A Work Project, presented as part of the requirements for the Award of a Master's degree in Economics from the Nova School of Business and Economics.

An economic review of the Bitcoin production market and resulting externalities

Katharina Louisa Lentge

Work project carried out under the supervision of:

Prof. Steffen Hörnig

16/12/2022

Abstract:

This paper reviews the existing economic theory on Bitcoin (BTC) production, analyzes the Bitcoin production market – as well as the associated externalities of the Bitcoin production process. It discusses how the underlying incentive mechanism further a competitive arms race that not only contradicts the philosophy of the underlying consensus scheme but results in an artificially high level of production demand that imposes significant damages onto society.

Keywords: Bitcoin, blockchain, production externalities, cryptocurrency mining

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

Table of Contents

1. Introduction

While several governing bodies such as the United States (US), the European Union (EU), the G20 have made pledges to achieve net-zero Greenhouse gas (GHG) emissions by the middle of the century and cutting emissions in half over the next decade (European Commission, 2019; US Government, 2021), global efforts to avoid climate crisis continue to be insufficient (United Nations, 2021, 2022). To address these damages, rapid action and systemic transformation are required. Cryptocurrencies represent a new, global, digital, transnational segment of the financial landscape that contributes significantly to the emission gap[1]. As the industry grows, an increasing strand of literature is becoming concerned with the production externalities of cryptocurrency mining (de Vries, 2019, 2021; Goodkind et al., 2020; Jones et al., 2022; Krause & Tolaymat, 2018; Stoll et al., 2019). Externalities refer to the social costs that are created during the cryptocurrency production process without being factored into the private costs borne by its global network of producers. Proof-of-Work (PoW) Blockchains, most prominently the first and largest cryptocurrency Bitcoin (BTC)[2], use an energy-intensive security mechanisms that results in a significant carbon footprint (de Vries & Stoll, 2021; Jones et al., 2022; Stoll et al., 2019). To secure, sustain, and expand the blockchain network, miners continuously 'produce' new blocks, the details of which are discussed throughout this paper. The underlying blockchain has been labelled an effective technology for decentralization that gives rise to autonomous, rule-based market structures (Catalini et al., 2019), allowing participants to make joint investments in shared infrastructure and digital public utilities. The externalities that accompany the production process and their costs to society and the planet are currently not factored into the production decisions by the miner network – or the broader investor network in general (Gschossmann et al., 2022). Formally, it is therefore assumed that Bitcoin production results in externalities e at cost $c(.,e)$ with $\frac{\partial \pi}{\partial .} > 0$ and $c(.,e)$ being u-shaped in e. This means that Bitcoin producers maximize profits by polluting the amount e, strongly reducing social returns.

Studying the economics and strategic behavior of participants in the consensus mechanism of such cryptocurrencies is relevant because public blockchains have been developed to circumvent regulation by design. At the same time, stakeholders in cryptocurrencies are indeed addressed when the UN highlights that a 'realignment of the financial system is a critical enabler

[11] Research by the ECB highlights, that past and target EU savings are offset by GHG emissions from cryptocurrency mining (Gschossmann et al., 2022).
[2] 'Bitcoin' is commonly used to refer to the protocol or broader ecosystem, while 'bitcoin' or 'BTC' are explicitly used when talking about the cryptocurrency

(…) to address the current climate crises' (United Nations, 2022). Lasting change must therefore come from within the network, which requires an understanding of its functioning and the decision processes of its members.

Following this introduction, Part 2 is dedicated to describing and analyzing the economic incentives and theory behind the Bitcoin production market. It considers the macroeconomic equilibrium between protocol design and the miner network as set forth by (Podhorsky, 2019) and analyzes the micro-economic theory of mining decisions, relying to a large extent on 'A cost of production model for Bitcoin' by (Hayes, 2015, 2019). Part 3 takes a deeper look at today's Bitcoin production market realities[3], largely characterized by a competitive arms race and technology lock-ins, resulting in an oligopoly competition and an artificially high level of production. Part 4 provides an up-to-date evaluation and quantification of the resulting Bitcoin production externalities. Part 5 is dedicated to highlighting potential alternatives and room for further research for a more environmentally friendly Bitcoin production. Part 6 concludes this work project by summarizing key results and outlining limitations.

[3] Using on-chain data sourced from https://data.nasdaq.com/, unless otherwise indicated, between 01.03.2020 until 30.09.2022. The timeframe of 1.5 years starting in March 2020 has been chosen to have sufficient data for analysis since the beginning of Covid-19. Additionally, the block-reward of 6.25 BTC/block was introduced in March 2020, therefore keeping the blockchain-native incentive level stable throughout the analysis.

