POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

A New Model for Bitcoin Mining Costs: An Econometric Analysis of the Bitcoin Price and Cost Dynamics

TESI DI LAUREA MAGISTRALE IN

MANAGEMENT ENGINEERING

INGEGNERIA GESTIONALE

Author: **Gianmarco Baleani**

Student ID: 953080
Advisor: Rocco Roberto Mosconi
Academic Year: 2020-21

Abstract

The Bitcoin miners' energy consumption and the Proof-of-Work paradigm are central themes debated in March 2022. Miners contribute to the growth of the blockchain and the production of bitcoins by using dedicated computer machines, application-specific integrated circuits (ASICs). An argument strongly discussed in the bitcoin mining literature concerns the bitcoin production costs and the price. Scholars focused their attention on whether the bitcoin costs can predict or explain the price. This work answers this issue through the development of a new model for the estimation of operating mining costs and the analysis between costs and the price. The introduction of estimates of miners' investments in ASICs requires a new methodology based on the increase of hashrate, the computational power. The mining operational costs are divided into energy and investments costs in order to provide additional details on the bitcoin costs and price dynamics. In the examined sample (24/01/2014 - 03/03/2022), the empirical results of cointegration tests and causality tests show a strong directionality from the price toward costs. These findings support the literature and the economic theory since an increase in price will naturally cause an increase in profitability, therefore new miners entering the business will increase the hashrate and lead the excess of profits to zero. In particular, the hashrate seems to have the best results in the causality tests compared with the other analyzed variables.

Key-words: bitcoin, mining, production costs, hashrate, bitcoin price, ASIC.

Abstract in italiano

Il consumo di energia dei miner di bitcoin e il suo paradigma di Proof-of-Work sono temi ancora fortemente discussi nel Marzo 2022. I miner, con i loro calcolatori elettronici specializzati (ASICs), contribuiscono alla crescita della blockchain e alla produzione di bitcoin. Un argomento che ha destato l'interesse di numerosi studi nella letteratura del mining di bitcoin riguarda la relazione esistente tra i costi di produzione dei bitcoin e il loro prezzo, in particolare, gli studi hanno concentrato la loro attenzione sul fatto che i costi possano effettivamente prevedere o spiegare il prezzo di bitcoin. Questo elaborato cerca di risponde a questo tema con lo sviluppo di un nuovo modello per la stima dei costi operativi dei miner e l'analisi tra i costi sostenuti e il prezzo. L'introduzione di stime per gli investimenti dei miner in ASIC richiede una nuova metodologia basata sull'aumento dell'hashrate, ossia la potenza di calcolo. I costi operativi dei miner sono così suddivisi in costi energetici e di investimento al fine di fornire maggiori dettagli sulla dinamica tra costi e prezzo. Nel campione esaminato (24/01/2014 - 03/03/2022), i risultati empirici dei test di cointegrazione e dei test di causalità mostrano una forte direzionalità dal prezzo verso i costi. Questi risultati sono coerenti con la letteratura e con la teoria economica secondo il quale un aumento del prezzo causa un aumento dei profitti, permettendo l'entrata di nuovi miner che aumenteranno l'hashrate e azzereranno gli extraprofitti. In conclusione, l'hashrate sembrerebbe avere i migliori risultati nei test di causalità rispetto alle altre variabili analizzate.

Parole chiave: bitcoin, mining, costi di produzione, hashrate, prezzo di bitcoin, ASIC.

Contents

Introduction

Bitcoin is the newest technology used for the function of money. It is *"a purely peer-to-peer version of electronic cash"* (Nakamoto, 2008) without the need for a financial institution. Starting from 2009 from an anonymous user "Satoshi Nakamoto", units of Bitcoin currency begin to be transmitted in the network and be used by a variety of computing devices. The key innovation was the use of a distributed computational system and the *Proof-of-Work* allowing the decentralized network to arrive at a *consensus* about the state of the transactions. This would solve the problem of double-spend the same currency unit instead of recurring to a central clearinghouse. The implementation of a Proof-of-Work algorithm provides more security and resilience as the computational power increases. During February 2022 the amount of hash per second reached the value of 200 exahash (200×10^{18}) and billions of dollars (Digiconomist, 2022) are spent in energy and machines to achieve such value.

In October 2021 Bitcoin reached a market capitalization of over one Trillion of dollars and a value of over $60,000. Despite its high volatility, Bitcoin security has never been in danger and rather than be used as electronic cash many experts prefer to attribute to Bitcoin the function of store as a value (Ammous, 2018). The invention itself is groundbreaking and spawned new science in the field of distributed computing, new cryptocurrencies, economics, and *econometrics*. Many scholars were attracted by this new technology and in particular studies regarding bitcoin mining operational costs and price. The focus of the studies is on the price of bitcoin whether the price can be explained by its costs and if the marginal costs are the fundamental value behind bitcoin.

This work throws light on these threads by sustaining that the price affects the costs for mining and not *vice versa*. When the price increases it pushes miners to invest in mining computer machines and increase the computational power, whereas a decrease forces miner to unplug their machines and cut energy costs. For supporting this thesis an analysis using Cointegration Tests (Engle-Granger and Johansen) and Causality Test (Granger Tests and Toda and Yamamoto) was performed on empirical data. Starting from the cost of production model (Hayes, 2017), a suitable model was developed for also integrating miners' investments. In this new model, miners' costs are divided into energy costs and investment costs. Energy costs are the operational expenses for running the machines and investment costs are the expenses for buying the machines. This model attempts to proxy reliable estimates of miners' ASICs spending for every period, however, the estimates are subject to limitations and rational assumptions based on the hashrate.

Secondly, in order to define a dataset used for the tests, the estimates of the variables require specific constructions as the energy costs that need the average Energy Efficiency of the network or the investment costs with the average costs per terahash per second (TH/s) of the network. The model is based on the hashrate, the increases or the decreases causes energy costs to rise or to fall, while for the investments the circumstances are more complex.

Finally, the empirical results of the causality tests show a significant unidirectionality from the bitcoin price to costs. In the two samples analyzed, price changes cause hashrate, energy and investment costs to change. These finding are in accordance with the economic theory, a price increase causes an increase of margins for miners, thus new actors will enter the mining business and increase the hashrate through investment in new machines to the point where the excess of profits will be equal to zero. On the other hand, when price drops machines are unplugged and hashrate drops as well, nevertheless the investment cannot be easily ceased. However, hashrate is the variable that shows superior performance in explaining this dynamic, while investments exhibit worse results, it may be caused by the inertia of the sunk costs when price drops.

In addition, this work provides a contribution to the Bitcoin mining literature with the introduction of a new model for describing the investment in mining hardware (ASICs). The empirical results highlight the unidirectionality of bitcoin price toward hashrate can also help analysts for performing on-chain analysis.

This work is divided into 5 Chapters: Chapter 1 explains the Bitcoin System, providing the basic knowledge to understand the bitcoin technology and the model. The literature focusing on the first version of cost of production model and the theoretical explanation of the new model are presented in Chapter 2. Chapter 3 describes the construction of the dataset and the variables used for the analysis. Chapter 4 concerns a brief explanation of the bitcoin price and costs dynamics, the methodology used for conducting the analysis, and the discussion of the results obtained. In the end, in Chapter 5 there are the final conclusions.

1 Bitcoin

The comprehension of the Bitcoin System is fundamental for understanding the dynamics between price and costs and the logic behind the cost of production model (CPM). Miners play a fundamental role in the network and they need to know the technical underlying of the blockchain. The halving events, the difficulty, the hashrate, the block reward are terms that will be familiar by the end of this chapter (to facilitate the reader a quick glossary is in Appendix A.1).

1.1. Keys, Addresses and Wallets

Bitcoin, as well as the other cryptocurrencies, is based on *cryptography* a branch of mathematics used in computer security. Cryptography means "secret writing" in Greek and its uses are not just limited to its meaning, *encryption,* but it is also used for digital signature and digital fingerprint. The ownership of bitcoins currency requires the use of *digital keys*, *bitcoin addresses* and *digital signatures*. The digital keys are stored by the user in a file, or a database, called *wallet*. The keys are completely independent from the bitcoin protocol and can be generated and managed by the user without any connection to internet or blockchain.

A bitcoin wallet contains a collection of key pairs, a *private* and a *public*. Private keys are generated using a random number between 1 and 2^{256} (1.1578×10^{77}) and using the private with a one-way cryptographic function to generate a public key (Figure 1.1 shows a simplified process of keys creation and storage). The random number must be random not generated by a deterministic algorithm and the key generation program is a trusted element. If these two characteristics are missing the keys generated may be not trustable.

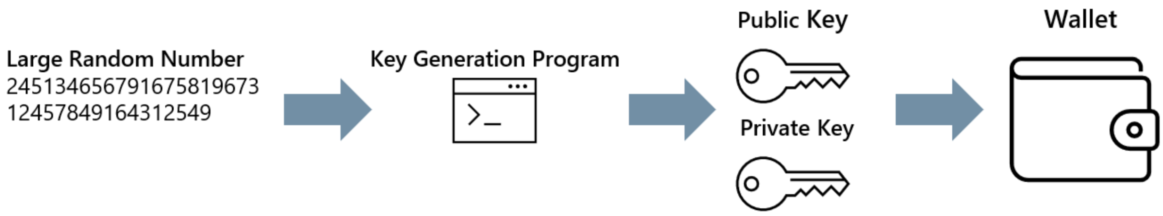


Figure 1.1: Process of creating and storing public and private keys.

Bitcoin addresses are used for sending and receiving bitcoins as a bank account number. They are generated from the public key using a one-way cryptographic hash function. In particular, “a hash function is a mathematical algorithm that takes data of arbitrary length as input and maps it to a fixed-length enciphered text as output” (Yasuda, 2010). This means that every Bitcoin address has a fixed constant length, and the address is not leaking information about the public key related to that address.

The Bitcoin wallet does not contain bitcoins but they contain only the keys, the “coins” are recorded in the blockchain and users control them by signing transactions with the keys of their wallets. Wallets are very similar to a keychain rather than a real wallet. There are many different types of wallets based on different technology, generally, a first distinction is based on the properties of the wallet to access the network: cold wallets are offline and offer more security from hacking attacks, but they still can be stolen physically. Typically, these wallets are paper or hardware wallets, for example, a printed paper with the private key and the public address or a simple USB device that stores the keys.

Figure 1.2: USB and paper wallets.

USB wallets or hardware wallets usually can store multiple sets of keys for different cryptocurrencies, while paper wallets can store only one type of cryptocurrency and one set of keys. On the other hand, the hot wallets are online and offer less security, however, they are user-friendly and most of the time is provided for free from an exchange[1] or using a mobile or pc app.

Investing a large capital in Bitcoin and storing it in a USB wallet or in a paper wallet may not be a good idea especially when users are not IT experts. There are possibilities to lose the wallet, password or be subject to hacks. High-capital investors usually rely on crypto custodians that store their keys and provide insurance in case of a cyber-attack. They charge a fee to keep their cryptocurrency safe and sound under their protected servers.

[1] An exchanger is platform that allows users to exchange cryptocurrency, it works similarly to a broker. Some of the most famous are Binance.com, Coinbase, Crypto.com, and Kraken.

1.2. Transactions

Transactions are the most important part of the bitcoin system (Antonopoulos, 2017), bitcoin is designed to ensure that transactions are created, propagated, validated, and added to the blockchain (the global ledger of transactions). Transactions are data structures that transfer value between participants, they are public, and they constitute the biggest part of each block size.

The fundamental building block of a bitcoin transaction is the *transaction output*. Transaction outputs are recorded on the blockchain and validated by the entire network. The representation of the money that a user possesses is given by the available spendable outputs referred to her, also known as *unspent transaction outputs* (UTXO). They are tracked by the network participants (full nodes) and the sum of all the UTXO of the user's wallet is the "balance" of the bitcoin she can spend or possess. In general, the wallet applications scan the blockchain transaction and aggregate the value of any UTXO that the wallet can spend with the keys that it has.

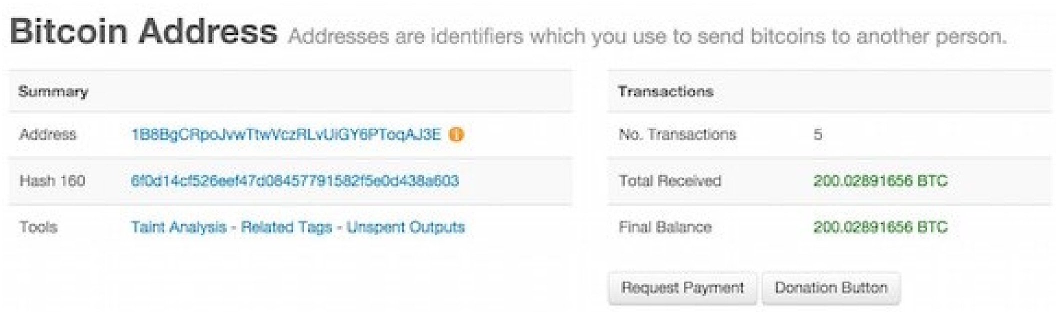


Figure 1.3: An example of a Bitcoin balance for an address.

On the other way, the transaction inputs identify which UTXO are consumed, but the owner of the UTXO needs to prove the ownership of them. This proof of ownership is done through an unlocking script, and it is usually a digital signature and a public key providing ownership of the bitcoin.

Transaction fees are an incentive for miners to include the transaction into the next block and a disincentive against the abuse of the system imposing a small cost for each transaction. The fees are calculated based on the size of the transaction not on the value in bitcoin meaning that sending high amounts of bitcoins is not more expensive than sending a small number of bitcoins. Miners prioritize transactions based on different criteria and transaction fees have a strong influence on that, this created a market economy for fees. Transaction fees are not mandatory but transactions without them are probably never going to be processed. It is important that transaction size and fees are well proportionated based on the user's time priority and market conditions.

In general, the transaction fees are below \$5 per transaction, nevertheless, in April 2021 the cost surged to an estimated average value of \$62.77. In this scenario the adoption of Bitcoin for daily commercial uses would be impossible. In the second quarter of 2021 the estimated transaction volumes reached a peach of over \$8.7 billion in a single day. In Q1 2022 the volumes are significantly lower also because of the decrease of the BTC/USD exchange price. Technically the number of transactions per day is limited by the size of the block (this will be explained in Section 1.5), hence the volumes depend mostly on the number of bitcoins exchanged per transaction.

1.3. The Network

Bitcoin is structured as a peer-to-peer network architecture on top of the internet. Peer-to-peer (P2P) is a term used for computers that participate in the network and they peer to each other. There is no server, no centralized system, no hierarchy in the network, the participants are nodes with equal privileges. Nodes in a P2P network provide, consume services, and at the same time model the P2P network in a shape that is resilient, decentralized, and open. Bitcoin is P2P digital cash system and this network architecture best constitutes the core values of the bitcoin system. The decentralized P2P consensus network allows the decentralization of control, and it can be maintained with a flat organizational structure. All the computers that participate as a node running the bitcoin protocol constitute the *bitcoin network*.

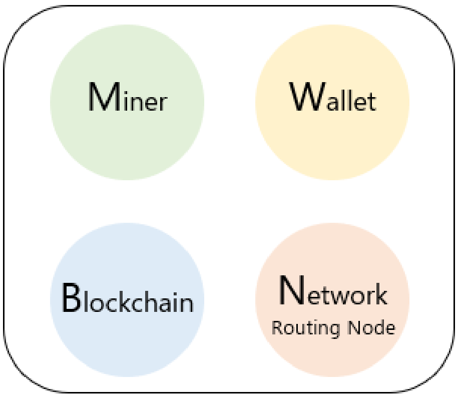


Figure 1.4: Bitcoin network node functions.

Nodes are equal but they can have different roles depending on the functionalities that are supporting. A bitcoin node can have different functions: mining, routing, storing the blockchain database or providing wallet services. Every node has a routing function, it is required to participate in the network and may include other functionalities. The nodes validate, propagate transactions, blocks and discover or maintain connections to other peers. The full nodes maintain a completely up-to-date copy of the blockchain and can autonomously and authoritatively verify any transaction without external reference. The nodes that maintain only part of the blockchain are called *simplified payment verification*.

Mining nodes, also called miners, are specialized in the creation of new blocks using the computational power of computer machines to solve the Proof-of-Work algorithm. Miners can store the full blockchain or not, it is not a mandatory requirement. There are also servers and nodes using specialized protocols that aggregate multiple miners in mining pools instead of solo working for a miner. User wallets can be part of a full node if they store all the blockchain and it is typically done by desktop bitcoin clients. However, user wallets that have limited resources such as smartphones are simplified payment verification nodes.

In recent studies (Park et al., 2019) measured the number of full nodes for each country and in the first place there was the United States with more than 30% of the all-network nodes followed by Germany and China. Today except for China the scenario is similar, the number of full nodes estimated is approximately 8,500 in 2018, however, there is an open discussion where the nodes should be more than 100,000.

1.4. The Blockchain

The blockchain, as the name may suggest, is a data structure similar to a chain in which the blocks of transactions are back-linked to each other. Each block is linked with the previous block in the chain forming a stack of blocks.

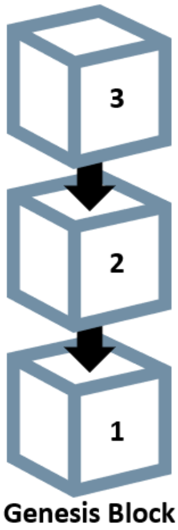


Figure 1.5: Stack of Blocks.

The "height" of a block refers to the distance from the first block, the *Genesis Block*, and the "top" block refers to the most recently added. Figure 1.5 is a simplified representation of a stack of blocks, the Genesis Block is the first block created by Satoshi Nakamoto on January 3rd, 2009, while the following blocks are linked to the previous.

A block is composed (Table 1.1) by a *block header*, containing metadata, and a long list of transactions that cover most of the block size. The maximum size of a block is 1 MB and this limits the maximum number of transactions that a block can have. Moreover, the creation of new blocks is limited by an algorithm that adjusts the difficulty of adding new blocks.

Every block is identified by a hash generated through a cryptographic algorithm. The previous block, known as parent block, is connected by having its own hash in the block header of the children. When the children's block header is hashed it clearly contains the reference of its parent block.

Size	Field	Description
4 bytes	Block Size	The size of the block
80 bytes	Block Header	Different fields from the block header
1-9 bytes	Transaction Counter	Number of transactions
Variable	Transactions	The transactions recorded in the block

Table 1.1: The structure of a block.

With this process a link between the blocks was created and it is going from the last one to the Genesis block. However, if any of the parent blocks change their identity, all the following children must change their identity as well. For this reason, when many blocks are added to the blockchain after the children (it has become great grandfather) changing the parent identity forces the recalculation of the following blocks, which requires an enormous number of computations.

The same blockchain concepts are applied in most of the blockchain used by other cryptocurrencies with small differences, for example, the Ethereum blocks are different, but the blocks are linked as Bitcoin does. The possible uses of blockchain technology cover many industries such as: finance, IoT, smart contracts, cybersecurity, cloud storage, blockchain government, real estate, and any other applications that need transparency, decentralization, immutable security, and a consensus-based system.

1.5. Mining

The validation of transactions done by the central authority is substituted by the mining process in the bitcoin system. Mining is the extraction of precious metals, and it focuses on the reward based on the quantity found. However, mining in the cryptocurrency world can be misleading, the reward is only an incentive for miners, the real role is to secure a mechanism for the basis of P2P digital cash.

The mining role is like a decentralized clearinghouse, validate and clear transactions. Miners record the new transactions on the global ledger, with a block containing them and added to the blockchain. Once a block is part of the blockchain, transactions are validated and users can spend the bitcoin received.

