UNIVERSITY OF TURKU

Dynamics of crypto mining

Software Engineering
Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Lassi Harju

Supervisors:
Antero Järvi (UTU)
Tuomas Mäkilä (UTU)

June 2024

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Software Engineering
Programme: Master's Degree Programme in Information and Communication Technology
Author: Lassi Harju
Title: Dynamics of crypto mining
Number of pages: 102 pages, 1 appendix page
Date: June 2024

This thesis studies the role of crypto mining in enabling the crypto phenomenon. Cryptocurrencies and blockchain technology were first described in 2008 by Satoshi Nakamoto in the Bitcoin whitepaper. The Bitcoin network was deployed at the beginning of 2009. It uses the Proof of Work consensus mechanism to validate data and secure the network in an anonymous and decentralized manner.

Crypto mining is the process of repeated hash calculation that secures the network and validates data. Depending on the cryptocurrency and network maturity, various types of equipment are used to calculate the hashes. Currently, Bitcoin mining is done with ASIC-miners that are purpose-built for repeated hash calculations.

The issues of the Proof of Work consensus mechanism are often discussed and presented as major limitations of the technology. Although Proof of Work is recognized as a central piece of blockchain technology, its role in enabling the crypto phenomenon is poorly understood and researched. This thesis looks at bitcoin mining from the environmental, financial, and community perspectives to establish whether mining has played an enabling role in the rapid rise of cryptocurrencies.

The environmental perspective consists of a literature review on the environmental impact of Bitcoin. The financial perspective calculates the gross profit of Bitcoin mining at various points in time. The community perspective analyses crypto and mining related communities and search trends to establish whether mining aids in community creation. Bitcoin provides the most applicable and widely adopted data point on Proof of Work cryptocurrencies.

The thesis finds that although the issues of Proof of Work are often presented as major limitations of the technology, at least currently they do not appear to have a major negative impact on the technology. The thesis concludes that mining has in part enabled the rise and popularity of the blockchain and cryptocurrencies, but further research on the matter is required to establish the extent of the contribution.

Keywords: bitcoin, crypto, cryptocurrency, crypto mining, proof of work, environmental impact, financial, community

Diplomityö
Tietotekniikan laitos, Teknillinen tiedekunta
Turun yliopisto

Oppiaine: Ohjelmistotekniikka
Tutkinto-ohjelma: Tieto- ja viestintätekniikan tutkinto-ohjelma (DI)
Tekijä: Lassi Harju
Otsikko: Dynamics of crypto mining
Sivumäärä: 102 sivua, 1 liitesivu
Päivämäärä: Kesäkuu 2024

Tämä diplomityö tarkastelee kryptolouhinnan roolia ja vaikutusta kryptovaluutat mahdollistavana tekijänä. Kryptovaluutat ja lohkoketjuteknologia kuvailtiin ensimmäisen kerran vuonna 2008 Satoshi Nakamoto -nimimerkillä julkaistussa artikkelissa nimeltä ”Bitcoin Whitepaper”. Bitcoin-verkko julkaistiin vuoden 2009 alussa. Se käyttää konsensusprotokollana työtodistusta, jolla taataan verkon turvallisuus ja tietojen oikeellisuus.

Tiivistefunktioiden toistuvaa laskemista kutsutaan louhinnaksi. Kryptovaluutasta ja verkon kehityksestä riippuen, kryptovaluuttoja voi louhia tavanomaisilla tietokoneillakin. Nykyään bitcoineja voi käytännössä louhia vain tarkoitukseen erityisesti kehitetyillä laitteilla.

Työtodistusprotokollan puutteista ja ominaisuuksista keskustellaan usein, ja ne esitetään merkittävinä haasteina teknologian tulevaisuudelle ja kehitykselle. Vaikka työtodistus tunnistetaan keskeiseksi osaksi kryptovaluuttoja, sen laajempi rooli kryptovaluutat mahdollistavana tekijänä on heikosti ymmärretty. Tämä diplomityö analysoi louhinnan roolia ilmasto-, talous- sekä yhteisönäkökulmista. Tarkoituksena on selvittää, onko kryptolouhinta osaltaan toiminut teknologian kehitystä ja käyttöönottoa tukevana vai rajoittavana tekijänä.

Ilmastonäkökulma tarkastelee Bitcoin verkon sähkönkulutuksesta tehtyjä tutkimuksia kirjallisuuskatsauksella. Talousnäkökulmassa analysoidaan Bitcoin-louhijoiden tuottavuutta eri ajankohtina. Yhteisönäkökulma analysoi kryptovaluuttojen ympärille rakentuneita ryhmiä ja hakukonetilastoja tarkoituksena selvittää, minkälainen rooli louhinnalla on yhteisöjen synnyssä ja valuuttojen suosiossa. Bitcoinia käytettiin tutkimuksen kohteena, koska se on tunnetuin, yleisimmin ja pisimpään käytössä oleva työtodistuskryptovaluutta.

Tutkimuksen tulokset osoittavat, että vaikka työtodistusprotokollan ominaisuuksia pidetään usein erittäinkin ongelmallisina, eivät ne näytä vaikuttava negatiivisesti verkon kehitykseen. Lopuksi työssä todetaan, että louhinta on osaltaan mahdollistanut kryptovaluuttailmiön ja lohkoketjujen suosion, mutta lisätutkimusta vaaditaan, jotta merkittävyyttä voitaisiin arvioida paremmin.

Avainsanat: bitcoin, krypto, kryptovaluutta, louhinta, työtodistus, ilmastovaikutukset, talous, yhteisö

Table of contents

Abbreviations and acronyms.

51% attack A situation where a malicious actor or actors control over the majority of decision power in a blockchain network.

Altcoin Cryptocurrency other than Bitcoin

ASIC Application-specific integrated circuit

BECI Bitcoin Energy Consumption Index (Digiconomist)

Byzantine General Problem Inherent challenge of distributed systems where one party cannot be certain that a message from another is valid.

CBECI Cambridge Bitcoin Electricity Connsumption Index (CCAF)

CCAF Cambridge Centre for Alternative Finance

Cold storage In the context of cryptocurrencies, cryptocurrencies stored offline.

Cold wallet same as **Cold storage**

CPA Customer Profitability Analysis. Accounting method used to attribute revenue and sales to a specific customer.

CPU Central processing unit

Fiat currency Government-issued currency

FPGA Field programmable array

Fully cooperative group action Shared interest and a common goal regarding interest in the context of participation ex. collaborative projects.

GH Gigahash

GPU Graphics processing unit

Gross profit Profit after direct costs. In chapter 4 calculations refers to profit after cost of electricity.

IC Integrated circuit

kWh Kilowatt-hour

Merkle root Hash summary of a **Merkle tree**.

Merkle tree a data structure where each node is associated with a hash of the data.

Minimally cooperative group action Shared interest, but not necessarily a common goal regarding that interest in the context of participation ex. help forums.

MW Megawatt

NIST National Institute of Standards and Technology

Nonce number used only once. Used together with data to alter resulting hash.

NSA National Security Agency

Partially cooperative group action Shared interest and some shared goals, but action not dictated strongly by common goals ex. forums on a highly specific topic.

PoS Proof of Stake

PoW Proof of Work

SNS Social Networking Sites

TH Terahash

USD United States Dollar

1 Introduction

Cryptocurrencies are a form of digital currency that utilize the blockchain, a type of public ledger that contains records of all transactions that have taken place within a specific blockchain. Many of the technologies used to create the blockchain are based on research and related works going back several years, even decades. Although previous partial implementations of similar concepts exist, the first time these separate ideas were brought together is considered to be in the Bitcoin whitepaper in 2008 and the release of the Bitcoin network in early 2009. The whitepaper described a solution for achieving consensus in a decentralized network, known as the Byzantine Generals Problem, by utilising proof of work. In the context of cryptocurrencies, these solutions are generally known as the consensus mechanism or consensus protocol.

The term proof of work can refer to either the mathematical concept or the consensus mechanism. The mathematical concept was first introduced in a paper titled "Pricing via Processing or Combatting Junk Mail" by Dwork and Naor in 1993. The idea behind proof of work was to demand users to exert a certain amount of effort for the message to be accepted as valid. For spammers sending millions of emails, this would require considerable computational resources to facilitate such a volume of messages.

The Bitcoin network adapted proof of work for validating data in a decentralized network, by demanding that computational resources must be exerted for data to be suggested to be added to the network. This consensus mechanism is called Proof of Work. For each data block, a specific number used only once, or *nonce* must be found, that when hashed together with the rest of the data produces a hash that fulfils the network requirements. The requirements or difficulty scale dynamically with the hash rate of the network to maintain a pre-defined block time. For the Bitcoin network the block time is defined as 10 minutes. In this thesis, the capitalized term Proof of Work and acronym PoW refer to the consensus mechanism. The process of finding the correct *nonce* in a PoW blockchain is called mining.

To find the correct *nonce*, miners perform repeated hash calculations. Each block is cryptographically linked to the previous by including a hash of the previous block in the current block, forming a chain of blocks. The miner who finds the correct *nonce* and the resulting hash that fulfils the network requirements receives the block reward and a share of the transaction fees of the specific block. Rewarding miners incentivises participation, offering a solution to some of the recognized challenges of peer-to-peer networks (Feldman et al., 2006) (Ihle et al., 2023). Block rewards also implement the gradual release of new coins as there is no centralized authority in charge of regulating the amount of currency in circulation, such as central banks. In the Bitcoin network, hash calculations were originally performed using generic computer hardware, but currently even the fastest computer hardware is obsolete as mining requires the use of specific, purpose-built hardware.

The PoW protocol, while revolutionary, is not without its flaws. The protocol is inherently power hungry and the process of calculating hashes is ultimately wasted effort. With Bitcoin mining growing from an enthusiast hobby to a billion-dollar industry, the issues produced by the inherent qualities of the protocol have been pushed to forefront of the conversation around cryptocurrencies. While various alternative solutions have been developed, PoW cryptocurrencies account for over 50% of the overall market capitalization of cryptocurrencies, driven largely by Bitcoin. The sustained popularity of Bitcoin suggests that mining could play a larger role in enabling the crypto phenomenon than is often recognized. Although PoW was originally widely recognized as a breakthrough, many seem to consider it as somewhat of a remnant of a bygone era, incompatible with the push for more sustainable technologies.

1.1 Goal of thesis

The goal of this thesis is to study the role of mining in enabling the crypto phenomenon by analysing the dynamics of crypto mining from different perspectives. The approach will focus on key aspects affecting and defining its nature. The specific approach will be defined based on a cursory overview of related academic works and other relevant materials and publications.

This analysis will focus on mining through Bitcoin, as it offers the most comprehensive and applicable data point on Proof of Work. Other cryptocurrencies are used as comparisons, when necessary, but they will not be featured extensively. The process of choosing the approach is explained in depth in chapter 1.3.

1.2 Problem statement

Since being first described in 2008, blockchain technology has been adapted for a wide range of applications in various fields, such as data management and verification, finance, and many others (Zīle & Strazdiņa, 2018). The technical implementation of the technology has evolved with the invention of new consensus mechanisms and other technical innovations, in some cases even replacing features in existing cryptocurrencies. The blockchain remaining relevant for over a decade since its inception has proven the validity and applicability of the underlying innovation and shown that it is here to stay.

As the technology ages and existing networks continue to mature, the rising electricity demand of many of the original PoW cryptocurrencies has become all too apparent. The ever-increasing computational demands that fuel the increasing electricity demand also results in equipment becoming obsolete in just a few years or even months. While some cryptocurrencies are still mineable with generic computer hardware, many cryptocurrencies, like Bitcoin, are currently only mineable with purpose-built application-specific integrated circuit (ASIC) miners. ASIC mining equipment is built for a single task, meaning that they have limited to no practical applications outside of mining. When the equipment becomes unprofitable it is often retired even if the equipment is perfectly functional, becoming e-waste long before its true end of life.

Cryptocurrencies utilizing the PoW consensus mechanism have been coming increasingly under criticism for the technology being eventually, if not already, unsustainable. With the voices calling for more sustainable approaches in the crypto industry growing louder, some crypto projects have already made the move to implementations of blockchain technology that claim to be more environmentally sustainable and efficient. The developers of the second largest cryptocurrency Ethereum quoted environmental concerns as one of the reasons for moving away from PoW, in addition to addressing potential future issues with scaling, reliance on other industries, and more[1].

While the limitations and shortcomings of the PoW consensus protocol are often cited as major issues, Bitcoin remains the most popular, well known, and adopted cryptocurrency to date, seemingly unhindered by criticism. While consensus mechanisms claiming to be more efficient have been developed and adopted by even some established cryptocurrencies, such as Ethereum, Bitcoin seems to have proven the resilience of the PoW protocol.

Although the validity of the underlying technology has been all but proven, with the blockchain being adapted for a wide variety of uses, and recognized as a frontier technology,

---

[1] *The Merge*. (2022). Ethereum.Org. https://ethereum.org/en/roadmap/merge/

PoW and mining in general are often viewed as little more than a waste of resources. A brute force approach to security, that is at best outdated and something cryptocurrencies should look to move on from. However, PoW and mining introduce several uniquely beneficial characteristics to the dynamic of cryptocurrencies, highlighted by the staying power of Bitcoin in particular. Bitcoin remaining relevant for as long as it has, suggests that mining as an activity plays a more holistic role in enabling the crypto phenomenon than is often recognized.

While new innovations solve some of the perceived issues with existing blockchain technology, they often introduce new considerations and challenges specific to each implementation. It is arguable that while PoW has its issues, it also enables many of the original ideas of cryptocurrencies highlighted in the Bitcoin whitepaper (Nakamoto, 2008). Solving the issues of the current consensus protocol by moving to alternative consensus protocols often introduces significant trade-offs that potentially undermine the original purpose, function, and dynamic intended.

1.3 Research questions

As the sustainability megatrend and other considerations push crypto communities and developers to move away from resource intensive consensus mechanisms, it becomes increasingly important to fully understand the role mining has played in the development and popularity of cryptocurrencies and the potential implications of moving to other implementations of the technology.

The main research question of this thesis is:

- R1. What is the role of crypto mining in enabling cryptocurrencies?

The research question presented is quite broad and it can be answered in many ways. To identify an effective approach, a cursory overview of related materials was conducted. This overview consisted of searching for related academic works using google scholar, reading related media publications, and familiarizing with content on various platforms. As a result, three distinct domains of interest were identified: environmental, financial, and community. In the scope of this thesis, studying these three domains should provide a sufficient basis for answering R1. The justifications for the selection of domains will be presented in more detail at the beginning of each research chapter.

The sheer number of cryptocurrencies in existence would make analysing all of them a monumental effort, going well beyond the scope of this thesis. To narrow the scope of the research, the environmental and financial research will be looking at Bitcoin mining specifically, as Bitcoin is by far the largest and most established example of a PoW cryptocurrency. For context, the market capitalization of Bitcoin was reported at 1,22 trillion USD and the total market capitalization of the 150 largest PoW cryptocurrencies was 1,28 trillion USD in early 2024.[2] Data and research availability were also considered. While Bitcoin is widely featured in research and data is publicly available, data availability for other PoW cryptocurrencies, even the more popular ones, is at best limited.

Due to the nature of the community research, other cryptocurrencies are featured in this chapter, as looking at Bitcoin alone would provide limited data on the importance of mining with regards to community creation. The selection here will feature several popular PoW cryptocurrencies.

Based on the three domains and the limitations of scope described, the following additional research questions were formulated to help answer R1:

- R2. What is the environmental impact of Proof of Work and how resource intensive is the activity?
- R3. What do the financials of mining Proof of Work cryptocurrencies look like?
- R4. How does crypto mining contribute to the community creation of a cryptocurrency?

Mining has been at the centre of the crypto phenomenon since the beginning, but its true role seems poorly understood. This thesis aims to study crypto mining not just in terms of being a technical solution, but as means to solving several issues that often hinder peer-to-peer (P2P) systems, limiting their usefulness and adoption. Furthermore, mining seems to play a misunderstood role in the crypto phenomenon being more than just an activity for profit or technical solution, but rather enabling key elements of a true grass roots movement designed to build a community by incentivizing adoption and engagement with tangible rewards.

---

[2] PoW Coins, Tokens, Cryptos & Assets. (n.d.). *CryptoSlate*. Retrieved May 8, 2024, from https://cryptoslate.com/cryptos/proof-of-work/

1.4 Structure

This thesis consists of six chapters in four sections, the introduction, background, research, and finally conclusions. The introduction gives the reader a concise overview of the contents of the thesis and describes the research problem. The background section provides a general background that gives a brief description of blockchain technology and describes the most relevant services and terms, and a more in-depth chapter on mining providing additional information relevant to the topic. Due to cryptocurrencies being still relatively unknown, it was deemed necessary to include a broader background section to give the reader a general context of the topic.

The research in this thesis consists of three separate chapters for the environmental (R2), financial (R3), and community (R4) perspectives. Each research chapter starts with a justification for the selected perspective, followed by the research, and a short discussion of the findings of the specific chapter and how it pertains to the research question associated with the chapter.

The findings of the individual research questions will be discussed in the conclusion in chapter 6 to answer R1.

1.5 Methodology

Different approaches were selected for each chapter of the research sections. The environmental and financial sections will focus on analysing PoW through Bitcoin, as it is the best example of a mature PoW cryptocurrency.

The environmental section will be based on a literature review of Bitcoin mining. Select databases will be searched using the appropriate keywords to find relevant research and form an idea of the environmental impact and overall resource intensity of the activity. This chapter answers R2 “What is the environmental impact of Proof of Work and how resource intensive is the activity?” An in-depth justification for the perspective can be found at the beginning of chapter 3. A description of the methodology and the research method of this section can be found in chapters 3.1 and 3.2 respectively.

The financial analysis will build on profitability calculations of mining Bitcoin at select points in time using various hardware. This chapter will use historical profitability data and publicly available data on mining equipment and its efficiency to estimate the profitability, prospects, and general dynamics of mining. This chapter answers R3 “What do the financials of mining Proof of Work cryptocurrencies look like?” An in-depth justification for the perspective can be found at the beginning of chapter 4. A description of the methodology and the research method of this section can be found in chapters 4.1 and 4.2 respectively.

Finally, in the community chapter the research will look at the community size and activity levels of select communities and subforums on bitcointalk.org and various subreddits, to gauge the community building aspects of mining. Additionally, google trends data of Bitcoin will be compared to other cryptocurrencies to see whether it tells anything about the relative importance of mining. This chapter answers R4. “How does crypto mining contribute to the community creation of a cryptocurrency?” An in-depth justification for the perspective can be found at the beginning of chapter 5. A description of the methodology and the research method of this section can be found in chapters 5.1 and 5.2 respectively.

2 Basics of cryptocurrencies

This chapter gives the reader a brief overview of various aspects of blockchain technology. First, the origins and motivations of the technology will be explained followed by a summary of the development stages from 2009 to present day. Next, the basics of blockchain technology, including an explanation of consensus mechanisms, most relevant services, and general terms will be presented. Note, that the focus of this thesis is not on the technical implementation of blockchain technology, and as such several finer technical details are omitted or simplified.

Regulatory challenges and security considerations are complex and nuanced topics that are covered only for the parts that are relevant to the topic of the thesis.

2.1 Origins

The 2008 Bitcoin whitepaper by pseudonymous author Satoshi Nakamoto described a digital, decentralized peer-to-peer currency that relies on a hash-based Proof of Work network for securing and validating transactions. These transactions are stored in a public ledger called the blockchain, which uses past transaction data to generate new blocks and cryptographically links them together, thus creating a chain of blocks (Nakamoto, 2008). While Bitcoin is generally viewed as the first cryptocurrency, some of the history of the technology dates back several decades with various pieces being described in academic works by multiple authors. Sherman et. al list the following timeline in Table 1 of published works related to cryptocurrencies in their 2018 paper “On the origins and variations of Blockchain Technologies.”

Table 1 Timeline of selected discoveries in cryptography and blockchain technology. (Sherman et. al, 2018)

Year	Title of paper
1970	James Ellis, public-key cryptography discovered at GCHQ in secret
1973	Clifford Cocks, RSA cryptosystem discovered at GCHQ in secret
1974	Ralph Merkle, cryptographic puzzles (paper published in 1978)
1976	Diffie and Hellman, public-key cryptography discovered at Stanford
1977	Rivest, Shamir, Adleman, RSA cryptosystem invented at MIT
1979	David Chaum, vaults and secret sharing (dissertation 1982)
1982	Lamport, Shostak, Pease, Byzantine Generals Problem
1992	Dwork and Naor, combating junk mail

Year	Title of paper
2002	Adam Bach, Hashcash
2008	Satoshi Nakamoto, Bitcoin
2017	Wright and Savanah, nChain European patent application (issued in 2018)

While many individuals have stepped forward claiming to be behind the pseudonym Satoshi Nakamoto, none have managed to produce convincing evidence. The author or authors behind the pseudonym thus remain anonymous even today leaving many open questions as to the specifics of how the technology was developed and the contributions of works beyond the references mentioned in the whitepaper.

Compared to traditional currencies, cryptocurrencies are purely digital, meaning they are not tied to anything physical such as coins, bills, or gold. While the transaction ledger is public, the decentralized P2P system allows for a degree of anonymity and limits the control of centralized authorities, such as governments or central banks. As there is no governing authority with control over the blockchain, anyone can create a wallet on the blockchain, send, and receive Bitcoin without interaction with a bank or other financial institution. Anonymity, decentralization, and independence from the financial system were among the key reasons cited in the Bitcoin whitepaper for developing a new method of payment (Nakamoto, 2008).

2.2 The blockchain

Cryptocurrencies utilize what is known as the blockchain to store transaction data. In simplest terms, a blockchain is as the name implies, a chain of blocks where each block contains some data and a hash of the previous block, linking them together. Hashing is a core concept commonly utilized in blockchain technology. A hash is the result of a hash-function, which takes an input of any length and outputs a fixed length string. Depending on the length of the hash the chances of a collision, or two distinct data sets producing the same hash, vary. For modern hashing algorithms this chance is negligible. The hash of the previous block is included in each block for security and data integrity, as any attempt to alter past data would immediately change the result of the hash, making manipulation immediately apparent. This method of linking data together creates a data structure that is immutable and resistant to manipulation, as any changes would not only force the recalculation of the hash in the block that was altered, but in all subsequent blocks. An illustration of the basic data structure of the blockchain is presented in Figure 1.

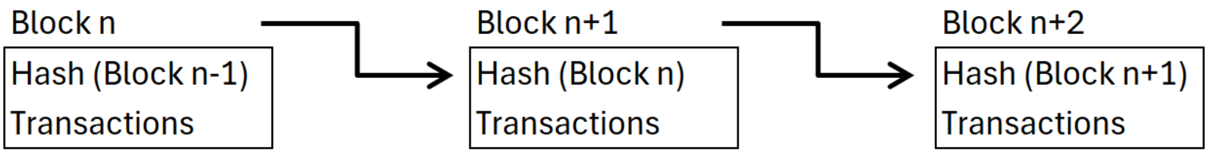


Figure 1 Simplified illustration of the structure of a blockchain.

In practice, the structure of the blocks is somewhat more complicated. Each block consists of a header and a body which contains the raw data. The headers are used to link blocks together and maintain data integrity, by including the hash of the current and previous blocks. The header contains various additional configuration data, such as timestamps and difficulty, but also a Merkle root of the transactions. A Merkle root is the hash summary of a Merkle tree, a data structure where each data block is associated with a hash of the data. While the Merkle root does not store all the transactions, it provides an efficient way of monitoring whether data has been altered, as any changes to the transactions would alter the hash of the transaction data and produce a different hash summary.

In a PoW blockchain, such as Bitcoin, the header also contains the *nonce* which facilitates mining. Miners repeatedly hash the block header to find a *nonce* that fulfils the difficulty target defined in the block header. The miner who finds a suitable hash earns the right to suggest data to the network. The suggested block is broadcasted to other nodes in the network, which verify the correctness of the *nonce* and block data. A more descriptive illustration of the structure of a PoW blockchain is presented in Figure 2.

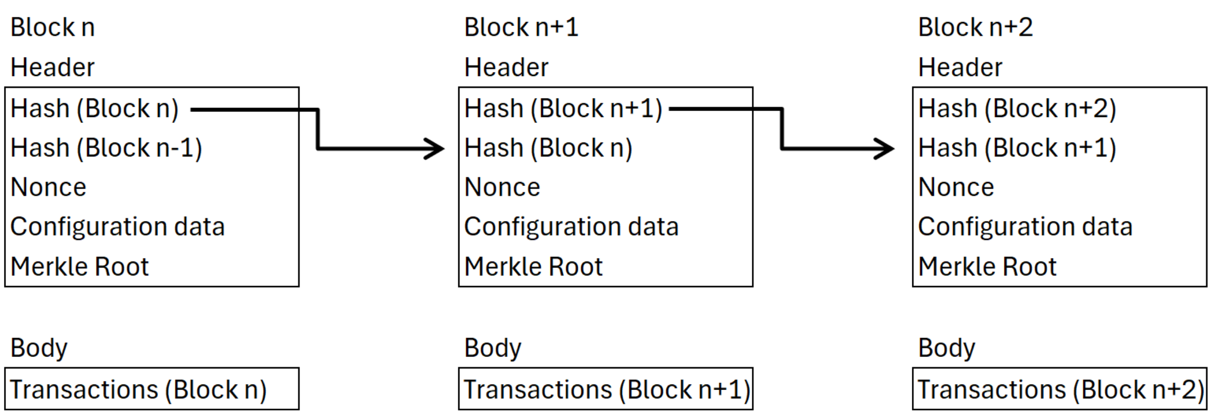


Figure 2 Detailed example of the structure of a PoW blockchain.

While the structure of the blockchain is relatively simple, the inner workings of the blockchain are much more complicated. Cryptocurrencies rely heavily on modern cryptography and one-way functions developed in the 70's (Sherman et al., 2019). For example, blockchain wallets are essentially just keypairs, where the private key is used to generate the public key and ultimately the wallet address. Transactions are signed using the private key, taking advantage of the qualities of public key cryptography, namely signatures. Signatures allow for the blockchain network to verify transactions without knowing the private key (Antonopoulos & Harding, 2023).

Although its structure gives the blockchain an inherent resistance to manipulation, it does not prevent it entirely. The Byzantine Generals Problem, or double spending, is an inherent issue with decentralized networks, where users cannot know for sure whether messages are genuine or not as there is no centralized authority in charge of verification. The major contribution of the Bitcoin whitepaper was a solution to validating transactions in a decentralized network using the PoW consensus mechanism. While robust, the mechanism has its limitations.

2.3 Consensus mechanisms

The consensus mechanism dictates how a blockchain adds and validates new data. Various methods and technological implementations have been developed, but it is important to understand how the choice of consensus mechanism is more than just a technical consideration. The purpose of this section is to give not only a brief technical overview of select consensus mechanisms, but to give some context as to its role in determining how a cryptocurrency is used and how its userbase develops. Several finer details and considerations regarding the technical implementations are omitted.

Since the launch of Bitcoin many cryptocurrencies have come out with new consensus mechanisms to solve existing issues. Despite offering solutions to some of the existing problems, each newer implementation has had its own pros and cons and ultimately failed to reach the level of adaptation of Bitcoin, at least for now. It is worth noting here, that some cryptocurrencies implement several consensus mechanisms or their characteristics in some capacity, and some, such as Ethereum have made the change from one protocol to another.

The following chapters on consensus mechanisms are based on (Chaudhry & Yousaf, 2018) and (Antonopoulos & Harding, 2023) unless otherwise stated.

2.3.1 Proof of Work

The Proof of Work consensus mechanism requires each block to be validated by computational work. The work is done by specialized nodes in the network called miners. While full nodes store the entire blockchain, relay transactions, and verify the results of the mining process, miners perform the hash calculations required to secure the network and make it immutable. In a Proof of Work blockchain each block has a set difficulty value. The difficulty is a predefined condition that the hash of the block must fulfil to be accepted. Miners perform repeated hashing calculations with different *nonces* to find the correct one that adheres to the difficulty condition. As a PoW network matures, the difficulty increases, and the number of hashes required to find the correct results subsequently increases. The nature of a hash-function is that while the hash is laborious to find initially, it is trivial to validate. The full nodes responsible for accepting or rejecting the result are therefore easily able to verify, whether the suggested *nonce* was correct or not.

The total network hashing power or hash rate is the approximate sum of the hashing power of all mining equipment. Network hash rate is always an estimate based on block time and difficulty and can vary largely depending on the cryptocurrency. For Bitcoin, in 2024 the network hash rate is measured in exahashes per second (EH/s, 10^{18}) range whereas equipment hash rate is measured in terahashes per second (TH/s, 10^{12}).

The computational work required to generate a new block ensures that it is practically impossible to alter data in past blocks as the computational resources required are not readily available. Once the correctness of the *nonce* has been validated, the miner who found the correct *nonce* is rewarded the block reward and a share of the transaction fees included in the block.

Although PoW offers an effective way of securing and validating blocks, it is arguably a brute force approach to security. The computational work expended to generate the hashes is ultimately wasted effort and while hashing is a straightforward process and the size of the data being hashed is not very significant, the sheer number of possibilities means that the process must be repeated a significant number of times to find the correct result. The devices used in the hashing process vary depending on the crypto, but regardless of the algorithm consume considerable amounts of electricity and generate e-waste in the process.

Despite its drawbacks the PoW consensus mechanism remains quite popular. Notable cryptocurrencies using the protocol include Bitcoin, Litecoin, Dogecoin and Ethereum until September of 2022.

2.3.2 Proof of Stake

In response to the issues of PoW, new consensus mechanisms have been developed. In a Proof of Stake (PoS) blockchain new blocks are validated by validator nodes that have staked or locked a predefined number of coins into the blockchain for a duration of time. Depending on the blockchain, the requirements of becoming a validator vary. On the Ethereum-blockchain for example, to become a validator a user must stake 32 Ethereum worth approximately 48 000-96 000 euros, depending on valuation.[3] Validators are chosen at random from the pool of all potential validators with a sufficient number of staked coins. The chance of becoming a validator is dependent on the number of coins staked, with more coins resulting in a higher chance of being chosen. Validators who correctly validate new blocks according to consensus are awarded a share of the block fees.

One of the main advantages of PoS over PoW is that there is no need for repeated hash calculations. While block data is still linked with hashes, the validation is done solely at the discretion of the chosen validators. The computational requirements of a PoS blockchain are therefore significantly lower than in PoW. As there is no mechanism that would lead to a significant rise in computational requirements as the network matures, the scaling of a PoS blockchain is also significantly more efficient, at least in this regard.