1. The Economics of Bitcoin

The characteristics of the Bitcoin network create a limited-supply, virtual commodity that can be obtained via exchanges, or by production. It is helpful to therefore distinguish two groups of stakeholders in Bitcoin economics: traders who buy and sell Bitcoin (BTC) via online platforms and miners who produce new Bitcoins (Z. Li & Liao, 2019). The latter is the primary focus of this work project. The economics of Bitcoin mining are best described as a stochastic production game embedded in a decreasing, but fixed-schedule supply monetary system enabled by blockchain technology.

1.1. Blockchain – The fundamental technology of Bitcoin

From a structural perspective, Blockchains are digital ledgers that store information on economic activity, such as asset exchange, in the form of timestamped, sequential blocks. The ledger is maintained across a network of computers that are linked in a peer-to-peer network. Instead of relying on a centralized, trusted entity to enter and verify new data entries, new information is dynamically agreed upon by the system of distributed computers in consensus. Consensus refers to a group decision-making procedure in which members develop and vote on proposals with the intent or requirement that they be accepted by everyone. This process is called *consensus process*. Adequate consensus processes must be designed such that they achieve a desired social or economic outcome given the constraints of individual's self-interest and incomplete information. Originally, the theory of distributed consensus was developed in the computer-communication network literature by Lamport et al. (1982)[4]. Adequate consensus mechanisms must be designed such that they permanently incentivize honest participation by a majority of the network, for example by making faulty communication costly (Davidson et al., 2016; Kroll, 2013; Lamport et al., 1982; Nguyen et al., 2019; Tang et al., 2022; Zheng et al., 2017). Reliable mechanism design is the most important security aspect of public blockchain-based economies and has been widely studied in the technical literature (Beikverdi & Song, 2015; Gencer et al., 2018; Nguyen et al., 2019; Rajendra & Gear, 2019; Sai, Buckley, Fitzgerald, et al., 2021)). This is unsurprising, given the proliferation of blockchain projects and the fact that security of Blockchain is considered central to the adoption (Akram et al., 2020). Besides being tolerant against faulty communication, consensus design in digital-ledger keeping should allow any rational transfer of value and ideally achieve resource-efficiency (Abadi & Brunnermeier, 2022).

---

[4] Often labelled the Byzantine Generals Problem is a game theory problem that describes the difficulty of reaching an agreement amongst generals for a common battleplan, when they can communicate only by messenger, and where it is not clear, whether they counterparties are loyal or traitors.

1.2. Bitcoin – A peer-to-peer monetary system

Bitcoin, which was first published as an open-source software in 2009, is designed as a peer-to-peer monetary systems that functions entirely as its own decentralized computer network (Nakamoto, 2008). It was the first monetary application to rely on distributed consensus to solve the double-spend problem[5] prevalent in digital transaction networks without a trusted central entity. The Bitcoin protocol statically incentivizes a network of miners, effectively computers that run the Bitcoin algorithm, to timestamp Bitcoin transactions and cryptographically hash them into an ongoing chain, thereby forming a record that cannot be reversed. Under the honest majority assumption, when the computational power of each miner is relatively small, this mechanism has been proven to be incentive compatible, meaning that it is a miner's best response to mine according to protocol design (Kiayias et al., 2016). Simultaneously, the chosen consensus mechanism achieves full transferability and fault-tolerance by forcing participants to incur ex-ante costs for the solving of resource-intensive computational problems (Abadi & Brunnermeier, 2022). In combination with a probabilistic chance of only one miner receiving the reward each round, the mechanism creates a type of all-pay auction, which inevitably leads to a deadweight loss of resources whose magnitude is analyzed throughout this paper.

1.3. The "supply side": Regular market interventions by the Bitcoin protocol

Bitcoin effectuates a monetary system characterized by a predetermined supply schedule of the blockchain-native currency Bitcoin and dynamic demand for that currency. The protocol itself thereby wants to create an equilibrium between supply and demand for new Bitcoins (Podhorsky, 2019). As the protocol designer highlights, the Bitcoin network itself requires little structure (Nakamoto, 2008); it foresees the creation of a total 21,000,000 native tokens over time. New Bitcoins are created with every block that is appended to the blockchain, whereby the protocol aims to achieve a target block-time of 10 minutes for the creation of new blocks. The amount of bitcoin per block halves every 210,000 blocks (Nakamoto, 2008), reducing the rate at which new coins are created. The halving policy in Bitcoin's mining algorithm is designed to counteract Bitcoin inflation and maintain scarcity throughout the mining process. As of May 11th, 2020, the Bitcoin reward per block stands at 6.25. An overview of (expected) halving dates and further information can be found in Appendix Table 2.