To sustain this process, miners receive two types of rewards: new coins and transaction fees every time that a block is added to the blockchain. For adding a new block, miners need to solve a complex mathematical problem based on a cryptographic hash algorithm. The *Proof-of-Work* proves that miners found this complex solution and they spent a significant amount of energy using expensive computer machines. This process, the Proof-of-Work is the basis of bitcoin's security model.

The mining reward causes the generation of new coins and it is how the bitcoin's money supply is increased, as mining for gold. There is no central bank that is printing money, only the reward can do it. The reward that a miner receives halves approximately every 4 years or after that 210,000 blocks are added to the blockchain. The reward started as 50 BTC per block and in November 2012 decreased to 25, in July 2016 to 12.5 and in May 2020 to 6.25. The number of halving is limited to 32 and it should last until approximately the year 2140, after the last halving miners will not collect any coin reward and receive only the transaction fees. Therefore, in 2140 the total amount of BTC issued will be 20.9999 million and it cannot be increased.

Every transaction can include a fee that is obtained by the difference between the transaction's input and output. For example, if Alice sent 0.20 BTC as transaction input and 0.15 BTC as transaction output to Bob, the remaining 0.05 BTC is the transaction fee left for the miners. Only the miner that adds the new block will receive all the transaction fees left by the users. In the last quarter of 2021, the transactions fees represent approximately 1,5% of the miners' revenues, as soon as the reward will decrease over time, the fees will be the largest part of the miners' revenues.

Today, miners use *application-specific integrated circuit* (ASIC) for the Proof-of-Work calculation (Figure 1.6). These rigs are designed with the only scope of solving the Proof-of-Work challenge, they cannot be used for any other purpose rather than this one. They are efficient machines that can compute an enormous quantity of calculations per second that completely overtake the general-purpose GPU and CPU.

Figure 1.6: ASIC Bitmain Antminer S9.

Only Bitcoin and other cryptocurrencies can use ASICs and they exist with different algorithms for solving the Proof-of-Work request. Ethereum miners do not use ASICs because the Proof-of-Work is designed to be *ASIC-resistant*, for this reason, miners typically use GPUs (Graphic Processing Unit). Therefore, Ethereum announced that at a certain point it will switch paradigm the mining paradigm to *Proof-of-Stake*[2] instead of Proof-of-Work making miners completely useless.

[2] The Proof-of-Stake is a different paradigm on how blocks are verified. It uses the machine of a cryptocurrency stake owner to validate blocks.

1.5.1. Creating a New Block

The block is constituted by the header and the transactions, for making a new block, miners need to aggregate validated transactions and create a new block header. The transactions sent by bitcoin users are validated by the bitcoin nodes and added to a *memory pool* or *transaction pool*, here the transactions wait until they are added into a new *candidate block*.

On the other hand, the new header's block needs to be filled with the field listed in Table 1.2. The field previous block hash is what links the new block with the previous, it is the component that keeps the blockchain connected. Target defines the level of difficulty for resolving the cryptographic problem by miners. The nonce is a counter used for the temps to find the solution of the problem.

Size	Field	Description
4 bytes	Version	Version number to track software protocols upgrades
32 bytes	Previous Block Hash	Reference to the hash of the previous block in the chain
32 bytes	Merkle Root	Hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate time creation of the block
4 bytes	Target	The Proof-of-Work algorithm target for this block
4 bytes	Nonce	Counter used for the Proof-of-Work algorithm

Table 1.2: The structure of the block header.

When all the fields of the header are completed except for the nonce, miners can start to race and find the solution. The goal of the miner is to find a value for the nonce that gives the solution to the problem.

The process of mining, in simple terms, is to hash the block header repeatedly, changing the nonce until the solution hash meets the target requirements. The hash function cannot be predicted in advance, or a pattern can create a specific hash value. This property of the hash functions means that a miner needs to try and try many times randomly changing the input (with the nonce) until he finds the exact solving hash.

The other nodes of the Bitcoin network can easily verify and validate the block using the same input data used by the winning miner. Once the block is validated by the network the winning miner can receive his reward. The reward is a *coinbase transaction*, a transaction written in the block newly created with the number of BTC rewarded that can be sent to any address. The dishonest miners who try to break the protocol's rules will have their block rejected losing the reward and wasting the energy used to find the solution.

In the crypto world, the *hashrate* refers to the number of hashes that are done in a second (H/s). ASIC rigs are typically described by using this unit of measure and by the algorithm that is used for hashing. For example, Bitcoin mining uses the SHA-256 hash function while the popular Dogecoin uses the Script algorithm. State of art Bitcoin ASICs can reach 100 TH/s while previous GPU models used for mining 400 MH/s.

1.5.2. Mining Difficulty

Bitcoin's blocks are generated approximately every 10 minutes regardless how much effort are putting miners into it. This property is designed by an algorithm that adjusts the difficulty according to the block generation pace. Technically, the algorithm adjusts the target increasing or decreasing the difficulty according to the speed of miners. This adjustment happens every 2016 blocks, it compares the ideal time to produce the blocks (20160 minutes) with the actual time to make them. If the time is lower than the ideal, the algorithm will increase the difficulty otherwise it will decrease it. The maximum limit for adjusting the difficulty is by a factor of 4. The difficulty adjustment is independent from the number of transaction or the value, meaning that the hashrate (the computational power) and electricity used is independent from the transaction. The bitcoin supply is also independent from the hashrate applied by miners, however, the hashrate in the network increases the network security by different types of attacks.

1.5.3. Blockchain Forks

The blockchain is decentralized and different copies can coexist simultaneously. Because a block can arrive at a different time to different nodes, certain nodes will have different views of the blockchain. The nodes will always resolve this issue by selecting the longest chain or the greatest cumulative work chain. If this rule is applied every node will select only one blockchain solving the problem of different blockchain *forks*. A "fork" occurs when two candidate blocks are competing to be added in the blockchain or when two different miners solve the Proof-of-Work at approximately the same time. Miners will send their solution immediately to the network starting from the neighbor nodes, however, if the two miners are far from each other some nodes will have different versions of the solution block.

The solution to solve the fork is simply a race to who will produce the longest chain to the blockchain. The remaining miners will choose one of the two winning blocks and will begin to solve the next block. This race will end when the winners beat the other miners and add to the blockchain the longest chain fork. The consequence of a fork is a waste of energy from the losers because they are not receiving any reward even though they found the winning block. In general, Forks are rare and the length is usually 2 blocks. For this reason, to be certain about a transaction confirmation a user should wait for 6 blocks, and for miners 100 blocks to be able to have access to the coin reward.

1.5.4. Mining Pools

The mining environment is extremely competitive, individual miners have almost no possibility to win, the solo miners are gambling like the lottery to have the chance to add a new block. For this reason, miners aggregate their hashing power to have more possibilities to find the winning block. When a block is found and the reward received, the mining pool splits their revenues proportionally to the hashrate provided to solve the problem, even without finding the block.

Mining pools coordinate many miners over specialized pool-mining protocols. In particular, the pool verifies the work done by every single member by assigning to them a range of the nonce and based on their results the pool will reimburse the members. There are different payment methods used by the pool to recognize the work done by the members. The *Pay-Per-Share* (PPS) method allows members to get paid even if the pool does not find the block, based on the *shares* of work that a miner has done he will receive a payment. A share is a hash that satisfies certain conditions imposed by the pool. Typically, the fees paid by members to the pool are higher compared to Pay-Per-Last-N-Shares (PPLNS) which pays the members only when a block is found. The PPLNS pays members proportionally to the shares sent to the pool.

The pools do not own the mining equipment and they cannot exert control over the miners, but they can decide to accept or not miners to be part of the pool. The top ten pools listed in Table 1.3[3] cover more than 96% of the total hashing power provided by the network.

Pool	Hashrate Share
Foundry USA	16.99%
AntPool	14.87%
F2Pool	14.85%
Binance Pool	11.45%
Poolin	10.86%
ViaBTC	10.76%
BTC.com	6.5%
SlushPool	5.76%
SBI Crypto	2.69%
unknown	2.25%

Table 1.3: Mining Pools Q1 2022.

1.5.5. Bitcoin Security

The solution created by the Proof-of-Work algorithm eliminates the double-spending of the same units of bitcoin used in a transaction, but it is not invulnerable. A *Consensus attack* is a scenario in which miners or pools by using their hashrate collude to attack Bitcoin. If most of the miners, the "51%" of the hashrate, join the forces they could mine most blocks, create deliberate forks and double-spend transactions or even execute denial-of-service (DOS) attacks against specific transactions or addresses. This attack affects only futures blocks and transactions.

However, this attack has never taken place in Bitcoin, because it would cause enormous losses to the whole Bitcoin Network. The price of Bitcoin will plunge to

[3] Data about pools was taken from https://btc.com/

a value close to \$0 and all the investments done by miners will be lost. Since there is no rational reason to make a consensus attack this has never happened. Increasing the hashrate of the network means increasing the level of security against this attack. Finally, for the other cryptocurrencies with low network hashrate it is important to attract miners in providing their computational power and increase the security.

2 Literature

The evolution of cryptocurrencies has caught the attention of academics, regulators, policymakers, central banks, and States. The popular opinion is divided between cryptocurrency advocates and opponents to cryptocurrencies. The central debate discussed in this work and between scholars concerns the cost of production of bitcoin, its value and its price. This thread created a new specific bitcoin mining literature.

2.1. Bitcoin's Literature

From the early days of bitcoin creation, the first significant literature about the cryptocurrency world began with the explanation of bitcoin innovation and its regulation (Grinberg, 2011). The role of the State is a necessary central point of coordination in society, and Atzori (2015) highlights the risk related to a dominant position of private powers in the distributed ecosystem. Regulatory issues are not only related to money-laundering but also to the taxation implication of cryptocurrencies, according to Marian (2013), cryptocurrencies could replace tax havens and be the "weapon-of-choice" for tax-evaders. Governments should pay more attention to this issue that seems to fail the identification of the acuteness of the potential problem.

Other studies (Ganadal et al, 2018) investigated the impact of suspicious trading activities and found that these trading activities have likely caused an increase of

BTC/USD price in late 2013 from a value of around $150 to $1000 in two months. Viglione (2015) suggests that bitcoin represents a disaster asset offering a new channel to evade domestic jurisdiction repression. Alternatively, Savelyev (2018) sustains that blockchain can introduce transparency in matters of copyright ownership chain and mitigate the risk of online piracy. Fletcher et al. (2021) describe the dispute on how to classify Bitcoin and determine an appropriate regulatory framework. As a result, there has developed an international mosaic of jurisdictional inconsistencies, with classification split mostly between a currency or an asset, and regulation ranging from an outright ban on Bitcoin usage to passive tolerance.

In parallel to the regulation, other studies focused on explaining bitcoin and blockchain technology. They were trying to falsify the accusation made by crypto opponents, as Harvey (2014) shows in addressing eight common claims about bitcoin and trying to separate the fact from the myths. He lastly concludes that bitcoin is not the best or ultimate model, but the idea of blockchain is not going away. More technical studies regarding the Bitcoin System and network (Feld & Werner, 2014) sustain the resilience of bitcoin of the Bitcoin ecosystem, the unambiguousness of the blockchain use, and the propagation and verification of transaction blocks. A critical aspect treated during the last years is the bitcoin energy consumption and carbon footprint, Stoll et al. (2019) in estimating the high energy consumption of the Bitcoin network suggests switching to a different protocol for cryptocurrency from Proof-of-Work to Proof-of-Stake reducing a large portion of CO_2 emission. However, the security that Proof of Work provides is exceptional (Rebello et al., 2021), there has been no successful attack on the protocol in more than 12 years of existence. Any other consensus that will replace it must prove this robustness to attacks.

2.1.1. Bitcoin's Econometrics Literature

The initial attempts in finding the economics behind Bitcoin began with the analysis of the price, Gronwald (2014) tested empirically the Bitcoin prices using an autoregressive jump-intensity GARCH model resulting that extreme price movements are a general behavior observed in immature markets. Using a period of observation of only 3 years from February 2011 and February 2014, he observed a high level of variance like the early stage of the crude oil market before 1986.

The first article that analyzed the bitcoin price formation in a tridimensional form is "The economics of BitCoin price formation" (Ciaian et al. 2016) considering at the same time: the traditional determinants of currency price, market forces of supply and demand and digital currency-specific factors. The analysis relied on testing three hypotheses. The first one on the Market forces of Bitcoin supply and demand recalling the fixed supply scheme behind bitcoin architecture as exogenous factor. The second the investment attractiveness considering different factors such as: news, security, number of views in Wikipedia, google research, and investment opportunities. Third the Global macroeconomic and financial developments captured by variables as stock exchanges indices, exchange rate and oil price measures in determining the bitcoin price. The empirical results confirm that market forces of bitcoin supply and demand have an important impact on Bitcoin price, in particular the demand side or the size of bitcoin economy have a strong impact on price. In the later periods the impact of news lost its effectiveness, and it cannot be rejected the hypothesis that investor speculations are also affecting the price.

2.2. Bitcoin's Mining Literature

The increasing popularity of cryptocurrencies together with the network users created the opportunity for focusing on detailed aspects of the cryptocurrency network as the important role played by the miners. Understanding the miners' environment became more relevant as more papers assumed that the computational power of the network is a fundamental value of cryptocurrencies.

In analyzing the large fluctuations of bitcoin price, Garcia et al. (2014) hypothesize that fluctuations were driven by the interplay between different social phenomena. For supporting the hypothesis, they assessed the fundamental value of bitcoin: the fundamental value of one bitcoin is equal to at least the cost involved in its production through mining. The cost of production was estimated through the number of bitcoins mined a day, the cost of energy and the efficiency of computer machines. The cost represents a lower bound for the bitcoin price. In particular, the cost is obtained by dividing the cumulated mining hashrate in a day by the number of bitcoins mined, this gives the number of SHA-256 hashes needed to mine one bitcoin. The power requirements are approximated to 0.5 W per MH/s, the average efficiency of the most common graphics processing units and the electricity cost as $0.15 kWh. This yields the fundamental value of bitcoin in BTC/USD. However, today these assumptions cannot hold anymore because of the differences in computational power and efficiency.

Further developments of this model were done by Hayes (2017). With the aim of identifying the likely determinants for cryptocurrency value formation, he presented a model to determine the fair value of a bitcoin-based on a formalized cost of production model (this model is analyzed in Section 2.3). By looking at the bitcoin mining efficiency over time, he highlights the rapid pace of technological advancement from 500 W per GH/s to 0.15 W per GH/s. Dividing the bitcoin mining equipment into 4 main eras of CPU mining, GPU mining, FPGA mining, and the latest ASIC mining. The latest type of mining machines started in late 2012 and it is today the only one used for bitcoin mining. It is important to note that in the pre-ASIC period the cost of the production model (CPM) does not hold, because the capacity utilization of a CPU or GPU to mine is simply not efficient enough. One would not expect the marginal cost to converge to marginal product when the hardware being used is not subject to competition.

In a second paper Hayes (2019), tested empirically the model proposed using data from June 2013 to April 2018. After estimating a new average energy efficiency miner hardware and stating the electricity cost at a constant value of $0.135 kWh, the cost of production model price prediction was compared with the observed price. Testing the result with a conventional OLS regression and a more rigorous multivariate vector autoregression (VAR), gave interesting results: the price of bitcoin tends to fluctuate around the model price, and with the model price predicting the market price in a statistically significant manner. Furthermore, the findings suggest that the attempts to find a correlation between the price and exogenous factors may be misguided.

Song and Aste (2020) estimated the lower bound mining cost by focusing on the energy cost of mining, thus it is excluding from the analysis the overheads for the maintenance of the mining farm and the cost of purchasing and renewing the mining hardware. The reasons for this simplification are that the maintenance costs for running a Bitcoin mining farm vary widely depending on the location, the sales price of mining hardware cost calculations is arduous because of the rapid rate of evolution in the industry and the information opacity regarding the market share of each hardware and the rate at which obsolete mining hardware is replaced. The maintenance and the hardware costs must be anyway proportional to the energy consumption costs. Ignoring them means underestimating the total mining costs, but the estimation of the overall behavior of the mining costs should not be significantly affected. The approach used is different from previous works, the energy consumed during bitcoin mining is converted into barrels of oil equivalent, the rationale behind is that the Brent Crude oil price is a publicly available daily value standardized around the world whereas electricity prices vary widely across different countries and suppliers. Considering at any point in time that the entire network is adopting the most energy efficient machine available at that time, the estimations give a lower bound cost of mining.

Alternatively, Prat and Walter (2021) proposed a model that predicts the computing power of the Bitcoin network given the BTC/USD exchange rate and highlighted that investment in mining hardware has two important characteristics. First, it cannot easily be reversed because machines have no resale value, they have been optimized for mining only. Second, the uncertainty about future revenues due to the extremely high volatility of the BTC/USD exchange rate. Taking into account how returns are endogenously determined by the whole mining network and combining the BTC/USD exchange rate with the total computing power of the Bitcoin network, Prat et al construct a new variable that measures miners' payoffs. The model predicts that miners buy new hardware only when the payoff measure reaches a reflecting barrier, considering that payoffs never exceed this threshold because new entries trigger increases in the difficulty of mining which pushes revenues down. The forecasts on how miners respond to changes in the BTC/USD exchange rate are a testament to the fact that miners operate in a market where perfect competition is a good approximation of reality. As a matter of fact, free entry holds because mining is not prevented by any regulation and does not require any specific skill. Miners face the same problem and earn the same rewards. The mining technology returns to scale are constant by nature and the elasticity of demand for computing power is commonly known.

The approach used by Kjærland et al. (2018) to enhance the understanding of which factors affect the price development of Bitcoin. Using an Autoregressive Distributed Lag (ARDL) and Generalized Autoregressive Conditional Heteroscedasticity (GARCH), the models estimate the short and long-term effect of potential drivers of Bitcoin. The dependent variable is the BTC/USD exchange rate and the explanatory variables are the hashrate, the total output volume of Bitcoin, S&P 500, Gold, Oil, VIX, and Google search on term “Bitcoin”. Increasing the processing power should in theory lead to an increased supply and exerts downward pressure on prices but adding more processing capacity to mining does not affect the output. Therefore, the authors believe that the causality between Bitcoin and hashrate is that Bitcoin price drives hashrate, not the other way around. In contrast with other studies, hashrate is irrelevant as an explanatory variable in models describing Bitcoin’s price drivers or fundamental values. However, past price performance, optimism, and Google search volume are significant in explaining Bitcoin prices. The optimism in financial markets and attention to Bitcoin push investors’ willingness to allocate funds to more risky assets like Bitcoin.

Starting from addressing the valuation of Bitcoin as a decentralized network Pagnotta and Buraschi (2018) characterized the demand for bitcoins and the supply of hashrate. From this analysis emerged an interesting theory of the Price-hashrate “spirals” that amplifies the demand and supply shocks. For example, a drop in the expected number of future network users will reduce the expected value of bitcoin. As a consequence, the price drops and reduce the economic incentives for miners to provide hashrate and reduce the network trust. The expected value of bitcoin drops again, and it puts additional pressure on Bitcoin prices. This loop continues until a new equilibrium price and hashrate are achieved. The authors also state that in perfect competition the mining costs become a constant proportion of the Bitcoin price, and that proportion depends only on the properties of the cost and not on other parameters of the hashrate supply environment. In contrast with previous studies, the authors sustain that the cost of mining bitcoin does not serve as a "price floor" because an increase in the marginal cost of mining induces miner to provide less hashrate, which reduce network trust and price.

The dynamics and interaction between Bitcoin price and mining cost have become of major interest. Kristoufek (2020) studied the connection between these two variables, concluding that they tend to a common long-term equilibrium. Mining cost adjusts according to the Bitcoin price with a time lag of several months up to a year. Sustaining that in this new era of bitcoin the electricity cost and mining efficiency play the primary role. By studying the cointegration relationship between price and costs of Bitcoin and implementing a vector error-correction model (VECM) the author concludes that bitcoin price drives mining cost and not the other way around.