Although there is nothing preventing a validator from trying to vote against consensus, the staked coins ensure that validators are always incentivized to follow network consensus, as attempts to validate false data could lead to a loss of confidence and a drop in value of the cryptocurrency. While this approach does provide some protection against manipulation it is not necessarily enough to discourage such attempts. PoS blockchains also implement a mechanism where any validators attempting to validate data against the consensus will lose their staked coins, resulting in immediate consequences.

---

[3] *Ethereum staking*. (2024). Ethereum.Org. https://ethereum.org/en/staking/

Several variations of the PoS consensus mechanism have been developed, each with slightly different implementations, but the core principle remains the same. Derivatives of Proof of Stake include Delegated Proof of Stake (DPoS) and Pure Proof of Stake (PPos).

2.3.3 Other protocols

In addition to PoW and PoS other, more exotic consensus mechanisms have also been developed. While some emulate many of the characteristic of previous consensus mechanisms, others are designed with a specific purpose in mind, allowing blockchain technology to be adopted for a wide variety of uses and niche applications. Many of these applications offer some novel way to allow users to "mine" the coin. While similar to PoW, in that an activity produces a coin, the specifics are often quite different. Proof of Burn is an example of an emulating consensus mechanism, where the right to mine the coin or validate transactions is earned by burning some of the currency. This introduces a deflationary mechanism, but also rewards miners or validators, depending on the specifics, for their efforts.

Proof of Space or Proof of Capacity require users to have a certain amount of storage capacity to validate data. PoC has been adapted for several use cases. STORJ and Filecoin utilize the storage space in their network for a decentralized file storage system whereas CHIA uses it simply to secure the blockchain. Although these consensus mechanisms are not technically PoW, their implementations have similar characteristics.

Mining is often used to describe any activity and protocol that grants the participant coins (ex. STORJ and CHIA), in the context of this thesis mining refers to the work done in a PoW blockchain.

2.4 Ecosystem

Cryptocurrencies have provided a platform for a host of new services and applications. The role of these services varies from all but necessary for the blockchain to function as intended, to little more than curiosities. Although these services can make the technology more useable and approachable by a wider audience, they are in many cases in major conflict with the core ideas of cryptocurrencies. The unintended side effect of a service of any kind being a requirement for using a cryptocurrency is the resulting centralization. Several high-profile data breaches and programming errors have made headlines since the start of the crypto boom, illustrating the potential consequences of centralization and the additional cumulative risk potentially introduced by these services (Charoenwong & Bernardi, 2021).

This section aims to give a general overview of the ecosystem created around cryptocurrencies. General terms and concepts explained in this section include wallets, exchanges, stablecoins, staking and mining pools. This list is by no means intended as all-encompassing, but it provides a sufficient level of background information and context around the topic.

2.4.1 Wallets

The following chapter on crypto wallets is based on (Suratkar et al., 2020) and (Antonopoulos & Harding, 2023).

Wallets are the blockchain equivalent to a bank account, they allow users to receive and send cryptocurrencies to other wallets in the blockchain. Crypto wallets implement a two key system, where the public key is used to generate the wallet address and another private key is used to sign transactions. Anyone with access to the private key can use the funds in a wallet. Wallets are blockchain specific, meaning a user must create a separate wallet for each cryptocurrency.

Although blockchains offer the tools to create wallets, using them directly requires at least some technical expertise and their use is often clunky and slow at the best of times. The use of various applications is consequently widespread and several applications for managing wallets have been developed. Seed phrases of 12 to 24 words are commonly used as the basis for generating the actual public and private keys. Carefully recording the seed phrases used to generate wallets allows users to recover access to their private keys. However, seed phrases do not allow for recovery of coins that have been transferred from the wallet. Keeping the seed phrase secure is equally important as keeping the private key secure.

Strictly speaking, the creation of wallets is somewhat misleading as all the possible wallets already exist, they are however not in use. When the public and private keys are generated, the wallet is in use. While nothing is inherently preventing another user from generating the same keys, the chances are infinitely small, proportional to the total number of possible wallets which depends on the blockchain. In the Bitcoin blockchain the total number of wallets is 2^{160} whereas the Ethereum wallet address space is 2^{256}. Despite the seemingly large difference between the number of total wallets, the chances of collision are negligible, even with Bitcoin. To date there are approximately 460 million or $2^{28.7}$ Bitcoin wallets in use.

Wallets are categorized as either hot or cold wallets, depending on whether they are connected to the internet. Wallets used through an app are generally software wallets and although exceptions exist, they are not recommended as stores of value as they are used on online devices. Alternative solutions offering arguably better security include hardware and paper wallets. Hardware wallets, such as those offered by Ledger[4], utilize custom hardware that generates the keys and seed phrases completely offline and only shares the public key and signed transactions. Although hardware wallets can sometimes be used through an application, their implementation is quite different to a software wallet and are not subject to the same security issues. A paper wallet on the other hand is as the name suggests a piece of paper with address details printed on it. As generating wallets does not require an internet connection, a wallet can be generated offline, printed, and any related files deleted.

While different blockchains exist individually, various multichain wallets have been developed where users can import all their various crypto wallets from different blockchains. Delegating the handling of private keys to an application can offer additional security and convenience, similar to a password manager, but this depends solely on the quality of the implementation and can in same cases be a double-edged sword in terms of security. Although the user does not have to worry about handling the private keys directly, there is significant trust placed on the software doing what its intended. Furthermore, as all the wallets are behind a single shorter pin this does introduce a new potential weakness.

2.4.2 Exchanges

The following chapter on crypto exchanges is based on (Arslanian, 2022).

Crypto exchanges are platforms where users can exchange their cryptocurrencies for fiat currencies or other cryptocurrencies. Depending on the structure and services provided, exchanges are either centralized or decentralized. Centralized exchanges require users to first transfer their cryptocurrency to the exchanges platform where the user can then convert their coins to either other cryptocurrencies or fiat currencies and transfer funds to a bank account. Decentralized exchanges do not require users to transfer their coins to the exchange, instead

[4] Hardware Wallet & Crypto Wallet—Security for Crypto. (2024). Ledger. https://www.ledger.com/

they only act as a platform facilitating exchange between two users willing to trade the corresponding pair of coins. They also do not allow for exchanging cryptocurrencies to fiat currency.

Centralized exchanges bridge the gap between traditional financial systems and the blockchain by bringing many of the services typically offered by banks to the crypto sphere. Although there are similarities between banks and exchanges, crypto exchanges are not subject to the same regulatory controls or protections as banks. Centralized exchanges are generally not recommended to be used as stores of value, as the user is not directly in possession of their coins. Should the exchange suffer a data breach or otherwise become insolvent, the user would be considered just another creditor with none of the insurance protections that would apply to regular bank accounts and deposits.

Notable centralized exchanges include Binance, Coinbase Exchange, and Bitfinex. Examples of notable decentralized exchanges include Uniswap and since 2023 dYdX.[5] Decentralized exchanges are often open source resulting in many of the same implementations under slightly different names and chains.

2.4.3 Stablecoins

The following chapter on stablecoins is based on (Roberts, 2022) and (Arslanian, 2022).

Stablecoins are cryptocurrencies that are designed to maintain a set exchange rate with some other asset. They aim to provide a non-volatile store of value. Stablecoins can be split into two broader categories, collateralized and non-collateralized. As the name suggest, collateralized stablecoins are backed by the corresponding amount of assets. Depending on the stablecoin, the pegged asset can be a fiat currency, a commodity, or even a regular cryptocurrency. The linked asset determines much of the characteristics of the stablecoin and largely the risks involved. Stablecoins that are linked to more volatile assets generally employ some form of mitigation to limit the effects of changing market rates and maintain the desired stability. Despite the mitigations, these stablecoins are considered somewhat riskier as sufficiently large changes in the value of assets held as collateral could still crash the value of the coin if they go beyond what the mitigations can comfortably manage.

---

[5] *Top Cryptocurrency Exchanges Ranked By Volume*. (2024). CoinMarketCap. https://coinmarketcap.com/rankings/exchanges/

Non-collateralized stablecoins rely on a purely algorithmic approach to maintain the exchange rate. Compared to collateralized stablecoins, the organization responsible for launching the coin does not maintain reserve assets corresponding to the amount of stablecoins in circulation. This approach requires significantly less capital but is much riskier in comparison to collateralized stablecoins as the loss of trust in the stablecoins operation is all that is needed to bring the value down to nothing.

The list of notable failed stablecoins is rather long, TerraUSD (UST) by Terraform labs being a recent prominent example. The value of UST was based on Luna, a token also launched by Terraform Labs which was priced freely on the market. A user who wanted to buy UST would buy the corresponding amount of LUNA from the free market. The LUNA tokens would then be burned, and the user would receive the UST. The burning of tokens was supposed to maintain the value of LUNA tokens and allow traders arbitrage opportunities which would maintain the system in the long run. Despite the seemingly clever approach, the LUNA-UST system was vulnerable to the same loss of confidence as any algorithmic solution. The loss of confidence would ultimately lead to the stablecoin becoming near worthless.

2.4.4 Mining pools

The following chapter on mining pools is based on (Antonopoulos & Harding, 2023).

The use of pools allows users to combine their resources with one another. They are implemented for various purposes by different blockchains and services. The specific uses vary, but the main idea is to lower the threshold of participation required by an individual user. Mining pools allow users to combine their hashing power to achieve a higher chance of finding the correct result. While they do not increase the returns of mining, the rate at which blocks are found is less varied with higher hash rates. As anyone can participate in the mining process, a solo miner might not have the resources to find a block in any reasonable amount of time. This would mean that the effort and resources expended would be completely wasted. Mining pools on the other hand, are able distribute the block rewards accordingly to miners based on their contribution to the pool in finding the block.

Mining pools are a necessity of PoW-blockchains, but they are yet another service that limits decentralizations and adds additional security considerations. Mining pools can consist of tens of thousands of users, but from the blockchains perspective they are a single miner. As the blockchain is based on a consensus protocol, a miner with 51% of the network hash rate would have sole decision power over what data and transactions are validated. Although this would still not jeopardize the private keys of other users, it would allow for other malicious activities, most notably double spending. The concept of a 51% attack is explained in more detail in chapter 2.7.

2.4.5 Staking pools

Like mining pools, staking pools allow users to combine their resources. In this application, users stake smaller amounts of crypto to a pool to combine their staked coins to reach the minimum staking requirements. As with mining pools, this does not result in higher overall returns, but it makes the results less varied and more predictable as a higher number of coins staked results in a higher chance of being chosen as a validator. While staking pools can introduce challenges with centralization, the issues are very similar in nature to the inherent issues with PoS to begin with. Limiting the maximum staking amount would only lead to users with more stakeable coins to divide their coins into smaller stakes, leading to the same outcome. Although again a challenge for decentralization, the nature of PoS significantly limits the potential benefits of voting against consensus as this will lead to the loss of staked funds. (Gersbach et al., 2022)

2.4.6 Other notable services

The crypto space is rapidly evolving with new innovations introduced frequently. In addition to the services mentioned in previous chapters, there are many others that could be listed and further explained. Notable mentions include various services to enhance the privacy of cryptocurrencies such as mixers and anonymizers, various DeFi or Decentralized Financial service platforms, and many others. (Arslanian, 2022)

2.5 Stages and development of cryptocurrencies

This chapter describes the main stages of development of the crypto industry and offers additional insight to the growth and adoption of Bitcoin. The cyclic nature of cryptocurrencies is explained and the coinciding release of new generations of coins and features extending the application of blockchain technology. The price and hash rate development of Bitcoin is also explored.

2.5.1 Stages of cryptocurrencies

Cryptocurrencies have gone through several market cycles since the deployment of the Bitcoin network in 2009. Each boom in the market has been driven by different catalysts and they have gradually introduced new applications for blockchain technology and pushed the market capitalization of cryptocurrencies to new records. The major cycles have taken place in 2014, 2017, 2021, and currently in 2024.

Defining the specific catalyst for each market move can be challenging, as often there are several contributing factors. The 2014 boom is often referred to as have been driven by Bitcoin by the crypto userbase. (Arooj et al., 2022) list the major catalyst for this cycle as cryptocurrencies beginning to receive mainstream attention and generally increased adoption. The 2017 boom is recognized by many as the “altcoin”-boom, driven by Ethereum and other cryptocurrencies that extended the functionality of cryptocurrencies to more than just means of payment. (Arooj et al., 2022) list alternative use cases as a major contributor to the 2017 cycle.

The 2020 cycle had such a wide range of contributing factors that pointing to a single catalyst is impossible. During this cycle several “Eth-killers,” offering similar functionality to Ethereum were introduced. Although each cycle up to this point was associated with a new generation of coins, the most popular cryptocurrencies from previous generations would often record new highs during these cycles. The saying “a rising tide lifts all boats” often associated with economic growth and its effects, applies quite well to the behaviour of the most popular cryptocurrencies during market moves.

Depending on the author, the development of cryptocurrencies can be told in many ways, but major boom cycles have been a hallmark of cryptocurrencies since the beginning. Bitcoin and other cryptocurrencies of the founding era are commonly referred to as 1st generation cryptocurrencies. 2nd generation cryptocurrencies that were the driving factors in the 2017 cycle are commonly called altcoins, however, this definition is often used to also describe any cryptocurrency other than Bitcoin. Ethereum is perhaps the most well-known altcoin. Ethereum started as a PoW cryptocurrency but moved to PoS in 2022. 3rd generation cryptocurrencies are also known as “Eth-killers,” mentioned previously. Later cryptocurrencies are sometimes referred to as 4th and 5th generation coins in some works such as (Hasan et al., 2022). However, the specific definition of 3rd, 4th and 5th generation cryptocurrencies can be challenging as many 3rd generation cryptocurrencies are still being developed and implement many functionalities of later generations. The definition is often done based on original release, rather than current characteristics.

The specifics of categorizing and characterizing cycles can vary depending on the source. The key takeaway is that cryptocurrencies have had several market cycles in this era, and each has been associated with a specific group of coins that has generally extended the functionality of blockchain. The most recent cycle of 2024 was largely set off by increased institutional interest in crypto funds and their eventual approval by the Securities and Exchange Commission.[6]

2.5.2 Development of Bitcoin price and network

Price and history of volatility

The initial stages of Bitcoin were previously explained in the Introduction in chapter 1.0 and Origins in 2.1. The basics of blockchain technology were explained in chapter 2.1. This chapter will give a general outline of the development of the Bitcoin network in terms of hash rate growth and notable events and its historic pricing to provide sufficient context for the research chapters, particularly the financial calculations and related discussions. The chapter is based on (Chohan, 2017) unless otherwise specified.

The first time Bitcoin is thought to have received a valuation was after a 2009 exchange between two users. A Finnish student sold some 5 050 bitcoins for INR 414,65. The transaction gave each bitcoin a valuation of 0,0009 USD.[7] At the time, the technology was still in its infancy and many of the services that users currently rely on to make such transactions were not available.

The lack of services and general adoption at the time means that the early price history is poorly recorded. Most services list the price of Bitcoin starting sometime in 2010. As there is no centralized authority in charge of setting the exchange rate, the price is formed by combining data from various exchanges. This practice of price formation can cause slight differences in the price depending on the resource used.

---

[6] *SEC.gov | Statement on the Approval of Spot Bitcoin Exchange-Traded Products*. (2024, January 10). https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023

[7] Ashmore, D. (2024, May 31). *Bitcoin Price History 2009 to 2024*. Forbes Advisor INDIA. https://www.forbes.com/advisor/in/investing/cryptocurrency/bitcoin-price-history-chart/

The price development of Bitcoin is shown in Figure 3. The first time Bitcoin was valued at 1 USD was in 2011, 100 USD valuation was reached in 2013, and 10 000 USD in 2018. During the 2017-2018 cycle the price of Bitcoin peaked at over 19 000 USD. A bear market following the peak would see the price of Bitcoin drop to below 4 000 USD in late 2018. Although each market cycle has been associated with a certain group of coins, as discussed in the previous chapter, the impact of Bitcoin as a major driver of the crypto market is undeniable. Although the 2017 cycle is commonly associated with altcoins, such as Ethereum, it is also considered to have largely been the result of major speculative investments and fear of missing out (FOMO) on the returns from Bitcoin specifically. In early 2017 Bitcoin was valued at under 1 000 USD climbing to over 2 000 USD by mid-2017. The major strides in valuation led to inflows of additional investments and culminated in the price peaking briefly at over 19 000 USD.

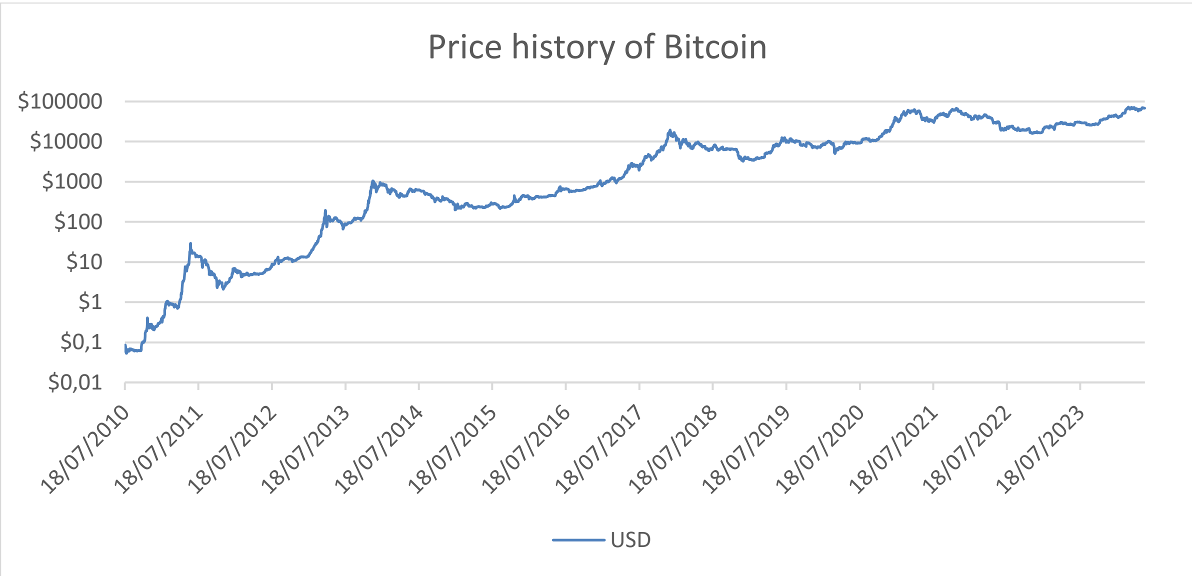


Figure 3 Historical pricing of Bitcoin from 07/2010-04/2024. Data from bitinfocharts.com. Logarithmic scale.

The market cycle which began in 2017 ended in a major crash. By late 2018 the price had plummeted nearly 80%. The crash resulted in much scepticism on whether the technology had any future at all. The price of Bitcoin would not recover or reach similar pricing until the start of the next major market cycle in late 2020, where the price eventually soared to over 60 000 USD in early 2021. The catalyst for the cycle is considered to be the Covid-19 pandemic. The various stimulus packages resulted in equities, real estate, and eventually cryptocurrencies to peak in sequence. Bitcoin peaked a second time in late 2021 before crashing in 2022 reaching a valuation of under 20 000 USD in early 2022. The price would continue to slide until eventually bottoming in late 2022 and early 2023 at approximately 16 500 USD.

(Chohan, 2017) describes the history of the Bitcoin price up until 2022. Starting in mid-2023, Bitcoin started making major gains in valuation following the news of investment companies filing for approval of Spot Bitcoin Exchange Traded Funds (ETF)[8]. The approval of the ETF filing was largely the catalyst of the most recent market cycle during which Bitcoin has pushed past previous highs to an all-time high valuation of nearly 70 000 USD in 2024.

Market capitalization

The market capitalization of cryptocurrencies has grown hand in hand with Bitcoin during each market cycle. Cryptocurrencies reached 10 billion USD valuation during the 2014 cycle but returned to lower levels for several years in the following down market. 10 billion USD valuation was again reached during the 2017 cycle which eventually saw the overall crypto market capitalization increase nearly hundred-fold to some 800 billion USD. 1 trillion USD valuation was reached for the first time during the 2020 cycle. The market peak was reached in late 2021, where the overall market capitalization was at 2,9 trillion USD. The following downturn would again see the market return to levels seen during the early stages of the 2020 cycle. The market capitalization remained at these levels until late 2023.

Bitcoin dominance is a commonly referenced ratio which measures the market capitalization of Bitcoin versus the overall market capitalization of cryptocurrencies. Figure 4 illustrates the development of market capitalization and how the overall market capitalization is highly dependent on the development of Bitcoin. Starting from the 2017 altcoin cycle, the crypto market has separated slightly from Bitcoin, but Bitcoin dominance remains at over 50% in 2024.

---

[8] *BlackRock's iShares Files for Spot Bitcoin ETF | CoinMarketCap*. (2023). CoinMarketCap Academy. Retrieved June 4, 2024, from https://coinmarketcap.com/alexandria/article/blackrock-s-ishares-files-for-spot-bitcoin-etf

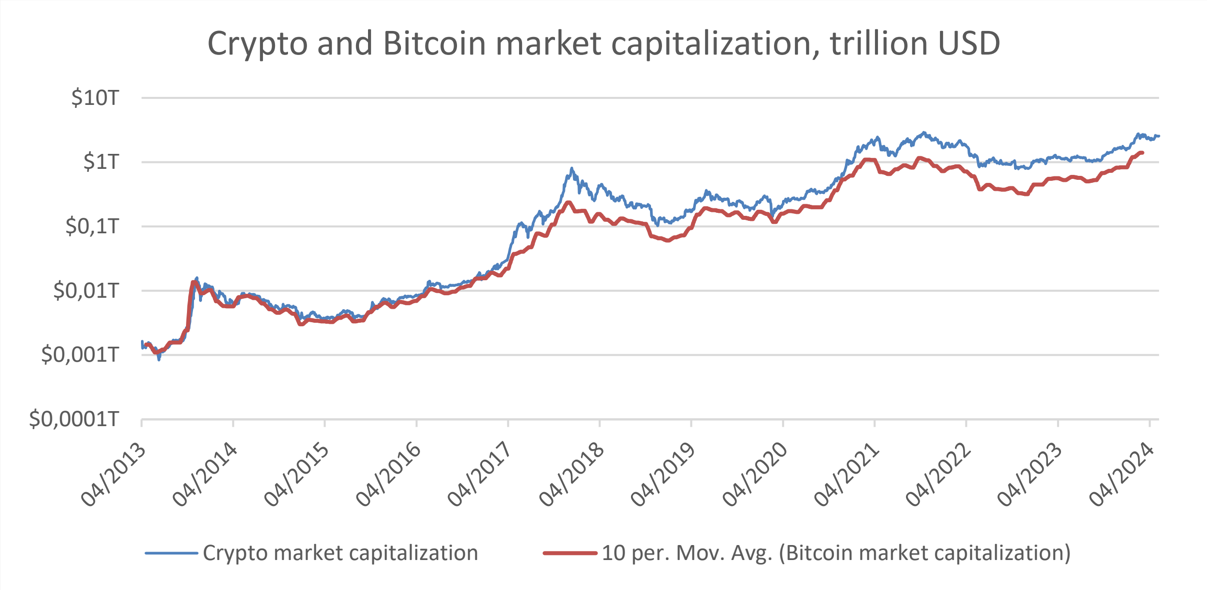


Figure 4 Market capitalization of the overall crypto market and Bitcoin in trillion USD. Due to differences in data granularity a period-10 moving average is applied to the market capitalization of Bitcoin to make the data more readable. Data from coinmarketcap.com. Logarithmic scale.

Network hash rate continues to climb

The increased adoption, maturation of the network, and improved mining equipment released throughout the years continue to push the network hash rate to new levels. Although the network hash rate has declined in the short-term, often following steep declines in mining profitability at various points in time, the overall trend is consistent and considerable growth. The evolution of the network hash rate is illustrated in Figure 5.

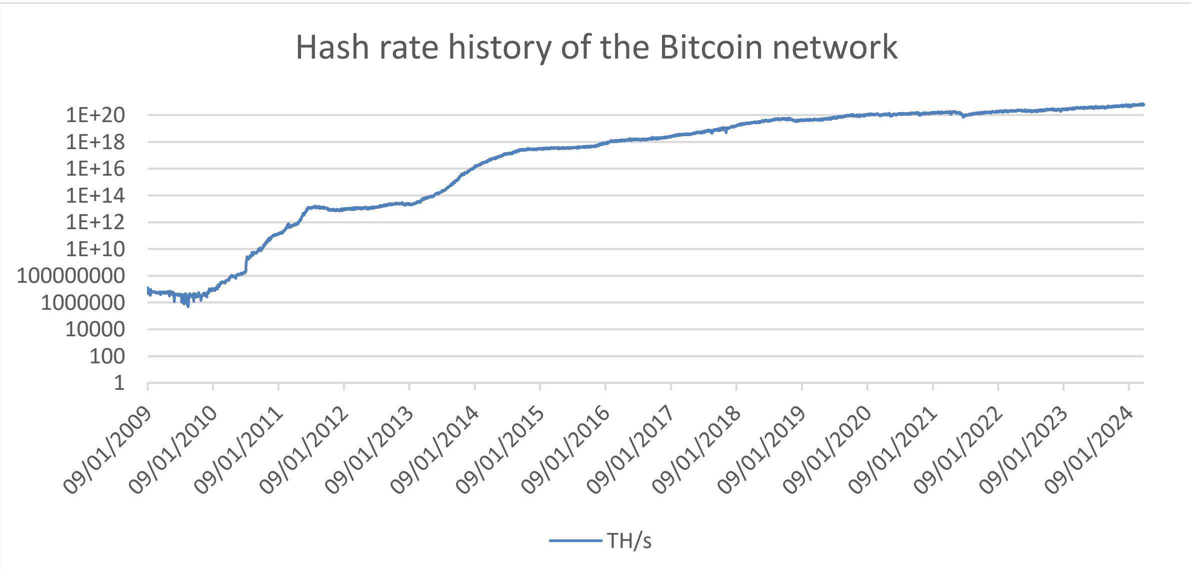


Figure 5 Historical hash rate of the Bitcoin network. Data from bitinfocharts.com. Logarithmic scale.

The single largest decrease in network hash rate, both in relative and absolute terms, occurred in 2021 following the Chinese ban on crypto mining[9]. The ban resulted in nearly half of the network hash rate going offline in the span of a few months and several exchanges and services based in China having to shut down. The networks' ability to survive the crash in the network hash rate was viewed by some commentators as testaments to its robustness[10]. The ban proved effective in the short term, but it has since been widely reported that crypto mining and cryptocurrencies have returned to China and are widely used[11] [12]. The reports are supported by research that found the approach of the Chinese officials to have been largely ineffective in reducing Chinese investor interest in cryptocurrencies (Chen & Liu, 2022). The development of the Bitcoin network hash rate is shown more clearly in the snapshot of the 2019-2024 era in Figure 6.

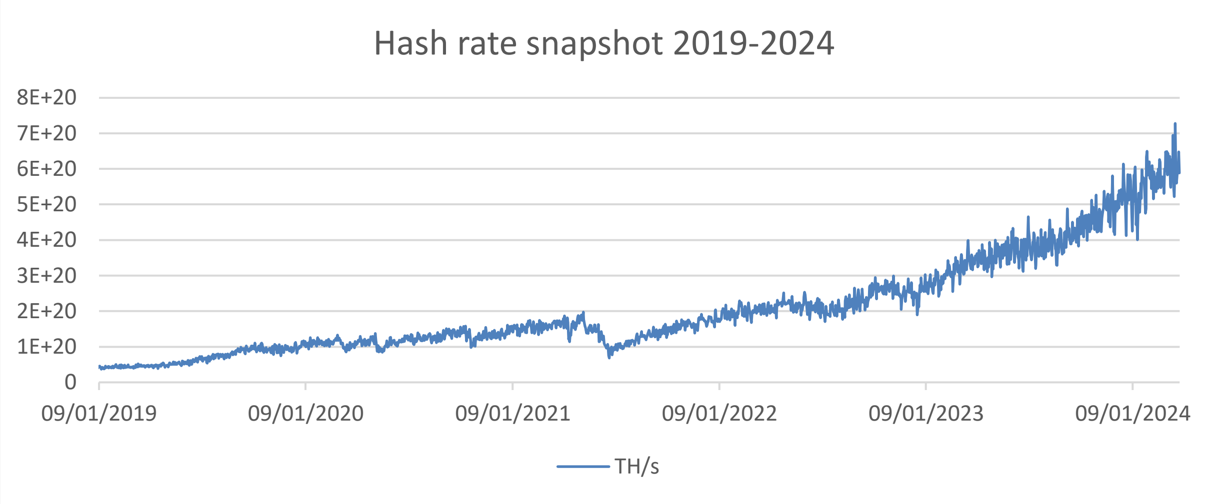


Figure 6 Snapshot of the Bitcoin network hash rate 2019-2024. The Chinese ban on mining in mid-2021 is clearly visible as an over 50% drop in network hash rate over the span of just a few months.

---

[9] *What's behind China's cryptocurrency ban?* (2022, January 31). World Economic Forum. https://www.weforum.org/agenda/2022/01/what-s-behind-china-s-cryptocurrency-ban/

[10] Huang, R. (2023, October 31). *After China's Bitcoin Mining Ban, Bitcoin Is Stronger Than Ever*. Forbes. https://www.forbes.com/sites/digital-assets/2023/10/31/after-chinas-bitcoin-mining-ban-bitcoin-is-stronger-than-ever/

[11] Ranganathan, V., Zhen, S., & Ranganathan, V. (2024, January 25). Bruised by stock market, Chinese rush into banned bitcoin. *Reuters*. https://www.reuters.com/technology/bruised-by-stock-market-chinese-rush-into-banned-bitcoin-2024-01-25/

[12] Parker, E. (2024, February 5). *China Never Completely Banned Crypto*. https://www.coindesk.com/consensus-magazine/2024/02/05/china-never-completely-banned-crypto/

2.6 Regulation

The following chapter on regulation is based on (Demertzis & Wolff, 2018) and (Cumming et al., 2019), unless otherwise stated.

Cryptocurrencies have drawn regulatory scrutiny since being first introduced over a decade ago. Despite the technology being recognized as potentially disruptive, the limited adoption and usability in the early years of the technology meant that regulatory action was limited for a number of years. For example, the Finnish tax authority released its first crypto taxation guidelines in late 2013, over four years after the technology was first introduced. The guidelines have been updated several times throughout the years, with the most recent update in 2020[13]. However, the contents of the guidelines have remained largely the same, with some additional mentions for specific edge cases. While there are some irregularities, crypto regulations are largely similar within the EU area. Recently, regulators have recognized the need to regulate exchanges among other services that offer similar function to the traditional banking system.