While the supply parameters are fixed, the actual time it takes to create new blocks depends dynamically on the level of demand for new Bitcoins. New blocks are 'discovered' in a

[5] Double spending is a problem that refers to the same tender being spent multiple times. The problem arises when a transaction in a digital currency is broadcasted multiple times without the receiver being able to verify, that it has not already been spent.

cryptographic, competitive process, during which miners expend computational effort to find a correct hash value, which is added to each new block in order to create an irreversible and immutable chain of activity.

The Bitcoin algorithm for PoW mining is known as Secure Hash Algorithm 256 (SHA-256), an algorithm computed with eight 32-bit word originally designed by the US National Security (Announcing Approval of FIPS Publication 180-2, 2002; Penard & van Werkhoven, 2017). Miners use data from a block header as an input and put it through a cryptographic hash function to find a target hash set by the network. If the correct output hash is found, the miner can add a new block to the blockchain, process the relevant transactions within this block, and receive the rewards associated with his success. The original probability of a randomly generated hash being correct thereby is $\frac{1}{2^{32}}$. It is adjusted over time based on hashing capacity input by the miner network. The adjustment to the level of difficulty of solving the cryptographic hash function is used by the protocol to ensure adherence to its target block-time given changing levels of demand for Bitcoin production. It is recalculated every 2016 blocks, based on the time it took to find the previous 2016 blocks (Nakamoto, 2008). Let $\delta(t)$ stand for a parameter of network difficulty at time t, whereby t is a period of 2016 blocks, then it is adjusted as:

$$\frac{\delta(t_2)}{\delta(t_1)} = \frac{20160min}{actual\ time\ to\ discover\ last\ 2016\ blocks}$$

Noting that the target blocktime is 10 minutes, or 600 second, the optimal difficulty δ^* in the network can be written as

$$\delta^* = \frac{600\emptyset}{2^{32}}$$

Whereby $\emptyset$ stands for the total hashing power of the network in hashes per second. In a symmetric market with n miners investing q, $\emptyset = nq$. With difficulty adjustments, the probability of a randomly generated hash being correct is in fact $\frac{1}{\delta 2^{32}}$. The difficulty adjustment is therefore an endogenous instrument to enforce an inflexible system of supply management given varying amounts of computational effort. Thus, while Bitcoin is designed as a decentralized network with no central authority, its protocol effectively and regularly intervenes in the market. The level of difficulty thereby works akin to a market clearing price (Hayes, 2015, 2019; Podhorsky, 2019; Thum, 2018). By raising (lowering) the level of difficulty the protocol increases (decreases) the system-wide costs of production by demanding more attempts to solve for the correct hash. Since more attempts increase the costs necessary to find the correct solution, it should cause the network to reduce effort proportionally, thereby lowering computational input to re-achieve target block time. Due to the lagged adjustment, $\delta(t) = \delta^*(t-1)$.

The magnitude of adjustments and development of overall cost level of production depends on the demand for new Bitcoins each round. The economics of this decision process by participants of the Bitcoin consensus mechanism, the miners, is analyzed next.

1.4.The "demand side": A mining game

We want to analyze the strategic decision process of miners in the Bitcoin production process. Therefore, we model participation as a series of games of production decisions with probabilistic transitions played by n players. It is in the following called, 'The mining game'.

Miners compete in quantities q, namely computational effort that results in hash guesses, and take the latest difficulty δ, and thus system-wide cost level, as given. Additionally, miners incur costs of c per unit of mining effort expended and may have to undertake capital investments into necessary equipment C. Miners compete for two types of rewards: fixed, blockchain-native subsidy S and time-varying transaction fees f. Transaction fees are measured as the sum of differences between each transactional input and output. They are offered by Bitcoin transaction senders to accelerate their transactions and heavily depend on the corresponding transaction size. Once the last Bitcoin is created, transaction fees will become the only direct renumeration to miners. However, at the time of writing and according to data from btc.com, transaction fees represent only 1.46% of the block reward and thus a negligible share in miner's revenue. Additionally, transaction fees affect block size, which in return affects the probability of a miner successfully mining a block (Jiang & Wu, 2019). For simplicity, we, therefore, hold block-size fixed and include f in a general reward R that is awarded to the first miner to solve for the correct hash.