Similarly, Fantazzini and Kolodin (2020) investigate the relationship between the bitcoin price and the hashrate. The purpose of the work is to explain the contradiction in the literature about the dynamics of bitcoin price using econometrics models and different sets of explanatory variables. In particular, the conflict about the significance of the hashrate in predicting the bitcoin price. The discrepancies between these results can be the different periods of time or the hashrate complex relationship. Based on these issues, two types of models were created: a bivariate model analyzing the relationship between hashrate and market price and the cost of production model (Hayes) and market price. A multivariate model including different explanatory variables and market price. For every model, each variable was tested for unit root, if there is one a significant break is found, and the sample is divided in two subperiods. The bivariate models were tested for cointegration. Finally, all subsamples were tested for Granger causality. The results of Granger-causality have shown no cointegration in the first sample (01/08/2016–04/12/2017), whereas in the second sample (11/12/2017–24/02/2020) there was evidence of unidirectional Granger causality and cointegration going from the bitcoin price to the hashrate (or to the CPMs) but not vice versa.

2.3. Cost of Production Model

Hayes (2017) introduced the cost of production model (CPM) for Bitcoin assuming that its value is explained by the cost of producing bitcoins. This approach attempts to derive the bitcoins cost of production for an individual miner. Considering the current state of the network, the energy prices, and the energy efficiency of the miner's equipment the CPM estimates the break-even cost of mining. The break-even cost is used to determine whether he should be involved in mining bitcoin.

The first assumption of his model relies on the value of computational power of the network as the main driver for bitcoin price. The higher is the computational power or *hashrate*, the higher would be the bitcoin price. In general, a cryptocurrency that does not have any computational power would have no value[4].

The second assumption is that miners are rational agents, meaning that they are willing to mine only if it is profitable. In particular, an individual would mine if the marginal cost per day were less than or equal to the marginal product. If bitcoin production is a competitive commodity market, theoretically the expected marginal cost is equal to the marginal product that is also equal to the selling price.

[4] This assumption is valid only for cryptocurrencies that uses the Proof-of-Work paradigm.

The main cost in bitcoin mining is energy consumption, however other costs are much smaller for example the costs of internet service, hardware maintenance, computer cables, warehouse expenses, which can be regarded as negligible. Therefore, the most important variables for the miners' decision to mine are the cost of electricity, the energy consumption per unit of mining effort, the monetary price of bitcoin in the market, and the difficulty of the Bitcoin algorithm.

The last assumption concerns the relationship between the network difficulty and the aggregate mining power. The difficulty of mining a block can be converted into a proxy of the hashrate used to mine a block. According to the Bitcoin protocol this assumption can hold, since the difficulty is adjusted, increasing or decreasing the number of expected hashes required to mine a block, in accordance with the production block time that must be constant at 10 minutes.

The first step for building the connection between computational power and expected profit for a miner is to estimate the expected number of BTC to be mined per day on average given the difficulty and block reward per unit of hashing power:

$$\frac{BTC}{day} = \left(\frac{\beta\rho \cdot sec_{hr}}{\delta \cdot 2^{32}}\right) hr_{day} \tag{2.1}$$

Where BTC/day is the expected level of daily bitcoin production, ρ is the hashrate employed by a miner (GH/s), β is the block reward (BTC/block), δ is the difficulty expressed in units of GH/block. The constant sec_{hr} is the number of seconds in an hour. The constant 2^{32} relates to the normalized probability of a single hash solving a block and is an attribute of the mining algorithm.

The main cost per mining is given by the energy used to perform the double SHA-256 computations by the ASICs machines. Heyes expresses the cost of mining per day E_{day} as:

$$E_{day} = \left(\frac{\rho}{1000}\right)\left(\frac{\$}{kWh} \cdot \frac{W}{GH/s} \cdot hr_{day}\right) \tag{2.2}$$

Where E_{day} is the dollar cost per day for a producer, ρ the hashrate is set a 1000 GH/s, the $/kWh is the dollar price per kilowatt-hour, and W/GH/s is the energy consumption efficiency of the producer's hardware.

According to established microeconomic theory, in a competitive market, the selling price is equal to the marginal cost. From Equation (2.2) cost per day is expressed in $/day and in Equation (2.1) the production in BTC/day, the $/BTC price level is simply the ratio of (cost/day) divided by (BTC/day). The resulting price, P, serves as a logical lower bound, below which a miner would operate at a marginal loss and presumably remove herself from the network. P is expressed in dollars per bitcoin, given the difficulty and cost of production:

$$P = \frac{E_{day}}{BTC/day} \tag{2.3}$$

Equation (2.3) calculates the fair value, P, for bitcoins. However, it simplifies the mining expenses removing the cost of the capital and the operational costs. It also neglects the bitcoin halving events, which miners can clearly predict and change the decision-making behavior of miners.

The model requires some inputs that cannot be directly observed or reliably approximated for example the *electricity cost* that is assumed constant equal to $ 0.135 per kWh. It can drive misleading results, because of the different locations and energy sources used by miners the price can largely change. The other input is the *mining computers' energy efficiency*, despite Bitcoin miners use only ASIC machines there is a variety of models that differs from the efficiency standpoint.

On the other hand, given an observed market price (P) and a known difficulty, it is possible to solve the break-even electricity cost per kilowatt-hour:

$$\frac{\$}{kWh} = \left(\frac{P\left(\frac{BTC}{day}\right)}{hr_{day}}\right)\frac{W}{GH/s} \tag{2.4}$$

Given a known cost of production and observed market price, one can solve for a break-even level of mining difficulty:

$$\delta = \left(\frac{\beta\rho \cdot hr_{day} \cdot sec_{hr}}{2^{32}E_{day}}\right)P \tag{2.5}$$

However, Equation (2.5) offers small interest since the difficulty is observable and based on a more precise algorithm. Finally, solving for a break-even hardware energy efficiency and rearranging the terms given a market price, cost of electricity per kilowatt-hour, and difficulty:

$$\frac{W}{GH/s} = \left(\frac{P\left(\frac{BTC}{day}\right)}{\frac{\$}{kWh} \cdot hr_{day}}\right) \tag{2.6}$$

These Equations (2.3), (2.4), (2.5), and (2.6) can be useful as they inform miners objectively: to what price they should mine or not, to stop or start mining given changes in difficulty and electricity costs. Furthermore, traders can estimate an expected price given knowledge of the input variables given the market prices for a certain difficulty and known average electricity cost, the average energy efficiency of equipment for the entire network can be imputed.

The empirical evidence using the cost-of-production model, in particular referring the Equation (2.3), shows that the market price from June 2013 to September 2017 tends to fluctuate about the price estimated. The average ratio between observed and estimated price is 1.04 with a $\sigma = 0.3$, which is noticeable accurate. The increased volatility from September 2017 through January 2018 indicates the emergence of a price bubble and the resolution in January 2018.

2.3.1. Cost of Production Model Critics

The bitcoin halving happens every 210,000 blocks or approximately every four years and divide the block reward in half. The CPM does not account for this effect; however, miners are aware of it and anticipate it. Therefore, the market price does not change significantly near the times of halving, whereas the CPM shows a sudden break in its equilibrium price.

Fantazzini and Kolodin (2020) tried to replicate and extend the Hayes' estimated energy efficiency by web scraping data from the previous "Mining hardware comparison" webpage. However, the energy efficiency estimated by Hayes (2019) with the scraped ASIC data shown some anomalies: at the end of 2015 and until the beginning of 2016, the estimated energy efficiency suddenly changes but the ASIC release data do not. Moreover, during the first months of 2018, several new releases were introduced but the estimated energy efficiency always stays above these releases. In Addition from what Kjærland et al (2018) already criticized, and Fantazzini and Kolodin (2020) proven, the model is not considering the transaction fees which cannot be completely excluded since during certain periods (e.i.

December 2017) the transaction BTC paid as a fee reached a peak of 1,496 BTC in a day almost the same amount of BTC that was earn though mining.

Finally, if the price of bitcoin is always equal to marginal cost of production in the long-term, they will suffer losses and miners will leave the market, not considering the fixed costs and the cost of the machines will always bias the model toward a lower cost of production and lower price of bitcoin.

2.4. A New Development of The Cost of Production Model

The new CPM which includes investments in mining hardware requires additional considerations and assumptions to deal with the cost of bitcoin production. This new model provides a complete overview of the profit function for miners and describes with greater precision the behavior of miners. The break-even price and other variables obtained by this new model can be estimated and analyzed together with the Bitcoin price. Considering only the cost of energy is an assumption that capture only marginal costs. The ASICs machines, the buildings, the energy factories, and the workers' salaries have a significant influence on the overall cost of production of bitcoin. In particular, as the ASIC rigs become more and more efficient[5] and miners build renewable energy factories, the cost of energy becomes less relevant, and the cost of the machines and buildings takes the lead. However, miners' costs can be simplified into two major components: energy costs and computer machines costs, for simplicity they will be called investment costs. The energy cost is given by Equation (2.2) while the cost of the investments for the

[5] State of art machines as Antminer S19 XP has an efficiency declared at 0.0215 kJ/TH, while the first machines released in 2013 (i.e Antminer S1) has an efficiency of 2 kJ/TH.

machines requires different assumptions. The CPM is based on the daily cost of energy, but the daily time-frequency is not matching the Bitcoin frequency of changing the difficulty: the time required for producing 2016 blocks. This is the interval in which the Bitcoin algorithm adjusts the difficulty according to the speed of production. The time-frequency can change over time, but the blocks produced are always 2016 and the difficulty of bitcoin mining is constant during this period. This change allows a clear estimation of the average hashrate, instead of estimating it day by day based on the theoretical daily production (144 blocks) that can lead to error because certain days can have different difficulty, hence the hashrate must be adjusted. Changing the time frequency requires Equation (2.2) to be adjusted:

$$E_t = \rho_t \cdot k_t \cdot EEF_t \cdot n_t \cdot 24h \qquad (2.7)$$

Equation (2.7) expresses the costs of energy required in the period of producing 2016 blocks. Where in this equation ρ_t is the average hashes per second applied by the entire network. Note that the same equation is true for a miner if we assume ρ_t has a determined value. The n_t parameter is the number of days required for producing 2016 blocks and not the theoretical 14 days (n_t also expresses the fractional part of the last day). EEF_t is the energy efficiency of the machines. The parameter k_t is the cost of electricity $\frac{\$}{kWh}$, it is kept at a constant value (other assumption are explained in section 3.4). Alternatively, to Equation (2.2) the hashrate is not limited to 1000 GH/s but it is taken the entire network hash power.

On the other hand, the additional assumptions that investment costs require are three. The first assumption is: *an increase in the hashrate that surpasses its maximum level is caused by the investments in new ASICs*. The investments in ASICs machines are recorded when the entire network hashrate surpasses its maximum value. In this scenario where there is a maximum hashrate level reached by the network, a decrease in the hashrate will not change the sunk investments. Hence, the investment costs take into account the previous investment done in the network even if the machines are turned off and miners are still paying for them.

The second assumption is*: the investment costs are divided according to the useful life of the machines*. The Investment costs represent the deprecation costs sustained for each period. The Investment costs work similarly to a leasing, after signing a 3 years contract, miners pay the same amount until the end of the useful life of the machines. There is no interest to be paid since this amount represents the daily depreciation of the machines.

The last assumption is: *at the end of the machines' useful life their hashrate is replaced by new machines' hashrate*. The hashrate produced by old ASICs are replaced with the hashrate produced by new ASICs. Only after 2 years the old machines are replaced with the new ones and starting in June 2016, thanks to more efficient ASIC models, the useful life is extended to 3 years[6]. In general, new ASICs can produce more hashrate per machine, so miners will need less machines but the cost per machines can be higher. For this reason rather than estimating the number of machines and converting them in hashrate produced, the model simply considers the cost per TH. The cost per TH is the cost associated to buying one TH (more information is described in Section 3.3).

These assumptions give more flexibility if compared with reality since the investments are like a leasing. Nevertheless, after that miners have invested, they cannot disinvest anymore and must pay for the machines. ASIC machines are extremely specific purpose machines, and they cannot be used for other scopes

[6]According to "The Bitcoin Mining Network" (Bendiksen and Gibbons, 2018) the useful life of machines is estimated using different depreciation schedules, 18, 24, and 30 months but most of the company mining companies depreciate the ASICs in 3 years. In 2019 some companies were still mining with Bitmain Antiminer S9 (release date June 2016).

other than mining a specific cryptocurrency, therefore the value after the useful life is substantially zero. For capturing the effect that new machines are purchased only when a new hashrate maximum is reached, the hashrate function used for the estimation of the investment costs is expressed as:

$$\Delta\vartheta_t = \Delta\rho_{t+l}^{max} \tag{2.8}$$

Where the term $\Delta\rho_{t+l}^{max}$ represent the increase in hashrate of the maximum function of the hashrate (ρ_t^{max}), l express the lag between the purchase of the machines and their installation and full deployment of their hashrate in the network. Note that the expression $\Delta\vartheta$ is always positive.

Given the cost per TH/s (c_t), the investments costs paid by miners during the period of producing 2016 blocks can be calculated as:

$$I_t = I_0 + \sum_{j=1}^{t}(c_j\Delta\vartheta_j)\frac{n_t}{d_t} \tag{2.9a}$$

$$I_t = \sum_{j=-r}^{t}(\Delta\vartheta_j c_j + \Delta\vartheta_{j-r}c_j)\frac{n_t}{d_t} \tag{2.9b}$$

Equations (2.9a) and (2.9b) express the amount of investment spent by miners during one period. Equation (2.9a) considers an initial value I_0, the product between the initial ϑ_0 and the estimated cost per TH of the previous machines (c_0) (other assumption are explained in section 3.8). Equation (2.9a) is used for the first 2 years (for instance from t=1 to t=57) of the model until the machines are not replaced. The parameter c_t is the average cost per TH/s at time t (other assumptions will be described in Section 3.3). After replacing the first machines (t=58), Equation (2.9b) is used for calculating the investment costs, the term $\Delta\vartheta_j c_j$ reflect the investment in new machines caused by the increase in hashrate, while the term $\Delta\vartheta_{j-r}c_j$ reflects the amount of hashrate replaced by new machines. In particular, the r index is used to express the lag of the useful life of the machines, meaning that the old machines purchased at time $t - r$ are replaced at time t with new machines paying a cost per TH equal to c_t. The parameter d_t is the number of deprecation days expected for the machines. This value starts at 730 and changes after June 2016 in 1095.

Considering revenues and assuming that miners are exchanging all the bitcoins mined during the period since every period has 2016 blocks and the block reward is constant for 210,000 blocks, by taking the average price of bitcoin during the period and the cumulated transaction fees, revenues can be easily calculated as:

$$R_t = (2016 \cdot \beta_t + F_t) \cdot P_t \tag{2.10}$$

Where F_t is the cumulated value of transaction fees in BTC, P_t is the average exchange price in USD for the period of 2016 blocks, and β_t the number of bitcoins received per block. Relaxing the assumption that miners can also do not exchange the mined bitcoins during the period and use future contracts is a possible dynamic that is not covered in this work. Having revenues and the costs is possible to write the profit function for miners, as well as to retrieve the break-even price of bitcoin:

$$\pi_t = R_t - E_t - I_t \tag{2.11}$$

Note that this is the profit function considering all the miners of the network. Solving for the price of Bitcoin and having $\pi_t = 0$, we obtain the break-even price P^*:

$$P_t^* = \frac{E_t + I_t}{(2016\,\beta_t + F_t)} \tag{2.12}$$

The break-even price adjusts immediately after a halving event, and it almost doubles the price. The halving event is known by miners know and it decreases their profitability. The only action that can take for maintaining the same revenues is to increase the Transactions Fees. Unfortunately, adjusting the model for dealing with halving events requires changes in the previous assumption, hence this issue like the CPM stays in this new model and is left for other studies

3 Dataset

The CPM described in Section 2.4 requires specific data construction and assumptions to estimate the key parameters necessary to calculate the Investment and Energy costs. This chapter focuses on the explanation of these parameters and the construction of the dataset. Differently from the previous CPMs, new variables are presented for having a complete analysis of the relationship between the price and costs.

3.1. Difficulty and Hashrate

The difficulty of Bitcoin can be retrieved using the target value present in every block header. Data about difficulty was taken from the website btc.com a reliable website used in other studies as well. The dataset interval goes from 24/01/2014 to 03/03/2022 for a total of 221 observations. The product between the difficulty and 2^{32}, the constant normalized probability, gives the number of attempts of hashes required per block. The hashrate per second of the network is estimated using the difficulty and the time for producing 2016 blocks. The ratio between the ideal time of producing 2016 blocks and the actual time spent is a good proxy of the average block production pace. If the ratio is lower than one the production pace of block is slower than the ideal 10 minutes, whereas if it is higher than one the time is shorter, meaning that the hashes per block applied in the network is higher than the hashes per block prescribed by the difficulty. The equation used for calculating the hashrate of the network is expressed as:

$$\rho_t = \frac{20160\,minutes}{\varphi_t} \cdot \delta_t \cdot 2^{32} \cdot \frac{block^*}{s} \tag{3.1}$$

Where φ_t is the time in minutes between two periods, while 2^{32} is the constant that normalized probability of a single hash solving a block and it is an attribute of the mining algorithm. The parameter $\frac{block^*}{s}$ was introduced for converting the hashes required per block to hashes per second. It is given by the ratio between one block and the theoretical time required in second:

$$\frac{block}{s} = \frac{1}{600s} \tag{3.2}$$

Equation (3.2) gives the average part of a block that is mined in a second. Note that if the production time ratio of the blocks is higher than one means that in a second the network is mining more than the ideal 0.166% of the block. Similar equations for calculating the hashrate per second are used by different websites, for example, blockchain.com in estimating the hashrate per second calculates the average time between mined blocks instead of the product between block per second and the production time ratio, obviously the results are the same. Figure 3.1 show the hashrate time series plot obtained by using Equation (3.2) and Figure 3.2 the difficulty. The hashrate is estimated through the difficulty, meaning that the hashrate and the difficulty have the similar fluctuation because of the direct relationship between the variables, the difficulty follows the hashrate.

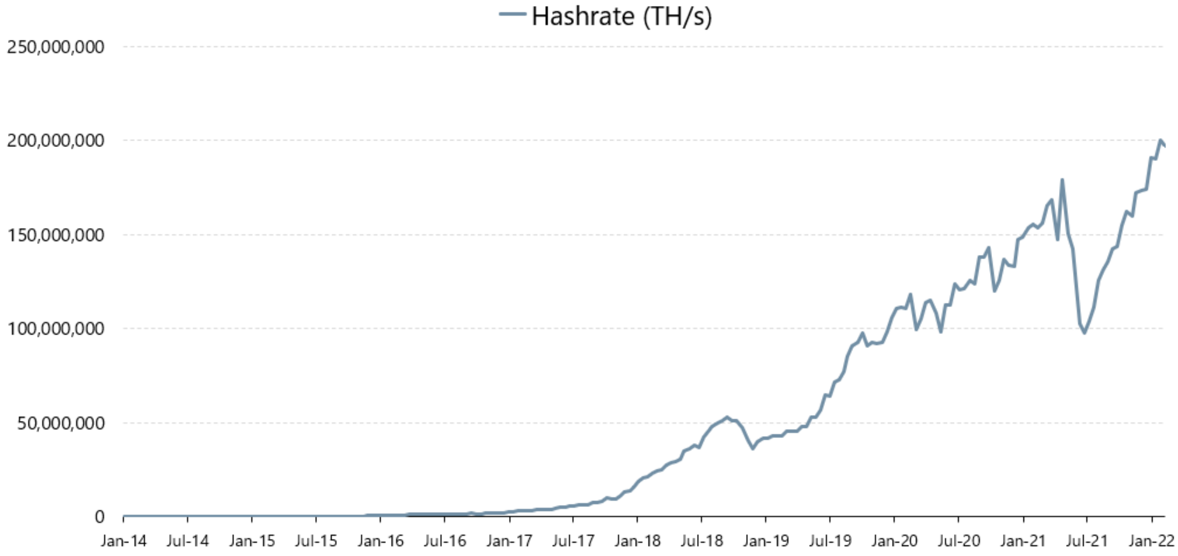


Figure 3.1: Hashrate time series Plot.