Even when regulators are willing to address potential regulatory issues, the lack of centralized control mechanisms and anonymity limit the reach of regulators. Cryptocurrencies and the blockchain being adapted for a wide variety of use cases further complicates the issue, as something as simple as defining what is a cryptocurrency becomes challenging. Categorizing cryptocurrencies as a commodity or a security has been at the centre of the debate. Securities regulations are generally much more stringent than commodity regulations, and such a categorization could have widespread implications regarding the future of the technology. In a 2024 communication titled “Statement on the Approval of Spot Bitcoin Exchange-Traded Products,” the Securities and Exchange Commission (SEC) chair Gary Gensler stated that Bitcoin is a non-security commodity, clarifying the current stance of at least US regulators.[14]

While taxation guidelines are mostly well established, much of the crypto space remains unregulated with limited safeguards in place for consumers. Exchanges and other services, such as stablecoins, are not subject to similar rules regarding collateral as banks. Cryptocurrencies are also not subject to deposit protections, regardless of whether they are

---

[13] *Virtuaalivaluuttojen tuloverotus*. (2013, August 28). vero.fi. https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojen_tuloverotu/

[14] *SEC.gov | Statement on the Approval of Spot Bitcoin Exchange-Traded Products*. (2024, January 10). https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023

stored using a service or platform, or just in a user's personal wallet. Despite the crypto industry booming to over 2 trillion USD market capitalization in 2024, consumers and institutions alike are still very much participating at their own risk. The potential for systemic risk is one of the major reasons for the recent push to establish regulatory guidelines for various services as is the widespread use of these platforms as part of money laundering schemes and other illegal activities.[15]

2.7 Security

Cryptocurrencies rely heavily on proven concepts of modern cryptography. These principles and techniques, such as public-key cryptography are widely used in various applications to securely broadcast data and are considered practically unbreakable, according to current understanding. While technically susceptible to brute force strategies, the sheer size of the number space used makes such approaches infeasible in any realistic time frames.

Although the underlying cryptographic principles are sound, cryptocurrencies are still subject to frequent high-profile breaches resulting in major losses to investors. These breaches are often the result of various programming errors and weaknesses in implementation. (Charoenwong & Bernardi, 2021) present three categories for breaches: security breach, human error, and agency problem ("inside job"). Most of the breaches listed between 2011-2021 were security breaches, costing investors an estimated 7 billion USD. While breaches are often reported to have caused losses in bitcoin, ether, or some other popular cryptocurrency, attackers do not generally target these networks directly. Security flaws are more often found in newer projects. The Bitcoin network has not been subject to breaches, apart from an early exploit that led to the creation of 180 billion additional Bitcoins.[16] This remains the single vulnerability ever discovered in the Bitcoin network (Chohan, 2017). The issue was promptly addressed in an update and the coins were subsequently removed from circulation.

Although the data structure of a blockchain is immutable, forking the blockchain from an earlier point allows for history to be altered. Users agree to revert to an earlier state and continue anew from that point onward. Such moves are highly controversial and require the

---

[15] *Markets in Crypto-Assets Regulation (MiCA)*. (2023, June). https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

[16] Reiff, N., Rasure, E., & Kvilhaug, S. (2024, May 11). *Can Crypto Be Hacked?* Investopedia. https://www.investopedia.com/articles/investing/032615/can-bitcoin-be-hacked.asp

backing of the userbase as a whole, not just miners, as they are expected to move to the "fixed" chain. Forks can also occur when there is disagreement as to the direction of the development of the blockchain.

The decentralized nature of the blockchain means that even when securely implemented there are additional considerations and potential risks. For consensus mechanisms that rely on some form of voting, such as PoW or PoS the possibility for a 51% attack exists. A 51% attack refers to a situation where a malicious actor or a group of actors control most of the voting power. For PoW this would mean having control of most of the hash rate, whereas for PoS this would mean owning the majority of the available supply. These attacks are technically possible even for established cryptocurrencies, but they are prohibitively expensive. The market capitalization of Ethereum following the move to PoS in 2022, was approximately 190 billion USD. An attacker would have needed to invest some 95 billion USD to gain majority control. At the time of writing in 2024, the market capitalization of Ethereum has climbed to over 400 billion USD. A 51% attack would require an investment of over 200 billion USD.

The situation is similar for a PoW crypto, such as Bitcoin. Considering the total hash rate of the Bitcoin network in 2024 at approximately 600 EH/s or 600 000 000 TH/s, at a cost of 27 USD/TH/s (Bitmain Antminer S21) an attacker would need an initial investment of some 16 200 billion USD to match the current network hash rate. Assuming such a number of devices was readily available to be sold, the attacker would also need further resources to power the equipment.

While 51% attacks targeting popular currencies such as Bitcoin and Ethereum are not realistic, such attacks can more easily target less established cryptocurrencies, especially ones using popular hashing algorithms. Because equipment often becomes unprofitable before breaking down, retired equipment that is no longer profitable on a matured PoW network could be repurposed to mine on a less established network. However, the technical expertise required to take advantage of such a situation would still be considerable and the cost will likely outweigh the benefits as the attacker would be left with worthless coins or equipment if the attack were successful, as significant breaches will often result in a project being shut down.

2.8 Mining

This chapter provides additional background information on mining. The concept of algorithms in terms of cryptocurrencies are explained and the reader is introduced to mining equipment, specifically the types of devices featured in the financial analysis section.

2.8.1 Algorithms

In the crypto space, the term “algorithm” refers to the hashing function used by the specific blockchain. The hashing function determines the calculations miners must perform and the hardware required to perform those calculations. For example, Bitcoin uses the SHA-256 algorithm, a 256-bit version of the SHA-2 family of hash functions, originally developed by the National Security Agency (NSA) and the National Institute for Standards and Technology (NIST) in 2001 and released for public use by the United States government. Mining Bitcoin involves repeatedly hashing data using the SHA-256 function to find the correct *nonce*. Although the SHA-2 family is considered cryptographically secure, in terms of mining it has some limitations especially with regards to ASIC resistance.

The choice of algorithm or hashing function used by a PoW blockchain depends on the desired characteristics and use case. The main consideration is often the algorithms ASIC resistance, referring to the difficulty of developing ASICs for the specific hash function. ASIC resistance depends on several characteristics of the algorithm. (Zamanov et al., 2018) found that algorithms requiring considerable amounts of memory were comparatively more ASIC resistant. Ethash and Equihash are examples of such algorithms.

The hardware requirements of ASIC resistant algorithms are often such that the design is so close to existing generic computer hardware, that using existing hardware is the most viable option. However, even highly ASIC resistant algorithms are not immune to hardware developed specifically for mining.

An additional consideration when implementing an algorithm is the history of cryptocurrencies that have used the algorithm in the past. While blockchains are unique and exist independently in their own networks, a blockchain using an algorithm with significant previous history should consider the potential consequences. A newly released cryptocurrency might offer a use case for equipment that has become obsolete for more mature blockchains, but it also means that significant hash rate is readily available that could lead to 51% attacks or the value of a coin tanking, as a result of massive amounts of hash rate suddenly being moved to the chain. A sudden influx of new coins on various exchanges will often lead to the value of such small cryptocurrencies to tank. The concept of 51% attacks is explained in more detail in chapter 2.7.

2.8.2 Equipment

The equipment used to mine a cryptocurrency depends on the algorithm used and the maturity of the network. Many of the cryptocurrencies using non-ASIC-resistant hashing functions were originally mined with generic computer hardware. Even Bitcoin was originally mined with generic computer hardware, despite using the SHA-256 algorithm (CBECI Mining Equipment List, n.d.). The "CBECI SHA-256 Mining Equipment List" provides a comprehensive listing of mining equipment, particularly of the ASIC equipment used to mine SHA-256. The generic computer hardware included is quite limited, as data from this era is not readily available.

Generic computer hardware was quickly made obsolete by first FPGAs and next ASICs. From Table 2 we can see that Bitcoin was originally mined using central processing units (CPU), but quickly moved to graphical processing units (GPU) as they offered much better performance, both in terms of total hashing power and efficiency. The nature of the SHA-256 algorithm was recognized by many in this era. Field programmable gate arrays (FPGA) were quickly adapted for mining. The FPGA era was however quite short lived, as availability was limited, and the creation of application specific integrated circuits (ASIC) was quickly theorized. (Bedford Taylor, 2017)

Table 2 List of mining equipment released between 01/2009 and 11/2013. Data source from (CBECI Mining Equipment List, n.d.)

Name	Type	Release	TH/s	W	Efficiency
Intel Core i5-650	CPU	01/2009	0,0000051	73	14313,73
Intel Core i7-990x (overclocked)	CPU	02/2011	0,000033	224	6787,879
Nvidia GPU GTX 570 (overclocked)	GPU	09/2010	0,000155	373	2405,161
AMD GPU 7970 (overclocked)	GPU	12/2011	0,000675	375	554,8148
Xilinx Spartan-6s	FPGA	06/2011	0,0008	60	75
X6500 FPGA Miner	FPGA	08/2011	0,0004	17	43
Avalon 1	ASIC	02/2013	0,06	595	9,9167
Bitmain Antminer S1	ASIC	11/2013	0,18	360	2

The first ASICs were released in 2013 and they offered major increases in performance. At this point, generic computer hardware was completely obsolete, as the hardware simply could not compete with the performance of ASICs. The first ASICs released were about one hundred times more power efficient than GPUs used at the time (Wang & Liu, 2015).

The creation of ASICs was viewed by many as being in direct contradiction with the ideas of Bitcoin. Generic computer hardware was widely available and had viable uses outside of mining. If mining became unprofitable, the equipment still had value on the 2nd hand market. The ability to use hardware that many already owned was key in enabling the decentralized structure of the blockchain. With mining now requiring purpose-built equipment the barrier of entry was considerably higher and required additional investment which was seen as a potential threat to decentralization.

3 Environmental

Environmental considerations have been a megatrend of the past decade gaining even more traction in the last few years. Climate change has pushed regulatory bodies to implement increasingly stringent demands on various industries, forcing businesses to adapt to the changing environment. Environmental regulations have evolved from being mere guidelines to strict requirements with heavy sanctions as deterrents as regulators try to catch up on the climate debt incurred throughout the years and decades.[17]

Traditional industries vital to the functioning of society have been met with new guidelines to meet targets of carbon neutrality in the next few decades.[18] In the automotive industry EURO regulations are placing ever tightening restrictions on new engines entering the European markets. Changes in regulatory policy have taken the environmental impact of operations from a mere moral consideration to an expense with potentially major impact on the bottom-line, forcing businesses to account for environmental considerations in their day-to-day operations. Traditional brands, such as GM, which have leaned heavily on technologies, such as combustion engines, throughout the years, have stated they are abandoning the outdated technology completely within the next decade and moving to electric vehicles entirely.[19]

With vital industries such as the automotive industry coming under increasing pressure over emissions, it is no surprise that the IT-sector is facing potential regulatory action as well. As digitisation continues to push existing services online while providing a platform for entirely new services, the sector as a whole has been recognized as the next driver of global emissions and rising energy usage.

Emerging technologies, despite their potentially revolutionary applications are not exempt from such attention. The energy consumption of cryptocurrencies and specifically crypto mining has been discussed since the technology was first introduced. Even the author of the Bitcoin whitepaper recognized that energy usage could be a point of contention in the future

---

[17] *How-stringent-are-environmental-policies.pdf*. (n.d.). Retrieved April 2, 2024, from https://www.oecd.org/economy/greeneco/How-stringent-are-environmental-policies.pdf

[18] *2050 long-term strategy—European Commission*. (2020, March). https://climate.ec.europa.eu/eu-action/climate-strategies-targets/2050-long-term-strategy_en

[19] Shepardson, D. (2023, December 13). GM still planning to end gas-powered vehicle sales by 2035—CEO. *Reuters*. https://www.reuters.com/business/autos-transportation/gm-still-planning-end-gas-powered-vehicle-sales-by-2035-ceo-2023-12-13/

as the network matures.[20] Considering the regulatory pressure and general push towards more sustainable technologies, the environmental perspective becomes increasingly important to fully understand the dynamic of cryptocurrencies in the modern setting.

Various aspects of the environmental impact of cryptocurrencies are periodically brought up as significant hurdles for the technology's future by various media outlets.[21] [22] Estimates of varying degree have been presented, with the more extreme research suggesting that the Bitcoin network alone could push global warming past current targets (Mora et al., 2018). More modest estimates exist, but they seem to generate less interest in the media and are seldom mentioned.

The relevance and lack of clarity around the subject were among the key factors for why the environmental perspective was selected to be featured in this thesis. The topic is inherently complicated with the decentralized nature of the Bitcoin network presenting several challenges. As anyone can mine the currency, limited bottom level data is available, and research has to rely on various models to estimate the device composition of the network. Miners are located all around the world and specific location information is also not necessarily always available.

The primary source of the environmental impact of the Bitcoin network is generally known to be the electricity consumption of mining, which introduces yet additional issues. The environmental impact of electricity consumption depends on the method of electricity generation. Although research has been done on the emissions of various methods of electricity generation there is some uncertainty as to the accuracy of the estimates. Additionally, the challenge especially for renewable energy is that seasonal variance can have an impact on the resulting emissions. These challenges are not specific to crypto mining, but rather to some forms of renewable electricity, regardless of use. Emission calculations as a whole are subject to uncertainty due to their reliance on various models. Detailed tracking of

---

[20] Rosen, P. (2024, February 23). Bitcoin's mysterious inventor Satoshi Nakamoto predicted crypto's contentious future and energy use, 2009 email shows. Markets Insider. https://markets.businessinsider.com/news/currencies/bitcoin-satoshi-nakamoto-cryptocurrency-inventor-energy-investors-email-2024-2

[21] Blinder, M. (2018, November 27). Making Cryptocurrency More Environmentally Sustainable. Harvard Business Review. https://hbr.org/2018/11/making-cryptocurrency-more-environmentally-sustainable

[22] Every Bitcoin payment "uses a swimming pool of water." (2023, November 29). https://www.bbc.com/news/technology-67564205

emissions at every stage of production or supply chain is simply not implemented to such a degree of accuracy that it would yield accurate data on the topic.

3.1 Methodology

Introduction

The complexities and considerations involved in studying the environmental impact of any activity, and crypto mining in particular, make conducting original research on the topic somewhat infeasible in the context of this thesis. Additionally, as the goal of this chapter is to provide such an answer to R2 that it contributes to answering R1, the approach must be chosen carefully that it provides more information on the topic than just quantitative data. A thorough understanding of not only the current state of research is required, but also of the development and tone of the research and overall conversation. Studying the existing academic literature and other related materials in-depth is therefore required.

Literature reviews as a research method

Literature reviews are commonly used in various fields of research to analyse and synthesize existing research in a structured way, and to present and evaluate aspects of research on a given topic in a concise format (Snyder, 2019). The general principles of literature reviews have been extensively described in journals and other resources of various disciplines[23] [24] and different approaches have been developed to meet the discipline specific needs of reviews. The descriptions of the key principles of the common types of literature reviews remain similar across disciplines. Although there might be some slight differences in terms of discipline specific considerations, the general principles are generally applicable in other fields of study as well.

Common types of literature review

(Snyder, 2019) gives three examples of different types of literature review: the systematic, semi-systematic, and integrative literature review. Systematic reviews are characterized by the paper as best suited for answering narrowly defined research questions, which considering the context of this section is not very well suited for the types of answers the section is looking

---

[23] Knopf, J. W. (2006). Doing a Literature Review. PS: Political Science & Politics, 39(1), 127–132. https://doi.org/10.1017/S1049096506060264

[24] Garrard, J. (2020). Health Sciences Literature Review Made Easy. Jones & Bartlett Learning.

for. Integrative reviews on the other hand can be used to provide insight into narrow or broadly defined research questions, but they also aim to the "…advancement of knowledge and theoretical frameworks…" from the findings. The description of the typical purpose or the type of results produced by neither systematic nor integrative reviews accurately describe the desired approach in this section. The typical purpose of the semi-systematic review is described by Snyder as to "Overview research area and track development over time." This characterization conveniently summarizes the goals of the Environmental section of this thesis quite accurately.

Additional type, the scoping review

The scoping review is another example of a literature review approach that could be applicable for this section. Scoping studies were first formally described by (Arksey & O'Malley, 2005) where a framework was provided to determine whether a scoping study was the appropriate choice and how to implement it. The paper describes four common reasons for why a scoping study might be undertaken, the following list provides a brief summary of these reasons:

1. Summarize extent of research quickly.
2. Determine value of a full systematic review.
3. Summarize existing research.
4. Identify gaps in research.

These reasons highlight the potential of using the scoping review as either a part of a more extensive review or as an independent review process, something the authors suggest as well. Considering the previously mentioned complex and even contentious nature of the topic, it is likely that there are gaps in the current research and understanding beyond what was already mentioned and hypothesized. Being able to identify these issues with current research is one of the goals of this section. Perhaps the most notable issue with the scoping review is how the superficial nature of the review does not necessarily allow for the quality of the data to be evaluated to a significant extent mainly due to the methodology being more suited to mapping, rather than in-depth analysis.

Choice of review type

Based on the comparison, the semi-systematic review appears best suited for the purposes of this section, in terms of its intended purpose and the type of the results it typically produces. Compared to a full systematic review, the semi-systematic review is described by (Snyder, 2019) to be less strict and formal in terms of the process of material selection. Considering the high number of scientific databases, it is likely that a search of select databases will not be able to find all of the most relevant studies on the topic. A semi-systematic review process where database searches are used as a starting point and the key references of these papers are further analysed should therefore allow for a more thorough review of relevant materials.

The semi-systematic approach limits the importance of database selection as they will only provide a starting point for the review. An approach similar to a scoping review will be used to evaluate the extent of the research on specific databases and gain an overall high-level understanding of the topic to determine the specifics of the review.

3.2 Method

The literature review implements a semi-systematic approach, as described in the previous chapter. The databases were selected based on a cursory review of the number of search results generated using general, crypto-related terms. Most of the databases associated with computer science related research returned a sufficient number of studies. The final selection of databases returned a comparatively high number of results that were relevant to the topic. The three scientific databases selected for the searches were: Web of Science, ScienceDirect, and the IEE Electronic Library.

Several keyword combinations and phrases were assessed for the database searches during the scoping process. Phrases using more general keywords, such as sustainability, returned a significantly higher number of results, many of which were however unrelated to answering R2 or even the topic. There seems to be some author keyword bloat in the research, as some papers appeared to be completely unrelated to the topic, even with quite stringent search terms being applied. Initial searches that provide context to the extent of the research were performed using the following terms:

cryptocurrency

bitcoin

Based on further testing and observations of the keywords used in select studies regarding the topic, the following search phrase was used:

bitcoin AND ((electricity OR energy) AND (consumption OR usage))

The databases were searched using a systematic process. The keywords were applied to the document title and author keywords as the results of these searches contained the highest ratio of relevant studies and articles. Applying the keywords to other fields, such as the abstract was tested, but the results contained a high number of irrelevant articles as many would simply mention the used keywords in passing. An exception was made for ScienceDirect, as the database does not allow for such a search without using an API key. On ScienceDirect the keywords were applied to the document title, author keywords, and abstract. Although the search phrase used might seem narrow in scope, the nature of crypto mining makes the various aspects of the environmental impact of the activity strongly linked. As electricity consumption is the primary contributor to the environmental impact of the activity, the search phrase used should allow the review to find the most relevant material.

All of the results of the final search term were evaluated using the same process. The relevancy of the material was first evaluated based on titles. Next, the abstract and content of these materials was then further reviewed to find the research relevant to the topic. The final number of topics was quite reasonable, in that all of the titles could be manually reviewed instead of relying on sorting. The materials selected from the database searches served as a starting point for the literature review. The process of reviewing the references was done more dynamically, without a systematic approach. The goal of this process was to include the most relevant works that were published and hosted on other scientific databases and build a view of the history and development of relevant research.

3.3 Literature review

3.3.1 Results of database queries

NOTE when discussing energy use in terms of TWh figures expressed as annualized consumption unless otherwise noted.

Cryptocurrencies are an extensively and actively researched topic with publication frequency reaching its highest point in 2022 and 2023, depending on the database. Blockchain technology has been adapted and applied in various fields since inception, but Bitcoin remains the most widely used and researched individual cryptocurrency or application. The number of search results generated using the different search strings are shown in Table 3.

Table 3 Number of search results on databases queried.

	cryptocurrency	bitcoin	bitcoin AND ((energy OR electricity) AND (usage OR consumption)
IEEE	1257	1367	51
Web of Science	3629	4588	38
**ScienceDirect	1855	1679	68

**The search phrase was applied to the document title, author keywords and abstract.

The database queries show that Bitcoin generates a large amount of research interest compared to cryptocurrencies in general. In the databases queried, the search terms bitcoin and cryptocurrency are featured almost equally. While the issue of electricity consumption seems to be a common point of contention in public discourse, only some 2% of research is on the electricity consumption of Bitcoin specifically.

3.3.2 Findings of the review

Preliminary findings

The environmental impact of the PoW protocol consists primarily of two components, the electricity consumption of mining equipment and the e-waste generated by equipment being retired. Although electricity consumption remains the primary contributor to the environmental impact of Bitcoin, the role of e-waste has been recognized as an additional driver of emissions (Cambridge Bitcoin Electricity Consumption Index (CBECI), 2024). The impact of other contributors in a blockchain network, such as non-mining full nodes is small in comparison to mining, as seen by the comparison of PoW and other, less computationally intensive solutions, such as PoS in Figure 7.

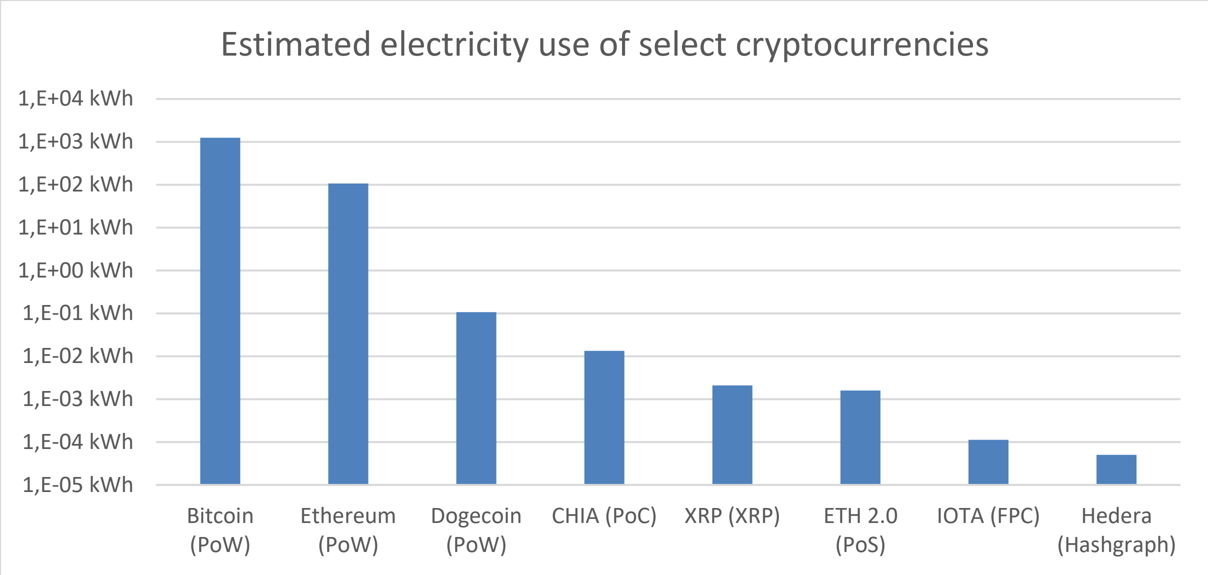


Figure 7 Estimated energy use of select cryptocurrencies with various consensus mechanism according to data compiled by (Kohli et al., 2023).

Description of the most common approaches

The energy consumption of PoW has been extensively studied, driven mainly by the popularity of Bitcoin. Various models have been developed to estimate the energy consumption of mining. These models are categorized in slightly different ways depending on the author. (Lei et al., 2021) describe four practically applicable models: the top-down approach, the economic approach, the hybrid top-down approach and extrapolation based on direct measurement. The models are further defined as follows.

The top-down approach was originally described and used by (O'Dwyer & Malone, 2014) and has since been adapted by many others with slight variations and varying degrees of reliability. This approach is based on an estimation produced by first estimating the efficiency of the average mining machine and dividing the total network hash rate with the estimate. This approach makes several simplifications and without adjustments is mostly suited for generating a lower bound, rather than an exact estimate. The results of (O'Dwyer & Malone, 2014) are largely obsolete, as Bitcoin mining has evolved significantly and the machinery described is no longer used, but the model is still widely used.

The economic approach looks at the revenues generated by miners. This approach is sensitive to price volatility and the corrective coefficients applied to the formulas result in significant uncertainty as to the accuracy of the estimates generated. The economic approach is used by the Bitcoin Energy Consumption Index (BECI) by (de Vries, n.d.) and (Stoll et al., 2019), among others. Note, that the BECI is hosted on the Digiconomist.net website maintained by the author.

The hybrid top-down approach attempts to adjust for the uncertainty of the economic approach by combining aspects of the economic and the top-down approaches to reach a more accurate estimate than either model on their own. The hybrid-top down model was first described by (Bevand, 2017). The model assumes that miners are economic actors who will only operate if the activity is profitable. This assumption is used to estimate what equipment could feasibly be used. As with most approaches, various additional assumptions are still required, such as cost estimates of electricity. The hybrid top-down approach is used in the Cambridge Bitcoin Electricity Consumption Index (CBECI).

Extrapolation based on direct measurement relies on estimating the energy consumption by measuring characteristics of a subset of the network. While the approach does yield accurate results of the various measurements, the applicability of the results is limited. Making accurate extrapolations would require the subset of the network to consist of a similar distribution of equipment as the whole network and be subject to similar costs otherwise. The measurements produced would largely be information that is already widely known, such as hash rates and energy consumption of individual devices. The model is therefore subject to the very same challenges that any other model that attempts to estimate the distribution of equipment.

An additional category mentioned, but deemed somewhat irrelevant is the bottom-up approach where, as the name suggests, energy consumption is calculated by directly measuring the consumption of the equipment use, rather than relying on estimates. While (Lei et al., 2021) list the bottom-up model as the most accurate approach, they conclude that using one for estimating the energy consumption of Bitcoin is not feasible, at least currently, as the data required is simply not available. Instead, applying a hybrid top-down approach is recommended as the next best thing among the recommended practices.

While the different approaches vary significantly in methodology there are similarities between them. A common method often utilized regardless of approach, is to form upper and lower bounds of consumption and a best guess estimate between them. Equipment efficiency is readily available, as performance figures are publicly available from various sources, such as manufacturer documentation, social media, and lists maintained by researchers (ex. (CBECI Mining Equipment List, n.d.) compilation maintained by University of Cambridge

Judge Business Schools Centre for Alternative Finance). The hardware distribution of the network on the other hand is not as clear.

Contentious history of inflated estimates

All four models have been used and featured widely in literature yielding varying results. Figure 8 from (Stoll et al., 2019) highlights the variance between estimates using different approaches.

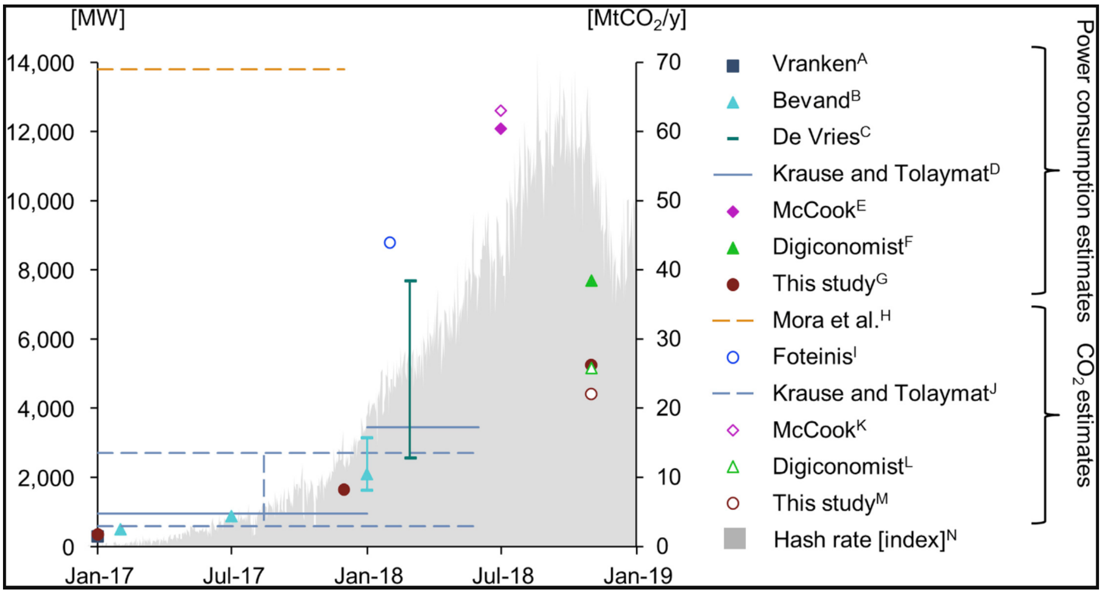


Figure 8 Stoll et al., 2019. Energy use/CO2 emissions of Bitcoin according to numerous studies.

A similar compilation by (Lei et al., 2021) includes some additional works, presented in Figure 9.