The mining-game is a 'winner-takes-all' game, where only one miner receives the block reward each mining round t. The probabilities of winning the reward per miner $p = (p_1, \dots, p_n)$ and round is thereby proportional to the relative hashing power contributed vis-à-vis that of the remainder mining network. Let q_i represent the number of hashes a representative miner i can generate, then the probability of winning can be written $p_i = \frac{q_i}{q_i + \sum_{j \neq i} q_j}$.

While players can infer the last total hashing input by the network from $\delta(t) = \delta^*(t-1)$ they cannot with certainty observe the remainder network input $\sum_{j \neq i} q_j$ when making their input decision. Thus, they choose their input quantity without knowledge of the quantities chosen by other players and effectively compete in a non-cooperative game whenever they turn on their equipment.

Modeling the behavior of miners under uncertainty as a game, we can say the Mining Game has three possible outcomes, depending on the player's choice of whether to participate or not: 1) return of zero for non-participation, 2) winning with probability p_i, and 3) loosing with probability $1 - p_i$. The first choice a miner faces is the one of not participating (Gamble 1), which puts probability 1 on zero return: $L_N = (1,0,0)$. Participation induces a gamble, with the probability of winning p_i: $L_M = (0, p_i, 1 - p_i)$. The choice between Gamble 1 and 2 depends on the utility miners receive when participating, the probabilities of winning, and their individual risk attitude.

Since miners effectively 'produce' hashes using relevant equipment and electricity, we extend the gamble to a production framework. Let q_i represent the number of hashes a representative miner i can generate by running his equipment. Then the probability of winning can be written $p_i = \frac{q_i}{q_i + \sum_{j \neq i} q_j}$. The probability of winning is concave in q_i, implying decreasing returns to higher input quantity q_i, which is optimized when marginal costs equal marginal product. Profit profit-oriented miners maximize their chances of winning by optimizing input quantity q_i subject to their budget constraint. Given that q_i is a choice variable, if more computational effort shall be dedicated to mining, miners must necessarily increase q_i by investing into more machines.

1.5. The production problem: How to generate profits in the mining game

Let $E\pi_i$ represent the profit a miner can expect from participating in the mining game when investing q_i, $p_{btc}(t)$ stand for the current market price of Bitcoin and R for the reward of Bitcoins and transaction fees the miner can expect when winning the mining game. Also let c_i represents the variable cost the miners incur per unit of mining effort and C_i represents capital investments, then the expected profit of a representative miner i can be written as:

$$E\pi_i = p_i \cdot p_{btc}(t) \cdot R - c_i \cdot q_i - C_i$$

C_i are sunk in the short run but have a significant effect on market-trajectory as the purchase of machines affects the number of hashes q_i the miner can invest per round if their budget allows for it. The equation shows that the mining costs $c_i \cdot q_i$ of participating in the mining are certain, while the payoff $p_i \cdot p_{btc}(t) \cdot R$ is not. The participation in the Bitcoin consensus process is thus effectively a lottery embedded in a production problem.

Traditional economic theory suggests that in a competitive market, post-investment, meaning already active miners who have already invested will participate until their marginal costs of production equal their marginal product to maximize profits. The marginal profit of a representative miner can be found by taking the first derivative of the expected profit and holding quantities fixed, leading to the first order condition:

$$\frac{\partial E\pi_i}{\partial q_i} = \frac{\sum_{j\neq i} q_j}{\left(q_i + \sum_{j\neq i} q_j\right)^2} \cdot p_{btc}(t) \cdot R - c_i = 0$$

In a symmetric equilibrium, where $q_i = q_j = q$ and at similar constant $c_i = c_j = c$ and with a total number of n miners in the network, the profit maximizing input per miner can be written as $q^* = \frac{n-1}{n^2} \cdot \frac{p_{btc}(t) \cdot R}{c}$. Optimal quantity q^* is a function of the current market price of Bitcoin, variable costs, and level of competition as measured in terms of active miners n. c depends on the current difficulty, the current electricity price, and the power efficiency of the mining equipment. Ceteris paribus, as input factors into the cost function increase, optimal quantity q^* is expected to go down. Likewise, as the market price for Bitcoin $p_{btc}(t)$ increases, so will the input quantity by a representative miner. The positive relationship between increasing hashing input in anticipation of higher (expected) rewards has been extensively studied and proven in the economic and financial literature (de Vries, 2021; Kubal & Kristoufek, 2022).