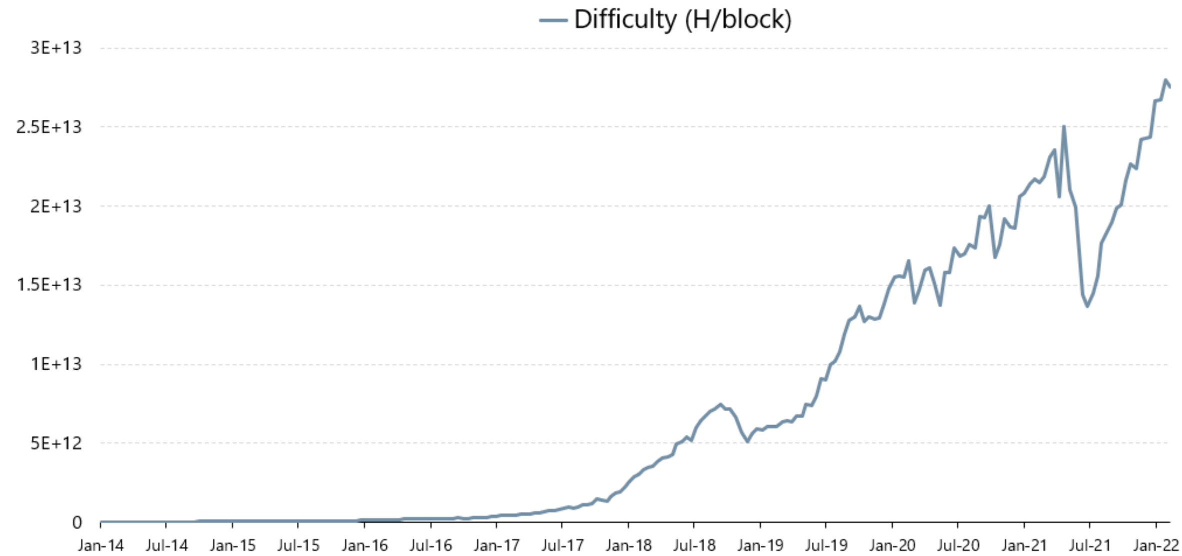


Figure 3.2: Difficulty time series Plot.

3.2. Energy Efficiency

One of the biggest challenges of the model is the correct estimation of the mining energy efficiency (EEF_t) of the network. The history of bitcoin mining hardware evolved until ASICs came into the market, their arrival completely outperformed the other hardware used for mining. At the beginning of 2013, the first ASIC machine was developed by the Chinese company Canaan Creative and was able to produce 0.063 TH/s[7] with an average consumption of 620 Watts. At the same time, the best FPGA machines were able to reach 0.02 TH/s with a similar amount of power consumption. This boost in efficiency increased the hashrate of the network enormously in a single year. For this reason, this work does not cover previous mining energy efficiency, the technology evolution has completely changed the role played by the previous hardware and their efficiency is hard to estimate.

3.2.1. Energy Efficiency Curve Construction

For the EEF_t calculation, the hardware used as a reference are ASICs produced by the company Bitmain, which has proven to be the market leader in this sector[8]. The first model released was in November 2013 (Table 3.1) and was offering a much higher efficiency than the previous competitor model.

From Antminer S1 to Antminer S9, the data was taken from https://en.bitcoin.it/wiki/Mining_hardware_comparison, while for the other ASICs from https://www.asicminervalue.com/. The Price of the ASICs from S15 to S19 XP was obtained by announced transactions done by mining companies or when it was possible the release price announced by Bitmain.

[7] The machine is the Avalon Batch 1, released in January 2013 at the price of $1,299 (Bevand, 2013).
[8] In 2018 the bitmain market share was approximately 75% (Olsen, 2022), other articles sustain 66% (Khatri, 2019).

According to Fantazzini (2019), a reasonable time used for the deployment in the market of a new ASIC goes from 2 to 3 months, this behavior is described by assuming a delay of approximately 90 days between the purchase date and the time of actual increase of the hashrate.

	Release Date	Hashrate (TH/s)	Power (W)	Price (USD)	Energy Efficiency (kJ/TH)	Cost per TH/s (USD/TH/s)
Antminer S1	Nov 2013	0.18	360	300	2	1,666.67
Antminer S2	Apr 2013	1	1100	2,260	1.1	2,260
Antminer S3	Jul 2014	0.478	366	382	0.766	799.16
Antminer S5	Dec 2014	1.155	590	370	0.511	320.35
Antminer S7	Sep 2015	4.73	1293	1,820	0.273	384.78
Antminer S9	Jun 2016	11.5	1127	2,400	0.098	208.7
Antminer S9	Sep 2017	13.5	1323	2,400	0.098	177.78
Antminer S15	Dec 2018	28	1596	1,475	0.057	52.68
Antminer S17	Apr 2019	53	2385	1,886	0.045	35.58
Antminer T17	May 2019	40	2200	1,270	0.045	31.75
Antminer S19	May 2020	95	3250	2,180	0.0342	22.94
Antminer S19Pro	May 2020	110	3250	2,920	0.0295	26.54
Antminer T19	Jun 2020	84	3150	1,749	0.0375	20.82
Antminer S19j	Jun 2021	90	3250	3,300	0.0361	36.67
Antminer S19XP	Jun 2022	140	3010	11,200	0.0215	80

Table 3.1: List of Bitmain ASIC models.

Alternatively from Fantazzini (2019) the overall EEF_t is built using a linear interpolation of the Bitmain models. Because of the better efficiency of these bitmain models, the efficiency was adjusted by increasing the EEF by 10%[9]. The linear coefficient is constructed by calculating the ratio between the difference in the efficiency of the ASICs and the difference in days from the release date.

$$linear\ coeffcient_1 = \frac{EEF_2 - EEF_1}{release\ date_2 - release\ date_1} \tag{3.3}$$

Equation (3.3) is an example showing how the linear coefficient was calculated for the first and second models. Note that the difference is in days, meaning that the constructed EEF curve is not matching the time frequency of the 2016 blocks. To solve this issue for each period is expressed the average EEF of the interval.

The models S17 and T17, as well as the S19, S19 Pro and T19 were released approximately during the same period, and because they belong to the same series instead of interpolating every single model the interpolation is constructed by using a machine representing the series. This machine is an average in hashrate, power, and price similar as the market share between the model were equal during the period.

3.2.2. Weighted Energy Efficiency

The EEF of the network changes with the purchase of the new machines, in particular, the EEF of the network is the weighted average energy efficiency (WEEF) between the old machines that are producing a determined hashrate and the new machines that are providing additional computational power.

[9] The weighted average of EEF considering the Bitmain ASIC having a market share of 70% and the other competitors 30% is approximately 10% higher than the EEF of the Bitmain models.

The estimation of the starter value WEEF follows a similar process: during the period from April 2013 to February 2014 the difficulty increased by approximately 340 times, and according to the logic of the model, this enormous increase in hashrate is fully attributed to the first ASIC (Canaan Avalon 1). Even though this increase cannot be practically attributed to the best hardware available at that time, similar ASIC models were released and assuming that the new hashrate is provided by the first Canaan model is not unrealistic.

Considering a high value of EEF of a low performance FPGA (70 kJ/ TH) and the tremendous increase in hashrate, the WEEF between the FPGA and the Canaan ASIC causes the WEEF to drop approximately by 76%. The total amount sold of the first Canaan ASIC was not enough to cover the entire increase, however in the same period other ASICs with similar specifications came into the market, hence the Avalon 1 is just a referring model for the others. Using as a starting value for the WEEF the best EEF offered by the market weighted with a low-performance FPGA, the resulting value will provide a lower bound for the energy cost. This initial estimation error will be adjusted by the model through the weighted correction mechanism and the replacement of old ASICs.

The model assumes that ASICs are replaced after 3 years or 1095 days with the last generation machines. However, the first generation of ASICs was enormously more inefficient than 2 years newer machines (from 2 kJ/TH to 0.27 kJ/TH), for this reason, the useful life is reduced from 3 years (adopted by many mining companies) to 2 years. The first machines with a useful life of 3 years start from the Antminer S9 ASIC models which shows a great efficiency performance even compared with newer ASICs.

The replacement of the machines affects the WEEF by decreasing it faster. The EEF is expressed in $\frac{kW}{TH/s}$ and is obtained as:

$$WEEF_t = \frac{EEF_t \Delta\vartheta_t + WEEF_{t-1}\vartheta_{t-1} + [EEF_t \Delta\rho_{t-r} - EEF_{t-r}\Delta\vartheta_{t-r}]}{\vartheta_t} \tag{3.4}$$

In Equation (3.4) the WEEF changes only when new ASICs are used by the network or when old ASICs need to be replaced. In particular, the expression in the square brakes represents the replacement of the hashrate of old machines with the new machines. Table 3.2 shows an example of the estimation of the WEEF for the period 07/02/16 to 04/03/16.

	ρ_t (TH/s)	$\Delta\vartheta_t$ (TH/s)	$EEF_t\left(\frac{kW}{TH/s}\right)$	$WEEF_t\left(\frac{kW}{TH/s}\right)$
07/02/16	1,031,472	173,197	0.248	0.656
19/02/16	1,169,612	138,139	0.239	0.599
04/03/16	1,169,612	0	0.229	0.595

Table 3.2: Example of WEEF estimation.

Note that on 04/03/16 the hashrate did not increase but the WEEF decreased because the machines that were working from 28/02/14 (2 years old machines) are now replaced with new ASICs machines. Figure 3.3 shows the WEEF of the network from 21/01/14 to 03/03/2022, the bitmain antminer ASIC models are the blue dot. The estimated WEEF is slightly more efficient than the one obtained by Hayes (2019) and similar to the Kristoufek (2020) from late 2017.

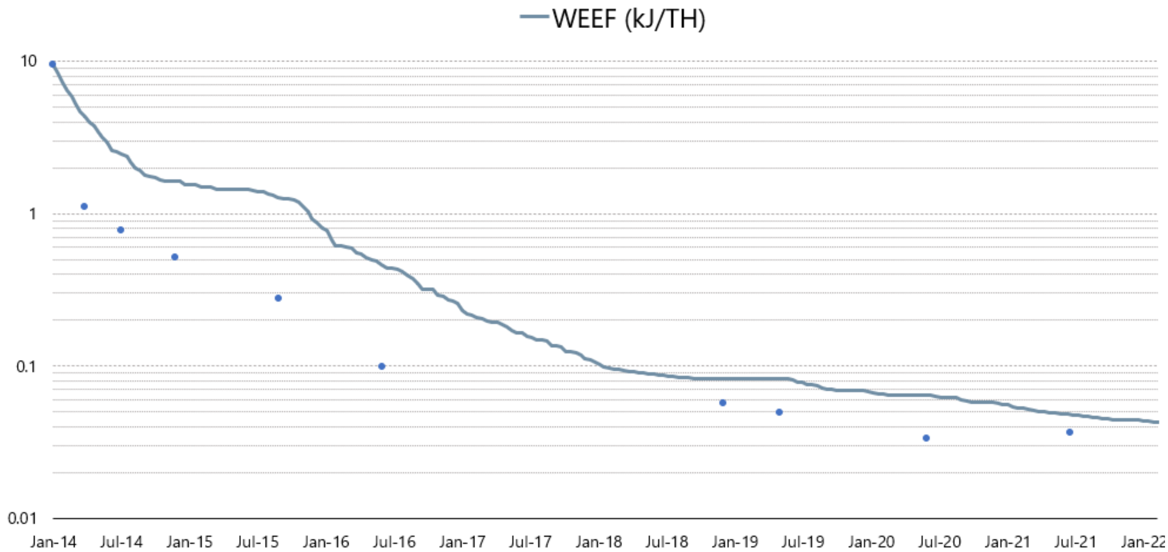


Figure 3.3: WEEF Chart.

3.3. Cost of Hashrate

The cost per hashrate is expressed by the parameter c_t ($\$/\ TH/s$) that indicates the amount of dollars required for buying the computational power equivalent to one TH/s and it is obtained by the ratio between the price of ASIC and its declared computational power. Similar reasoning and logics applied for the EEF_t are also being applied for the cost per hashrate and the difference in this approach is that the cost per hashrate is not weighted and investments follow Equations (2.9a) and (2.9b).

3.3.1. Cost per TH Construction Curve

As explained in Section (3.2.1) for the construction of the curve representing the energy efficiency (EEF) of the ASICs, the same mechanism is applied for the cost per TH. The curve is constructed by interpolating the cost per TH between the model using Equation (3.3) substituting the EEF value with the cost per TH of the ASIC in Table 3.1.

Figure 3.4 shows the chart of the cost per TH of the ASIC machines. The cost per TH can also increase during time because of the increase in efficiency and market dynamics. In early 2021 the cost per TH starts to increase because of the increase in the price of the last model of Antminer S19 XP and at the end of 2021 the company Marathon digital announced an order of 78,000 ASICs worth approximately $879 million[10].

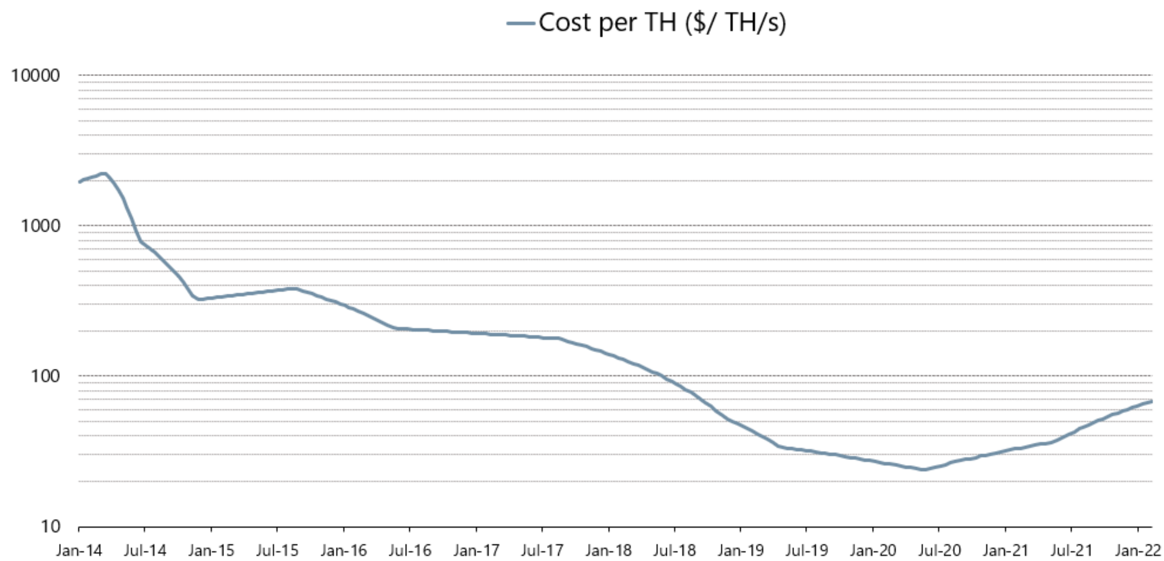


Figure 3.4: Cost per TH Chart.

3.3.2. Limitations

The ASICs' price can be influenced by different variables that the model cannot describe. The demand and offer dynamics of machines are also guided by the price of Bitcoin, in bullish periods the same machine could increase its price high as ten times. However, in the last periods mining companies preorder machines a long time in advance and the price is settled at the moment of signing the contract. This

[10] The price per machine is approximately $11,270 and it will increase the overall hashrate hashrate of Marathon Digital by 600% by early 2023 (Otieno, 2021).

will prevent miners will buy at exaggerated prices ASICs even if the price of Bitcoin is skyrocketing.

Another issue is represented by the inclusion of the necessary accessories for the ASIC machine installation, for example, some of them did not include the power supply unit, an essential component for running the machines, or other necessary hardware components. Moreover, the cost per TH is referred to the best hardware available at that time, the cost can be lower if miners are willing to accept low-efficiency machines hence spending more money on energy.

Finally, the price is not considering taxation or tariffs, they may be subject to different rules based on where ASICs are bought, shipped, and sold. These limitations can create estimation errors in the investment costs sustained by miners, moreover, most of the prices come from the empirical world and real transactions, and because the price variations affect mostly the small players, by considering all investments done by the network the error is limited.

3.4. Electricity Price

The price of a kilowatt-hour (k_t) is constant at a value of 0.046 $/kWh which is substantially lower compared to the previous works (Hayes, 2019), (Fantazzini, 2020). Using the Nord Pool electricity price or IESO (Independent Electricity System Operator) the price of kilowatt-hour is substantially closer. High electricity prices capture other expenses, so the CPMs computed using Nord Pool or IESO prices can be considered as proxies for the marginal cost of production.

The cost of the electricity ($/kWh) of 8 public mining companies (see Table 3.3) is on average 0.0279 $/kWh, the median is $0.0277, and represent approximately 21% of the total hashrate during the last quarter of 2021 (considering an average hashrate of 160 EH/s). Using this average value would provide a lower bound for the cost of energy because the high energy cost efficiency achieved by these companies is extremely low. By taking the least energy price efficiency company (Bitfarms Technologies Ltd. or Hive Blockchain Technologies Inc.) and the maintenance cost declared by Marathon Digital Holdings, Inc.[11] of $0.006 per kilowatt-hour, the value of 0.046 $/kWh will provide an upper bound cost of energy estimation, especially during the last periods. As discussed by Stoll (2019) by assuming potentially higher electricity costs can capture other different operational expenses.

Other works consider the price of energy referring to the Nord pool or taking it from IESO despite miners having their own energy factory and some using renewable energy[12]. Future studies can be conducted with the aim of describing the price of energy specifically for the mining companies to have a better estimation of the real price of energy for miners.

Companies	EH/s	$/kWh
Argo Blockchain PLC	1.7	0.029
Bitfarms Technologies Ltd.	2.6	0.040
Cipher Mining	19.5	0.027
Greenidge	1.4	0.022
Hive Blockchain Technologies Inc.	1	0.040
Hut 8 Mining Corp.	1.17	0.0274
Marathon Digital Holdings, Inc.	3.5	0.028
Riot Blockchain	4.1	0.025

Table 3.3: Mining companies energy cost.

[11] Marathon Digital Holdings, Inc. (2021, March 31). Form 10-Q.
[12] Greenidge is fully carbon neutral and uses for most of its operation green energy.

3.5. Bitcoin Price

The daily closing prices of Bitcoin ($/BTC) are taken from the website investing.com from 13/01/14 to 03/03/2022. The price is the average exchange price offered by the major exchanges of bitcoin present in the market. Because the time frequency is the time for producing 2016 blocks, the price referring to each period is the average of the daily closing price of the period P. Other studies consider weakly or monthly averages price, however since this model is not based on a fixed time length but on fixed volume length, the price P time-frequency changes according to the production speed, which is on average 2 weeks.

3.6. Bitcoin Fees

The bitcoin fees were directly retrieved from the bitcoin blockchain using Google cloud BigQuery platform[13]. It is possible to query data from an updated database containing the same information present on the blockchain. Subsequentially fees need to be cumulated in 2016 blocks corresponding to the total amount of fees for the period. The historical trend of Bitcoins fees (Figure 3.5) reached a peak end of 2017 when the price of Bitcoin was close to $20,000. In general Bitcoin fees constitute a small portion of the reward for miners, but when the production of bitcoin will further decrease through halving events fees will play an important role.