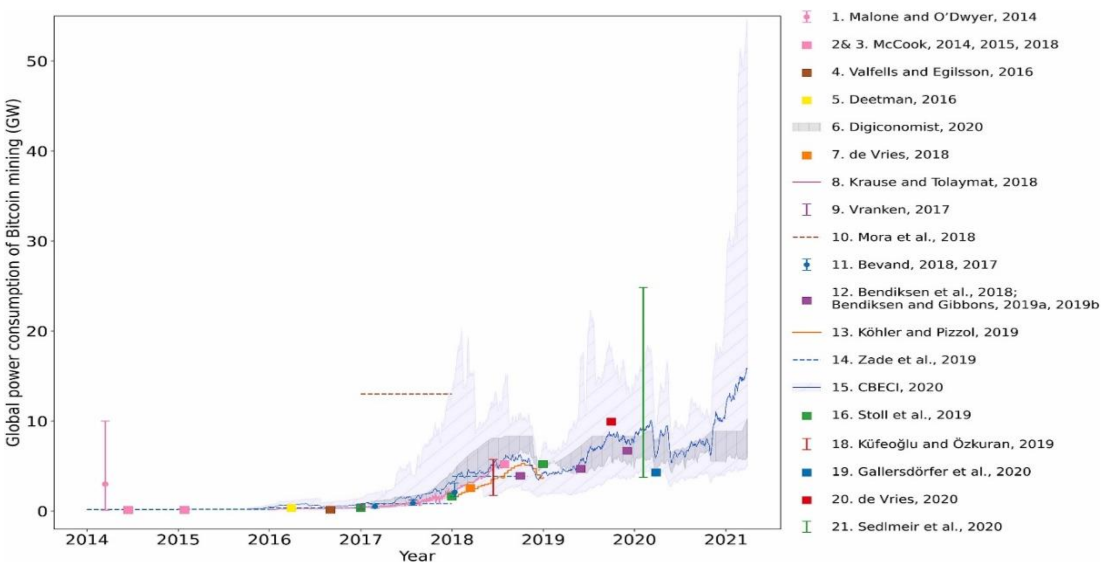


Figure 9 (Lei et al., 2021) compilation of related works.

From Figure 8 and Figure 9 we can see that the studies featured in the comparison are mostly in agreement at various points in time. There are however some outliers. (Mora et al., 2018) estimated that the Bitcoin network would consume 114TWh of electricity in 2017 and be a major driver of emissions in the coming years and decades. The estimates have since been heavily criticized by multiple authors in various releases and research including (Masanet et al., 2019), (Lei et al., 2021), (Houy, 2019), and (Dittmar & Praktiknjo, 2019) for a host of issues with the approach in general and specific methodology used, leading to inflated and inaccurate estimates.

The Bitcoin Energy Consumption Index (BECI) by Digiconomist has produced similarly inflated results when compared to other studies at several points in time. The model estimates the electricity consumption of the Bitcoin network to have dropped significantly in 2022, from 200 TWh to less than half by year end. From 2023 to current day the model estimates a significant rise in the energy consumption up to approximately 160 TWh. Similar to (Mora et al., 2018), Digiconomist has been criticized for producing inflated estimates. However, it is regularly featured as a source by various organizations and even research despite criticism dating back several years.[25] [26] The prediction of the Digiconomist model is presented in Figure 10.

[25] Bevand, M. (2017a). *Serious faults in Digiconomist's Bitcoin Energy Consumption Index*. http://blog.zorinaq.com/serious-faults-in-beci/

[26] DiChristopher, T. (2017, December 21). *No, bitcoin isn't likely to consume all the world's electricity in 2020*. CNBC. https://www.cnbc.com/2017/12/21/no-bitcoin-is-likely-not-going-to-consume-all-the-worlds-energy-in-2020.html

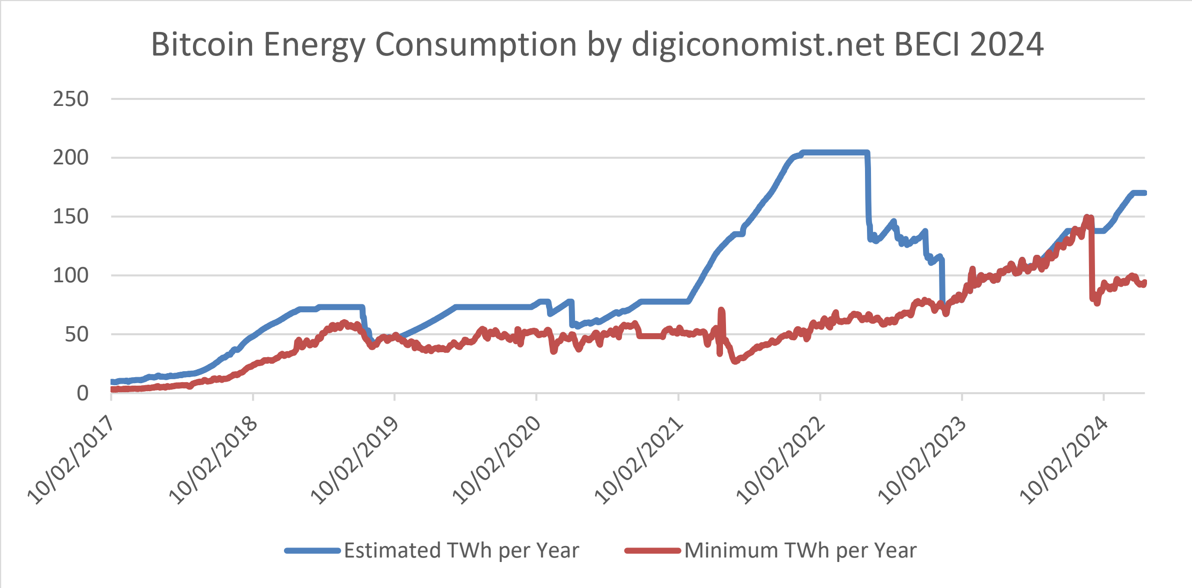


Figure 10 Energy consumption of the Bitcoin network according to the BECI. Data collected from digiconomist.net.

Reliable estimates from numerous studies using different approaches

Perhaps the most widely cited source for the electricity consumption of Bitcoin is the Cambridge Bitcoin Electricity Consumption Index (CBECI) by the University of Cambridge Judge Business School Centre for Alternative Finance (CCAF). The CBECI website is a vast resource of both original research and compilatory works. The original creator of the hybrid top-down approach has also contributed to the creation of the CBECI.

The CBECI relies on the hybrid top-down approach and adheres to the highest number of best practices, according to a comparison of studies by (Lei et al., 2021). As per the comparison the CBECI provides the most accurate estimate as to the energy consumption of Bitcoin.

The model generates upper and lower bounds and a best guess estimate for the electricity consumption of the Bitcoin network. The upper bound is calculated using the most inefficient equipment still profitable while the lower bound is calculated using the most efficient equipment currently available. The best guess estimate attempts to gauge the distribution of hardware used in mining as the scarcity of the equipment means that not all equipment used will be of the latest, most efficient generation of devices. The electricity consumption estimate by the CBECI is presented in Figure 11.

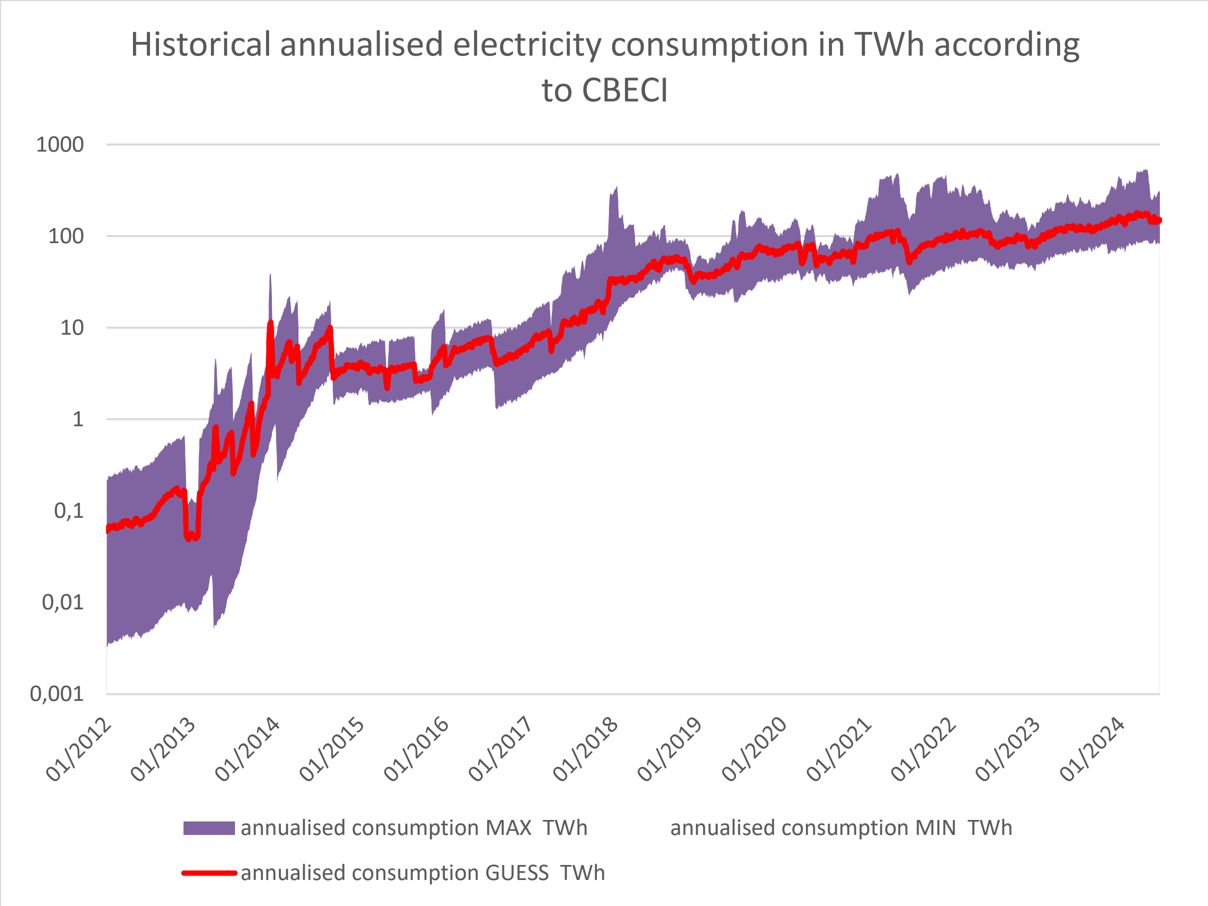


Figure 11 Cambridge Bitcoin Electricity Consumption Index (CBECI) by the University of Cambridge Judge Business Schools Centre for Alternative Finance (CCAF). The blue colour shows the range of the estimates produced by the model. Logarithmic scale.

According to the CBECI best guess estimate the Bitcoin network consumed an estimated 98 TWh of electricity in January 2022 and 85 TWh in January 2023. It is noteworthy that the difference between the upper and lower bound estimates remains considerable, 38-215 TWh and 47-135 TWh in January 2022 and 2023, respectively.

(Stoll et al., 2019) reached similar figures as the CBECI at the time, estimating that the Bitcoin network consumed 35,0-72,7 TWh in November 2018. The study used the economic approach showing that the model can produce accurate results. Although (Lei et al., 2021) evaluate the study quite highly in terms of adherence to their list of best practices, it is noteworthy that other economic models, such as Digiconomist have been in agreement with other estimates at specific points in time.

While e-waste generation has been recognized as a source of additional emissions in several studies, research on the topic is limited. (de Vries & Stoll, 2021) estimate the e-waste generation of the Bitcoin network by using data from the CBECI to evaluate the lifetime of mining equipment. Together with publicly available information on equipment specifications the e-waste generation is estimated at 30 700 tonnes in 2021. The figure is described to be "…comparable to the amount of small IT and telecommunication equipment waste produced by a country like the Netherlands" by the authors. Due to advances in equipment efficiency, devices are often retired within a few years or even less.

Many of the studies on electricity consumption also attempt to estimate the overall carbon footprint, but this introduces yet additional uncertainties. While miners can be geographically placed using publicly available IP-address information and regional electricity generation capacity is often known, exact figures on the specific method of electricity generation for the power used are not available. Furthermore, the carbon emissions resulting from electricity generation can vary greatly depending on the time of year (de Vries, 2019). Considering the overall goal of this thesis, delving deeper into the carbon emissions was deemed unnecessary as the focus is not on evaluating the accuracy of carbon emission estimates. The electricity consumption of mining provides sufficient information on the environmental impact.

3.4 Discussion

Environmental impact in the context of equipment development

The environmental impact of PoW and Bitcoin has been studied using various approaches resulting in varying estimates. While the development of mining equipment is well established, there remains significant uncertainty as to the hardware currently being used. This uncertainty seems to be a key factor in explaining the large ranges of estimates produced by research. In (Mora et al., 2018) one of the criticisms voiced was the assumption that miners would continue using outdated and unprofitable equipment resulting in a hardware distribution consisting mostly of older equipment.

Figure 12 shows the development of mining efficiency since 2018. Equipment before the modern ASIC era is omitted. For context, generic computer hardware originally used for mining achieved efficiencies of up to 14 000 J/GH. FPGA devices were considerably more efficient at 75-43 J/GH. The first ASICs were significantly more efficient even still at 10 J/GH. As can be seen from Figure 12 the efficiency of mining equipment continues to improve to date. This explains in part the increasing hash rates, but based on research does not result in an overall reduction of the electricity consumption of the network. The improvements in efficiency have slowed down considerably, but they still contribute significantly to equipment becoming obsolete before reaching its end of life.

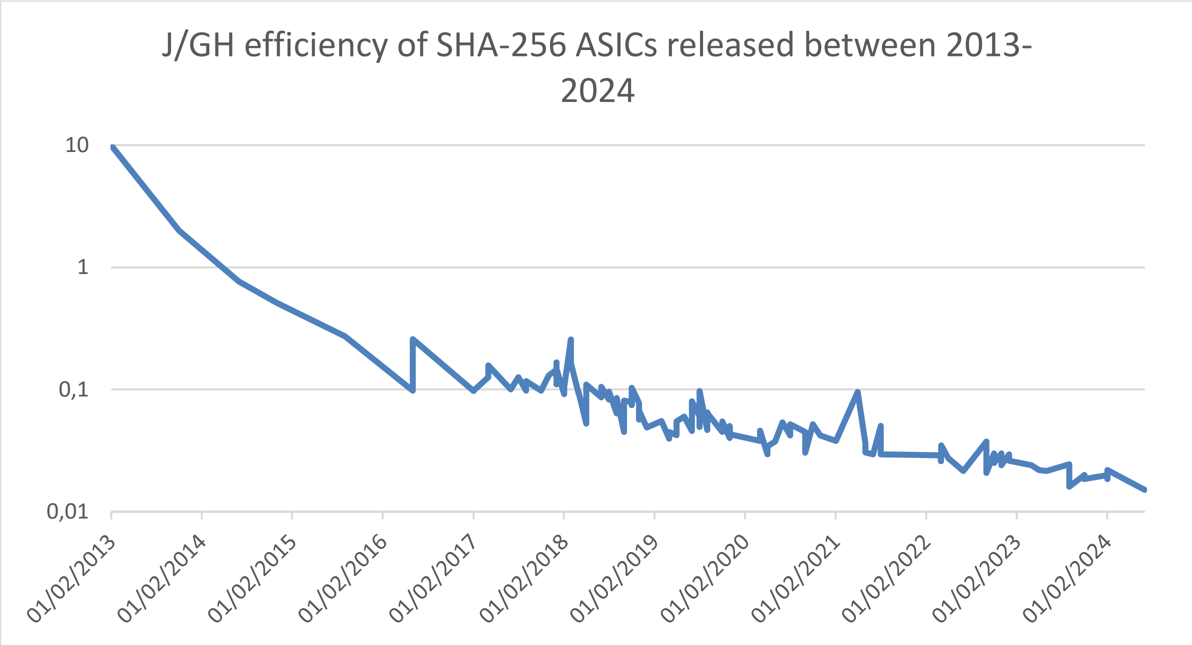


Figure 12 Efficiency of Bitcoin mining equipment. Logarithmic scale.

Uncertainty and accuracy of current estimates

The issue of accurately estimating hardware distribution has been addressed in many studies, and resources, such as the CBECI. While the CBECI by CCAF seems to be the most reliable resource currently available for the energy consumption of Bitcoin, it should be noted that the CCAF revised their methodology in 2023 due to "… evidence indicating a periodic overestimation of electricity consumption." The overestimation resulted primarily from the hardware distribution. Ultimately, the problem that all studies run into is that bottom-level data directly from miners is not available, and various estimates are required. Manufacturer reporting and economic realities can provide some bounds for estimates, but even still accurate data is simply not available, and studies are always reliant on utilizing models to some extent.

While the scope of this thesis does not allow for in depth exploration of methodology of each study, as previously stated, the CBECI makes a compelling case for its best guess estimate and follows the expected behaviour of hash rate and energy consumption derived from literature. The relationship between the network hash rate and energy consumption seems to be well established only in the short term. Meaning, that while sudden changes in hash rate should be observable in an accurate representation of the network energy consumption, long term changes occurring in the span of several months or even years are not responsible for similarly proportional changes in the energy consumption.

This relationship can be seen clearly when comparing the hash rate and energy consumption estimates in Figure 13. Drastic and sudden changes in hash rate, such as the one in the early part of 2021 resulting from the Chinese ban on crypto mining are immediately apparent and observable in both graphs. However, long term increases do not result in linear increases of energy consumption. The hash rate of the network was reported at approximately 172 TH/s in the beginning of January 2022 at an estimated network energy consumption of 97TWh according to the (Cambridge Bitcoin Electricity Consumption Index (CBECI), 2024). Using the same sources, in January 2024 the network hash rate was calculated at 505 TH/s at an estimated electricity consumption of 155TWh.

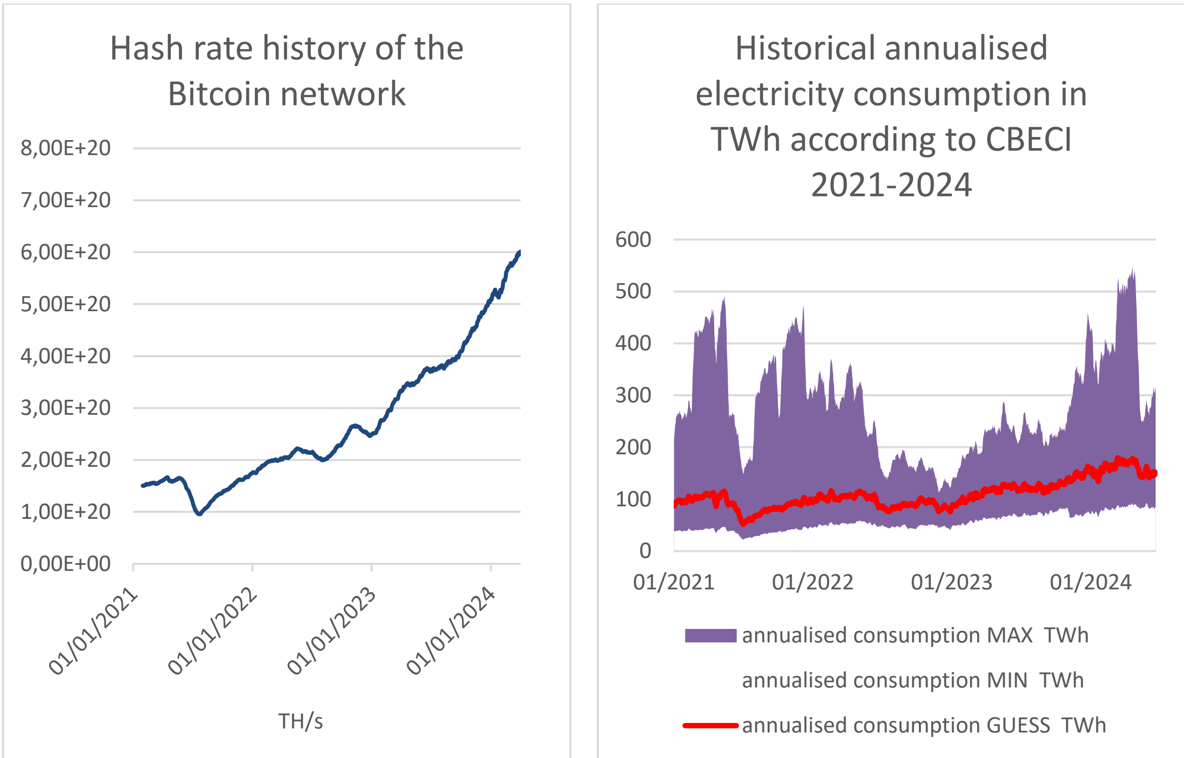


Figure 13 Bitcoin network hash rate and CBECI energy consumption estimate.

The seemingly inconsistent dynamic of the electricity consumption seems to be the result of changes in equipment used. While the dramatic pace of development in the efficiency of mining equipment has slowed down considerably in recent years, the changes are still notable and explain the substantial rise in network hash rate while the electricity consumption has increased at a comparatively modest pace. (Figure 12)

Use of inaccurate resources

Applying the same review process to the BECI presented in Figure 10, reveals some potential issues. Observing the same time frame from 2021-2022 we can see that the BECI model predicts a near threefold increase in energy consumption despite network hash rate plummeting nearly 50% in the early part of 2021 (Figure 6). Furthermore, the BECI model frequently predicts rapid rises that when extrapolated produce lofty estimates of future electricity usage.

The authors of both the BECI and (Mora et al., 2018) have defended their respective approaches and seemingly inflated estimates. In their 2019 reply Mora et al. stated that "Scenarios are commonly used in multiple disciplines to assess the consequences of certain actions," justifying the assumptions used in the model. A representative for the BECI defended their respective model in a heated conversation with Bevand regarding the criticism.[27]

While (Mora et al., 2018) and Digiconomist ((de Vries, n.d.)) are singular examples that have been vocally criticized by various authors, they are good examples of how sensational information can maintain presence in a field. Both models have been frequently cited in the media and various publications, even years after release. These resources still appear frequently in various search results on the topic. For instance, the BECI remains one of the top search results on google for "bitcoin electricity consumption" and it is featured as a source on several top-ranking search results from Statista providing various statistics on the energy consumption of Bitcoin. Additionally, the site was cited in multiple applied works screened during the initial review process. Without applying a review process, such as the one here, it is quite easy to view this information as credible and comparable to more thorough resources such as the CBECI.

Summary

To summarize, the electricity consumption of Bitcoin has been studied extensively using various approaches. The most credible resource on the topic, the CBECI estimates Bitcoin mining to consume approximately 150-180 TWh in 2024 according to the best guess estimate. The hypothetical range formed between the upper and lower bounds is 55-547 TWh in 2024.

---

[27] Bevand, M. (2017a). *Serious faults in Digiconomist's Bitcoin Energy Consumption Index*. http://blog.zorinaq.com/serious-faults-in-beci/

The difference between the upper and lower bound estimates highlights the uncertainties inherent to even the most rigorous estimates. Although major outlier studies exist, they do not cast significant doubt on these conclusions, as the approaches in these studies are heavily criticized by other authors and seem to exhibit obviously flawed behaviour at various points in time.

3.5 Conclusion

R2 presented the question “What is the environmental impact of Proof of Work and how resource intensive is the activity?”

The literature review focused on research regarding the electricity consumption of Bitcoin as it provided the best current example of the extent that a PoW network could grow to. Bitcoin mining was shown to be a resource intensive activity. For context, the Bitcoin network is estimated to consume 150-180 TWh while the total global data centre electricity consumption is estimated to be 240-340 TWh by the IEA report “Data Centres and Data Transmission Networks” in 2023. However, in the context of global electricity consumption, the impact of Bitcoin mining is small. According to data from 2022, global electricity consumption was approximately 26 573 TWh.[28]

Bitcoin mining is a resource intensive activity due to the qualities of the Proof of Work protocol. Based on the literature review it is fair to estimate that the electricity consumption of mining will likely continue to grow at a modest pace, as seen in recent years. However, since access to bottom level data from miners is limited or non-existent, figures are always going to be reliant on various models resulting in a degree of uncertainty.

Although the environmental impact of mining was found to be considerable, none of the models in this review suggest that miners would consider environmental concerns a factor in whether equipment is operated. The CBECI assumes equipment will be run if it is profitable and does not exceed its feasible lifetime. These assumptions are consistent with at least some

[28] International—U.S. Energy Information Administration (EIA). (2022).

of the findings regarding consumer attitudes towards sustainability and green products that have been established in literature.[29] [30](Gan & Kao, 2008)

3.6 Limitations

Many of the materials featured in this review are somewhat dated. This is in part due to the selection process of including works that have been sufficiently cited, but also due to lack of recent research on the matter. The literature review suggests that the matter of electricity consumption is relatively solved by the CBECI, to the extent that producing more accurate results is unlikely without new data.

This review focused on Bitcoin, but it is recognised that other PoW cryptocurrencies exist, and they do contribute to the overall environmental impact of PoW. The research is however limited.

This review simplifies the evaluation of the environmental impact by looking just at the electricity usage and e-waste generation. The environmental impact of electricity consumption ultimately depends on the method of electricity generation. Although this data is included to an extent in the studies and resources covered in this review, they are not as thorough as with the electricity consumption. Elaborating further on the resulting emissions would require this review to go much more in depth on this particular topic, which goes beyond the purpose of this review.

[29] White, K., Hardisty, D. J., & Habib, R. (2019). People say they want sustainable products, but they don't tend to buy them. Here's how to change that.

[30] Gan, C., & Kao, H. (2008). Consumers' purchasing behavior towards green products in New Zealand. *Innovative Marketing*, *4*(1).

4 Financial

Analysing the financials of any activity that is vital in enabling a technology is key in understanding the dynamics involved. Profitability and financials of the activity directly relate to whether the technology is sustainable without good Samaritan types, willing to put in the time, effort, and other resources to support the technology without compensation. In the case of Bitcoin and PoW, mining is at the core of the technology and something the network requires to remain functional and safe. Understanding the financials of mining is an important aspect in determining the role and motivations off miners and analysing their dependence on the volatility of the asset.

The revenue generation of Bitcoin mining is well understood and accurately calculated from block times, block rewards, fees, and the price of Bitcoin. The industry consistently generates monthly revenues of over 1 billion USD according to data from Blockchain.com.[31] However, revenue generation alone does not tell much about the nature and profitability of the activity. Mining is associated with high operating costs from electricity and upfront costs from equipment. Other costs include pool fees and for industrial operations, general business expenses depending on the size of the operation, such as rent, administration, and interest.

The constant evolution of mining equipment means that miners must upgrade their equipment frequently to stay competitive. Bitcoin mining generates 30 700 metric tons of e-waste, primarily because of equipment being retired, according to the review in chapter 3.1. Functional equipment being retired before its end-of-life results in unnecessary e-waste, but it also puts additional pressure on the profitability of mining as the cost of equipment must be recouped within a relatively short period of time while running the equipment is still profitable.

Resources that miners rely on to calculate profitability are mostly simple calculators that look at current profitability and provide extrapolations of the data. Literature on the profitability of mining is quite lacking, often looking at snapshots of data. (Delgado-Mohatar et al., 2019) concluded that the limit for profitable Bitcoin mining was 0,14 USD/kWh in June 2018. (Islam et al., 2023) predicted that Ethereum mining would remain profitable only if the price of the coin continued to increase. These studies provide previously mentioned snapshots in time, but they do not provide a comprehensive view of the profitability of mining neither

[31] *Blockchain.com | Charts—Miners Revenue (USD)*. (2024). https://www.blockchain.com/explorer/charts/

Bitcoin nor Ethereum. To answer R3 in a meaningful way in the context of R1 a thorough analysis and understanding of the financials of crypto mining is required.

As R1 discusses the role of the technology throughout time, rather than at a single point, snapshots of profitability do not provide sufficient data on profitability. Instead, the approach must be such that it provides information at several points in time for extended periods.

4.1 Methodology

Introduction

This chapter provides the theoretical background for the model used to calculate the financials of Bitcoin mining. The basics of financial analysis are presented followed by a description of feasibility studies and a brief description of asset management and Customer Profitability Analysis. The requirements of the model and the justification for the chosen approach is provided.

Basics of financial analysis

The following two paragraphs on financial analysis are based on (Peterson & Fabozzi, 1999).

The principles of financial analysis have been described by various authors throughout the years. Financial analysis refers to the practice of evaluating a business's financial performance. It is typically conducted by calculating various figures and ratios from financial statements and filings. The choice of calculations depends on the extent, perspective, and purpose of the analysis. Liquidity, activity, profitability, and financial leverage represent the four different facets of financial analysis. Each facet can be further split into components, depending on the purpose of the analysis. For example, profitability analysis can look at gross profit, operating profit, or net profit, depending on which costs are accounted for.

Return ratios provide another way of evaluating business prospects and performance. Operating return on assets, return on assets, and return on equity are commonly used to evaluate return on investment, depending on which income and assets are used in the calculation (**NOTE**: Return On Investment or ROI is commonly misused in the crypto mining space to refer to the Payback period of mining equipment, rather than the official definition of measuring the ratio of income and assets as a percentage.) Although financial analysis is typically done in a retrospective manner, the figures can be used to calculate limits for profitable operation and forecast results.

Feasibility studies introduce additional considerations

Forecasts based on extrapolation from past data do not necessarily provide sufficiently reliable information on expected results and more in-depth analysis may be required. Feasibility studies are used to evaluate the viability of a planned project, development, or approach in several disciplines.[32] Depending on the target of study, feasibility studies can look at different aspects of feasibility. (Overton, 2000) describes the typical design of a feasibility study, listing technical-, economic-, and operational feasibility as the three types of feasibility that studies often look at. Technical feasibility, as the name implies, looks at whether a solution is achievable with the current level of technology. Financial feasibility evaluates the cost, returns, and overall financials related to the project often using tools from financial analysis, whereas operational feasibility looks at the applicability of the solution from the organization's practical viewpoint and its limitations.

Although the different types of feasibility can be studied independently, all three are interlinked. Operational considerations can directly impact financial feasibility. For example, distribution related challenges, such as delays in production or delivery, can have direct implications on expected results. Overlooking technical feasibility can have similar effects, as planned reliance on non-existent technology isn't necessarily reliable or justified.[33] (Overton, 2000)

Asset management

Evaluation of the performance of equipment and assets is called asset management. [34] Asset lifecycle management looks at the management and results of assets throughout their entire usable lifetime.[35] While these approaches are technically applicable in this section, they often look at the performance of assets over longer periods and apply complex models to account for several factors going beyond the intended scope of this section. As the goal here is to

---

[32] Bowen, D. J., Kreuter, M., Spring, B., Cofta-Woerpel, L., Linnan, L., Weiner, D., Bakken, S., Kaplan, C. P., Squiers, L., Fabrizio, C., & Fernandez, M. (2009). How We Design Feasibility Studies. American Journal of Preventive Medicine, 36(5), 452–457. https://doi.org/10.1016/j.amepre.2009.02.002

[33] Arvesen, A., Bright, R. M., & Hertwich, E. G. (2011). Considering only first-order effects? How simplifications lead to unrealistic technology optimism in climate change mitigation. Energy Policy, 39(11), 7448–7454. https://doi.org/10.1016/j.enpol.2011.09.013

[34] What is Asset Management? (n.d.). Retrieved June 18, 2024, from https://theiam.org/

[35] Best Asset Lifecycle Management Practices & Systems to Manage the 4 Key Stages. (n.d.). Comparesoft. Retrieved June 18, 2024, from https://comparesoft.com/asset-management-software/asset-life-cycle/

study the direct results of mining, rather than establish an in-depth account of the entire cost structure of a crypto mining company, these models have limited applicability.

