useful. It can be used as a rough estimate for where the IV of the altcoin lies. This is supported by the fact that the coins market price and model price move bidirectionally for major changes in

the production inputs for the altcoin. This gives major credibility to the altcoin model as a good estimate in theory, however the data constraints makes this difficult to prove imperially.

To answer the question of whether the intrinsic value for cryptocurrencies can be estimated, one needs to consider all possible valuation techniques. The answer is yes, the intrinsic value can be estimated, especially for bitcoin in which case the cost of production model is the best suited valuation technique. The intrinsic value of other cryptocurrencies such as altcoins can, analogously to bitcoin, be estimated via a cost of production model. The interpretability of the usefulness of obtaining such an estimate is left for the reader, where many areas of further research can be explored on this subject.

REFERENCES

Antonopoulos, A.M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Riley Media. ISBN 9781449374044.

Arsov, D.A. (2018). Periodic Table of Cryptocurrencies: Blockchain Categorization. *SSRN Electronic Journal*, pp. 1–20. ISSN 1556-5068.
Available at: `https://www.ssrn.com/abstract=3095169`

Back, A. (2002). Hashcash - A Denial of Service Counter-Measure. *Http://Www.Hashcash.Org/Papers/Hashcash.Pdf*, , no. August, pp. 1–10.

Batiz-Benet, J., Clayburgh, J. and Santori, M. (2017). The SAFT Project: Toward a Compliant Token Sale Framework.
Available at: `https://saftproject.com/static/SAFT-Project-Whitepaper.pdf`

Bitcoin Wiki (2015). Bitcoin Wiki - Block Hashing Algorithm.
Available at: `https://goo.gl/bDLJD9`

Bitcoin Wiki (2018*a*). Bitcoin Wiki - Difficulty.
Available at: `https://en.bitcoin.it/wiki/Difficulty`

Bitcoin Wiki (2018*b*). Bitcoin Wiki - Merkle Damgard Construction.
Available at: `https://goo.gl/soGUSj`

Bitcoin Wiki (2018*c*). Bitcoin Wiki - Token.
Available at: `https://en.bitcoinwiki.org/wiki/Token`

Bull Jenssen, T. (2014). Why Bitcoins Have Value, and Why Governments Are Sceptical. Tech. Rep..

Coron, J.-S., Dodis, Y., Malinaud, C. and Puniya, P. (2005). Merkle-Damgård Revisited: How to Construct a Hash Function. In: Shoup, V. (ed.), *Advances in Cryptology – CRYPTO 2005*, pp. 430–448. Springer Berlin Heidelberg, Berlin, Heidelberg. ISBN 978-3-540-31870-5.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016). Applied Innovation Review. *Applied Innovation Review*, , no. 2.

Dolce, A. (2017*a*). A Guide to Hard and Soft Forks.
Available at: `https://masterthecrypto.com/guide-to-forks-hard-fork-soft-fork/`

Dolce, A. (2017*b*). Differences between Cryptocurrency and Tokens.
Available at: `https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/`

Dyhrberg, A.H. (2016). Bitcoin, gold and the dollar - A GARCH volatility analysis. *Finance Research Letters*.

Garcia, D., Tessone, C.J., Mavrodiev, P. and Perony, N. (2014). The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy. *Journal of The Royal Society Interface*, vol. 11, no. 99. ISSN 1742-5689.
Available at: `http://rsif.royalsocietypublishing.org/content/11/99/20140623`

Grant, K. (2018). Bitcoin Is Like Gold Not the U.S. Dollar.
Available at: `https://www.thestreet.com/story/14447914/1/bitcoin-is-an-asset-like-gold-not-a-currency-former-fed-governor-kroszner.html`

Hayes, A.S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, vol. 34, no. 7, pp. 1308–1321. ISSN 07365853.
Available at: `https://doi.org/10.1016/j.tele.2016.05.005`

Hayes, A.S. (2018). Bitcoin price and its marginal cost of production: support for a fundamental value. *Applied Economics Letters*, pp. 1–7.
Available at: `https://doi.org/10.1080/13504851.2018.1488040`

Jiang, J. (2011). The Price of Electricity in Your State.
Available at: `https://www.npr.org/sections/money/2011/10/27/141766341/the-price-of-electricity-in-your-state`

King, S. and Nadal, S. (2017). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, vol. 1919, no. January, pp. 1–27. ISSN 1098-6596.
Available at: `http://arxiv.org/abs/1606.06530`

Kroll, J.a., Davey, I.C. and Felten, E.W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, , no. Weis, pp. 1–21. ISSN 15437221.

Moore, G.E. (1922). *The Varieties of Intrinsic Value*. Routledge and Kegan Paul.

Mwale, M. (2016). Modelling the Dynamics of the Bitcoin Blockchain.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, p. 9. ISSN 09254560.
Available at: `https://bitcoin.org/bitcoin.pdf`

Rogaway, P. and Shrimpton, T. (2004). Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. pp. 371–388. ISSN 03029743.
Available at: `https://goo.gl/ruUJBs`

Saberhagen, N.V. (2013). CryptoNote.
Available at: `https://cryptonote.org/whitepaper.pdf`

Shroff, N. and Venkataraman, P. (2012). Regulating ICO Tokens and Cryptocurrency In India. , no. 1, pp. 1–18.

Van Alstyne, M. (2014). Why Bitcoin has value. *Communications of the ACM*. ISSN 00010782.

Yermack, D. (2013). NBER WORKING PAPER SERIES IS BITCOIN A REAL CURRENCY? AN ECONOMIC APPRAISAL Is bitcoin a real currency? Tech. Rep..
Available at: `http://www.nber.org/papers/w19747`