[13] Google cloud BigQuery platform can be found https://cloud.google.com/bigquery. The table name used for the query is bigquery-public-data.crypto_bitcoin.transactions.

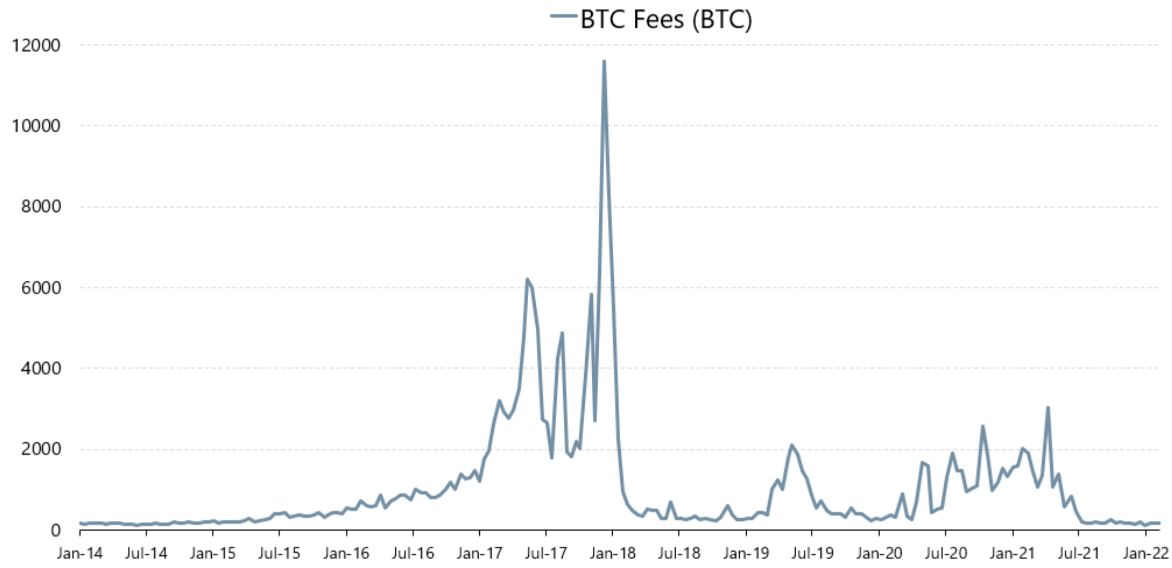


Figure 3.5: Bitcoins Fees.

3.7. Energy Cost

The Energy Cost time series is constructed by using Equation (2.7) substituting the parameter EEF_t with the values of $WEEF_t$ obtained in Section (3.2.2) and the electricity cost (k_t) at \$0.046 kWh as previously explained. Clearly, the energy costs are mostly dependent on the amount of hashrate applied by the network: *ceteris paribus* of energy efficiency more hashrate means more machines at working and more energy consumption. The Energy cost time series has a total of 221 observations from 24/01/2014 to 03/03/2022.

Moreover, in analyzing the cost of energy it is relevant to evaluate the energy cost of production for a single bitcoin. Instead of estimating the break-even price with Equation (2.12) the energy cost for a single bitcoin can be expressed as:

$$e_t = \frac{E_t}{2016 \cdot \beta} \tag{3.5}$$

Where e_t represents the cost of energy for producing a single bitcoin, for simplicity it will be call bitcoin energy cost. Note that in Equation (3.5) the transaction fees (F_t) are not taken into consideration as Equation (2.12) because fees are just an extra source of revenues for miners. In the future this cost will rise as halving events will decrease the production of bitcoins.

3.8. Investment Cost

The Investment Cost time series is constructed by using Equation (2.9a) from 26/10/2013 to 26/01/16 and from 07/02/16 to 03/03/2022 with Equation (2.9b). The investment costs I_t represent the costs sustained by miners for buying the ASICs during the period of producing 2016 blocks. Following the assumptions explained in section 2.4, the investment costs are similar to a leasing. Rather than accounting all the investment costs at the financial event causing a time series with periods of high peaks and periods with no investments, they are divided according with the useful life of the machines. Therefore, what miners are paying is comparable with the usage of the machines in the period of producing 2016 blocks.

The problem in estimating the first value of the investments I_0 in equation (2.9) is that CPU and GPU are multifunctional, while ASICs can only mine bitcoins. Attributing the investment cost of a GPU for bitcoin mining can be misleading because GPU can be easily converted and used for personal pc or workstations. Before 2013 the cost per hashrate could be higher than $1 million per TH/s using just GPU. When in early 2013 the Avalon 1 (batch 1) selling at $ 1,299 was providing a computational power of 0.066 TH/s, and the cost per hashrate decreased approximately to $19,600. As the estimation of the initial WEEF (section 3.2.2), the initial cost per TH/s (c_0) is the best cost per TH/s offered by the market weighted with a high cost per TH/s of FPGA. This will provide a lower bound for the investment costs. After determining the value of c_0, the value I_0 is given by:

$$I_0 = c_0 \cdot \vartheta_t \cdot \frac{14}{730} \tag{3.6}$$

Where $(\frac{14}{730})$ represent the ratio between the theoretical days of producing 2016 blocks and the useful life of the machines. I_0 is the estimate cost of the investment at time 0, this investment lasts only 2 years, because the Equation (2.9a) will be replaced with Equation (2.9b). This estimation error could be higher than expected, however in the long run thanks to the correction mechanism of the model, the initial value estimation will be irrelevant.

Clearly, the hashrate plays an important role in the investment costs, a decrease in hashrate stops the investment in new machines. On the other hand, according to time of deployment of ASICs (see section 3.2.1) the investments should reflect an increase in hashrate 3 months later, when the machines are fully deployed. For this reason, the value l in Equations (2.8) represent a lag approximately of 90 days. However, the ASICs' useful life begins after the deployment whereas the investments take place 90 days before. An example of the estimation from the period 18/02/17 to 14/07/17 is reported in Table 3.4. The increase in hashrate (258,017 TH/s) on 23/05/17 is paid \$191.48 per TH/s and the investment is recorded 90 days before, hence on 18/02/17. This process estimation can be described as a big mining company that bought approximately 22,400 Antiminer S9 on 18/02/17. The mining company start paying on the same date about \$50,000 per day and it will fully deploy the machines on 23/05/17. Note that in the last few observations the hashrate is assumed to be fixed, this may lead a small percentage error from the true value, but the inclusion of the latest observations was essential for capturing the effects of the increase in the price of ASICs in the last period.

Similar to the cost of energy for producing one bitcoin, a new variable can be expressed by the investment costs for producing a single bitcoin. This variable represents the cost of machines for producing one bitcoin.

$$i_t = \frac{I_t}{2016 \cdot \beta} \tag{3.7}$$

Where i_t is the cost of the investment for a single bitcoin, for simplicity bitcoin investment cost. Equation (3.7) shares the same characteristic of Equation (3.5) about the halving events. Note that the sum of i_t and e_t is not equal to the break-even price estimated with Equation (2.12) because the break-even price considers the bitcoin fees.

	ϑ_t (TH/s)	$\Delta\vartheta$ (TH/s)	c_t	I_t (USD Thousand)
18/02/17	3,153,469	131,566	**$191.48**	$17,721
03/03/17	3,298,156	144,687	$190.56	$18,453
17/03/17	3,404,454	106,298	$189.65	$18,664
30/03/17	3,574,955	170,501	$188.74	$19,795
13/04/17	3,728,040	153,085	$187.82	$20,939
27/04/17	3,735,472	7,432	$186.88	$22,888
10/05/17	4,006,568	271,096	$185.96	$21,248
23/05/17	4,264,585	**258,017**	$185.08	$21,484
04/06/17	4,857,205	592,620	$184.24	$22,751
17/06/17	5,090,089	232,884	$183.39	$25,026
02/07/17	5,090,089	0	$182.45	$27,437
14/07/17	5,758,807	668,718	$181.53	$27,684

Table 3.4: Example of I_t calculation.

3.9. Revenues, Profit and Break-Even Price

The miners' revenues time series is constructed with Equation (2.10), Profit with (2.11) and break-even price with Equation (2.12). Each series have 221 observations and start from 24/01/24 to 03/03/2022.

The key assumption in estimating the revenues is that: *all the bitcoins mined are exchanged with dollars by the end of the period*. However, the behavior of miners can act differently, miners keep their bitcoin when Bitcoin prices are low and exchange them when prices are high. The company Riot Blockchain explained[14] another typical miners' dynamic: in period of low margins selling rapidly bitcoins will potentially depress bitcoin prices by increasing the trading volume of Bitcoin, hence the best choice will be to hold bitcoins until the margins rise again. The volatility and unpredictability of bitcoin price expose miners at high market and trading risk, however, in December 2017 the bitcoin futures were introduced on the Chicago Mercantile Exchange (CME). The consequences and the miners' behavior of this known Bitcoin characteristic is not covered in this work and future development of it would be interesting.

Profits are the difference between miners' Revenues and Energy and Investment costs, for simplicity the sum of energy cost and investment cost can be expressed by the Total costs for miners:

$$C_t = E_t + I_t \tag{3.8}$$

[14] Riot Blockchain, Inc. (2020, December 31). Form 10-K.

A variable representing the profitability for miners can be expressed by the ratio between the price of bitcoin and its break-even price:

$$m_t = \frac{P_t}{P_t^*} \tag{3.9}$$

Where m_t is the margin, if the ratio is higher than one miners are profitable, if not, miners are taking losses. Finally, the list of the dataset variables obtained with the CPM are in Table 3.5 (one period is the time of producing 2016 blocks).

Simbol	Dataset Name	Description	Estimation Process
$\boldsymbol{P_t}$	Price	Price of Bitcoin	The average of the price of daily closing price of Bitcoin.
$\boldsymbol{R_t}$	Rev	Miners' Revenues	The product between 2016 blocks, the fees and the price of bitcoin.
$\boldsymbol{E_t}$	EnCost	Miners' Energy Costs	The estimated cost of energy for producing 2016 blocks Eq (2.7).
$\boldsymbol{I_t}$	InCost	Miners' Investment Costs	The estimated investment cost during the period of producing 2016 blocks Eq (2.9).
$\boldsymbol{C_t}$	TotCost	Miners' Total Costs	The sum of the miners' energy cost and investment cost.
$\boldsymbol{\pi_t}$	Profit	Miners' Profit	The difference between the miners' revenues and total cost.
$\boldsymbol{P^*{}_t}$	Price_BE	Break-Even Price of Bitcoin	Total cost divided the total BTC produced Eq (2.12).
$\boldsymbol{\rho_t}$	Hash	Hashrate	Miners' Hashrate.
$\boldsymbol{e_t}$	BTC_EnCost	Energy costs for a single bitcoin	The ratio between Energy cost and bitcoin produced Eq (3.5).
$\boldsymbol{i_t}$	BTC_InCost	Investment costs for a single bitcoin	The ratio between Investment cost and bitcoin produced Eq (3.7).
$\boldsymbol{m_t}$	Margin	Ratio representing miners' margins.	The ratio between bitcoin price and its break-even price Eq (3.9).

Table 3.5: List of the Dataset Variables.

4 Methodology and Results

The cointegration tests and the causality tests take as input the variables constructed in Chapter 3, moreover, before moving to the results, the methodology and the dynamics on which the model is based are shortly explained.

4.1. Bitcoin Price Dynamics

The hypothesis that bitcoins production costs can estimate the price is found only in Hayes' (2019) work, and it is hardly criticized (Shanaev et al., 2019) for the inconsistency of the test results. Fantazzini (2020) found that the only granger causality is going from the price of Bitcoin to the hashrate or the cost of production of bitcoin, and similar results are also found by Kristoufek (2020). Furthermore, in investigating the mechanism between CPM or hashrate and price, the hashrate shows better results than CPM models. The analysis supports the reasoning and results of previous studies, where the price granger causes the costs of bitcoin and the price of bitcoin explains the cost of production of bitcoin rather than the inverse.

The results of the directionality from price to costs can be interpreted by the following dynamic: an increase in the Bitcoin prices will increase the miners' profit, at *ceteris paribus* of miners' costs (same hashrate provided, same energy consumption and mining machines) an increase in price would increase their profits. The presence of profits causes the entrance of new miners in the business and the increase of the hashrate, hence it distributes the profit between miners. By considering all the miners present in the network, an increase in the hashrate increases the energy and investment costs for all the network and clearly it decreases the profit.

Therefore, a growth in hashrate also contribute to an additional reduction of profits caused by the adjustment mechanism of difficulty. Since there was an increase in the hashrate, in the next period the difficulty will increase meaning that for producing the same number of bitcoins the hashes required are higher than before.

Miners entering the market (or even the same miners by increasing their computational power) have a double effect in decreasing the profits:

1. Division of profits between miners;
2. Decrease of bitcoin productivity with the same hashrate.

The opposite mechanism is applied when the price decreases and miners leave the market and increase miners' profits.

4.1.1. Hashrate, Energy and Investment Costs

Energy and Investment Costs are closely related to hashrate. The hashrate affects the Energy in a mechanism that is easily comprehensible: an increase in hashrate at *ceteris paribus* of machines' energy efficiency increases the energy spending. On the other hand for Investment Costs, an increase in hashrate does not necessarily require an investment in new machines, however, when the hashrate surpasses the maximum hashrate reached, an investment in new machines must occur. The presence of the hashrate in Equations (2.7) and (2.9) clearly highlight these dynamics and strongly influence these costs.

4.2. Methodology

The purpose of the analysis is to investigate the dynamics between price, hashrate, and costs of production of Bitcoin. Thanks to the results of previous studies, the analysis is focused on performing tests to prove the granger causality going from the bitcoin price to the cost of production of bitcoins and the possibility of cointegration between these variables.

Tests are conducted to bivariate models formed by the Bitcoin price and a variable expressing the costs related to the bitcoin production. The full list of the bivariate models is in Table 4.1. The last pair Miners' Revenues and Miners' Total Costs are similarly representing the Bitcoin price and the price of break-even because Revenues are obtained by using Equation (2.10) and Total Costs by the product between the break-even price Equation (2.12) and $(2016\ \beta_t + F_t)$.

Simbol	Dataset Name	Description
$\boldsymbol{log}(\boldsymbol{P_t}), \boldsymbol{log}(\boldsymbol{P^*}_t)$	**Log (Price), Log (Price_BE)**	Bitcoin Price and Break-even Price
$\boldsymbol{log}(\boldsymbol{P_t}), \boldsymbol{log}(\boldsymbol{e_t})$	**Log (Price), Log (BTC_EnCost)**	Bitcoin Price and Bitcoin Energy Cost
$\boldsymbol{log}(\boldsymbol{P_t}), \boldsymbol{log}(\boldsymbol{i_t})$	**Log (Price), Log (BTC_InCost)**	Bitcoin Price and Bitcoin Investment Cost
$\boldsymbol{log}(\boldsymbol{P_t}), \boldsymbol{log}(\boldsymbol{m_t})$	**Log (Price), Log (margin)**	Bitcoin Price and Margin
$\boldsymbol{log}(\boldsymbol{P_t}), \boldsymbol{log}(\boldsymbol{\rho_t})$	**Log (Price), Log (Hash)**	Bitcoin Price and Hashrate
$\boldsymbol{log}(\boldsymbol{R_t}), \boldsymbol{log}(\boldsymbol{C_t})$	**Log (Rev), Log (TotCost)**	Miners' Revenues and Miners' Total Costs

Table 4.1: Bivariate Models.

After a log transformation, variables are tested for stationary using the Augment Dickey-Fuller test (ADF). If a non-stationary variable is found, then the ADF test is repeated on the first difference. Tests are performed in two samples: the first from 24/01/2014 to 03/03/2022 takes into account also the halving events which are typical characteristics of the Bitcoin nature, whereas the second from 18/07/2016 to 21/04/2020 excludes the halving events because the issues of the CPM (see section 2.3).

The second step is to test for cointegration using the Engle and Granger (1987) approach with constant and trend. The third step is to find the optimal VAR lag length k using the Bayesian information criteria with maximum lag order of 4, and test for cointegration using the Johansen (1988) approach. If any cointegrating vector is found, then a VECM model is analyzed for further information. After testing for cointegration, a VAR with k lags is used to test the Granger (1969) causality to check the causality relationship between the variables. Finally, the Granger causality is checked also using Toda and Yamamoto (1995) test. This approach requires to model a VAR with a lag length $(k + d_{max})$, where d_{max} is the maximum order of integration of between the variables and test for linear or nonlinear restrictions only for the k coefficient matrices, the other coefficient matrices must be ignored. The advantage of this method relies on unnecessary of the process to be integrated or cointegrated of the same order.

4.3. Literature

The first step of the analysis tests the stationarity of data, the test used for this purpose is the Augmented Dickey-Fuller proposed by Dickey and Fuller (1979). In determining if trending data should be first differenced or regressed on deterministic functions of time to render the data stationary, unit root tests are extremely useful. Nevertheless, finding long-run equilibrium relationships between non-stationary time series variables require pre-testing for unit roots.

If these variables are integrated of the first order I (1) and there is at least one linear combination of these variables that is stationary, then the variables are said to be cointegrated. Engle and Granger (1987) have shown that cointegration is equivalent to an error correction mechanism (ECM). The ECM captures both short- and long-run features. The two-step procedure consists in testing the null hypothesis of no cointegration between variables. The first step is to estimate an OLS regression and then apply an ADF to residuals for checking the stationarity. Rejecting the null hypothesis of a unit root is the evidence of a cointegration.

The Johansen (1988) method is based on maximum likelihood approach applied to a VAR model. This procedure relies on the rank (r) of the *impact matrix* Π, where r is the number of cointegrating relationships. This method can be seen as a second-generation approach, instead of relying on least squares it depends on maximum likelihood. Johansen's procedure is nothing more than a multivariate generalization of the ADF test.

In understanding the direction of causality between two variables, Granger (1969) "throw light" for describing this relationship by using cross-spectral methods. Granger causality is mostly used for investigating bivariate processes because when more than two variables are present, non-causality conditions become more complicated (Lütkepohl, 1993). In addition, in a bivariate model, a variable can be non-causal for another one and becomes causal if the information set is extended to include other variables. This scenario is known as spurious causality.

Toda and Yamamoto (1995) show how an estimation of levels VAR using a lag length $(k + d_{max})$ can be tested for linear and nonlinear restriction on the first k coefficient matrices using the asymptotic theory. The drawback is in the "loss of power" caused by intentionally over-fit VAR models. In particular, if a VAR has many variables and short lag length, then adding an extra lag may cause a significant inefficiency, whereas a system with few variables but with long lag length may suffer from a relatively small inefficiency. In the end, this method should not totally replace the conventional hypothesis testing, but it should be regarded as a complementing test.