Customer Profitability Analysis the closest analogy

Customer Profitability Analysis (CPA) offers perhaps the closest analogy to what this section aims to achieve. CPA looks at the revenue and profitability of individual customers and how they contribute to the bottom line (Gupta et al., 1997). Customers are analogous to mining equipment in several ways. For example: they produce revenue irrespective of other equipment (customers), the value of revenue in terms of profitability can vary greatly, and profitable mining periods can vary in length (contract length). CPA can be done in a retrospective or prospective manner, depending on the purpose of the analysis (Jacobs et al., 2001).

Model description

Although the described approaches study the financials of an activity from slightly different perspectives and the use cases vary, they are all built on principles and concepts of financial analysis. Profitability is at the centre of not only financial analysis, but also financial feasibility and CPA. Profitability analysis offers a natural way of evaluating the financials of mining. Estimating net profit or operating profit would require deeper insights into business-related structures and costs. To limit the scope of the research in this section, only gross profit will be evaluated. This limits the assumed costs to only the cost of goods sold (COGS). In the case of mining this translates to the cost of equipment and electricity.

The total number of ASIC-devices released presents challenges to equipment selection and the specific method of profit calculation. At the time of writing the (CBECI Mining Equipment List, n.d.) lists a total of 140 ASIC-devices. A hypothetical miner could theoretically choose to purchase any device and the total number of combinations would be limited only by the total number of purchases assumed and the length of the observation period. Forming realistic “chains” of purchases would present significant challenges to justifying the selections as they ultimately depend on several factors such as budget, availability etc. The selection of equipment in these “chains” could impact the results significantly, producing uncertainty as to the reliability of the results by potentially hiding crucial details regarding the financials at specific times or for specific devices. To avoid these issues the analysis will calculate profitability at a per device basis. Although device selection will still play a role, a realistic selection process based on availability and performance characteristics typical of devices at the time will mitigate the impact of the selection.

As described, the analysis in this section will take the form of a profitability analysis that calculates gross profit of specific devices at various points in time. Operational and technical feasibility will be considered in the application of the model. The application of these principles is explained in detail in chapter 4.2 describing research methods.

4.2 Method

The financial analysis will first present the relevant general data collected from various sources. The data is then used to first calculate revenue on a per-device basis. Revenue calculation is based on USD/day/THash data from bitinfocharts.com and equipment specifications from the (CBECI Mining Equipment List, n.d.). The profitability data was validated by cross-referencing the profitability figures with data from calculators on whattomine.com, minerstat.com, and manual calculations. The mining equipment list is a publicly available Google sheets document maintained by the Cambridge Centre for Alternative Finance, the authors of the CBECI. The list provides information on ASIC-mining equipment, such as performance specifications and release dates. The list is based on (Bedford Taylor, 2017) and manufacturer specifications. The number of entries before 2014 is somewhat limited, but ASIC-era devices are thoroughly covered with 140 entries between 07/2014 and 01/2024.

The mining equipment list provides the equipment wattage required for partial COGS calculation, but it does not contain data on equipment pricing. Data availability of historical equipment pricing is somewhat limited regardless of source, and multiple sources had to be used to collect the data. The pricing data from these sources is not necessarily directly comparable as manufacturer pricing is often lower than third-party reseller pricing. However, no other data exists on the topic. Pricing data was sourced from:

bitmain.com – manufacturer website

web.archive.org – snapshots of bitmain.com

camelcamelcamel.com – amazon price history

hashrateindex.com – various statistics including ASIC prices

The profitability of mining Bitcoin was calculated in four periods following the release of select equipment in 2014, 2017, 2020, and 2023. The equipment selection is presented in Table 4.

Table 4 Mining equipment used in the calculations and their respective release dates.

Name	Release data
Bitmain Antminer S3	01/07/2014
Bitmain Antminer S9 (12,5 TH)	01/02/2017
Bitmain Antminer S19 (95 TH)	01/05/2020
Bitmain Antminer S19 Pro Hydro	01/01/2023
Bitmain Antminer S21	01/09/2023

Equipment was selected based on the release date and so that it would provide a comprehensive representation of the different development stages of the network. The S3 was included in the analysis as it is one of the first ASIC miners developed and the first to achieve a sub 1 J/GH performance, a considerable advancement compared to existing equipment. The S9 and S19 were popular devices at the time of their respective releases and various editions of both miners have been released throughout the years offering increased hashing power at similar efficiency. The Antminer S21 is the most efficient SHA-256 miner to date, according to the CSMEL.

Operational feasibility was a key consideration in defining the specific parameters of the models. Bitinfocharts offers daily profitability data, however monthly profitability averages are perhaps a more realistic way of evaluating profitability, as reacting to day-to-day changes in profitability would require equipment to be on stand-by and constant monitoring or equivalent automation. While not particularly difficult to implement, considering that profitability and hash rate are values calculated from past results, rather than real-time measurements, it is unrealistic that miners could effectively react and mine only on the most profitable days. Maintaining such a setup would incur significant related costs, depending on the size of the operation, making such strategies somewhat infeasible. It is therefore assumed, that miners will only mine during months where it was profitable on average for the whole month. This is a practical example of how demanding operational feasibility can impact the results of a model.

Equipment lifetime and delivery- and installation periods are an additional operational challenge that must be accounted for. ASIC equipment often comes with limited length warranties, meaning operation is only guaranteed for duration of the warranty. Although some models have extended warranties of up to 12-months, many manufacturers only offer 6-month warranties or even less.[36] [37] However, (de Vries & Stoll, 2021) suggest the lifespan of ASICs is between 12-24 months. The CBECI review of 2023 states that "…no consensus exists," but estimates in academia are generally "18 months or less." Warranty related issues are common point of conversation on social media platforms and crypto mining related forums that although difficult to validate, paint a grim picture of the warranty policies of many manufacturers, suggesting even shorter expected lifespans of less than a year.[38] [39] To account for the possibly limited lifespan of devices 6- and 12-month profitability and gross profit figures are presented in addition to the "full" time frame figures. The "full"-time frame refers to the equipment being run for as many months as the equipment is profitable. This figure is presented as an upper bound-type figure, as expecting the equipment to run for such extended periods of time is unrealistic.

Lengthy delivery times further complicate the issues, as these can result in the equipment being unprofitable to run when it finally does arrive. The CBECI assumes a 2-month delivery and installation period, but they appear to express some uncertainty as to the accuracy of this assumption (Cambridge Bitcoin Electricity Consumption Index (CBECI), 2024). As definitive data on the topic appears lacking the calculations in this section will present three variations assuming 0-, 2-, or 4-month delivery and installation periods.

The final requirement for calculating the COGS and gross profit is the price of electricity. The CBECI assumes that the average electricity price for Bitcoin miners is 0,05 USD/kWh. However, the price of electricity can be even lower in areas with access to abundant energy

---

[36] *Product Warranty*. (2023, June 23). BITMAIN Support. https://support.bitmain.com/hc/en-us/articles/223400048-Product-Warranty

[37] *Warranty*. (n.d.). Coin Mining Central. Retrieved June 19, 2024, from https://coinminingcentral.com/pages/warranty

[38] Icy_Hovercraft_7050. (2022, July 28). *BITMAIN SUPPORT/ WARRANTY* [Reddit Post]. R/BitcoinMining. www.reddit.com/r/BitcoinMining/comments/w9z6bh/bitmain_support_warranty/

[39] *Bitmain's Refused From S9 Warranty, Buy at your own risk*. (2015, January 5). https://bitcointalk.org/index.php?topic=914354.0

resources, whether renewable or otherwise.[40] For smaller scale operations higher electricity costs of 10-15 US cents are also common. While mining is possible at even higher costs in some situations, these operations are quickly priced out or they rely on other mechanisms to sustain profitability. Including electricity prices beyond 15 US cents would offer little additional information. The electricity prices used in the calculations are 3, 5, 10, and 15 US cents.

Finally, it needs to be emphasized that the 6- and 12-month periods for different electricity prices did not necessarily occur at the same time. At 3 cents equipment is often profitable immediately following release, but miners at 15 and even 10 cents electricity rely heavily on periods of higher profitability for revenue generation. The assumption made in this model is that miners will only start mining when it is profitable in their situation and the delivery and installation periods are calculated off profitable months.

4.3 Analysis

This chapter presents the profitability calculations. Chapter 4.2.1 provides general background information on the topic. Chapters 4.2.2-4.2.6 present the profitability calculations of select equipment in chronological order. Finally, the findings are discussed, and the relevant research question is answered based on the findings. Limitations of the approach are also briefly discussed.

4.3.1 General

The profitability of Bitcoin mining has evolved rapidly throughout the years. Miner revenues have steadily increased, while profitability in terms of USD/day/TH has continued to drop. The development of profitability is illustrated in Figure 14.

---

[40] *Electricity price by country 2023*. (2023, September). Statista. https://www.statista.com/statistics/263492/electricity-prices-in-selected-countries/

Figure 14 Profitability of Bitcoin mining in terms of USD/day/TH, data from bitinfocharts.com(BitInfoCharts.com, 2024). Logarithmic scale.

The decrease in profitability per TH is driven by improvements in the efficiency of mining equipment and growth of the Bitcoin network. The rapid evolution of equipment efficiency, especially in the early years of ASICs is immediately apparent. The improved efficiency is still clearly visible, but differences in equipment released within the same period are more clearly seen. The release dates of the equipment featured in calculations are displayed on the timeline in Figure 15.

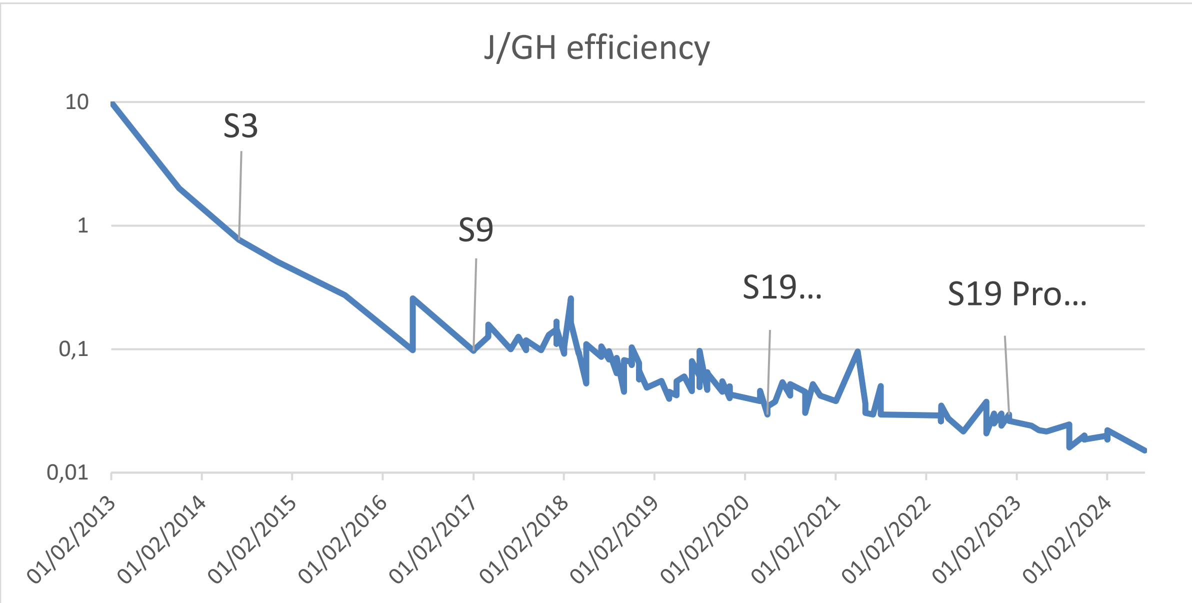


Figure 15 Evolution of J/GH efficiency according to data from the CCAF (Cambridge Bitcoin Electricity Consumption Index (CBECI), 2024) with timeline of miners. Logarithmic scale.

While equipment has become more efficient, the wattage of ASICs has steadily climbed from sub-thousand-watt devices all the way to over 7000 watts for some models in the last decade or so. Although some early models, such as the Bitfury B8, had lofty wattage requirements, most devices in the earlier years had relatively modest power draws, comparable to consumer electronics. As seen from Figure 16, in 2014-2017 ASICs required between 370-1290 watts, or 810 watts on average. In 2017-2020 ASIC power requirements varied between 1000-6400 watts, with an average power demand of 2350 watts for equipment released in the time period. Most of the newer ASICs come with significantly higher power requirements. Miners released in 2022-2024 require between 3010-7260 watts of power at an average of 4580 watts. The power draw of modern miners is commonly beyond the capacity of what regular residential fuse sizes can deliver. The equipment featured in the calculations are again displayed on the timeline.

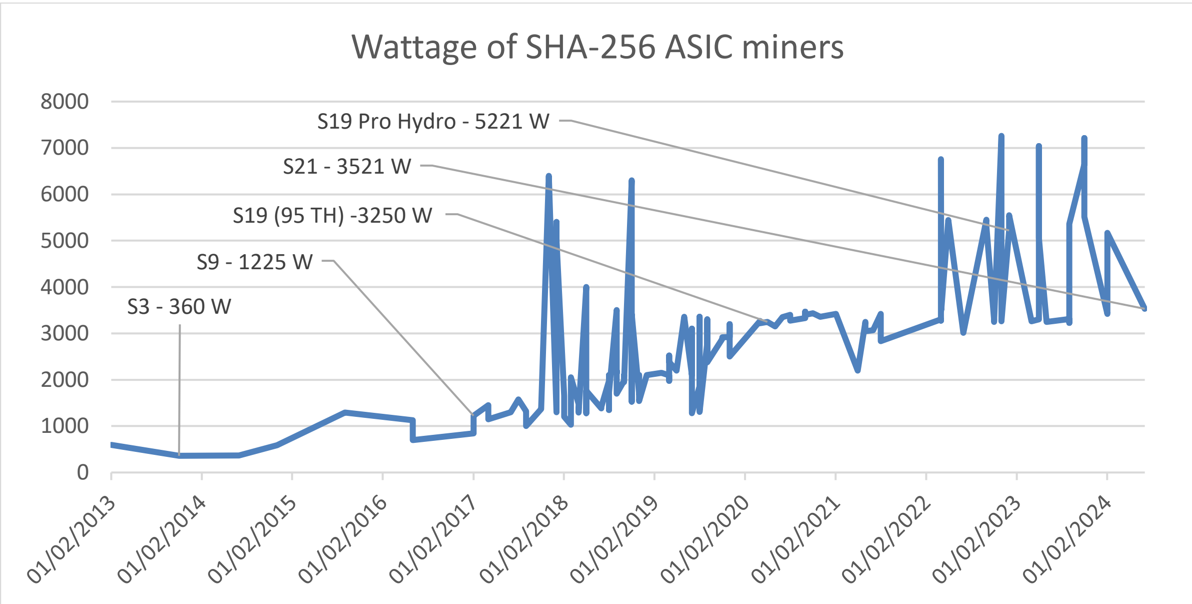


Figure 16 Wattage of SHA-256 ASIC miners, compiled from the CSMEL.

Another performance characteristic that has improved significantly over the years is the total hashing power of equipment. Originally, the S3 offered mere 0,478 TH while the hashing power of newer ASIC devices is generally between 150-300 TH. The development of the hashing power of equipment released is shown in Figure 17.

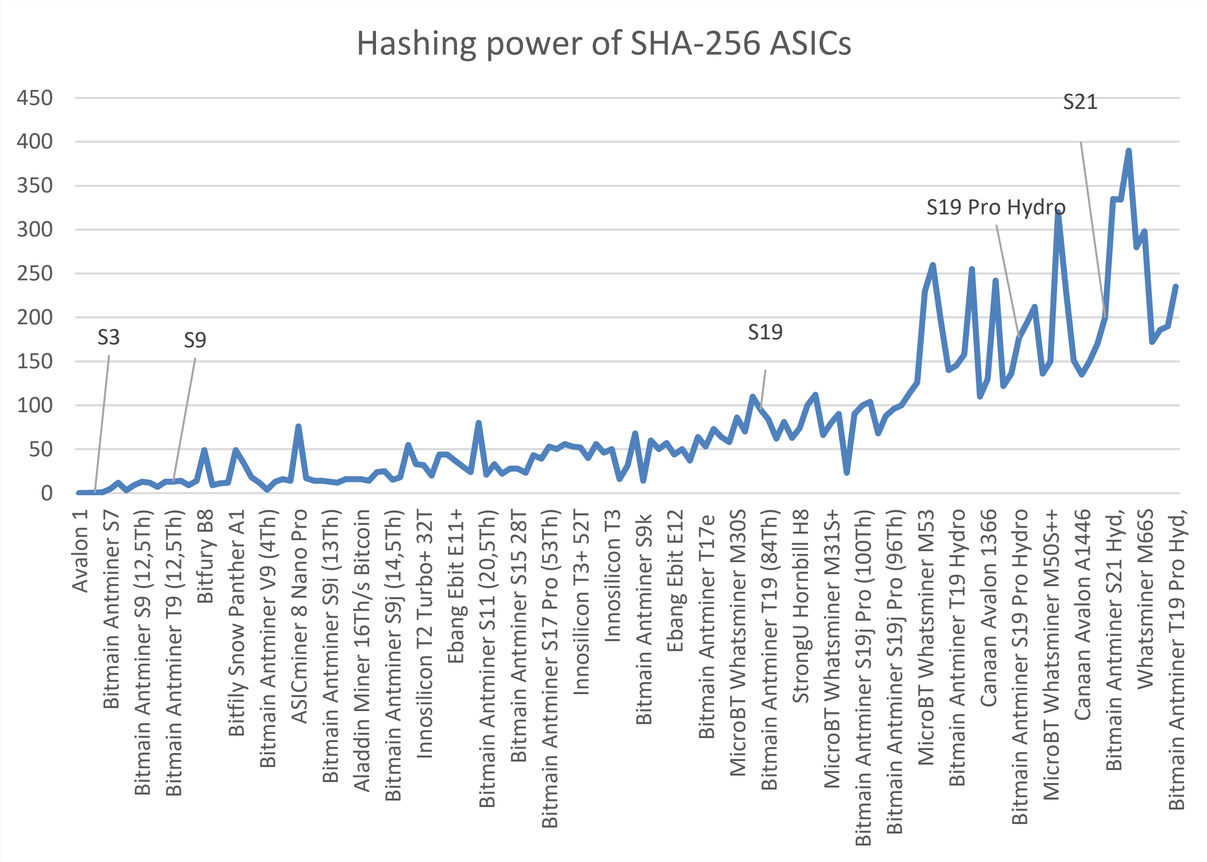


Figure 17 Hashing power of SHA-256 ASICs since 2014 according to the CSMEL.

The data presented in previous figures is compiled into Table 5 for the relevant miners. The evolution of various performance characteristics is clearly observed from the chart. Although the average power draw has clearly increased, the latest generation of Antminers, the S21 is more in line with the previous generation of miners in terms of power draw.

The increased computational performance of miners has pushed equipment prices higher in almost every generation. Access to historical pricing information is quite limited. The price column represents the best estimate based on various resources. The full list of prices and their sources is available in appendix 1.

Table 5 Compiled basic details of ASICs featured in later calculations.

Name	Release	TH/s	W	J/GH	Price	kWh/day
Bitmain Antminer S3	01/07/2014	0,478	366	0,7657	550	8,784
Bitmain Antminer S9 (12.5Th)	01/02/2017	12,5	1225	0,098	2710	29,4
Bitmain Antminer S19 (95Th)	01/05/2020	95	3250	0,0342	2475	78
Bitmain Antminer S19 Pro Hydro	01/01/2023	177	5221	0,0344	3363	125,3
Bitmain Antminer S21	01/09/2023	200	3500	0,0175	5400	84

In Table 6 the USD/day/THash profitability limits are calculated at select electricity prices. The impact of improved efficiency throughout the years is clearly visible in the profitability limits.

Table 6 Calculated breakeven limits of select ASICs.

		Cost of electricity per kwh							
		0,03		0,05		0,1		0,15	
Name	kwh/day	Cost/day	Limit	Cost/day	Limit	Cost/day	Limit	Cost/day	Limit
S3	8,784	0,26	0,551	0,44	0,919	0,88	1,838	1,32	2,756
S9 (12.5Th)	29,4	0,88	0,071	1,47	0,118	2,94	0,235	4,41	0,353
S19 (95Th)	78	2,34	0,025	3,90	0,041	7,80	0,082	11,70	0,123
S19 Pro Hydro	125,304	3,76	0,021	6,27	0,035	12,53	0,071	18,80	0,106
S21	84	2,52	0,013	4,20	0,021	8,40	0,042	12,60	0,063

4.3.2 S3

The profitability of the S3 era is presented in Figure 18 from the release date to the end of 2019. The evolution of profitability follows an expected trajectory of profitability dropping significantly following the release of significantly improved equipment. However, the drop in profitability cannot be attributed entirely to increasing hash rate or difficulty resulting from new equipment, as the price of Bitcoin dropped nearly 70% in the 6 months following the release of the S3.

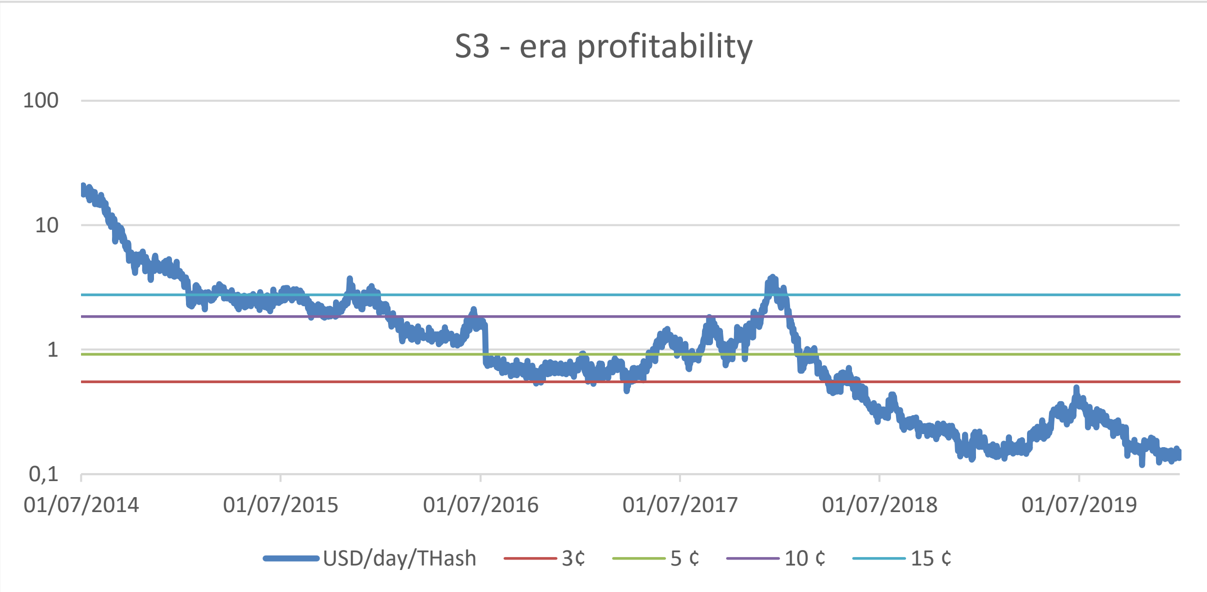


Figure 18 S3 - era profitability with profitability limits. Logarithmic scale.

The sustained profitability is highly dependent on the price of electricity and time of entry. For the S3, the last date the profitability exceeded the limit for 3 cents, was on the 21st of May

2018. The final full month where the average profitability exceeded the same limit was March 2018. For higher electricity prices mining became unprofitable much earlier. Average monthly profitability and profitability limits are illustrated in Figure 19.

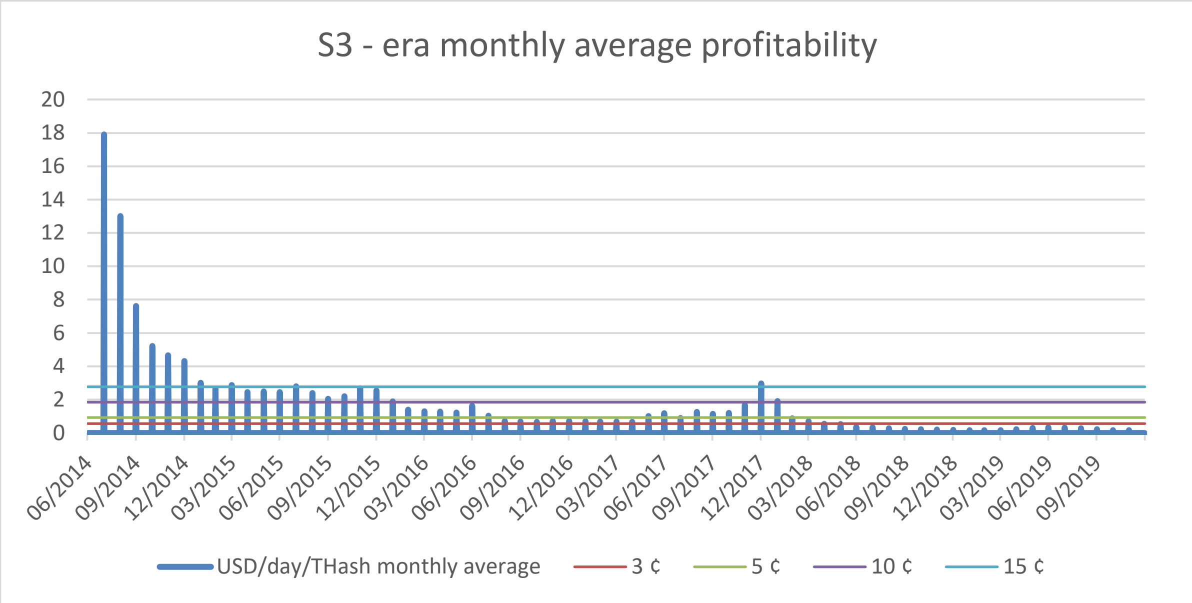


Figure 19 S3 - era monthly average profitability.

The monthly profitability data and profitability limits provide us with the data presented in Table 7. The length of profitable mining periods depends heavily on the cost of electricity, as expected.

Table 7 S3 total number of profitable months

Cost	Profitable months
3c	45
5c	33
10c	21
15c	10

Accounting for extended delivery and installation periods shortens the profitable periods even further. In the S3 era the improvements associated with new equipment releases were considerable as seen earlier from Figure 12 and Figure 17. This, together with the Bitcoin price movements at the time explain the dramatic differences in average profitability between 0-,2-, and 4-month figures. Daily profitability ranges from 1,715-8,783 USD/day/THash, depending on the parameters. The average profitability being higher for higher electricity costs is simply the result of more stringent limits being applied to these datasets. Similarly, the identical profitability in some columns is the result of profitability being above the lowest limit for the whole duration of the period.

Note, * denotes the value is not applicable as the total number of months is not sufficient to calculate the value.

Table 8 S3 average profitability depending on mining period and delivery and installation time

Cost	Delivery and installation in months								
	0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	8,783	5,719	2,534	4,577	3,575	1,933	3,327	2,861	1,715
5c	8,783	5,719	3,193	4,577	3,575	2,402	3,327	2,861	2,125
10c	8,783	5,719	4,288	4,577	3,575	3,113	3,327	2,861	2,725
15c	8,783	*	6,433	4,611	*	4,177	3,434	*	*

The gross profit generated by the S3 is presented in Table 9. The gross profit figures in this and subsequent gross profit tables only account for the cost of electricity. The profitability after equipment cost is illustrated by the green-red colour scheme. A red colour indicates that the gross profit is not sufficient to cover the cost of equipment and running the equipment for the time period at that cost was not profitable.

Accounting for the release price of the S3 at 550 US dollars, profitability is somewhat limited at realistic delivery and installation periods. Assuming the device stays functional for the full profitable time period, the device can generate a profit with 3 and 5 cent electricity. However, as discussed in 4.2.1 this is somewhat unrealistic and should by no means be interpreted as a guarantee.

Table 9 S3 gross profit.

Cost	Delivery and installation in months								
	0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	717,7	901,1	1296,8	351,0	527,3	903,8	242,0	402,7	761,1
5c	685,7	837,0	1090,3	318,9	463,2	711,0	210,0	338,6	578,6
10c	605,5	676,8	747,8	238,8	303,0	389,1	129,9	178,4	270,9
15c	525,4	*	534,2	161,7	*	206,4	59,1	*	98,5

4.3.3 S9

The rate of equipment development was considerably slower in 2017 versus 2014. Looking at Figure 15 and Figure 17 presented previously in chapter 4.3.1, it took nearly a year for newer equipment to surpass the S9 in terms of efficiency. Consequently, we do not see a similar crash in profitability following the release of the S9 as shown in Figure 20. Instead, profitability follows the Bitcoin boom of 2017-2018 closely, with the highest profitability coinciding with the market peak at the time.

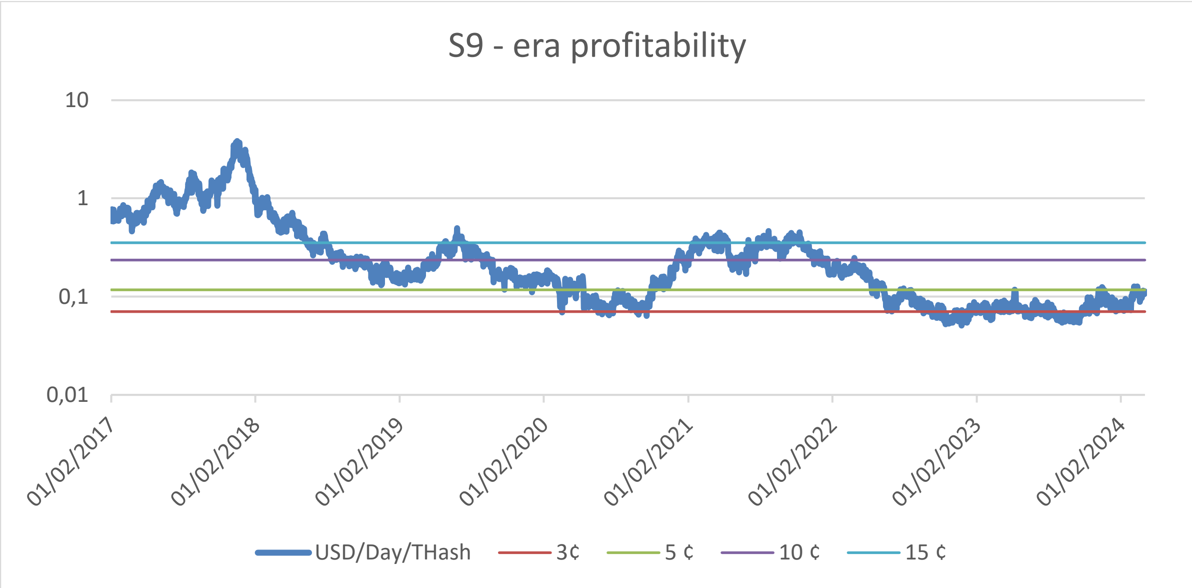


Figure 20 Daily profitability following the release of the S9. Logarithmic scale.

The values used in the calculations are show in Figure 21.

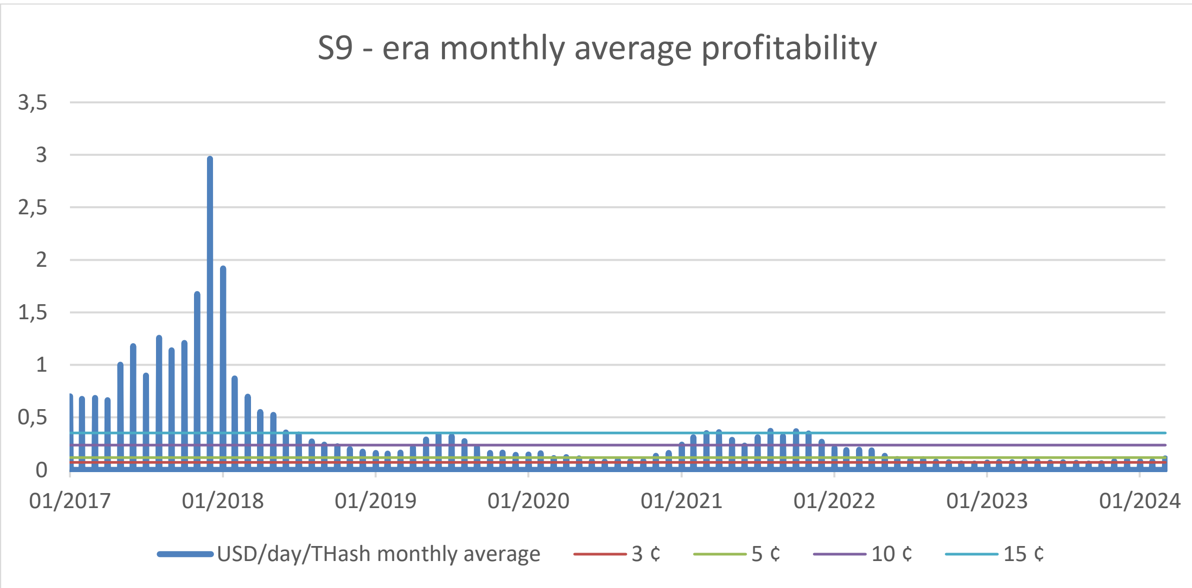


Figure 21 Monthly profitability following the S9 release.

The much-improved efficiency and resulting staying power of the S9 is seen clearly from the number of profitable months. At 3 cents the S9 has been profitable for a total of 81 months. Even at 15 cents, the equipment was profitable for a total of 21 months.

Table 10 S9 total number of profitable months.

Cost	Profitable months
3c	81
5c	58
10c	36
15c	21

Although the S9 has remained profitable for an extended period of time, the major decrease in profitability for the full time period of 81 months is noteworthy. Also, the 12-month profitability being significantly higher than the 6-month profitability yet again highlights the price movement of Bitcoin at the time and the impact it has on mining profitability.

Table 11 S9 average profitability depending on mining period and delivery and installation time

Cost	Delivery and installation in months 0			2			4		
	Mining period 6	12	Full	6	12	Full	6	12	Full
3c	0,817	1,171	0,375	0,947	1,288	0,368	1,114	1,280	0,360
5c	0,817	1,171	0,490	0,947	1,288	0,483	1,114	1,280	0,476
10c	0,817	1,171	0,682	0,947	1,288	0,682	1,114	1,280	0,682
15c	0,817	1,171	0,955	0,947	1,288	0,984	1,114	1,280	1,020

Considering the purchase price of the S9 at 1350 USD at release, from Table 12 S9 gross profit. we can see that miners generated considerable returns with the device. Even with an amazon release price of 2700 USD a miner would have made considerable profits. The figures somewhat justify or at least explain the peak price of the equipment at over 5000 dollars during the height of the 2017-2018 boom. Despite the equipment maintaining profitability far beyond 12-months, the gross profit per year is quite modest. For instance, at 3 cents the S9 remained profitable for a total of 81 months but generated only some 8900-9400 USD gross profit compared to 5000-5500 USD in the first 12 months.

Table 12 S9 gross profit.

Cost	Delivery and installation in months								
	0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	1702,1	5015,9	9385,4	1998,6	5552,9	9142,1	2378,6	5514,8	8896,8
5c	1594,9	4801,4	8202,5	1891,4	5338,4	8046,7	2271,4	5300,3	7890,2
10c	1326,7	4265,2	6116,8	1623,2	4802,1	6112,4	2003,3	4764,0	6119,0
15c	1058,6	3728,9	4808,3	1355,1	4265,9	5033,1	1735,1	4227,8	5323,3

4.3.4 S19

The profitability around the time of the S19's release is similar to that of the S9. The crypto market entered another major boom in late 2021-early 2022, which seems to have driven the profitability of miners at the time. The profitability following the release of the S19 is shown in Figure 22.

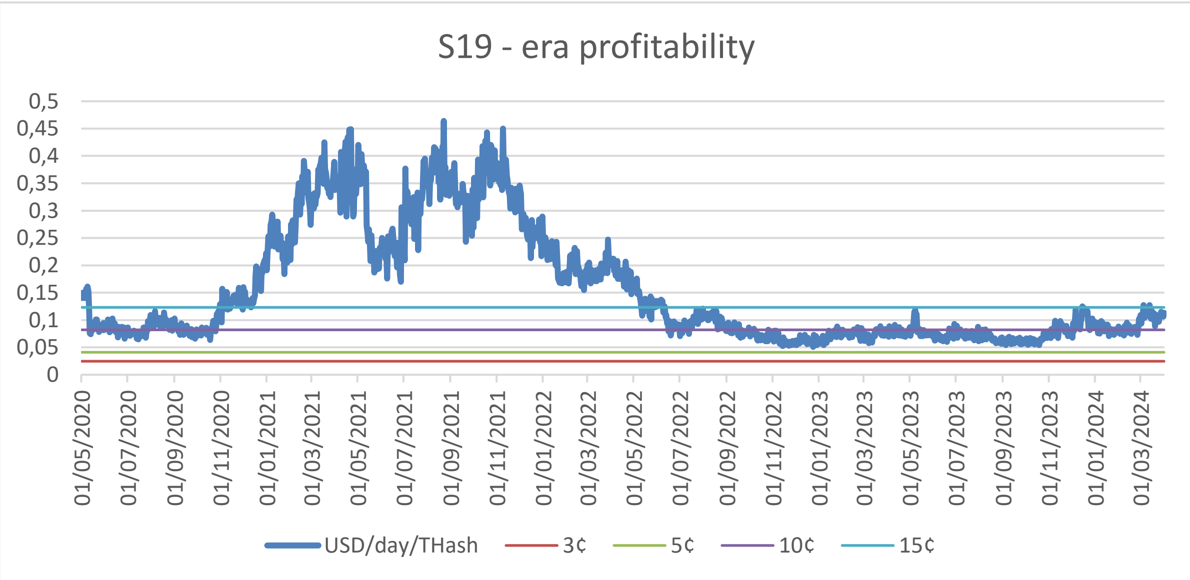


Figure 22 Daily profitability following the release of the S19.

The high profitability is again shown in the monthly averages in Figure 23.

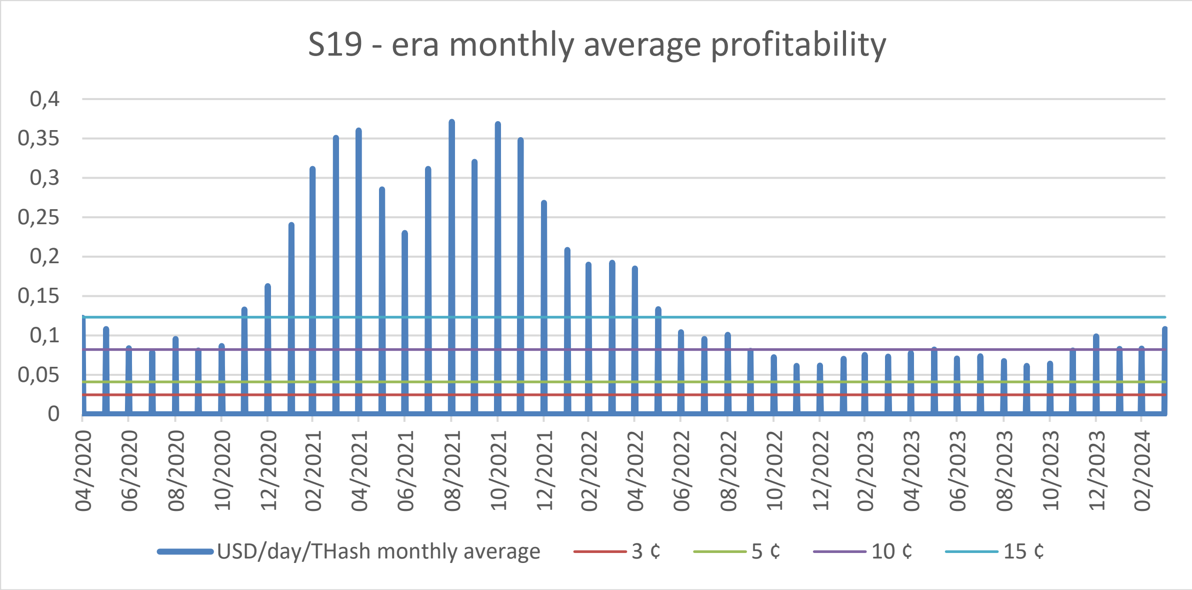


Figure 23 Monthly profitability following the release of the S19.

The number of profitable months extends all the way to present day for 3 and 5 cent electricity costs for the S19, making it the first miner featured in these calculations to extend profitability from release to current day. The number of profitable months for 10 and 15 cents falls just short of the S9, however considering the equipment was released in 04/2020 it is likely that it will eventually surpass the S9 in these figures.

Table 13 S19 number of profitable months.

Cost	Profitable months
3c	48
5c	48
10c	32
15c	19

The seemingly irregular profitability data in Table 14 S19 average profitability depending on mining period and delivery and installation time is explained by a period of reduced profitability following the release of the S19 before the 20-21 boom. According to the model applied, a miner with an electricity cost of 3 cents would have started mining immediately following the 05/2020 release, whereas at 15 cents a miner would have only started mining several months later, on 11/2020. The difference in these figures is a good example of the inherent randomness involved with the activity and how applying the same principles at various points in time can produce vastly different results.

Table 14 S19 average profitability depending on mining period and delivery and installation time.

Cost	Delivery and installation in months 0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	0,095	0,154	0,154	0,093	0,189	0,155	0,133	0,221	0,159
5c	0,095	0,154	0,154	0,093	0,189	0,155	0,133	0,221	0,159
10c	0,105	0,195	0,194	0,134	0,221	0,200	0,214	0,264	0,208
15c	0,260	0,287	0,262	0,296	0,314	0,275	0,318	0,301	0,275

The impact of the major uptick in the crypto market between 6 and 12 months after the release of the S19 is clearly seen from the gross profit figures in Table 15. A purchase price of 2800 USD is assumed in the highlights. Interestingly, with 15 cent electricity cost a miner would not have started mining until the beginning of the major market move, resulting in the equipment paying itself back in just 6 months only at 15 cents assuming a 4-month installation and delivery. The numbers even out significantly when extending the time frame to 12 months, as this extends the mining period to the price peak of the 20-21 uptick regardless of cost.

Table 15 S19 gross profit

Cost	Delivery and installation in months 0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	1218	4500	17874	1186	5700	18106	1878	6793	18571
5c	934	3931	15598	902	5130	15829	1594	6224	16294
10c	394	3912	10380	891	4810	10868	2286	6288	11594
15c	2365	5679	7592	3002	6605	8328	3380	6162	8321

4.3.5 S19 Pro Hydro

The S19 Pro Hydro is the first ASIC featured in this analysis that is considered modern, in terms of release date. Compared to the S19, the S19 Pro Hydro offers slightly improved efficiency of 0,0295 J/GH up from 0,0342 J/GH for the S19. However, comparing the device to other equipment at the time reveals that the efficiency of the S19 Pro Hydro is somewhat lower than other devices released at the time. The profitability following the 01/2023 release is presented in Figure 24. Compared to the profitability after the release of other miners featured in this analysis, the profitability is quite stable, despite the price of Bitcoin climbing from lows of 16 500 USD at release to over 60 000 USD by 03/2024. The increased value of Bitcoin is largely offset by the increases in hash rate in the same period.

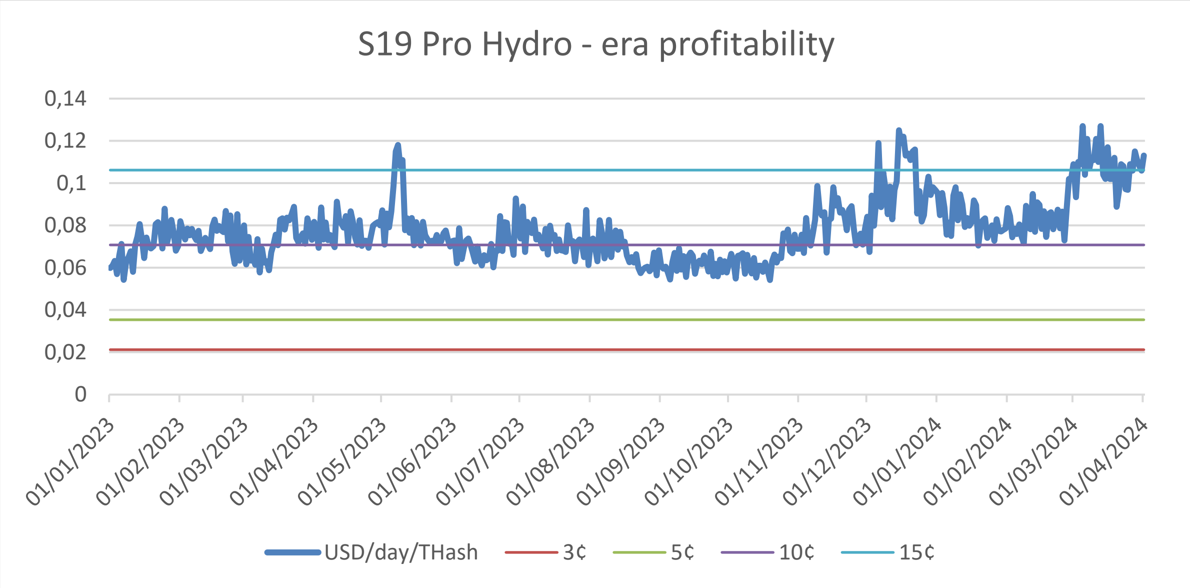


Figure 24 S19 Pro Hydro - era profitability

The monthly profitability in the same period is presented in Figure 25.

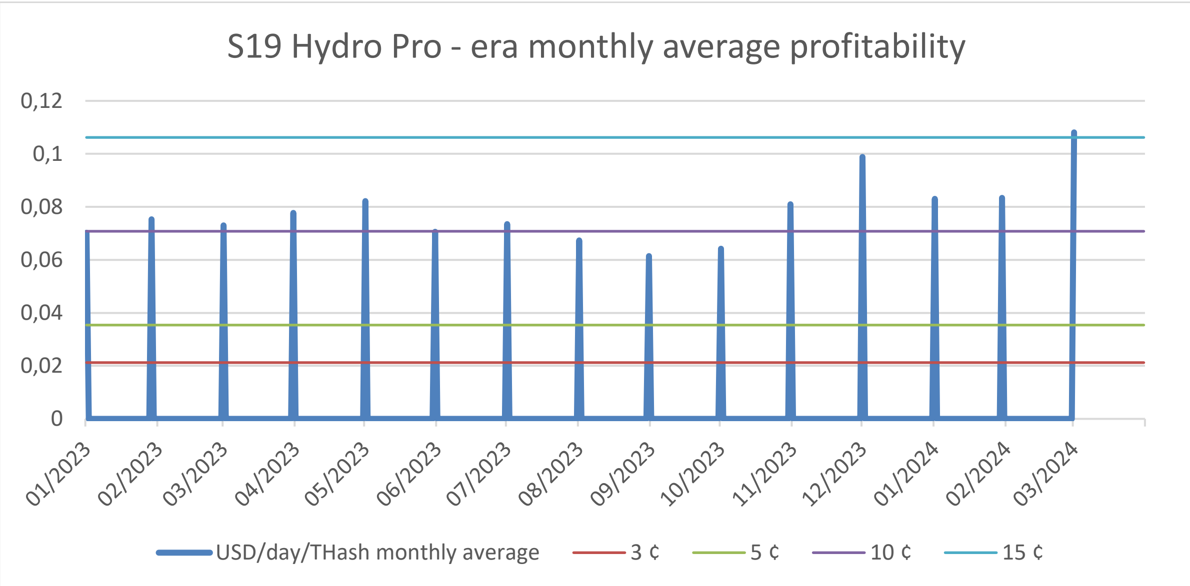


Figure 25 S19 Pro Hydro monthly profitability.

Similar to S3, S9, and the S19, the S19 Pro Hydro has been profitable for a significant number of months at 3 and 5 cent electricity. Even at 10 cents the equipment has been profitable for 10 months, but as shown in Figure 25, the profitability is quite limited. For 15 cents, the equipment has been profitable to mine with only in March 2024.

Table 16 S19 Pro Hydro number of profitable months.

Cost	Profitable months
3c	15
5c	15
10c	10
15c	1

The average profitability during various periods is shown in Table 17, highlighting the stable profitability, despite the volatility of Bitcoin.

Table 17 S19 Pro Hydro average profitability.

Cost	Delivery and installation in months								
	0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	0,075	0,075	0,078	0,074	0,076	0,079	0,070	0,079	0,079
5c	0,075	0,075	0,078	0,074	0,076	0,079	0,070	0,079	0,079
10c	0,077	0,084	0,084	0,083	0,086	0,086	0,088	0,088	0,088
15c	*	*	0,108	*	*	*	*	*	*

The gross profit figures in Table 18 show that despite being the most efficient equipment available at the time, the S19 Pro Hydro struggles to generate enough revenue to cover the cost of the equipment in 12 months, even with 3 cent electricity. In comparison to previous devices analysed, the post Pro Hydro release era has not seen a similar uptick in the crypto market, resulting in decreased profitability, which as previously stated, is something that miners with higher electricity cost heavily rely on.

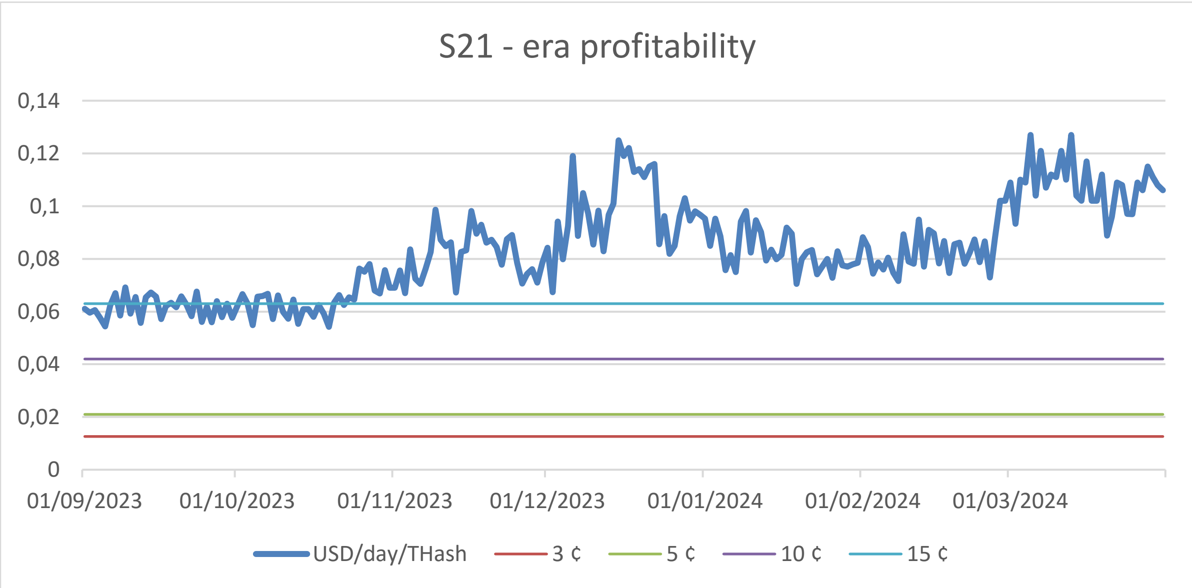
Despite being one of the more recent releases, accurate data for the release price of the S19 Pro Hydro is somewhat lacking. The bitmain.com website archived in February 2023 lists the release price of the 191 TH model at 3629 USD. As no other credible sources were found for the 171 TH model featured in the calculations, the 3629 USD figure was used in the highlights. Considering the release dates of these two versions are so close to each other their official pricing would have likely been similar.

Table 18 S19 Pro Hydro gross profit.

Cost	Delivery and installation in months								
	0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	1731	3447	4581	1705	3559	4646	1571	3757	4696
5c	1273	2532	3438	1248	2645	3503	1114	2843	3554
10c	204	827	689	385	979	816	555	1109	924
15c	*	*	10	*	*	*	*	*	*

4.3.6 S21

Although the S21 does not have an extended history like other devices in this analysis, the S21 was included to present an example of the most efficient equipment available at the time of writing. Compared to the S19 Pro Hydro's 0,0295 J/GH efficiency the S21 is significantly more efficient at 0,0175 J/GH. The S21 Pro announced to be released in 07/2024 is said to offer 0,0151 J/GH. The S21 and S19 Pro Hydro era have considerable overlap, as there is only some 8 months between the release of the devices. The impact of the significantly improved efficiency is immediately apparent in comparing the profitability of the S21 in Figure 26 to the S19 previously.



The monthly profitability for the S21 is presented in Figure 26.

Figure 26 S21 - era profitability

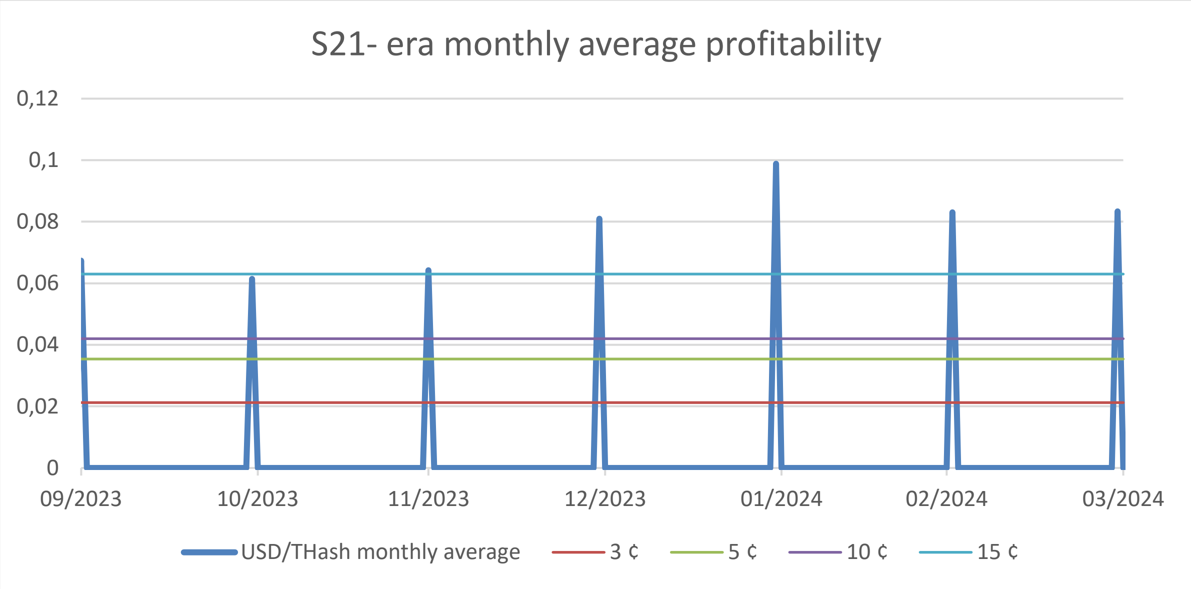


Figure 27 S21 - era monthly average profitability

The efficiency of the S21 is clearly on display in the data in Table 19. The equipment has been profitable even at 15 cent electricity for 7 of the 8 months since release.

Table 19 S21 number of profitable months.

Cost	Profitable months
3c	8
5c	8
10c	8
15c	7

The data on profitability in Table 20 is quite limited, as the S21 was only released in 09/2023. The figures are similar to the S19 Pro Hydro some 8 months earlier.

Table 20 S21 average profitability.

Cost	Delivery and installation in months								
	0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	0,076	*	0,081	0,086	*	0,086	*	*	0,093
5c	0,076	*	0,081	0,086	*	0,086	*	*	0,093
10c	0,076	*	0,081	0,086	*	0,086	*	*	0,093
15c	0,080	*	0,084	0,091	*	0,091	*	*	0,092

The data on gross profit in Table 21 is similarly limited due to the release date. Surprisingly, although the S21 was released very recently, reliable data on release pricing is limited.

Bitmain lists the price of the S21 currently on 04/2024 at 5 400 USD. At the time of the release of the S21, the updated versions of the S19 were selling at 33 USD/THash, which would make the release price of the S21 approximately 6 600 USD at 200 TH. However, as there is no credible to source to verify this estimate, 5 400 USD was used as the assumed purchase cost in the highlights in Table 21.

Although the S21 is the most efficient SHA-256 ASIC currently available, it has not generated sufficient revenues since release to account for the purchase cost of the equipment. As shown in Table 21, assuming a purchase cost of 5 400 USD, the S21 falls short of generating a profit in the first 8 months since release. While the equipment has only been out for a limited period of time, assuming profitability maintains at current levels miners would struggle to recoup their initial investment in most situations even in 12 months. As has been shown with previous generations of mining equipment, a major market move can cause a surge in the profitability and allow miners to generate considerable returns in short periods of time.

Table 21 S21 gross profit.

Cost	Delivery and installation in months								
	0			2			4		
	Mining period								
	6	12	Full	6	12	Full	6	12	Full
3c	1994	*	2870	2331	*	3108	*	*	3405
5c	1687	*	2462	2024	*	2699	*	*	2997
10c	921	*	1440	1258	*	1678	*	*	1975
15c	273	*	471	635	*	741	*	*	765

4.4 Discussion

In this chapter the profitability and gross profit of several miners was calculated at select points in time. The calculations show that early generations of ASIC equipment (S3 and S9) generated considerable revenue, easily recouping the initial cost of the equipment, even in just 6 months. The profitability of Bitcoin mining has since dropped significantly, even when accounting for more efficient equipment. The combination of reduced profitability and higher equipment costs seems to have produced a situation where even miners with access to affordable electricity are struggling to generate revenues to cover the cost of equipment.

(Delgado-Mohatar et al., 2019) estimated the limit for profitable operation to be 0,14 USD/kWh in June 2018 using a marginal cost estimate of 1952 USD per bitcoin and accessible equipment, such as the S9. The profitability calculations presented in this section in chapters 4.3.2 and 4.3.3 reached similar conclusions. Delgado-Mohatar et al. found that for the most efficient equipment at the time and 0,05 USD/kWh electricity mining was not profitable after November 2018. These conclusions are similarly in line with our findings. Although this section did not look at the most efficient equipment available at the time, the period described by Delgado-Mohatar et al. coincides with decreases in profitability shown in Figure 20 and Figure 21. The operational feasibility considerations in the form of delivery and installation periods make the calculations presented in chapter 4.3 a more accurate account of the expected real-world results.

A repeating theme across all the generations of miners analysed, was that miners with higher cost electricity were very dependent on periods of exceptionally high profitability to even operate the equipment profitably. In fact, looking at profitability during more level periods within each era shows, that market entry is one of the key aspects of generating sufficient revenue to recoup the cost of equipment within a reasonable time frame, regardless of electricity cost. For example, the S21 has been profitable since release for miners with an electricity cost of less than 10 US cents but has still failed to generate sufficient revenues to cover the cost of equipment, at least so far.

The calculations indicate that miners are heavily reliant on periods of high profitability to recoup the cost of equipment and generate a profit. The periods of high profitability are the result of significant increases in the price of Bitcoin. Periods of extreme profitability as a result of several fold price increases are therefore unlikely to occur anymore, as they would push the market capitalization to the 10 trillion-dollar range. These findings appear to be in line with the conclusions by (Islam et al., 2023) regarding Ethereum mining, that sustained profitability would require significant price increases. Islam et al. also found that organic growth alone would not be sufficient to maintain profitability, but the calculations in this study did not consider this aspect.

The price and power requirements of hardware have raised the barrier of entry for mining considerably. Although the era of generic computer hardware in mining Bitcoin was rather short lived, early ASICs were much more affordable and their electricity use was more in line with consumer electronics. Modern ASIC miners can cost over 5 000 USD (S21) and draw several kilowatts of power.

4.5 Conclusion

This chapter was associated with R3. What do the financials of mining Proof of Work cryptocurrencies look like?

The profitability of mining depends heavily on associated costs and the price movements of Bitcoin. Although mining continues to be profitable for efficient modern equipment, revenue generation does not appear to be sufficient to recover the cost of equipment within the 6- or 12-month time frames. The stark difference in gross profit between the S19 and the newer S19 Pro Hydro and the S21 is the result of the relatively stable market conditions of the last few years.

Earlier generations of equipment produced impressive revenues at times, but entry timing was shown to be a key factor. The calculations highlight, that mining can be a lucrative business depending solely on entry. A miner who manages to acquire equipment heading into periods of increased profitability, whether due to strategy or sheer luck, will generate impressive revenues, whereas a miner with poor timing will never recoup their initial investment.

Depending on the maturity of the network, other phenomena can be a major factor in impacting profitability. Following the release of the S3, which was at the time a massive improvement to previously existing hardware, the profitability of mining dropped rapidly. Such phenomenon was not observed with later generations of equipment, as these were not as significant improvements over previous generations.