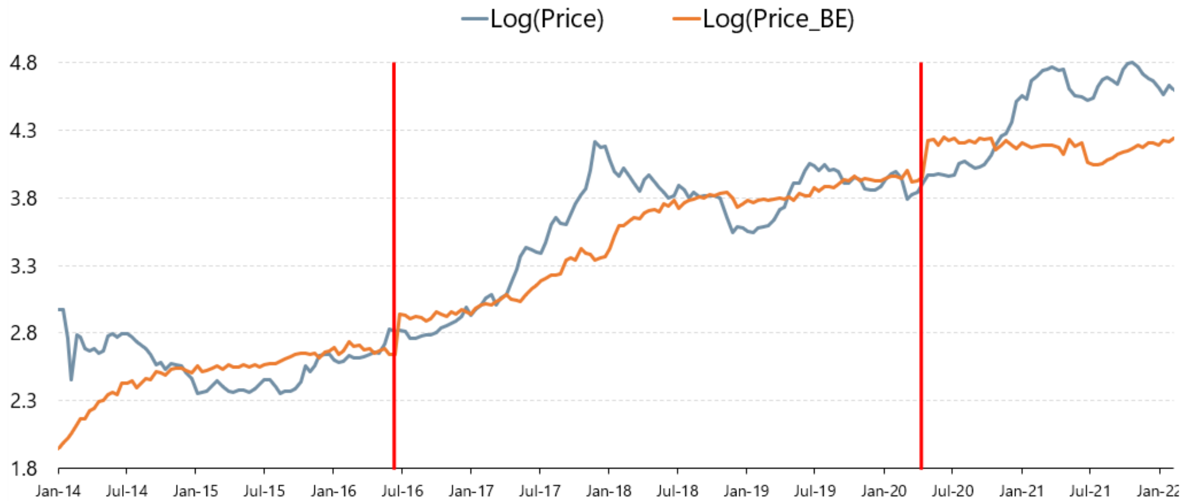
4.4. Results

Unit root tests may have limited power to distinguish between a unit root and a close alternative, but the ADF test results strongly accept the unit root (see p-value in Table 4.2) and the time series plots (Figure 4.1) clearly show non-stationary trends. In Table 4.2 are expressed the order of integration of the variables used for the analysis and the p-value of the ADF tested with constant and trend using the BIC criterion. All the variables, except for margin, are integrated of the first order which is a required condition for investigating the cointegration. Margin is the only variable that is stationary in sample 1, this should be expected because of how it is constructed. In sample 1 the mean value is 0.297, where a value equal to 0 means 0 profits for miners. If the assumptions of the model hold miners' business is profitable with high peaks in late 2017 and in the second quarter of 2021, while after the halving events margins plunge and stays below profitable territories until a vigorous bullish period pushes back margins to high values.

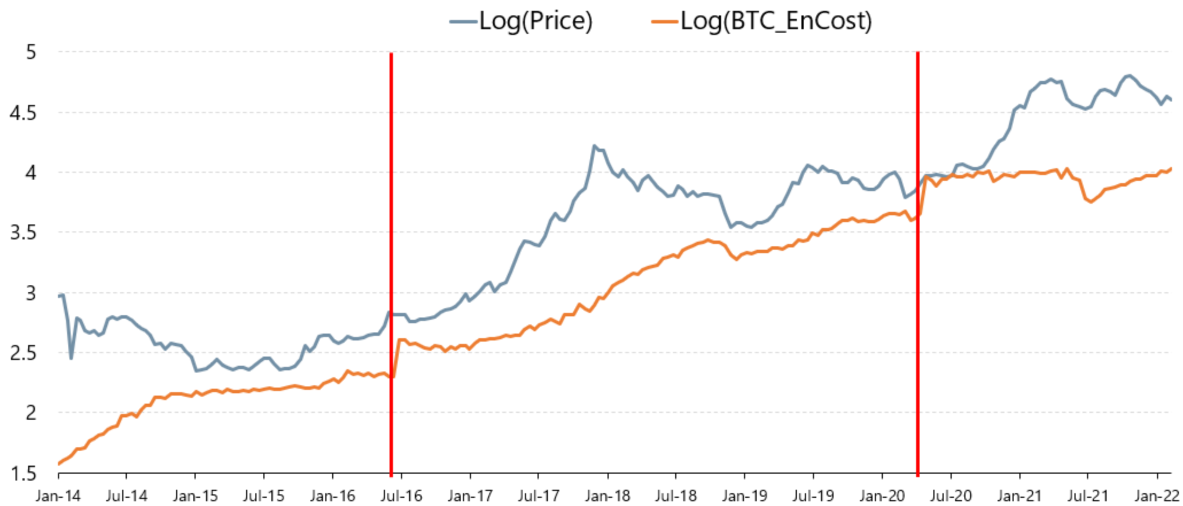
Simbol	Dataset name	Sample 1 24/01/2014 -03/03/2022 Order of Integration	Sample 2 18/07/2016 - 21/04/2020 Order of Integration
$log(P_t)$	Log (Price)	1 [0.1269]	1 [0.8095]
$log(P^*{}_t)$	Log (Price_BE)	1 [0.5011]	1 [0.5038]
$log(e_t)$	Log (BTC_EnCost)	1 [0.7505]	1 [0.6524]
$log(i_t)$	Log (BTC_InCost)	1 [0.9247]	1 [0.999]
$log(m_t)$	Log (Margin)	0 [**0.0411**]	1 [0.7461]
$log(\rho_t)$	Log (Hash)	1 [0.4279]	1 [0.9893]
$log(R_t)$	Log (Rev)	1 [0.1116]	1 [0.7261]
$log(C_t)$	Log (TotCost)	1 [0.8856]	1 [0.9968]

Table 4.2: Order of Integration (ADF tests).

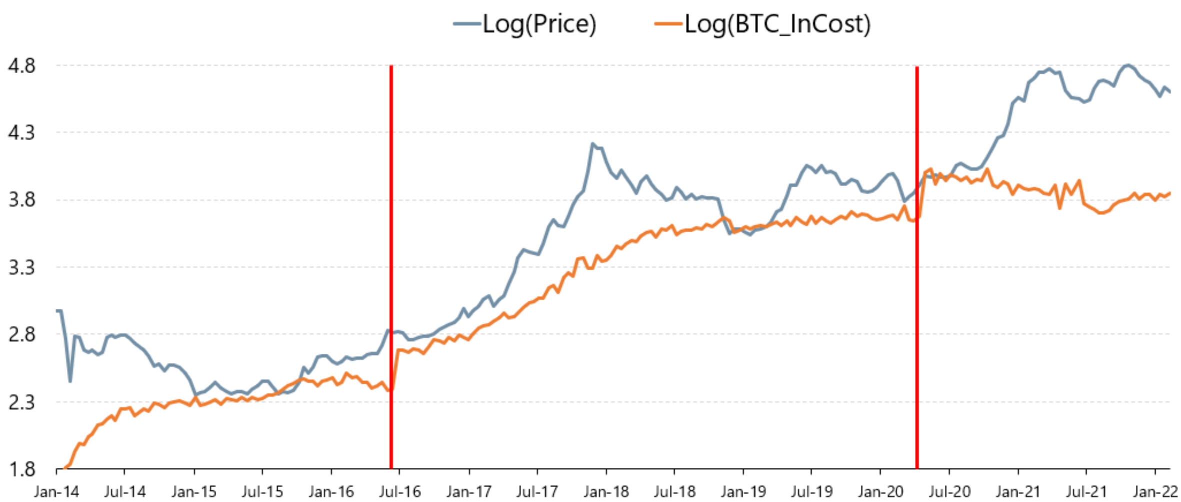
Plots of the bivariate models are in Figure 4.1. The red vertical lines indicate the halving events and the interval between them is the second sample interval. Clearly, the halving events are also visible in the time series plots due to the immediate jumps in costs or drops in revenues. Price and hashrate is the only bivariate model that is resistant to the halving event shocks because hashrate is affected only by the difficulty changes.



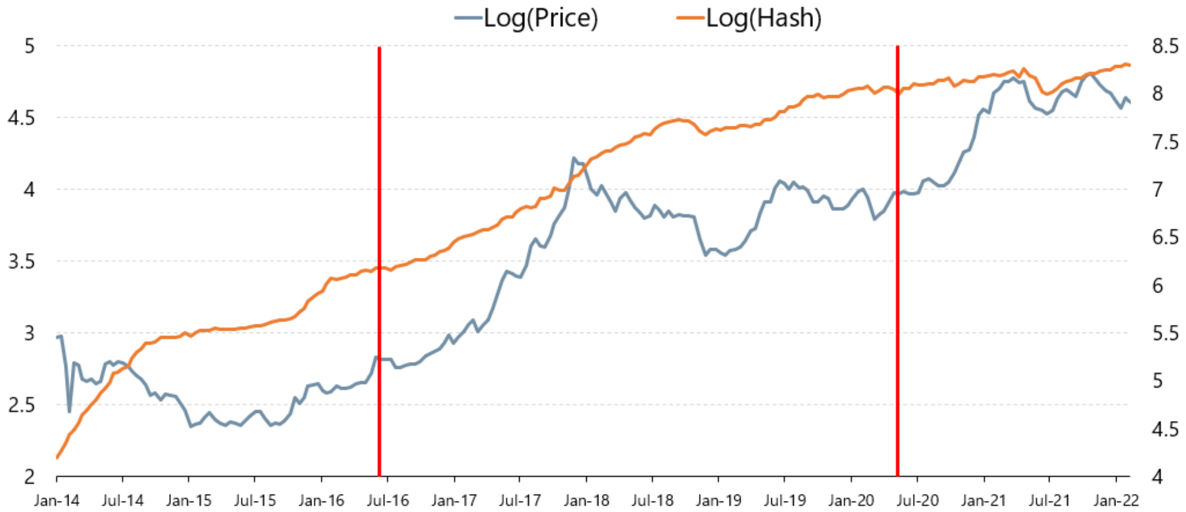
(a) Plot Log price and Log bitcoin break-even price.



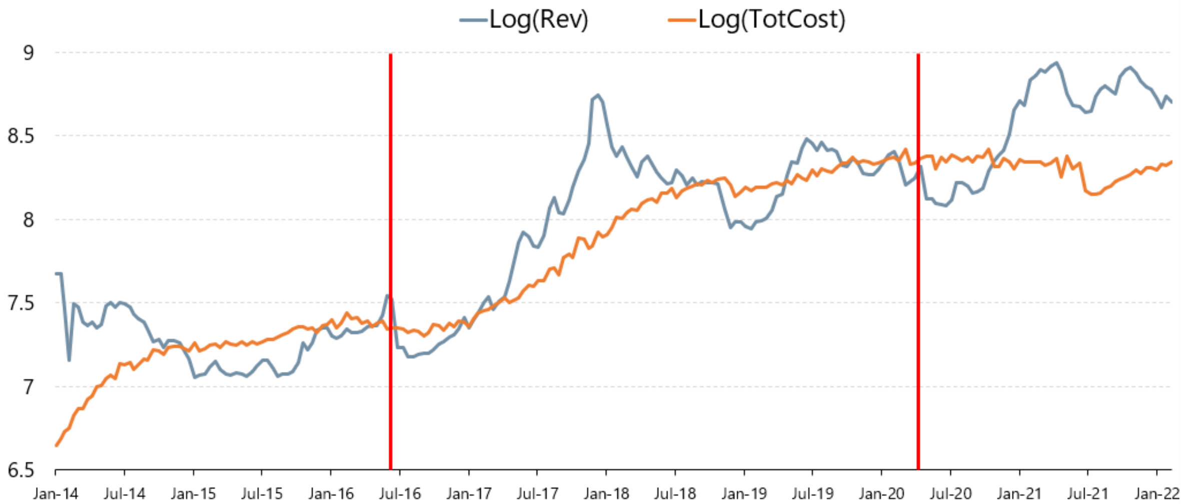
(b) Plot Log price and Log bitcoin energy cost.



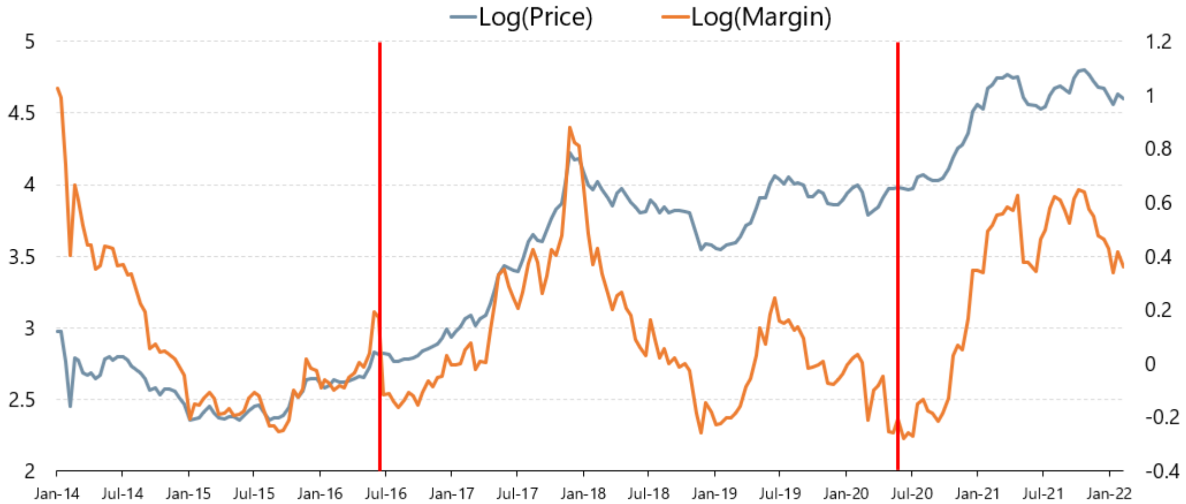
(c) Plot Log price and Log bitcoin investment cost.



(d) Plot Log price and Log hashrate.



(e) Plot Log revenues and Log total costs.



(f) Plot Log price and Log margin.

Figure 4.1: Bivariate Models' time series plots.

The Engle-Granger cointegration results are in Table 4.3 and the closest relevant finding is the cointegration between the bivariate model price of bitcoin and the bitcoin investment cost, but the ADF on the residual of the OLS regression has a p-value of 0.126 that accepts the null hypothesis and concludes the absence of cointegration.

Engle - Granger Cointegration		
Variable Pair	**Sample 1 24/01/2014 -03/03/2022 p-value residuals**	**Sample 2 18/07/2016 - 21/04/2020 p-value residuals**
Log (Price), Log (Price_BE)	0.1654	0.7864
Log (Price), Log (BTC_EnCost)	0.5394	0.8459
Log (Price), Log (BTC_InCost)	0.1258	0.5275
Log (Price), Log (Margin)	-	0.9611
Log (Price), Log (Hash)	0.9033	0.7432
Log (Rev), Log (TotCost)	0.1361	0.6847

Table 4.3: Engle-Granger cointegration.

The Johansen cointegration includes a restricted trend on the cointegrating vectors to capture possible trend effects. In the first sample (Table 4.4) only the bivariate models price and hashrate, revenues and total costs have one cointegrated equation (C.E.). For the other sample the C.Es. are present in more bivariate models, the exclusion of the halving events from the sample seems to improve the cointegration results.

Johansen Cointegration				
	Sample 1 24/01/2014 -03/03/2022		**Sample 2 18/07/2016 - 21/04/2020**	
Variable Pair	**Number of C.E.**	**Lags**	**Number of C.E.**	**Lags**
Log (Price), Log (Price_BE)	0	1	0	1
Log (Price), Log (BTC_EnCost)	0	2	**1**	1
Log (Price), Log (BTC_InCost)	0	1	**1**	2
Log (Price), Log (Margin)	-	-	0	1
Log (Price), Log (Hash)	**1**	1	**1**	1
Log (Rev), Log (TotCost)	**1**	2	**1**	3

Table 4.4: Johansen cointegration.

In Table 4.5 there are the R^2 values of the bivariate models' regression on the first difference of the dependent variable and Error Correction (EC) term. The R^2 values are reasonably low, especially when the dependent variable is the first difference of bitcoin price, while the R^2 values are substantially higher when the dependent variable is a cost variable. Further information about the cointegrated vectors beta are reported in appendix B.

VECM - Regression			
Y	EC	Sample 1 24/01/2014-03/03/2022 R^2	Sample 2 18/07/2016-21/04/2020 R^2
ΔLog (Price)	**Log (BTC_EnCost)**	-	0.0760
ΔLog (BTC_EnCost)	**Log (Price)**	-	0.1409
ΔLog (Price)	**Log (BTC_InCost)**	-	0.1209
ΔLog (BTC_InCost)	**Log (Price)**	-	0.2264
ΔLog (Price)	**Log (Hash)**	0.0333	0.0268
ΔLog (Hash)	**Log (Price)**	0.2080	0.1909
ΔLog (Rev)	**Log (TotCost)**	0.0726	0.1655
ΔLog (TotCost)	**Log (Rev)**	0.2053	0.3500

Table 4.5: VECM regression.

The Granger causality tests show similarities with previous works. In the first sample, the causality direction goes only from the price to the costs but not vice versa. The most significant variable is hashrate follows total costs and price of break-even. In the second sample, some variables show bidirectional causality, hashrate and bitcoin energy costs, while the others have a significant causality going from price to cost. In general, the p-values of CPM variables causing the price are substantially lower, even in the case of bidirectionality. The lags used for VARs reach a maximum of 3, and from sample 1 to sample 2 the bivariate models bitcoin investment costs and total cost increased by a lag, while bitcoin energy costs decreased by a lag.

Granger Causality Test – Sample 1				
Y_1	Y_2	Y_1 *does not cause* Y_2	Y_2 *does not cause* Y_1	VAR Lags
Log (Price)	**Log (Price_BE)**	**0.0192**	0.8429	1
Log (Price)	**Log (BTC_EnCost)**	0.0972	0.3882	2
Log (Price)	**Log (BTC_InCost)**	0.0907	0.2819	1
Log (Price)	**Log (Margin)**	0.5585	0.8429	1
Log (Price)	**Log (Hash)**	**0.0000**	0.9140	1
Log (Rev)	**Log (TotCost)**	**0.0004**	0.9797	2

Table 4.6: Granger Causality test Sample 1.

Granger Causality Test - Sample 2				
Y_1	Y_2	Y_1 *does not cause* Y_2	Y_2 *does not cause* Y_1	VAR Lags
Log (Price)	**Log (Price_BE)**	**0.0003**	0.1289	1
Log (Price)	**Log (BTC_EnCost)**	**0.0001**	**0.0004**	1
Log (Price)	**Log (BTC_InCost)**	**0.0109**	0.5296	2
Log (Price)	**Log (Margin)**	0.3887	0.1289	1
Log (Price)	**Log (Hash)**	**0.0000**	**0.0269**	1
Log (Rev)	**Log (TotCost)**	**0.0002**	0.9439	3

Table 4.7: Granger Causality test Sample 2.

Finally, the Toda and Yamamoto tests (Table 4.8 and Table 4.9) have analogous results to Granger causality tests, the directionality is always from price to cost variables and the same behavior in which p-values show less significance when the costs are causing the price is present.

Toda and Yamamoto Test – Sample 1				
Y_1	Y_2	Y_1 *does not cause* Y_2	Y_2 *does not cause* Y_1	VAR Lags
Log (Price)	**Log (Price_BE)**	0.7679	0.9787	1+1
Log (Price)	**Log (BTC_EnCost)**	0.1493	0.6435	2+1
Log (Price)	**Log (BTC_InCost)**	0.2305	0.4741	1+1
Log (Price)	**Log (Margin)**	**0.0435**	0.9787	1+1
Log (Price)	**Log (Hash)**	**0.0597**	0.5971	1+1
Log (Rev)	**Log (TotCost)**	0.1787	0.8040	2+1

Table 4.8: Toda and Yamamoto test Sample 1.

Toda and Yamamoto Test – Sample 2				
Y_1	Y_2	Y_1 *does not cause* Y_2	Y_2 *does not cause* Y_1	VAR Lags
Log (Price)	**Log (Price_BE)**	0.2874	0.9230	1+1
Log (Price)	**Log (BTC_EnCost)**	**0.0253**	0.6435	1+1
Log (Price)	**Log (BTC_InCost)**	0.2193	0.7393	2+1
Log (Price)	**Log (Margin)**	**0.0025**	0.9230	1+1
Log (Price)	**Log (Hash)**	0.3319	0.4683	1+1
Log (Rev)	**Log (TotCost)**	0.2031	0.8040	3+1

Table 4.9: Toda and Yamamoto test Sample 2.