The results of this study were found to be in line with the findings of previous works by (Delgado-Mohatar et al., 2019) and (Islam et al., 2023).

4.6 Limitations

This analysis focused on analysing Bitcoin mining. Bitcoin is mined using ASIC hardware that is only suited for the SHA-256 algorithm. It is possible that other cryptocurrencies could have produced vastly different results, in terms of profitability. However, the applicability of those results would not necessarily be as wide, as they are less representative of cryptocurrency due to limited adoption and use.

The calculations featured equipment from just a single manufacturer. The analysis represents a small subset of all available miners and again, the results could be somewhat different for other devices. However, the pricing of hash rate seems to have been quite efficient throughout the years. It is unlikely that different equipment would have produced very different results. Still the possibility remains that these same calculations could produce different results with different equipment. However, data availability is often even more limited with other manufacturers and the quantity of devices delivered at the time of release was significantly lower compared to Bitmain. The applicability of these results would therefore be limited, even if they were significantly different.

This analysis utilized a simplified, but repeatable and well justified model for evaluating profitability following the release of equipment. The model used assumes a simple mining strategy, more advanced and data driven strategies could produce better results. The model attempted to account for miner reaction times by using monthly profitability averages to determine when equipment was operated. However, even this could be considered as taking advantage of information from the future. A more realistic approach would perhaps be to assume that it takes a miner one extra month to react to profitability increases. This would produce more accurate data, but the impact would likely be negligible as the profitability at the beginning of a cycle is low compared to peak profitability.

Another approach not considered in this model is for miners to hold to the mined coins and sell some time in the future. Such a strategy could produce inflated gains, but it would be highly speculative and more akin to simply purchasing the coins in the first place.

Finally, perhaps biggest limitation in evaluating profitability is the price of equipment. The data on the price of even current equipment is limited and the reliability is somewhat called into question, looking at the results of mining in the last year or so. It is possible, and even likely, that wholesale prices of equipment are considerably lower, meaning miners are able to generate sufficient revenues to turn a profit. Access to this sort of pricing information is however not widely available.

5 Community building

Cryptocurrencies have amassed a major following since the launch of the Bitcoin network in 2009. The userbase has grown at a rapid pace with the number of identity-verified users estimated to have increased from 5 million in 2016 to 575 million in 2023, according to statistics compiled by Statista.[41] The popularity of cryptocurrencies has created many communities on several platforms around the various aspects, use cases, and services developed around the technology.

In 2024, Reddit is a popular social media platform that hosts several of the largest communities around cryptocurrencies, such as r/CryptoCurrency, r/Bitcoin, and r/Ethereum. Communities formed in the early days of the crypto phenomenon like bitcointalk.org maintain a following, but they are perhaps more aimed at advanced users. Groups such as miners, traders, and developers have their own dedicated communities focused on these topics. The community creation potential of cryptocurrencies is well established by the existence of such varied communities.

Community composition and user motivations are an important aspect in analysing factors contributing to community creation. Depending on the community, user motivations for participation can vary significantly. Communities built around cryptocurrencies are focused on the technology, regardless of the specific focus of the community, and they undoubtedly play a role in promoting the technology. However, although the growth of the crypto related communities displays the community creation potential and the popularity of cryptocurrencies, the relative importance of factors contributing to the phenomenon are poorly understood. This section aims to provide an answer to R4. How does crypto mining contribute to the community creation of a cryptocurrency?

---

[41] *Crypto users worldwide 2016-2023*. (2023, December). Statista.
https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/

5.1 Methodology

Introduction

This section describes the methodological background for the research method selected. Currently, no established or proven method exists for answering a question such as R4. This chapter describes the relevant applicable research and demonstrates, how it can be applied for the purposes of this chapter. The structure of the chapter is as follows, first the foundational research regarding community engagement and participation is presented, next the applicable research on cryptocurrencies is briefly discussed, and finally methodological justification for the chosen approach is outlined.

Community related methodology

Community engagement has been defined by the CDC in 1997 as

> "…the process of working collaboratively with and through groups of people affiliated by geographic proximity, special interest, or similar situations to address issues affecting the well-being of those people."

According to (McCloskey et al., 2011) it aims to promote participation and involvement of individuals in processes that concern them. On a practical level the community can be engaged in multiple ways such as organizing meetings and providing other opportunities to express concerns and opinions. (McCloskey et al., 2011) further states that the organizing concepts of community engagement are drawn from community participation, community mobilization, constituency building, community psychology, and cultural influences. Community engagement, specifically in terms of community participation, community mobilization, and constituency building are of particular interest in evaluating the role of mining in enabling the crypto phenomenon.

User motivations affecting participation have been extensively studied. (Bagozzi & Dholakia, 2002) analysed participation in online chat rooms and found that anticipated positive emotion was among the key factors for participation. For social networking sites (SNS) , (Brandtzæg & Heim, 2009) report that according to their 2007 questionnaire, new relations, friends, socializing, information, and debating are the five most common reasons for participating in SNS-communities. The paper did not differentiate between communities based on their type, which likely in part explains the varying motivations. (Foster et al., 2010) provide a thorough account of distinct types of communities listing five types depending on their characteristics:

collaborative projects, blogs, content communities, social networking sites, and virtual game worlds.

The characteristics of these categories can be simplified by applying the principles of cooperative group action described by (Bagozzi & Dholakia, 2002). *Fully cooperative group* action is a characteristic typical for collaborative projects, where the group coordination controls the actions of individuals entirely. *Partially cooperative group* action is a characteristic of a community where group coordination is present, but not as strict such as communities facilitating transactions. *Minimally cooperative group* action is essentially a community of individuals with the same goals, but no common intention of achieving them such as help forums.

Search trend analysis

Trend analysis attempts to analyse data and spot patterns from the data, often to forecast future events. It is commonly used in finance to identify market patterns. Trend analysis consists of estimating at least the following characteristics of the current phase: direction, length, and amplitude of the move. Technical indicators can be used to determine the characteristics of the phase, but they are not definitive. Trend interruptions refer to situations where the direction of the market suddenly changes. In such situations it is important to recognize if the underlying fundamentals have shifted, or the interruption is facilitate by short term catalysts. (Logan, 2014)

Search trend analysis applies a similar pattern recognition process used in trend analysis to search term usage. Currently, search trend analysis is largely facilitated by Google trends, a service offered by Google that allows anyone to see the relative popularity of any search term going back to 2004. The popularity is expressed as a figure between 0 and 100. The data can be limited to a specific geographical area and the service displays related terms for context.

Google trends data has been used extensively in literature to estimate popularity and forecast events. (Choi & Varian, 2012) found that Google trends data could be used to predict the present more accurately than other models. Predicting the present is known as a *contemporaneous forecast* or *nowcasting*. It refers to the use of accessible data to predict figures that are usually only available after major delays. (Kim & Malek, 2018) demonstrated that Google trends data could be incorporated into existing models to produce more accurate forecasts of casino revenues. (Malagón-Selma et al., 2023) found that Google trend data could be used to explain and to an extent predict player popularity and even market value to a degree.

Description of approach

Bitcoin miners have been recognized as a subset of the wider Bitcoin community in previous research. (Xu et al., 2021) highlight that while the role of miners in maintaining the Bitcoin network is widely known, the body of research on understanding the characteristics and behaviour of this group is limited. The analysis by Xu et al. looked at the activity of Bitcoin addresses to estimate the total number of miners at different stages of the network. The research found that as the network matured the number of active addresses associated with mining decreased, leading to mining becoming more centralized. The paper is one of the few pieces of academic literature providing insight to the development of miners as a group.

The limited amount of research on the topic presents challenges to the research method of this section. Lack of proven methodology and basic research forces the section to look at the fundamental aspects of communities. Studies looking at specific aspects of discussion forums are widely featured in literature. Qualitative[42] analysis of forum posts is a commonly used approach, while quantitative[43] methods are less frequent. (Holtz et al., 2012) provides guidelines for analysing online forums focusing specifically on qualitative methods. No similar resource on quantitative analysis of discussion forums is available, but examples of quantitative methods applied to data from these platforms are available. (Glenski et al., 2019) looked at conversations and how they spread on different subreddits. The study separated official subreddits and the crypto-ecosystem and found that conversations behave differently depending on whether they were on the official crypto subreddits or on one of the crypto-ecosystem subreddits.

Although the methodology of these studies is not directly applicable in this section, they highlight the value of discussion forums as a data source. This section will utilize discussion forums as a data source by comparing the size of official and crypto ecosystem subreddits, to establish the share of users interested in mining specifically. Activity levels will be analysed

---

[42] Baek, J., & Shore, J. (2020, May 11). *Forum Size and Content Contribution per Person: A Field Experiment | Management Science*. https://pubsonline.informs.org/doi/10.1287/mnsc.2019.3484

[43] Shi, X., Zhu, J., Cai, R., & Zhang, L. (2009). User grouping behavior in online forums. *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 777–786. https://doi.org/10.1145/1557019.1557105

as well to see, whether they produce similar figures as the comparison of community sizes. The research will be conducted as a quantitative analysis of data collected from select platforms.

To complement the community analysis a search trend comparison will be performed. The analysis will look at the search trend popularity of several crypto related terms to first establish the current trend and phase of the market and then compare those figures to the search trend popularity of Ethereum at the time it moved away from PoW. The specific use of this data is described in detail in chapter 5.2.

5.2 Method

Mining has created many dedicated communities around the activity with varying scopes, some more general in nature, while others are focused on a single cryptocurrency or a subset of mining. While the birth of such communities is to be expected, their role in the community building and general characteristics are less well established. The communities built around cryptocurrencies and crypto mining are quite spread out among several different social media platforms, ranging from reddit to various dedicated forums which presents challenges for the analysis.

The communities chosen for this analysis were select subreddits and bitcointalk.org. This selection of platforms was primarily due to size, popularity, and previous research. As these platforms do not provide access to the same metrics and their categorization differs slightly, different evaluation methods were applied in each case. For Bitcointalk.org, the number of topics and threads under each sub-forum was recorded. On reddit, subreddits were screened by a search using the keywords “crypto” and “cryptocurrency,” the most relevant subreddits were selected and the number of followers was recorded. The subreddits were divided to official and mining related subreddits, similar to (Glenski et al., 2019), and the figures were compared to determine the share of users participating in mining related communities versus official communities. As these figures are only compared within the same platform, the platform specific methods do not jeopardize data quality.

For the search trend analysis Google trends data was collected using several crypto related terms. The data was queried from 2004 onwards and compiled into the figures and statistics presented. Ethereum offers an interesting although singular data point in terms of search interest as it is the first popular and established cryptocurrency to make major changes to its consensus algorithm, moving away from PoW to PoS. If mining is comparatively effective at creating engagement and building community, a drop in search interest should be observable after the move to PoS. For the comparison search trend data was collected of the following terms: ethereum, bitcoin, cryptocurrency, dogecoin, litecoin, and monero.

5.3 Social networking sites

Table 22 Number of posts on various sub-forums on bitcointalk.org. Data updated on 04/2024

Bitcointalk			
		Posts	Topics
	Bitcoin discussion	2 631 302	100 868
	Dev and tech	334 525	25 579
	Mining	962 049	27 434
	Bitcoin Tech support	118 833	13 140
	Project development	185 444	16 036
	Altcoin discussion	3 455 381	108 514
	Altcoin mining	862 348	33 999
	Speculation	1 052 941	14 948
Excluded	Announcement	8 678 666	52 788
Excluded	Marketplace	11 052 489	48 936

From numbers compiled in Table 22 mining related conversation accounts for 23% of all posts and 15% of topics on Bitcoin as a share of related conversations. The figures are similar for altcoins with 16% of posts and 22% of topics on mining, when excluding announcements and marketplace content. These topics and posts were excluded as they seem to mainly consist of various types of advertisements and other commercially motivated content, rather than organic conversation. Localized subforums were also excluded as the division of topics was less clear and it was subsequently impossible to accurately attribute posts and topics to their respective categories without manually translating and evaluating each topic.

The total number of users reported by the site was 3,6m in April 2024.

A similar analysis on reddit looking instead at the follower counts of various subreddits produces the following numbers in Table 23.

Table 23 Follower counts of various crypto and mining related subreddits.
*Ethereum mining has stopped since 09/2022

General		**Followers**
	Cryptocurrency	7 800 000
	Bitcoin	6 500 000
	BTC	1 100 000
	Crypto	300 000
	Altcoin	225 000
*	Ethereum	2 900 000
*	EthTrader	2 300 000
	Dogecoin	2 500 000
	Litecoin	359 000
	Monero	322 000
	BCH	102 000
Mining		
*	EtherMining	194 000
	BitcoinMining	101 000
	GPUmining	95 000
	MoneroMining	73 000
	CryptoMining	46 000
	LitecoinMining	22 000
	DogecoinMining	18 000
	BCHMining	Does not exist

The topic of some of the subreddits listed is less clearly defined here in terms of Bitcoin versus altcoins. For instance, r/Cryptocurrency and r/CryptoMining are a mix of both Bitcoin and altcoin related content. Comparing the follower counts of r/Cryptocurrency and general mining communities reveals that mining related subreddits have only a fraction of the follower counts of more general subreddits.

The overlap of topics makes it challenging to attribute the follower counts to either Bitcoin or altcoins. However, many altcoins have their own dedicated subreddits for general conversation and mining. Extending the analysis to these communities provided additional data. Comparing the data collected from various subreddits of Bitcoin and the three most popular altcoins by market capitalization, we can see that the follower count of various subreddits and their mining counterparts varies widely. In Table 24 the High and Low rows represent the upper and lower bounds of the share of users, assuming that users are either part of both communities (High) or only part of one community (Low). For Bitcoin, the size of the mining communities is only a fraction of the size of the overall community, with a follower share of 1,53-1,55%. For altcoins, the average is similar, but varies significantly for individual coins: Dogecoin 0,62-0,62%, Litecoin 5,77-6,13%, and 18,48-22,67% for Monero.

For Ethereum, the figures used are from 09/2022 as this was the last date the currency was mineable and comparing the current sizes of communities would produce largely inapplicable data. The follower share of the mining community was 12,01-13,66%.

The more general mining related subreddits produce some uncertainty to the accuracy of these numbers. However, the overall impact of these is quite limited as the communities are often small in comparison and they would likely not make any meaningful difference to the data presented here.

Table 24 Comparison of the follower counts of general and mining related subreddits.
*Ethereum mining has stopped since 09/2022
**Figures from 09/2022

Bitcoin			
	General	**6 500 000**	
	Mining	**101 000**	
	High	**1,55**	
	Low	**1,53**	
Doge			
	General	**2 900 000**	
	Mining	**18 000**	
	High	**0,62**	
	Low	**0,62**	
Lite			
	General	**359 000**	
	Mining	**22 000**	
	High	**6,13**	
	Low	**5,77**	
Monero			
	General	**322 000**	
	Mining	**73 000**	
	High	**22,67**	
	Low	**18,48**	
***Ethereum**			
	General	**1 450 000**	**
	Mining	**198 000**	**
	High	**13,66**	
	Low	**12,01**	

5.4 Google trends

The market peaks of 2014, 2017-2018, and 2021-2022 are clearly visible from the data as are the down markets lasting several years in between. The data corresponds perfectly with the known history of the market and its cycles described in chapter 2.5.

For Bitcoin, Litecoin, and Monero the 2017 peak represents the highest point of interest, whereas for Ethereum and Dogecoin the interest peak occurred during the 2021 market peak.

The data used in the analysis is presented in Figure 28-Figure 33.

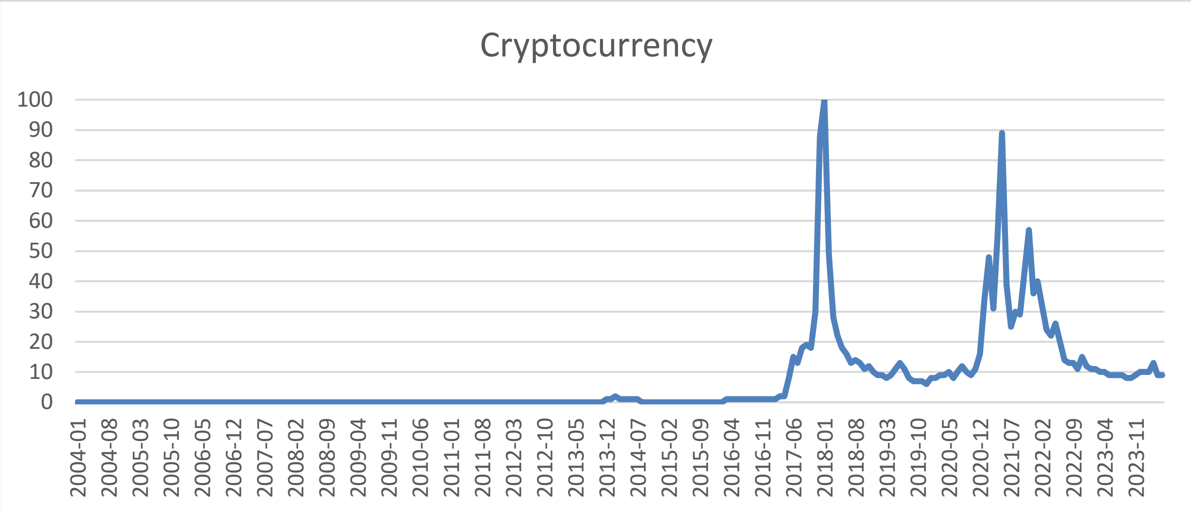


Figure 28 Google search interest for "cryptocurrency"

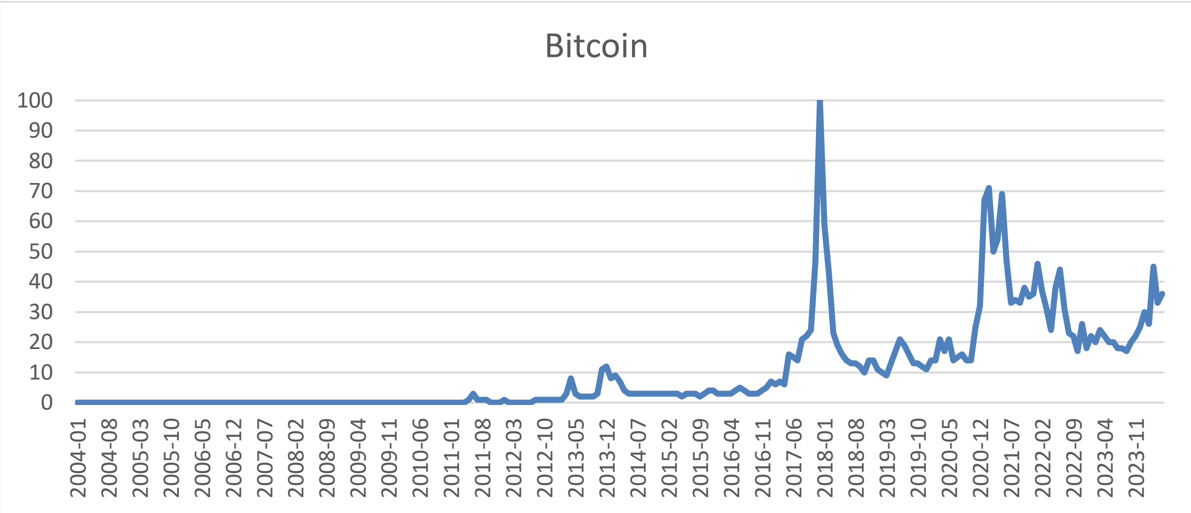


Figure 29 Google search interest for "bitcoin".

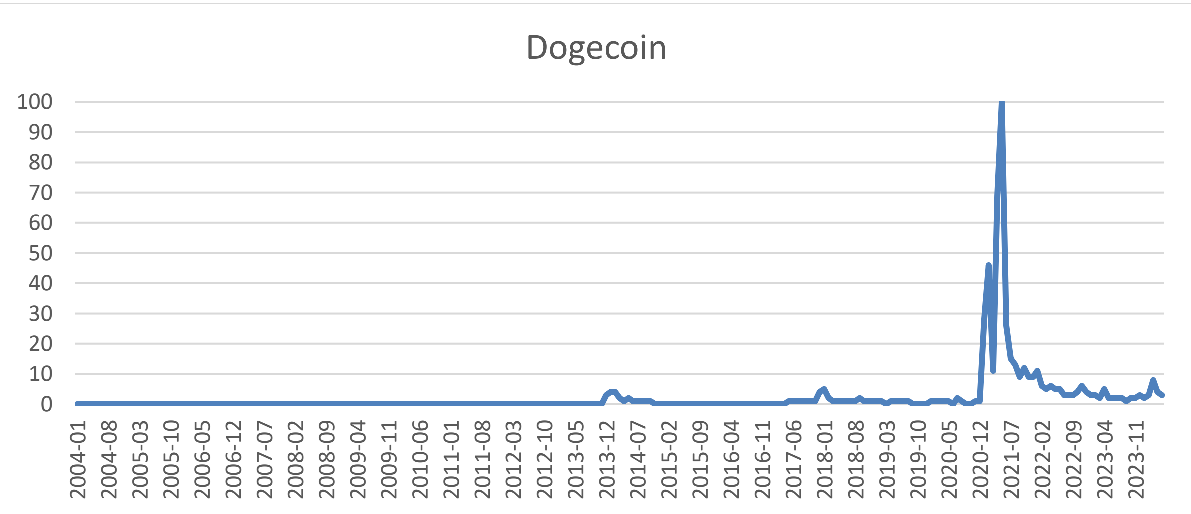


Figure 30 Google search interest for "dogecoin".

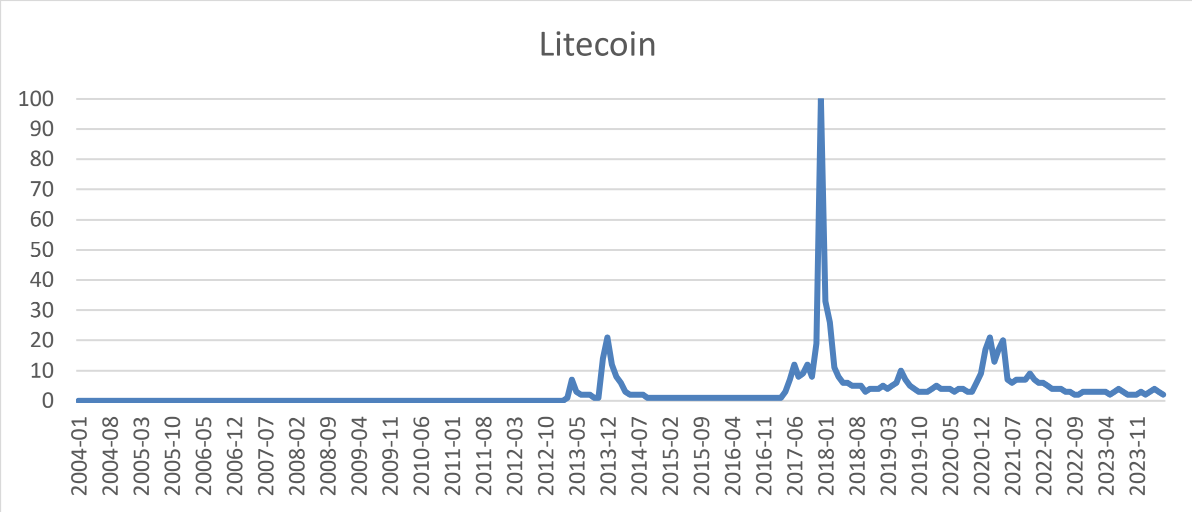


Figure 31 Google search interest for "litecoin".

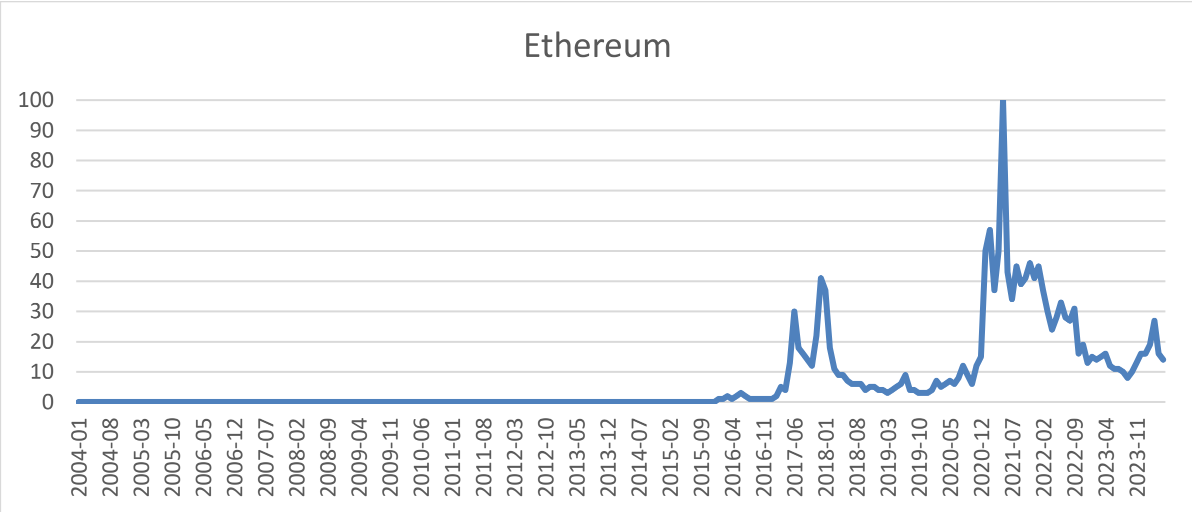


Figure 32 Google search interest for "ethereum".

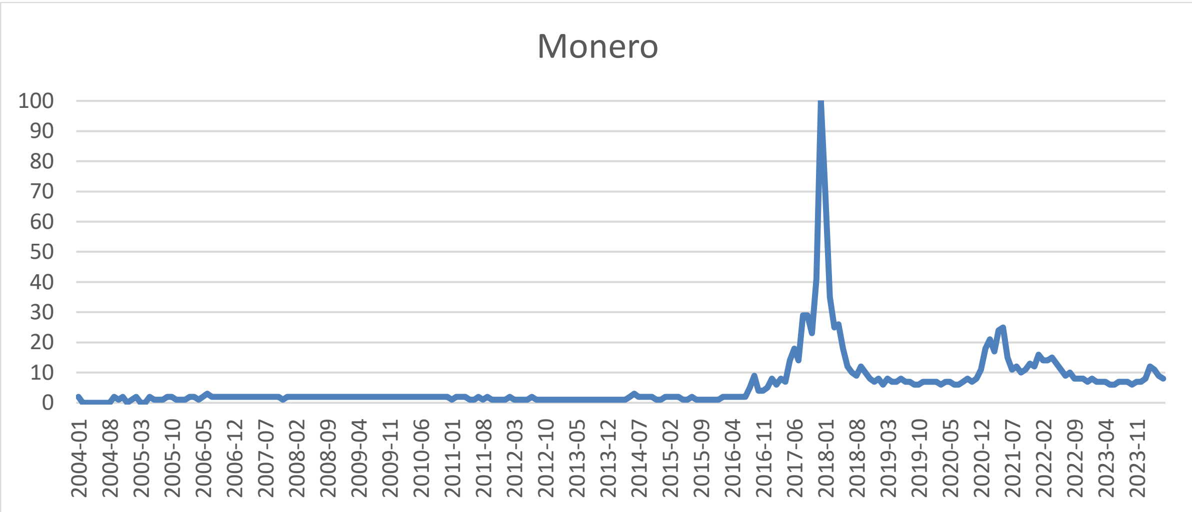


Figure 33 Google search interest for "monero".

The relationship between Bitcoin and other cryptocurrencies is well observed in the literature, with the price movements of Bitcoin impacting the direction of the market significantly as discussed in chapter 2.5. This relationship is visible in search trend data as well. Bitcoin appears to maintain its search interest better than other cryptocurrencies during down markets.

Looking at the search interest of the cryptocurrencies featured in the comparison around the time of the Ethereum Merge in September 2022 reveals some interesting findings. Based on the data, markets had reached their bottom in the months leading up to 09/2022 with search interest largely maintaining at this level for the next several months for the other search terms until the uptick in mid-2023. Ethereum seems to be an anomaly after 09/2022, going against the expected trend established by the other search terms featured in this analysis. Although divergence from expected behaviour is a phenomenon described in trend analysis, the amplitude of the move suggests a shift in the fundamentals.

A statistical analysis of the correlation of Ethereum and Bitcoin before and after 09/2022 shows the divergence clearly. The relative search interest for Ethereum was 30 in 09/2022 and dropped to 8 by 09/2023. Such major drops in search interest are not observe for any of the other search terms in this comparison in that time period.

From the regression analysis looking at the correlation between the search interest of Bitcoin and Ethereum, we can see the two have been quite strongly correlated at an R value of 0,85 and R^2 of 0,72 since the launch of Ethereum. Limiting the observation time frame to the time of the transition to PoS on 09/2022 produces similar values at an R of 0,85 and R^2 of 0,73. After the move there is some evidence of a degree of disconnect between the search interest at an R of 0,76 and R^2 of 0,58. These results are shown in Table 25.

Table 25 R and R^2 for the Ethereum-Bitcoin search term pair highlighting the separation between the two

Time frame	R	R^2
ETH-BTC Full	0,8946	0,8004
ETH-BTC Eth release-current	0,8463	0,7162
ETH-BTC beginning-09/22	0,8961	0,8029
ETH-BTC Eth release-09/22	0,8534	0,7284
ETH-BTC 09/22-current	0,7609	0,5790

Similar drops did not occur for other cryptocurrencies featured in the comparison. However, extending the beginning of the observation time frame of Bitcoin to 06/2022 results in a somewhat comparable drop, from 40 in 06/2022 to 18 in 09/2023.

5.5 Discussion

On bitcointalk.org mining related conversations accounted for 23% of posts and 15% of topics on Bitcoin, figures were similar for altcoins at 16% and 22%. These results do not appear to show a similar trend in difference of depth as demonstrated in analysis by (Glenski et al., 2019) on subreddit posts and conversation depth. However, this phenomenon was somewhat subtle in the original data, and it is possible that the difference between Bitcoin and altcoin communities plays a role in hiding the same dependence in our data.

The post and topic data from Bitcointalk.org suggests that mining plays a larger role in generating involvement, than the follower numbers of various subreddits would indicate. The discrepancy between the data from bitcointalk.org and subreddits could be explained by the same phenomenon. Bitcointalk is the original community on cryptocurrencies formed in 2009 by Satoshi Nakamoto.[44] The appearance of the forum is somewhat dated and the accessibility of alternative platforms such as Reddit appears to have had an impact on the general activity levels, especially following the data breaches[45] throughout the years. It is possible that the forums peak user count was reached in the early days of the network when the share of miners was higher which would explain the discrepancy.