4.4.1. Discussion

The results from the empirical analysis provide a clear direction of the bitcoin price and costs dynamics: CPM variables and hashrate do not Granger cause the price, the bitcoin technological factors and mining dynamics support the same results. The impact of the halving events is evident for costs and revenues and the reaction is reflected in the next observation after the halving, while for price occurs several months (Meynkhard, 2019) to react. Moreover, the cointegration between the bitcoin price and production costs has limited significance, there is no real reason why the bitcoin price should depend on its production costs and why there should be a significant ECM that binds the variables. Especially at the beginning of 2014 and late 2017 during the bitcoin price bubbles (Gerlach et al., 2019), the price pushed margins to skyrocket values. In December 2017, the bitcoin price reached a value of over $16,000 whereas the break-even price was approximately $2,200. The gap (Figure 4.2) formed between costs and price is extremely large to think about a possible cointegration.

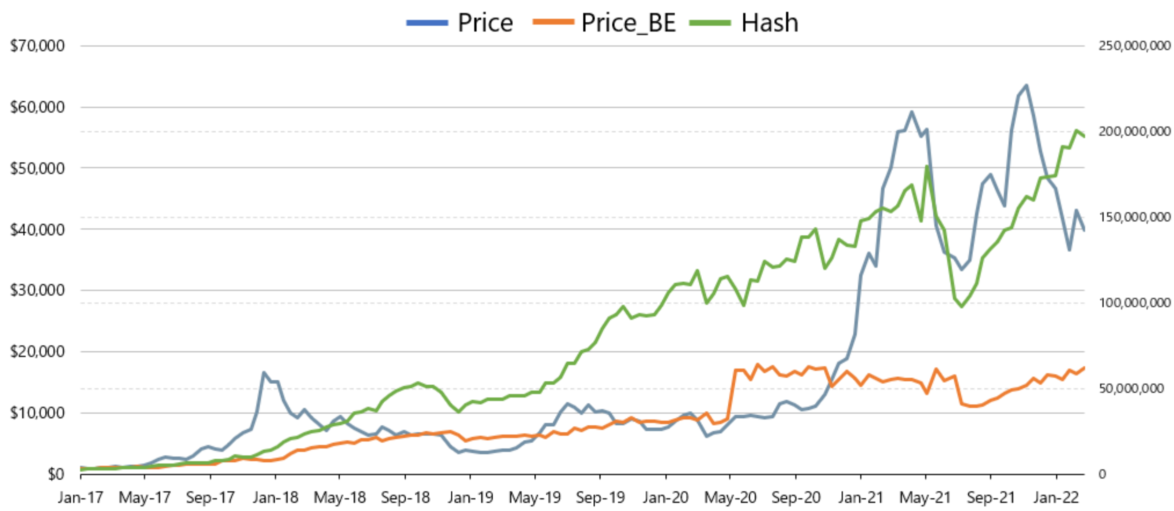


Figure 4.2: Bitcoin Price, break-even price and hashrate time series plot (Jan-17 - Mar-22).

In the period from 24/01/2014 to 03/03/2022, the hashrate has lower p-values in Granger causality and Toda and Yamamoto tests compared with the variables constructed with the CPM, similar to Fantazzini's (2019) results. A possible explanation of these results relies on the impacts of halving events: the impossibility to reflect the anticipation of this event by miners may cause defects in the CPM but not in the hashrate. Excluding them by the period of the analysis is not enough to describe the relationship between price and costs. Even though the CPM variables are estimated with the hashrate and other variables that should increase the precision in describing the relationship between bitcoin price and costs, the limitations and assumptions of the model may describe with excessive simplicity the miners' cost structure and the hashrate to be more precise in approximating the causality dynamic. In addition, the velocity of the adjustment of the hashrate with the price is faster compared with the break-even price that considers both energy and investments costs. Since investment costs reflects fixed costs, movements in price are slowly affecting them, while the hashrate and energy costs have a quick reaction. This behavior is evident in price drops (Figure 4.2), in December 2018 the price felt from \$6,500 to \$3,500 and the hashrate from 51 EH/s to 36,5 EH/s, and in May 2021 the price was about \$56,000 and suddenly plunged to \$33,400 while the hashrate from 179 EH/s to 97,8 EH/s.

Nevertheless, in the cointegration tests the scenario is slightly different. The hashrate has one C.E. in each sample as well as Revenues and Total Costs, but the latter bivariate model have higher R^2 on the first difference regressions. On the other side, in the two-step cointegration tests the bitcoin investment cost achieved the best results (the lowest p-value). During the 2017 price bubble (Figure 4.3), investments follow the price trend better than bitcoin energy cost. Normally, the energy costs are more sensitive to changes in the hashrate, while investment costs anticipate future hashrate increases. These dynamics can explain why in the 2017 bubble period miners' investments are superior in pursuing the price than energy expenses: when the price entered in the bull period miners invested millions of dollars[15] in new ASICs for increasing the computational power, but the energy and the hashrate provided were still not increasing until the machines were installed. Starting from 2021 the bitcoin investment costs are distant from the price, even though there are two peaks in April and November looking similar to a bubble, the investment did not follow the price as the 2017 bubble. A rational explanation behind it is associated to a more mature and experienced miners' behavior, after the bitcoin bubble miners experienced a long period of losses (8 months) with the hashrate stable around 45 EH/s. Furthermore, in July 2021 the announcement of the Chinese Government of banning the cryptocurrency mining[16] provoked fears and doubts, hence the price plunged and due also to the law restriction the hashrate dropped drastically.

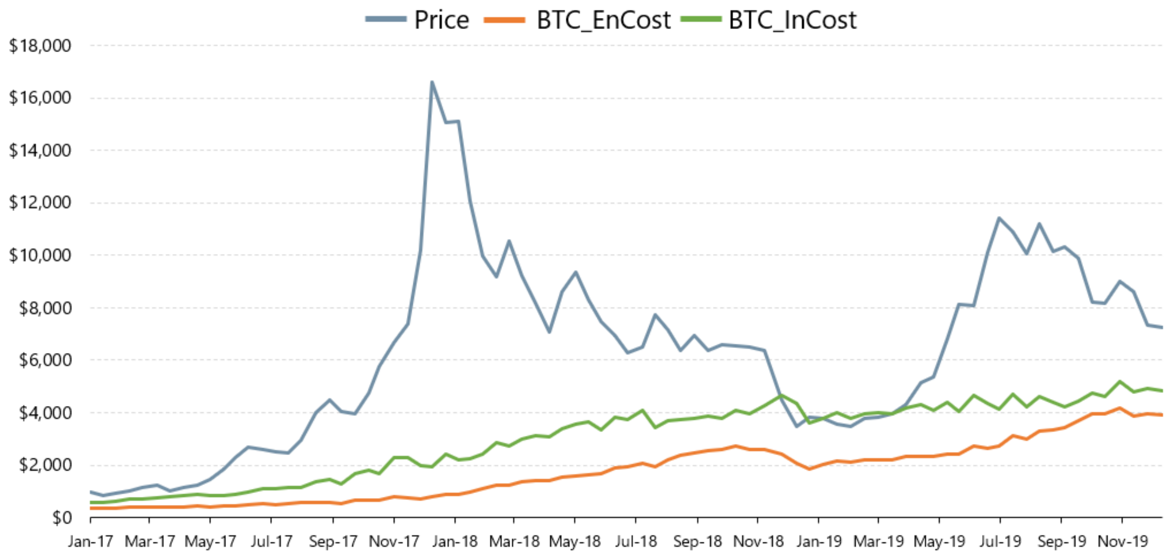


Figure 4.3: Price, bitcoin energy and investment cost time series plots (Jan-17 - Dec-19).

[15] In November 2017 the estimated investments were about $117 million and in January 2018 $470 million, investments in only 3 months quadruplicated.

[16] Chinese miners were forced by the Government to shut down their facilities and they have to move to other countries such as Texas or Kazakhstan, the alternative was to sell the mining equipment (Shen and Galbraith, 2021).

Moreover, in the second sample (18/07/16 – 03/03/22) the Granger tests highlight bidirectionality from price to hashrate or from price to energy. However, Toda and Yamamoto tests (i.e. the bitcoin energy cost) suggest unidirectionality from price to costs. This evidence and the visible lower p-values in price causing costs reject the hypothesis that costs granger cause the price, contrary to what was found by Hayes (2019). The Toda and Yamamoto tests also contribute to the founding of the directionality of Margin, the variable representing the profitability of miners. In both samples of the Granger test, the significance is absent, while in the last tests clearly (p-value 0.0435, 0.0025) show that price is granger causing miners' profits. This dynamic is coherent with Kjærland et. al (2018) and what is described in section 4.1, furthermore, the increase in costs, even during halving, seems to marginally affect the margin, whereas the bitcoin price strongly causes margin. Finally, periods of high volatility (Figure 4.4) suggest favoring miners' profitability rather than a period where the price is more stable.

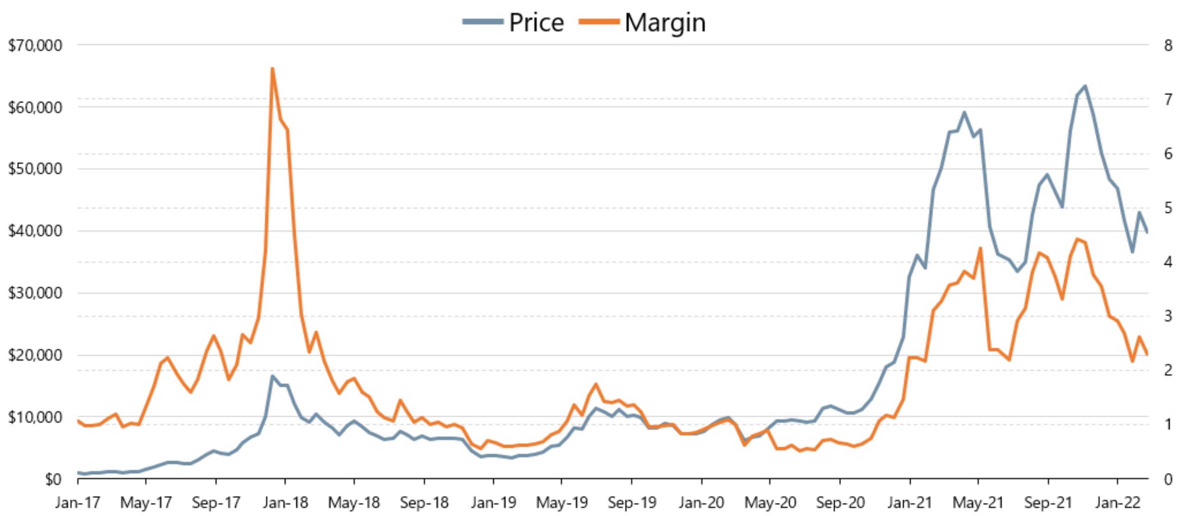


Figure 4.4: Bitcoin price and margin time series plots (Jan-17 - Mar-22).

5 Conclusions

In January 2009 the first bitcoin was created by Satoshi Nakamoto and the decentralized cryptocurrency world was initialized. Bitcoin always dominated the cryptocurrency market and has experienced explosive growth as well as high volatility. The role of central authority was replaced by a decentralized network where miners validate transactions and build the blockchain. Without miners bitcoin cannot exist, even though the Proof-of-Work paradigm is strongly debated for its waste of energy. Bitcoin's paradigm has never failed until now and proves Bitcoin to be a reliable and secure asset if sufficient precautions are applied.

Proving empirically that the bitcoin price is affecting the hashrate and the bitcoin production costs verifies that costs are useless in explaining the bitcoin price and supports the controversial thread of the last years. These results also help cryptocurrency analysts with an important notion for performing on-chain analysis. In particular, the sample analyzed (24/01/2014 - 03/03/2022) shows a significant unidirectional Granger causality going from the price to hashrate or CPM variables. After a price drop follows a hashrate or a cost drop, this particular causality is more evident when price falls (i.e. December 2018, May 2021). For this dynamic, the hashrate have superior results if compared with the variables obtained with the CPM in accordance with the founding of previous studies.

However, the development of the CPM highlights the consistency of the economic theory because an increase in price will clearly increase the miners' profitability, therefore new miners will enter the market and will increase the hashrate. The overall effect is that profits will be shared by a higher number of miners and costs will rise because for producing the same number of bitcoins is now required more energy. Generally, during Bitcoin bullish period miners are profitable, so they heavily invest on mining ASICs, for instance, from April 2017 to January 2018, mining investment grew rapidly from $831 investment cost per single bitcoin to $2,244 and the hashrate from 3.7 EH/s to 18.6 EH/s, while energy costs only doubled. Moreover, when the price reaches unprofitable territories, miners can easily unplug their machines and stop investing to save energy costs, that eventually causes hashrate to drop. However, sunk costs cannot be avoided, hence the investment costs drop is lower in magnitude and slower in time. Investment costs is an indicator having more inertia compared with energy or hashrate and this could be a reason why in the causality results show worse performance. On the contrary, when the price returns to be profitable for miners, they plug the machines to restore in few weeks the hashrate, as well as energy costs, while investments require a longer period.

The risk taken by miners is extremely high because of the volatility of bitcoin and it seems that in high volatility periods miners are more profitable. After the introduction of Bitcoin futures (December 2017) miners' revenues should be more stable, however, the price movement in April 2021 showed that is possible to have a 50% drop in barely 3 months. In the long-term, revenues outperform costs: in the period examined miners' profits are approximately $16 Billion. Nevertheless, if miners can hold bitcoins mined in low-price periods (i.e. Q1 2019) and exchange them in high-price periods (i.e. Q1 2021), they will make astonishing returns.

This work also contributes to the development of a new model for describing the operational costs sustained by miners. The key innovation is the introduction of the estimates of the investments on ASIC rigs, the logic behind is based on rational assumptions of the increases in hashrate. Although it may have limitations, this can settle the basis for new studies and market research about investments in mining ASICs. In addition, changing the time-frequency according to the time of producing 2016 blocks allows a clear estimation of the hashrate and revenues, instead of daily proxies of hashrate. Future studies should remove the limits of the cost per TH and find ASICs' price by looking at mining company deals since they represent a significant size of the network hashrate. Furthermore, developments may also include the introduction of futures contracts in estimating miners' revenues. Finally, in this work the CPM was completely transformed into a new model including the miners' investments, but it would be interesting to improve it by removing the effect of halving events.

References

Ammous, S. (2018). *The Bitcoin Standard: The decentralized alternative to central banking* Wiley.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain*. O'Reilly.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation, 6*(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5

Bendiksen, C., & Gibbons, S., (2018). The Bitcoin Mining Network. Trends, Marginal Creation Cost, Electricity Consumption & Sources. *CoinShares Research*.

Bevand, M. (2013, January 31). "*The Insane Bitcoin ASIC Race — And The Winner is…*". Mrb's blog. http://blog.zorinaq.com/the-insane-bitcoin-asic-race-mdash-and-the-winner-is/

Ciaian, P., Rajcaniova, M., & Kancs, D. (2016). The economics of BitCoin price formation. *Applied Economics*, *48*(19), 1799–1815. https://doi.org/10.1080/00036846.2015.1109038

Dickey, D. A., & Fuller, W. A. (1979). Distribution of the Estimators for Autoregressive Time Series With a Unit Root. *Journal of the American Statistical Association*, *74*(366), 427. https://doi.org/10.2307/2286348

Digiconomist. (2022). *Bitcoin Energy Consumption Index*. https://digiconomist.net/bitcoin-energy-consumption/

Engle, R. F., & Granger, C. W. J. (1987). Co-Integration and Error Correction : Representation , Estimation , and Testing*: The Econometric Society Stable, 55*(2), 251-276. https://www.jstor.org/stable/1913236

Fantazzini, D., & Kolodin, N. (2020). Does the Hashrate Affect the Bitcoin Price? *Journal of Risk and Financial Management, 13*(11), 263. https://doi.org/10.3390/jrfm13110263

Feld, S., Schönfeld, M., & Werner, M. (2014). Analyzing the deployment of bitcoin's P2P network under an as-level perspective. *Procedia Computer Science, 32*, 1121–1126. https://doi.org/10.1016/j.procs.2014.05.542

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance, 56*(January), 101387. https://doi.org/10.1016/j.ribaf.2021.101387

Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics, 95*, 86–96. https://doi.org/10.1016/j.jmoneco.2017.12.004

Garcia, D., Tessone, C. J., Mavrodiev, P., & Perony, N. (2014). The digital traces of bubbles: Feedback cycles between socio-economic signals in the Bitcoin economy. *Journal of the Royal Society Interface, 11*(99). https://doi.org/10.1098/rsif.2014.0623

Gerlach, J.-C., Demos, G., & Sornette, D. (2018). Dissection of Bitcoin's Multiscale Bubble History. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3164246

Granger, C. W. J. (1969). Investigating Causal Relations by Econometric Models and Cross-spectral Methods. *Econometrica. 37* (3): 424–438.

Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal, 4*, 160.

Gronwald, M. (2021). The Economics of Bitcoins -- Market Characteristics and Price Jumps. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2548999

Harvey, C. R. (2014). Bitcoin Myths and Facts. *SSRN Electronic Journal, 2014*, 1–10. https://doi.org/10.2139/ssrn.2479670

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics, 34*(7), 1308–1321. https://doi.org/10.1016/j.tele.2016.05.005

Hayes, A. S. (2019). Bitcoin price and its marginal cost of production: support for a fundamental value. *Applied Economics Letters, 26*(7), 554–560. https://doi.org/10.1080/13504851.2018.1488040

Ilie, D. I., Werner, S. M., Stewart, I. D., & Knottenbelt, W. J. (2021). Unstable Throughput: When the Difficulty Algorithm Breaks. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–5. https://doi.org/10.1109/ICBC51069.2021.9461086

Johansen, S. (1988). Statistical analysis of cointegration vectors. *Journal of Economic Dynamics and Control*, *12*(2-3), 231-254. https://doi.org/10.1016/0165-1889(88)90041-3

Khatri, Y. (2019, December 12). *Chinese bitcoin miners control 65% of the crypto network's processing power; Bitmain's market share continues to decline*. The Block. https://www.theblockcrypto.com/post/50274/chinese-bitcoin-miners-control-65-of-the-crypto-networks-processing-power-bitmains-market-share-continues-to-decline

Kjærland, F., Khazal, A., Krogstad, E., Nordstrøm, F., & Oust, A. (2018). An Analysis of Bitcoin's Price Dynamics. *Journal of Risk and Financial Management, 11*(4), 63. https://doi.org/10.3390/jrfm11040063

Kristoufek, L. (2020). Bitcoin and its mining on the equilibrium path. *Energy Economics*, *85*, 104588. https://doi.org/10.1016/j.eneco.2019.104588

Lütkepohl, H., (1993). *Introduction to Multiple Time Series Analysis* (2nd edition). Springer-Verlag, Berlin.

Marian, O. (2013). Are Cryptocurrencies Super Tax Havens? Mich. L. Rev. *First Impressions*, *112*, 38–38.