Considering the categorization of communities based on the extent of cooperative group action by (Bagozzi & Dholakia, 2002), official subreddits can be characterized as examples of *minimal cooperative group action*. Although users share a common interest, there is no clear common pursuit in the community. Mining related communities on the other hand can be characterized as undertaking *fully*- or *partially cooperative group action* as miners not only share a common interest, but their intentions are aligned as they are dependent on the same aspects for profitable operation.

---

[44] *Donations*. (n.d.). Retrieved June 20, 2024, from https://bitcointalk.org/donate.html

[45] *When (or was) the Bitcointalk database hacked? Was it in 2016 ?* (n.d.). Retrieved June 20, 2024, from https://bitcointalk.org/index.php?topic=5302011.0

Follower data seems to show that as the overall size of the community increases, the share of miners decreases as a proportion of the overall userbase. The share of miners varied between communities from 0,62% for Dogecoin and 22,67% for Monero. This finding corresponds with previous research on the development of miners as a group by (Xu et al., 2021), which found that the number of miners decreases as the network matures. Bitcoin and Dogecoin related communities were the largest in the comparison and their mining related subreddits were the smallest in relative terms.

Analysing the search interest of Ethereum around the time of its consensus mechanism transition shows a clear drop in interest following the move to PoS that is not attributable to the overall market trend based on the search interest of other cryptocurrencies in the analysis. Estimating the size of the various communities from the follower data of r/Ethereum and r/EtherMining suggests that mining accounted for roughly 12,01-13,66% of the community size. The observed drop in search interest appears to be inflated when accounting for the size of the mining community as established by the subreddit comparison. This seems to support the idea that miners play a more active role in the community in generating interest. This interpretation is supported by the characterization of miners as a group with not only shared interests, but intentions as well.

Ethereum reached its peak search interest in 2021 and it is possible that the level of search interest was maintained at an inflated level due to recent history and in anticipation of the upcoming Merge. Although the regression analysis points to the search term pair Ethereum-Bitcoin to be somewhat disconnected following the Merge, there is some evidence for this interpretation as Ethereum appears to have sustained interest better than other cryptocurrencies in the months leading up to 09/2022.

Accurately estimating the contribution of various factors is impossible based on the data featured in this research and further work is required. However, the data does indicate that mining could play a significant role in maintaining interest and involvement in a project and that the drop in interest should be accounted for when making the decision to move to other technologies. This interpretation is supported by previous literature using Google trends data.

Changes in search trend popularity were shown by (Kim & Malek, 2018) to allow for forecasting of casino revenue, which is highly dependent on user count.[46]

5.6 Conclusion

The goal of chapter five was to provide an answer to R4. “How does crypto mining contribute to the community creation of a cryptocurrency?”

The sizes of various subreddits somewhat suggest, that mining plays a larger role in community creation for smaller, less established cryptocurrencies. The larger the userbase grows and the more recognition a cryptocurrency has the smaller the mining related communities were relative to the total number of members. The activity levels of the subforums analysed show a similar trend.

These findings support the idea, that mining plays a more important role during the early stages of the cryptocurrency’s lifecycle, suggesting that a move to another consensus mechanism after early adoption could be a viable strategy. However, the Google trend analysis of Ethereum indicates, that even for established cryptocurrencies mining does still play a role in generating at least search interest and that moving to another protocol could negatively affect recognition and interest.

5.7 Limitations

Although community engagement and participation are extensively studied, limited examples of existing research looking at the contribution of different aspects of technology to overall popularity exist. The lack of existing research limited the potential approaches that this section could take. Ultimately a novel approach was chosen with limited previous examples to estimate its validity. This reality presents some uncertainty as to the results of this section as no established and proven point of comparison is available.

The number of communities in this analysis was limited to a manageable number to maintain proper scope. Including other communities could produce different results, although the selection in this study attempts to mitigate these effects.

---

[46] *Las Vegas Statistics, Research, and Frequently Asked Questions*. (n.d.). Retrieved June 20, 2024, from https://www.lvcva.com/research/

6 Conclusion

This chapter compiles the findings of the environmental, financial, and community research to discuss the combined implications of the research. The interlinkage of the individual research chapters is highlighted by presenting the various cause and effect relationships discovered in the research. Chapter 6.2 collects the findings of the various research chapters and compiles the answers to the research questions presented in this thesis. Recommendations on future research and gaps in current research are also described.

For discussion on the findings of only the specific research chapters refer to chapters 3.4 and 3.5 for the Environmental section, 4.4 and 4.5 for the Financial section, and 5.5 and 5.6 for the Community section.

6.1 Combining the findings

The role of environmental considerations appears negligible

The literature review conducted on the environmental impact of crypto mining found that the energy consumption and resulting environmental impact of a mature PoW network is considerable. The literature review concentrated on analysing research on the Bitcoin network, as it is the most established PoW cryptocurrency to date. While the power demand of the consensus mechanism is well established in literature, the specifics remain difficult to estimate as the composition of equipment can only be modelled. The number of resources producing current estimates is limited and their quality varies greatly. Even the most reliable resources, such as the CBECI, produce large potential ranges. Despite reliable resources existing, the more sensationalistic estimates are still some of the most accessible information available on the topic, still appearing even in academic literature.

Research on the topic has a somewhat contentious history with several resources deemed unrealistic, such as (Mora et al., 2018) and digiconomist.net, still commonly referenced in the media and literature. However, the current state of the research suggests that the environmental impact of the Bitcoin network can be considered solved, to the extent that additional data would be required for more accurate estimates.

Although the environmental impact of the PoW protocol was shown to be considerable and still growing in chapter 3.3, the overall effect seems minor. While sustainability is undoubtedly a megatrend of the last decade and frequently brought up, especially with regards to crypto mining, such considerations do not seem to have any effect on the development of the network. Consumer ignorance on the general topic of sustainability is well documented[47] and for miners, the main and only consideration is the profitability of the equipment. None of the studies featured in this review considered the environmental impact of equipment to be a factor in whether hardware is operated or not. Instead, miners were assumed to run equipment for as long as it was profitable, even if more efficient equipment was already available (Cambridge Bitcoin Electricity Consumption Index (CBECI), 2024). The assumption by the models appears reasonable, considering the documented relative ignorance of many individuals on the topic of sustainability.

Profitability the main consideration for miners

While the financial analysis shows that miners have been able to profit in the past even at an electricity cost of 10 or even 15 US cents, the more recent examples of equipment released between 2020-2023 presented in chapters 4.3.4-4.3.6 challenge this expectation. At higher operating costs miners are heavily reliant on periods of exceptional profitability during major market hikes for any kind of profitable operation. Considering the current price of Bitcoin, it is unlikely such major increases will occur during future market cycles as the inflow of funds would have to be considerable to facilitate such a move. In the past it was more reasonable to expect such moves with the price and resulting market capitalization of Bitcoin being considerably lower.

Excluding the exceptional periods of increased profitability, mining is shown by the analysis to be highly competitive, requiring electricity costs of 5 US cents or less for sustained profitability through extended down markets. This seems to be the case especially as the network has matured. Analysis by (Delgado-Mohatar et al., 2019) came to similar conclusions, finding that during an extended down market even the most efficient operations at 0,05 USD/kWh were struggling to generate sufficient revenue to cover costs. Even though miners can technically operate equipment profitably at these prices, generating returns beyond recouping the cost of electricity is questionable. The model used in the analysis was simplified to not include potential additional costs, looking only at gross profit. The results are mostly applicable for small-scale operations or individuals, but they also provide a starting point for more extensive reviews of financial feasibility. Larger operations would benefit from

[47] White, K., Hardisty, D. J., & Habib, R. (2019). People say they want sustainable products, but they don’t tend to buy them. Here’s how to change that.

scale, but incur additional business-related costs as well, making the profitability estimates of these operations difficult based on the calculations presented.

The ASIC miners used to mine Bitcoin have grown considerably more efficient since being first introduced in 2014, but also more powerful. Modern era SHA-256 ASICs commonly require more power than regular residential fuses can even deliver. As these devices are purpose-built for mining, they have little value outside of the activity requiring specific investment to participate, compared to the era of CPU and GPU mining when generic computer hardware was usable. Together with the cost requirements for electricity, small-scale operations that are unrealistic to re-locate to areas of lower electricity costs will likely become completely obsolete as devices in the modern era are barely able to recoup initial investments even at 3 and 5 US cents within the 12-month time frame. The requirements of profitable operation will likely continue to contribute to the industrialization and centralization of mining demonstrated in previous research by (Xu et al., 2021).

Community creation and mining

The community research shows quite clearly that as a cryptocurrency matures, mining related communities represent a smaller share of the overall community. Community activity suggests a similar reality. The increasing barrier of entry is one of the reasons explaining why mining related communities are relative larger and more active when adoption is limited. The phenomenon has been previously described by Xu et al. and it evidently impacts all three perspectives featured in this thesis. The increasing barrier of entry is caused in part by the specialized nature of the equipment, higher wattage requirements, and cost, as demonstrated in chapter 4.

This phenomenon is explained in part by these communities being generally aimed at individuals and becoming less relevant as crypto mining becomes more centralized and industrialized. There are however other contributing factors. As a cryptocurrency becomes more established its userbase naturally grows. As the transaction capacity of the Bitcoin network is not directly derived from hash rate, it is not a limiting factor on the number of users. The network can grow without requiring a higher hash rate.

While the higher relative user count and general activity of mining related communities in early stages of adoption seem well established based on the analysis in chapter 5.3, making accurate estimates of the true impact is difficult as the effect varies greatly between cryptocurrencies. However, the Google trends analysis supports the idea that mining plays a role in generating interest in a cryptocurrency and creating community. Ethereum moving to PoS from PoW in late 2022 provides a compelling, albeit single datapoint on the matter. Following the move the search interest of Ethereum dropped significantly more compared to several other popular cryptocurrencies. Again, there are other factors that could have contributed to the lower than anticipated search interest, but estimating their relative impact is not possible based on the data used.

Future of mining

Considering the requirements set by current profitability and the comparatively high environmental impact, the future of mining seems uncertain in the developed world. As an industry, crypto mining is unique in the sense that it does not require much in terms of surrounding infrastructure. Apart from a stable internet connection and reliable yet affordable power, facilities can be located in even remote areas. The industry could therefore take advantage of abundant renewable resources, which would otherwise be wasted, as the capacity for moving electricity across large distances is still somewhat limited.

Solutions used to utilize waste heat generated by data centers could also be used with mining farms making the cost of electricity less of a limitation and reducing the environmental impact of mining to just the manufacturing of equipment. If the electricity is used regardless, even dated hardware could be used until it is no longer functional as most of the electricity consumed by miners is turned into heat. The literature review conducted on the environmental impact of Bitcoin mining showed that current models do not consider such practices, even hypothetically, even though these solutions have already been described in literature[48] [49]and commercial applications targeting data centers already exist. [50]

---

[48] Asgari, N., McDonald, M. T., & Pearce, J. M. (2023). Energy Modeling and Techno-Economic Feasibility Analysis of Greenhouses for Tomato Cultivation Utilizing the Waste Heat of Cryptocurrency Miners. *Energies*, *16*(3), Article 3. https://doi.org/10.3390/en16031331

[49] Parrado-Duque, A., Dubé, Y., Charrel, S., Gaden, C., Henao, N., Agbossou, K., & Guibault, Y. (2023). Potential for Waste Heat Recovery in a Digital Currency Mining Facility: A Building Infrastructure Case Study. *2023 IEEE 64th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON)*, 1–7. https://doi.org/10.1109/RTUCON60080.2023.10413188

[50] What are AgroDomes? (2024). *Agrodomes*. https://agrodomes.com/what-are-agrodomes/

6.2 Answering the research questions

This thesis proposed four research questions regarding mining. The primary research question of this thesis was:

- R1. What is the role of crypto mining in enabling cryptocurrencies?

Three additional research questions were formulated to narrow and define the approach selected for answering R1:

- R2. What is the environmental impact of Proof of Work and how resource intensive is the activity?
- R3. What do the financials of mining Proof of Work cryptocurrencies look like?
- R4. How does crypto mining contribute to the community creation of a cryptocurrency?

R2

The literature review in chapter three answered R2 extensively. The environmental impact of PoW was estimated by looking at the Bitcoin network. The environmental impact is primarily the result of the electricity consumption of mining equipment, but also e-waste generated by equipment being retired. The electricity use of a mature PoW network was shown to be considerable, comparable to that of some small countries. The environmental impact can be considered solved, to the extent that making more accurate estimates would require new and more accurate data on the topic, specifically on the equipment used. Electricity usage or e-waste generation do not appear to have an impact on the development of the network. None of the models discovered in the literature review consider the environmental impact of equipment to be a factor in determining whether equipment is operated or not.

A more comprehensive analysis can be found in chapters 3.4 and 3.5.

R3

R3. was answered in chapter four by profitability calculations using various equipment. The calculations and analysis highlight the importance of entry timing and access to low-cost electricity. The profitability of mining was shown to have declined considerably in the last few years and to often be reliant on major price hikes of Bitcoin. In the modern era, despite significant advances in equipment efficiency, modern devices such as the S21, have struggled to generate revenues sufficient to cover operating costs and the cost of equipment.

A more comprehensive analysis can be found in chapters 4.4 and 4.5.

R4

Chapter five answered R4. How does crypto mining contribute to the community creation of a cryptocurrency? Mining related communities were significantly larger the smaller the communities, but there were some outliers in the data. A similar finding was made when analysing the size and activity levels of bitcointalk.org subforums. Google trends analysis points to mining having a positive impact in terms of search interest even for mature cryptocurrencies.

A more comprehensive analysis can be found in chapters 5.5 and 5.6.

R1

This thesis studied the role of crypto mining in enabling cryptocurrencies, by looking at mining from three perspectives. Research questions 2-4 provided a thorough basis for the analysis in this thesis.

In chapter three the environmental impact of mining was found to be considerable, but it does not appear to negatively affect the development of the network. Models evaluating the environmental impact do not consider environmental concerns a factor in determining whether equipment is operated or not. The overall impact of environmental concerns appears to be in line with consumer sentiment regarding sustainability, rather than regulatory attitudes. This is perhaps expected, as cryptocurrencies are based on a decentralized P2P system, rather than relying on centralized control. The models used to estimate the environmental impact and equipment composition of the network assume profitability as the sole concern for miners.

The profitability of mining was shown in chapter four to vary greatly. The changes in profitability coincide with price increases of Bitcoin throughout the history of the technology. In the modern setting, equipment development is slower and new releases do not have such an impact on profitability as they did in the initial stages of the Bitcoin network. Bitcoin miners appear reliant on similar up-markets as investors and owners of the asset, especially for sustained operation. Profitability was shown to be low for extended periods of time making market entry a major factor in determining profitability or feasibility of the operation. Despite issues showcased by the calculations, Bitcoin mining generates consistent and growing revenues. PoW offers a novel way of securing a decentralized network, that at the very least has the potential to be profitable. The consensus mechanism appears to provide a valid and financially sustainable method of incentivising participation in a P2P network. As with any industry, sustained and profitable operation is not guaranteed for all operations nor does mining offer a “get-rich-quick”-scheme by any means. Despite profitability challenges at certain periods, crypto mining can justifiably be called a profitable industry.

The community analysis in chapter five used a novel approach to study the community building and popularity impact of mining. The share of miners of the overall userbase was found to be lower for more established cryptocurrencies in relative terms. Mining appears to contribute to interest in a cryptocurrency especially during the early stages. For more established cryptocurrencies, miner influence and impact appear lower. However, the drop in search interest following Ethereum moving from PoW to PoS suggests that mining contributes to the popularity of even established cryptocurrencies. The various contributing factors point to crypto mining playing an enabling role in the crypto phenomenon when analysing community activity, size, and popularity, but accurately attributing the impact of various parts is challenging based on the research conducted and the limited context of existing research.

To summarize, Proof of Work is not without its issues, but the often perceived and discussed problems of the consensus mechanism do not appear to hinder the adaptation of Bitcoin, at least currently. The analysis in this thesis points to Proof of Work being an enabling aspect of the crypto phenomenon by providing an incentivised solution to securing a Peer-to-Peer network that is financially sustainable, although reliant on the price development of the underlying asset.

6.3 Future works

The approach chosen in this thesis was found to be effective, but the primary research question was still difficult to answer. The three perspectives chosen were found to provide the desired holistic understanding of crypto mining as intended, but the limited research and established methodology, especially regarding the community perspective proved challenging. Although individual research questions were answered in a satisfactory manner, quantifying the extent of the impact of mining beyond stating it played some role in enabling cryptocurrencies is questionable. Ultimately, the issue with analysing well established cryptocurrencies is that attributing outcomes to causes cannot be done with certainty regardless of research methods. While several factors point to mining playing an important role in enabling the crypto phenomenon, the size of the impact is difficult to quantify.

This thesis should be viewed as an indicative starting point for future research. The results produced are best described as basic research on the topic. Each section included in this thesis provides additional insight on the currently limited body of research and advances the understanding of the specific section. The financial and community sections in particular.

The model applied for the financial analysis was quite simplified but based on the economic and operational realities of mining. Future works on the topic should dive deeper into developing a more accurate model of the cost structure and include more examples of equipment. Data from manufacturers could be used to further establish the most realistic devices miners have had historical access to.

The community section was the most challenging section of this thesis. The theoretical background on the topic is extensive, but it does not appear well suited for the sort of analysis required. It seems fair to hypothesize that miners are incentivised to not just participate, but also promote the network as they are relying on price increases for extended operation. Studying this aspect was one of the original ideas of this thesis, but the lack of existing research and methodology did not facilitate such research, especially since the community perspective was just one part of this thesis. Further study of the group motivations of miners could make the argument of miners playing a major enabling role much more convincing. Group motivations offer a compelling albeit challenging topic for future study.

Detailed exploration of community activity data could offer a potential method for studying group motivations and action. Data availability and reliability could be a factor here, but more research is required to determine the quality of the data and results. A questionnaire directed at certain communities would offer another natural way to further the understanding of the motivations of miners as a group.

7 References

Antonopoulos, A. M., & Harding, D. A. (2023). *Mastering Bitcoin*. O'Reilly Media, Inc.

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19–32. https://doi.org/10.1080/1364557032000119616

Arooj, A., Farooq, M. S., & Umer, T. (2022). Unfolding the blockchain era: Timeline, evolution, types and real-world applications. *Journal of Network and Computer Applications*, *207*, 103511. https://doi.org/10.1016/j.jnca.2022.103511

Arslanian, H. (2022). *The Book of Crypto: The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets*. Springer International Publishing. https://doi.org/10.1007/978-3-030-97951-5

Bagozzi, R. P., & Dholakia, U. M. (2002). Intentional social action in virtual communities. *Journal of Interactive Marketing*, *16*(2), 2–21. https://doi.org/10.1002/dir.10006

Bedford Taylor, M. (2017). The Evolution of Bitcoin Hardware. *Computer*, *50*(9), 58–66. https://doi.org/10.1109/MC.2017.3571056

Bevand, M. (2017, March 10). *Electricity consumption of Bitcoin: A market-based and technical analysis*. http://blog.zorinaq.com/bitcoin-electricity-consumption/

BitInfoCharts.com. (2024). *Bitcoin Mining Profitability Chart*. BitInfoCharts. https://bitinfocharts.com/comparison/bitcoin-mining_profitability.html

Brandtzæg, P. B., & Heim, J. (2009). Why People Use Social Networking Sites. In A. A. Ozok & P. Zaphiris (Eds.), *Online Communities and Social Computing* (Vol. 5621, pp. 143–152). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-02774-1_16

Cambridge Bitcoin Electricity Consumption Index (CBECI). (2024). https://ccaf.io/cbnsi/cbeci

CBECI Mining equipment list. (n.d.). Google Docs. Retrieved March 26, 2024, from https://docs.google.com/spreadsheets/d/15bkGk6cpIGK9DKcytnErB0VZfihPkF1TsAYd4_Nac_Y/edit?usp=embed_facebook

Charoenwong, B., & Bernardi, M. (2021). *A Decade of Cryptocurrency 'Hacks': 2011 – 2021* (SSRN Scholarly Paper 3944435). https://doi.org/10.2139/ssrn.3944435

Chaudhry, N., & Yousaf, M. M. (2018). Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, 54–63. https://doi.org/10.1109/ICOSST.2018.8632190

Chen, C., & Liu, L. (2022). How effective is China's cryptocurrency trading ban? *Finance Research Letters*, *46*, 102429. https://doi.org/10.1016/j.frl.2021.102429

Chohan, U. W. (2017). A History of Bitcoin. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3047875

Choi, H., & Varian, H. (2012). Predicting the Present with Google Trends. *Economic Record*, *88*(s1), 2–9. https://doi.org/10.1111/j.1475-4932.2012.00809.x

Cumming, D. J., Johan, S., & Pant, A. (2019). Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty. *Journal of Risk and Financial Management*, *12*(3), Article 3. https://doi.org/10.3390/jrfm12030126

de Vries, A. (n.d.). *Bitcoin Energy Consumption Index*. Digiconomist. Retrieved April 18, 2024, from https://digiconomist.net/bitcoin-energy-consumption/

de Vries, A. (2019). Renewable Energy Will Not Solve Bitcoin's Sustainability Problem. *Joule*, *3*(4), 893–898. https://doi.org/10.1016/j.joule.2019.02.007

de Vries, A., & Stoll, C. (2021). Bitcoin's growing e-waste problem. *Resources, Conservation and Recycling*, *175*, 105901. https://doi.org/10.1016/j.resconrec.2021.105901

Delgado-Mohatar, O., Felis-Rota, M., & Fernández-Herraiz, C. (2019). The Bitcoin mining breakdown: Is mining still profitable? *Economics Letters*, *184*, 108492. https://doi.org/10.1016/j.econlet.2019.05.044

Demertzis, M., & Wolff, G. B. (2018). *The economic potential and risks of crypto assets: Is a regulatory framework needed?*

Dittmar, L., & Praktiknjo, A. (2019). Could Bitcoin emissions push global warming above 2 °C? *Nature Climate Change*, *9*(9), 656–657. https://doi.org/10.1038/s41558-019-0534-5

Feldman, M., Papadimitriou, C., Chuang, J., & Stoica, I. (2006). Free-riding and whitewashing in peer-to-peer systems. *IEEE Journal on Selected Areas in Communications*, *24*(5), 1010–1019. https://doi.org/10.1109/JSAC.2006.872882

Foster, M. K., Francescucci, A., & West, B. C. (2010). Why Users Participate in Online Social Networks. *International Journal of E-Business Management*, *4*(1), 3–19. https://doi.org/10.3316/ijebm0401003

Gan, C., & Kao, H. (2008). Consumers' purchasing behavior towards green products in New Zealand. *Innovative Marketing*, *4*(1).

Gersbach, H., Mamageishvili, A., & Schneider, M. (2022). *Staking Pools on Blockchains*.

Glenski, M., Saldanha, E., & Volkova, S. (2019). Characterizing Speed and Scale of Cryptocurrency Discussion Spread on Reddit. *The World Wide Web Conference*, 560–570. https://doi.org/10.1145/3308558.3313702

Gupta, M., Foster, G., & Sjoblom, L. (1997). Customer Profitability Analysis: Challenges and New Directions. *Journal of Cost Management*, *10*.

Hasan, M. K., Akhtaruzzaman, Md., Kabir, S. R., Gadekallu, T. R., Islam, S., Magalingam, P., Hassan, R., Alazab, M., & Alazab, M. A. (2022). Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption Using BIoT for Smart Government and Industry 4.0. *IEEE Transactions on Industrial Informatics*, *18*(12), 9153–9161. https://doi.org/10.1109/TII.2022.3164066

Holtz, P., Kronberger, N., & Wagner, W. (2012). Analyzing Internet Forums: A Practical Guide. *Journal of Media Psychology*, *24*(2), 55–66. https://doi.org/10.1027/1864-1105/a000062

Houy, N. (2019). Rational mining limits Bitcoin emissions. *Nature Climate Change*, *9*(9), 655–655. https://doi.org/10.1038/s41558-019-0533-6

Ihle, C., Trautwein, D., Schubotz, M., Meuschke, N., & Gipp, B. (2023). Incentive Mechanisms in Peer-to-Peer Networks—A Systematic Literature Review. *ACM Computing Surveys*, *55*(14s), 308:1-308:69. https://doi.org/10.1145/3578581

Islam, N., Marinakis, Y., Olson, S., White, R., & Walsh, S. (2023). Is BlockChain Mining Profitable in the Long Run? *IEEE Transactions on Engineering Management*, *70*(2), 386–399. https://doi.org/10.1109/TEM.2020.3045774

Jacobs, F. A., Johnston, W., & Kotchetova, N. (2001). Customer Profitability: Prospective vs. Retrospective Approaches in a Business-to-Business Setting. *Industrial Marketing Management*, *30*(4), 353–363. https://doi.org/10.1016/S0019-8501(01)00155-9

Kim, W.-H., & Malek, K. (2018). Forecasting casino revenue by incorporating Google trends. *International Journal of Tourism Research*, *20*(4), 424–432. https://doi.org/10.1002/jtr.2193

Kohli, V., Chakravarty, S., Chamola, V., Sangwan, K. S., & Zeadally, S. (2023). An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions. *Digital Communications and Networks*, *9*(1), 79–89. https://doi.org/10.1016/j.dcan.2022.06.017

Lei, N., Masanet, E., & Koomey, J. (2021). Best practices for analyzing the direct energy use of blockchain technology systems: Review and policy recommendations. *Energy Policy*, *156*, 112422. https://doi.org/10.1016/j.enpol.2021.112422

Logan, T. (2014). *Profiting from Market Trends: Simple Tools and Techniques for Mastering Trend Analysis*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/kutu/detail.action?docID=1598283

Malagón-Selma, P., Debón, A., & Domenech, J. (2023). Measuring the popularity of football players with Google Trends. *PLOS ONE*, *18*(8), e0289213. https://doi.org/10.1371/journal.pone.0289213

Masanet, E., Shehabi, A., Lei, N., Vranken, H., Koomey, J., & Malmodin, J. (2019). Implausible projections overestimate near-term Bitcoin CO2 emissions. *Nature Climate Change*, *9*(9), 653–654. https://doi.org/10.1038/s41558-019-0535-4

McCloskey, D. J., Akintobi, T. H., Bonham, A., Cook, J., & Coyne-Beasley, T. (2011). *Principles of Community Engagement (Second Edition)*.

Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., & Franklin, E. C. (2018). Bitcoin emissions alone could push global warming above 2°C. *Nature Climate Change*, *8*(11), 931–933. https://doi.org/10.1038/s41558-018-0321-8

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

O'Dwyer, K. J., & Malone, D. (2014). Bitcoin mining and its energy footprint. *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information* *and Communications Technologies (ISSC 2014/CIICT 2014)*, 280–285. https://doi.org/10.1049/cp.2014.0699

Overton, R. (2000). *Feasibility Studies Made Simple Martin Books Success in Business*. https://www.academia.edu/28816329/Feasibility_Studies_Made_Simple_Martin_Books_Success_in_Business

Peterson, P. P., & Fabozzi, F. J. (1999). *Analysis of Financial Statements*. John Wiley & Sons.

Roberts, C. (2022). *Stablecoins -Types and Definitions*. https://doi.org/10.13140/RG.2.2.27163.95526

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the Origins and Variations of Blockchain Technologies. *IEEE Security & Privacy*, *17*(1), 72–77. https://doi.org/10.1109/MSEC.2019.2893730

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The Carbon Footprint of Bitcoin. *Joule*, *3*(7), 1647–1661. https://doi.org/10.1016/j.joule.2019.05.012

Suratkar, S., Shirole, M., & Bhirud, S. (2020). Cryptocurrency Wallet: A Review. *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, 1–7. https://doi.org/10.1109/ICCCSP49186.2020.9315193

Wang, L., & Liu, Y. (2015). Exploring Miner Evolution in Bitcoin Network. In J. Mirkovic & Y. Liu (Eds.), *Passive and Active Measurement* (pp. 290–302). Springer International Publishing. https://doi.org/10.1007/978-3-319-15509-8_22

Xu, J., Bai, W., Hu, M., Tian, H., & Wu, D. (2021). Bitcoin miners: Exploring a covert community in the Bitcoin ecosystem. *Peer-to-Peer Networking and Applications*, *14*(2), 644–654. https://doi.org/10.1007/s12083-020-01021-1

Zamanov, A. R., Erokhin, V. A., & Fedotov, P. S. (2018). ASIC-resistant hash functions. *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 394–396. https://doi.org/10.1109/EIConRus.2018.8317115

Zīle, K., & Strazdiņa, R. (2018). Blockchain Use Cases and Their Feasibility. *Applied Computer Systems*, *23*(1), 12–20.

Appendices

Appendix 1. ASIC price sources

Name	Release	Th/s	W	J/GH	Bitmain Release	Amazon Release	Amazon Peak	Hashrateindex.com Release	Miningstore.com
Bitmain Antminer S3	01/07/2014	0,478	366	0,7657	549[1]	431	770	-	
Bitmain Antminer S9 (12.5Th)	01/02/2017	12,5	1225	0,098	1352[2]	2710[6]	5179	-	
Bitmain Antminer S19 (95Th)	01/05/2020	95	3250	0,0342	-	-	-	2220-2400[5]	<3000
Bitmain Antminer S19 Pro Hydro	01/01/2023	177	5221	0,0344	3629[3]	-	-	-	
Bitmain Antminer S21	01/09/2023	200	3500	0,0175	5400[4]	-	-	-	

* 0,75 btc at release, converted to USD
Manufacturer PSU added to price, 120 USD
191THash model
current price in 04/2024
Inconsistencies with release dates
Several models 11-14TH. Used data for 13TH model.

The prices of the select equipment at release according to Bitmain.com: S3 549 USD, S9 1352 USD, S19 not listed, S19 Pro Hydro 3629, and S21 5400. The price of the S3 is calculated from the devices BTC price at 0,75 BTC at release. For the S9 the price includes the manufacturer PSU price of 120 USD. Several versions of the S9 exists at 11-14 TH, the data presented is for the 13 TH version. For the S19 there data is slightly inconsistent with release dates. For the S19 Pro Hydro the price of the 191 TH model is presented. According to amazon at release and peak: S3 431 USD and 770 USD, S9 2710 USD and 5179 USD, no data listed for other equipment. Hashrateindex.com lists the price of the S19 at release at 2220-2400 USD, Miningstore.com lists the price at below 3000 USD.