Meynkhard, A. (2019). Fair market value of bitcoin: Halving effect. *Investment Management and Financial Innovations*, *16*(4), 72–85. https://doi.org/10.21511/imfi.16(4).2019.07

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3440802

Olsen, R. (2022, January 2). *Billionaire Crypto Pioneer Jihan Wu Says Market Will Grow To Tens Of Trillions Of Dollars*. Forbes. https://www.forbes.com/sites/robertolsen/2021/12/23/billionaire-crypto-pioneer-says-market-will-grow-to-tens-of-trillions-of-dollars/?sh=2ab84f5274d9

Pagnotta, E., & Buraschi, A. (2018). An Equilibrium Valuation of Bitcoin and Decentralized Network Assets. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3142022

Park, S., Im, S., Seol, Y., & Paek, J. (2019). Nodes in the Bitcoin Network: Comparative Measurement Study and Survey. *IEEE Access*, *7*, 57009–57022. https://doi.org/10.1109/ACCESS.2019.2914098

Prat, J., & Walter, B. (2021). An Equilibrium Model of the Market for Bitcoin Mining. *Journal of Political Economy*, *129*(8), 2415–2452. https://doi.org/10.1086/714445

Rebello, G. A. F., Camilo, G. F., Guimarães, L. C. B., de Souza, L. A. C., Thomaz, G. A., & Duarte, O. C. M. B. (2021). A security and performance analysis of proof-based consensus protocols. *Annals of Telecommunications*. https://doi.org/10.1007/s12243-021-00896-2

Savelyev, A. (2018). Copyright in the blockchain era: Promises and challenges. *Computer Law and Security Review*, *34*(3), 550–561. https://doi.org/10.1016/j.clsr.2017.11.008

Shanaev, S., Sharma, S., Shuraeva, A., & Ghimire, B. (2019). The Marginal Cost of Mining, Metcalfe's Law and Cryptocurrency Value Formation: Causal Inferences from the Instrumental Variable Approach. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3432431

Shen, S., & Galbraith, A. (2021, June 25). *China's ban forces some bitcoin miners to flee overseas, others sell out*. Reuters. https://www.reuters.com/technology/chinas-ban-forces-some-bitcoin-miners-flee-overseas-others-sell-out-2021-06-25/

Song, Y.-D., & Aste, T. (2020). The Cost of Bitcoin Mining Has Never Really Increased. *Frontiers in Blockchain*, *3*(October), 1–8. https://doi.org/10.3389/fbloc.2020.565497

Stoll, C., KlaaBen, L., & Gallersdörfer, U. (2019). The Carbon Footprint of Bitcoin. *SSRN Electronic Journal, June*. https://doi.org/10.2139/ssrn.3335781

Toda, H. Y., & Yamamoto, T. (1995). Statistical inference in vector autoregressions with possibly integrated processes. *Journal of Econometrics*, *66*(1–2), 225–250. https://doi.org/10.1016/0304-4076(94)01616-8

Viglione, R. (2015). Does Governance Have a Role in Pricing? Cross-Country Evidence from Bitcoin Markets. *SSRN Electronic Journal*, 1–31. https://doi.org/10.2139/ssrn.2666243

Yasuda, K., & Sasaki, Y. (2010). Cryptographic Hash Functions. *IEICE ESS Fundamentals Review*, *4*(1), 57–67. https://doi.org/10.1587/essfr.4.57

Data Source

Cipher Mining Inc. (2021, November 12). *Cipher Mining Provides Third Quarter 2021 Business Update*. GlobeNewswire News Room. https://www.globenewswire.com/news-release/2021/11/12/2333244/0/en/Cipher-Mining-Provides-Third-Quarter-2021-Business-Update.html

Difficulty - Bitcoin(BTC) - BTC.com Professional Data Service for Global Blockchain Enthusiasts. (2009). [Dataset]. https://btc.com/btc/insights-difficulty

Haig, S. (2020, March 23). *Bitmain S19 Antminers Sell Out, Won't Ship Until May 11*. Cointelegraph. https://cointelegraph.com/news/bitmain-s19-antminers-sell-out-wont-ship-until-may-11

Madore, P. H. (2018, November 10). *Bitmain Releases Antminer S15: How it Stacks Up Against Competitors*. Yahoo Finance. https://finance.yahoo.com/news/bitmain-releases-antminer-s15-stacks-131706332.html#:%7E:text=Bitmain%20Releases%20Antminer%20S15%3A%20How%20it%20Stacks%20Up%20Against%20Competitors,-P.%20H.%20Madore&text=Bitmain%20has%20released%20(and%20already,bargains%20as%20mining%20hardware%20goes

Marathon Digital Holdings, Inc. (2021, March 31). Form 10-Q. https://ir.marathondh.com/sec-filings/all-sec-filings/content/0001493152-21-010910/0001493152-21-010910.pdf

Mining hardware comparison (2018, January 22). In Bitcoin Wiki. https://en.bitcoin.it/wiki/Mining_hardware_comparison

Otieno, N. (2021, December 29). *Marathon Digital Buys 78,000 Antminer S19 XP Bitcoin Miners Worth Almost $900M*. Blockchain & Bitcoin News. https://blockchain.news/news/marathon-digital-buys-78-000-antminer-s19-xp-bitcoin-miners-worth-almost-$900-million-from-bitmain

Pagliari, E. (2019, May 20). *Bitmain Antminer S17: i nuovi ASIC a 7nm per il mining di bitcoin*. The Cryptonomist. https://cryptonomist.ch/2019/04/09/bitmain-antminer-s17-asic-7nm-mining-bitcoin/#:%7E:text=Nella%20modalit%C3%A0%20risparmio%20energetico%20invece,%2C%20infatti%2C%20costa%201886%20dollari

Realtime mining hardware profitability. (2022). Asic miner value. https://www.asicminervalue.com/

Riot Blockchain, Inc. (2020, December 31). Form 10-K. https://www.riotblockchain.com/investors/sec-filings/annual-reports##document-4279-0001079973-21-000221-2

Strack, B. (2022, January 5). *Bitcoin Miners Marathon Digital, Hut 8 Plot Hashrate Growth*. Blockworks. https://blockworks.co/bitcoin-miners-marathon-digital-hut-8-plot-hashrate-growth/

Whinstone U.S. (2021). Riot Blockchain, Inc. https://www.riotblockchain.com/bitcoin-mining/whinstone-u-s

A Appendix A

A.1. Glossary

ASIC: An application-specific integrated circuit (ASIC) is an integrated circuit (IC) customized for a particular use. In Bitcoin mining hardware, ASICs can perform the cryptographic calculation (the cryptographic function is SHA256 for Bitcoin) and produce more than 100 Tera Hashes in a second (100 TH/s).

Block: A group of transaction with a fingerprint of the previous block. The block header is hashed to produce the Proof-of-Work. Blocks are added to the blockchain. Miners receive a reward every time they add a new block.

Block Reward: After adding a block to the blockchain, the winner miner receives a reward. The reward is a determined number of bitcoins.

CPM: Cost of production Model, a model developed by Hayes (2017) for estimating the cost of producing bitcoins.

Difficulty: The difficulty is a measure of how difficult is to mine a Bitcoin block. It is updated every 2016 blocks added to the blockchain. It is expressed by a number starting from 1 in January 2009 and in march 2022 was about $2.73 \cdot 10^{13}$.

EEF: Energy Efficiency, ASICs require a significant amount of power to work. The ratio between the power consumption and the Hashes per second gives the Energy Efficiency. In general, It is expressed in kj/TH, j/TH or j/GH.

Exchange: A bitcoin exchange is a digital marketplace where traders can buy and sell bitcoins using different fiat currencies or altcoins. A bitcoin currency exchange is an online platform that acts as an intermediary between buyers and sellers of the cryptocurrency.

Halving: Every 210,000 blocks added to the blockchain the number of bitcoin rewarded for adding a block halves. There are a total of 32 halving planned and after the last one the bitcoin supply stops, only the existing bitcoin can be exchanged.

Hash: The hash is a non-invertible function that maps an arbitrary length string to a predefined length string. There are numerous algorithms that implement hash functions with particular properties that depend on the application, in Bitcoin case is SHA256.

Hashrate: The hashrate is a measure of the computational. It expresses the number of hashes computed in a second (H/s).

Nonce: A counter used to change the values hashed and solve the Proof-of-Work challenge.

Miner: A network node that finds a valid Proof-of-Work for new blocks to be added to the blockchain.

Network: A peer-to-peer network that propagates transactions and blocks to every node on the network.

Proof-of-Work: A piece of data that requires significant computations to find. In bitcoin miners need to find a value that is below the target value established by the algorithm.

Target: The Proof-of-Work value must produce a hash that is value less than the target. The target works inversely to the difficulty, high target means that is easy to find a hash solution, low target means that is hard to find a hash that wins the Proof-of-Work.

B Appendix B

ADF tests, cointegration tests, Granger causality tests were conducted using Gretl 2021a.

B.1. Additional Material

Log Margin Sample 1 summary statistics			
Mean	**Median**	**Minimum**	**Maximum**
0.29741	0.077705	-0.65088	2.3627
Std. Dev.	**C.V.**	**Skewness**	**Ex. kurtosis**
0.65994	2.2190	0.70144	-0.29914
5% Perc.	**95% Perc.**	**IQ range**	**Missing obs.**
-0.52560	1.4450	1.0571	0

Table B.1: Margin Sample 1 summary statistics.

Engle-Granger Cointegrating Regression Dependent Variable Log Price				
	coefficient	**std. error**	**t-ratio**	**p-value**
const	3.57988	0.464064	7.714	**4.31e-013**
l_BTC_InCost	0.340284	0.0982274	3.464	**0.0006**
time	0.0177627	0.00234050	7.589	**9.26e-013**

Table B.2: Engle-Granger Cointegration Regression Sample 1.

Additional information on the regression Price and BTC_InCost

Mean dependent var	7.999818	S.D. dependent var	1.748018
Sum squared resid	80.05058	S.E. of regression	0.605974
R-squared	0.880917	Adjusted R-squared	0.879824
Log-likelihood	−201.3722	Akaike criterion	408.7444
Schwarz criterion	418.9389	Hannan-Quinn	412.8608
rho	0.944756	Durbin-Watson	0.065213

ADF test on Residuals

Augmented Dickey-Fuller test on residual of the regression

unit-root null hypothesis: a = 1

test without constant

including one lag of (1-L)uhat

estimated value of (a - 1): -0.0582373

test statistic: tau_ct(2) = -3.3924

asymptotic p-value 0.1258

1st-order autocorrelation coeff. for e: 0.014

Normalized Beta – Sample 1				
Y_1	Y_2	Y_1	Y_2	**Trend**
Log (Price)	**Log (Hash)**	1	-0.4027 (0.1731)	-0.0188 (0.0072)
		-2.4833 (0.4189)	1	0.0466 (0.0115)
Log (Rev)	**Log (TotCost)**	1	-0.6056 (0.308)	-0.0136 (0.0056)
		-1.6512 (0.3118)	1	0.0226 (0.0066)

Table B.3: Normalized Beta Sample 1.

Normalized Beta - Sample 2				
Y_1	Y_2	Y_1	Y_2	**Trend**
Log (Price)	**Log (BTC_EnCost)**	1	-4.3826 (0.9288)	0.0995 (0.0279)
		-0.2282 (0.0686)	1	-0.0243 (0.0021)
Log (Price)	**Log (BTC_InCost)**	1	-1.6601 (0.4652)	0.0079 (0.0128)
		-0.6024 (0.1336)	1	-0.0048 (0.0044)
Log (Price)	**Log (Hash)**	1	-1.5501 (0.3151)	0.0383 (0.0148)
		-0.6451 (0.1061)	1	-0.0247 (0.0034)
Log (Rev)	**Log (TotCost)**	1	-1.5302 (0.4500)	0.0089 (0.0127)
		-0.6535 (0.1095)	1	-0.0058 (0.0036)

Table B.4: Normalized Beta Sample 2.

VECM Regression Price and Bitcoin Energy Cost Sample 2 Dependent Variable: Log First Difference Price					
	Coefficient	**Std. Error**	**t-ratio**	**p-value**	
const	0.780892	0.200879	3.887	0.0002	***
EC_1	0.0229709	0.00608608	3.774	0.0003	***

Table B.5: VECM Regression Price and Bitcoin Energy cost Sample 2.

Mean dependent var	0.024185	S.D. dependent var	0.135235
Sum squared resid	1.650862	S.E. of regression	0.127848
R-squared	0.123611	Adjusted R-squared	0.106257
rho	0.212249	Durbin-Watson	1.566954

VECM Regression Bitcoin Energy cost and Price Sample 2 Dependent Variable: Log First Difference BTC EnCost					
	Coefficient	**Std. Error**	**t-ratio**	**p-value**	
const	0.488554	0.139530	3.501	0.0007	***
EC_1	0.0139226	0.00422738	3.293	0.0014	***

Table B.6: VECM Regression Bitcoin Energy cost and Price Sample 2.

Mean dependent var	0.029915	S.D. dependent var	0.092538
Sum squared resid	0.796486	S.E. of regression	0.088803
R-squared	0.096979	Adjusted R-squared	0.079097
rho	0.023022	Durbin-Watson	1.464061

VECM Regression Price and Hashrate Sample 2 Dependent Variable Log First Difference Price					
	Coefficient	**Std. Error**	**t-ratio**	**p-value**	
const	0.582054	0.346541	1.680	0.0961	*
EC_1	0.0439817	0.0273010	1.611	0.1103	

Table B.7: VECM Regression Price and Hashrate Sample 2.

Mean dependent var	0.024185	S.D. dependent var	0.135235
Sum squared resid	1.836519	S.E. of regression	0.134846
R-squared	0.025052	Adjusted R-squared	0.005746
rho	0.288034	Durbin-Watson	1.420030

VECM Regression Hashrate and Price Sample 2 Dependent Variable Log First Difference Hashrate					
	Coefficient	**Std. Error**	**t-ratio**	**p-value**	
const	0.759736	0.147451	5.152	1.28e-06	***
EC_1	0.0566187	0.0116164	4.874	4.07e-06	***

Table B.8: VECM Regression Hashrate and Price Sample 2.

Mean dependent var	0.041577	S.D. dependent var	0.063145
Sum squared resid	0.332490	S.E. of regression	0.057376
R-squared	0.190422	Adjusted R-squared	0.174391
rho	−0.035938	Durbin-Watson	2.066037

VAR Dependent Variable Log Hash – Sample 1					
	Coefficient	**Std. Error**	**t-ratio**	**p-value**	
const	0.106411	0.0915044	1.163	0.2461	
l_Hash_1	0.982775	0.00730354	134.6	<0.0001	***
l_Price_1	0.0338207	0.00711539	4.753	<0.0001	***
time	−0.000542280	0.000355434	−1.526	0.1286	

Table B.9: VAR(1) Log Hash and Log Price Sample 1.

Mean dependent var	15.90408	S.D. dependent var	2.616143
Sum squared resid	0.922922	S.E. of regression	0.065367
R-squared	0.999384	Adjusted R-squared	0.999376
F(3, 216)	116860.4	P-value(F)	0.000000
rho	0.031866	Durbin-Watson	1.935110

F-tests of zero restrictions:
All lags of l_Hash F(1, 216) = 18107 [0.0000]
All lags of l_Price F(1, 216) = 22.593 [0.0000]

VAR Dependent Variable Log Price – Sample 1					
	Coefficient	**Std. Error**	**t-ratio**	**p-value**	
const	0.201165	0.201441	0.9986	0.3191	
l_Hash_1	0.00173830	0.0160783	0.1081	0.9140	
l_Price_1	0.956431	0.0156641	61.06	<0.0001	***
time	0.00122294	0.000782466	1.563	0.1195	

Table B.10: VAR(1) Log Price and Log Hash Sample 1.

Mean dependent var	8.005096	S.D. dependent var	1.750239
Sum squared resid	4.472772	S.E. of regression	0.143900
R-squared	0.993333	Adjusted R-squared	0.993240
F(3, 216)	10727.27	P-value(F)	1.1e-234
rho	0.176274	Durbin-Watson	1.643747

F-tests of zero restrictions:
All lags of l_Hash F(1, 216) = 0.011689 [0.9140]
All lags of l_Price F(1, 216) = 3728.2 [0.0000]

VAR Dependent Variable Log Revenues – Sample 1					
	Coefficient	**Std. Error**	**t-ratio**	**p-value**	
const	0.848244	0.512327	1.656	0.0993	*
l_Rev_1	1.15129	0.0671540	17.14	<0.0001	***
l_Rev_2	−0.206641	0.0662928	−3.117	0.0021	***
l_TotCost_1	0.0265293	0.135391	0.1959	0.8448	
l_TotCost_2	−0.0240966	0.134092	−0.1797	0.8576	
time	0.00112260	0.000589759	1.903	0.0583	*

Table B.11: VAR(2) Log Rev and Log TotCost Sample 1.

Mean dependent var	18.24992	S.D. dependent var	1.340731
Sum squared resid	5.359912	S.E. of regression	0.158631
R-squared	0.986322	Adjusted R-squared	0.986001
F(5, 213)	3071.925	P-value(F)	2.5e-196
rho	0.025892	Durbin-Watson	1.915232

F-tests of zero restrictions:

All lags of l_Rev	F(2, 213) =	1342.9 [0.0000]
All lags of l_TotCost	F(2, 213) =	0.020513 [0.9797]
All vars, lag 2	F(2, 213) =	4.8861 [0.0084]

VAR Dependent Variable Log Total Cost – Sample 1					
	Coefficient	**Std. Error**	**t-ratio**	**p-value**	
const	−0.0319146	0.239281	−0.1334	0.8940	
l_Rev_1	0.0336375	0.0313641	1.072	0.2847	
l_Rev_2	0.00112956	0.0309619	0.03648	0.9709	
l_TotCost_1	0.583542	0.0632340	9.228	<0.0001	***
l_TotCost_2	0.386593	0.0626273	6.173	<0.0001	***
time	−0.000372772	0.000275445	−1.353	0.1774	

Table B.12: VAR (2) Log TotCost ang Log Rev Sample 1.

Mean dependent var	17.97101	S.D. dependent var	1.138115
Sum squared resid	1.169175	S.E. of regression	0.074088
R-squared	0.995860	Adjusted R-squared	0.995762
F(5, 213)	10246.06	P-value(F)	1.4e-251
rho	−0.043967	Durbin-Watson	2.087044

F-tests of zero restrictions:

All lags of l_Rev	F(2, 213) =	8.2033 [0.0004]
All lags of l_TotCost	F(2, 213) =	2384.8 [0.0000]
All vars, lag 2	F(2, 213) =	19.064 [0.0000]

List of Figures

List of Tables

List of symbols

Variable	Description	Unit
$\boldsymbol{\beta_t}$	Block reward	BTC/block
$\boldsymbol{\delta_t}$	Difficulty	H/Block
$\boldsymbol{\varphi_t}$	the time between two periods	s
$\boldsymbol{\rho_t}$	Hashrate	Hash/s
$\boldsymbol{\vartheta_t}$	The maximum hashrate reached by the network	Hash/s
$\boldsymbol{E_t}$	Energy costs for producing 2016 blocks	$
$\boldsymbol{EEF_t}$	energy efficiency value of ASIC machines	J/H
$\boldsymbol{WEEF_t}$	Weighted average energy efficiency of the network	J/H
$\boldsymbol{k_t}$	Electricity price	$/kWh
$\boldsymbol{n_t}$	Number of days for producing 2016 blocks	d
$\boldsymbol{I_t}$	Miners' investment during the period of producing 2016 blocks	$
$\boldsymbol{I_0}$	The initial estimated investment of the network	$
$\boldsymbol{d_t}$	Depreciation days of the machines	d
$\boldsymbol{c_t}$	Cost per TH	$\frac{\$}{H/s}$
$\boldsymbol{R_t}$	Miners' revenues for producing 2016 blocks	$
$\boldsymbol{P_t}$	Price of Bitcoin	$
$\boldsymbol{F_t}$	Trasaction Fees of 2016 blocks	BTC

$\boldsymbol{\pi_t}$	Miners' Profit for 2016 blocks	$
$\boldsymbol{P_t^*}$	Break-even Price of bitcoin for producing 2016 blocks	$
$\boldsymbol{C_t}$	Miners' Total Cost for producing 2016 blocks	$
$\boldsymbol{e_t}$	Energy cost for producing a single bitcoin	$
$\boldsymbol{i_t}$	Investment costs for producing a single bitcoin	$
$\boldsymbol{m_t}$	Miners' margin ratio	-

Acknowledgments

Vorrei ringraziare la mia famiglia. Il professore Rocco Roberto Mosconi e tutti quelli che mi sono stati accanto, i miei amici, la mia ragazza e i compagni di corso.