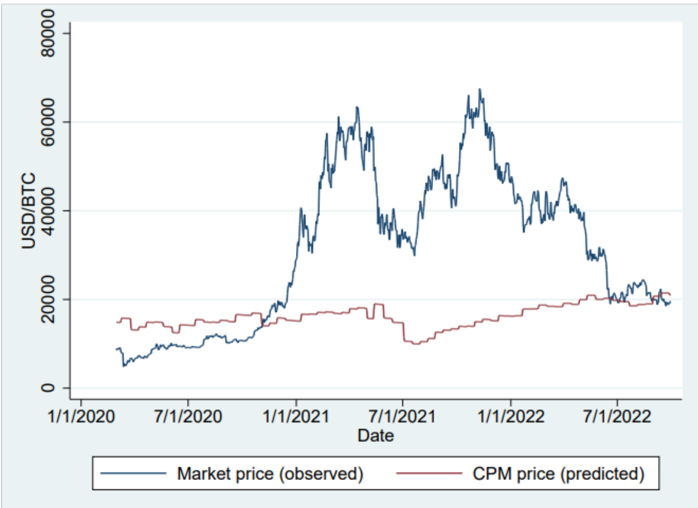
Rational miners that have already invested in mining gear should participate in the mining round if they expect their potential gains to outweigh associated costs of participating at the optimal choice of q^*.

$$p_i \cdot p_{btc}(t) \cdot R - c \cdot q^* > 0$$

To test whether this condition holds true at a given moment in time, miners must verify the above condition by calculating their expected profit as well as associated costs. One framework commonly cited to aid the decision process of active miners, is the Cost of Production (CPM) model set forth by Hayes (2015). According to Hayes 'if Bitcoin production is a competitive commodity market' (Hayes, 2015), the marginal product of mining should theoretically equal its marginal cost and in turn, equal its selling price. CPM therefore calculates expected Bitcoin production and electricity costs, taking as input parameters the price of electricity in USD/kWh, the energy consumption per unit of mining effort in J/GH or watts/GH/s, the (expected) market price of Bitcoin in USD/BTC and the current level of mining difficulty for a given block reward and hashing power of equipment. The model derives the cost of production price of Bitcoin p^* as the ratio between expected Bitcoin production and energy costs that serves as a theoretically lower bound for the market price of Bitcoin, below which a miner would operate at marginal loss and may therefore decide to not participate[6] in the current round of the mining game. According to Hayes, if $p_{btc}(t) < p^*$, then the miner may anticipate $p_i \cdot p_{btc}(t) \cdot R - c \cdot q^* \leq 0$, which means he will not participate in the consensus scheme of the mining market in that round.

In 2019 Hayes empirically validated over a sample period June 2013 and March 2018 that the model provided a surprisingly good fit and was able to Granger-cause the Bitcoin price. CPM assumes that the production market for Bitcoin is that of a competitive commodity market (Hayes, 2015) and that electricity is the only cost driver. Indeed, the biggest share of miner's operational expenditures are electricity costs (Blandin et al., 2020; Hayes, 2019; Podhorsky, 2019; Stoll et al., 2019; Thum, 2018). This is particularly true for Bitcoin (CCAF, 2022)[7] and despite the fact that miners today pay industrial prices rather than residential electricity prices (Blandin et al., 2020).

Figure 1: Cost of production price versus market price for Bitcoin



Empirically back testing the model over the sample period from March 2020 until September 2021 however indicates that CPM has lost some of its predictive power. In line with Hayes, two

[6] The framework is only applicable to active miners, which have already invested in necessary mining equipment.
[7] The CCAF finds, that between 2020 and 2021, capital expenditures for cryptocurrency miners amounted to 45% of miner's total costs, while 55% fund operational expenditures. However, in the case of Bitcoin, electricity costs constitute a relatively higher share; Here, utility costs correspond to 79% of operational expenditures, with electricity being the main cost factor identifies throughout the literature (de Vries, 2021; de Vries et al., 2022; Hayes, 2015; Jones et al., 2022; J. Li et al., 2019; Thum, 2018).

OLS regressions are performed with $p_{btc}(t)$ and p^* as well as the log transformation of each time series. The first regression is used to obtain a proxy for model fit, which produces an $R^2 = 0.442$, indicating that 44% of the observed market price can be explained by CPM. The second regression on log transformations produces an $R^2 = 0.609$, indicating that roughly 60% of the marginal change in market price can be explained by the change in marginal costs[8]. This is not negligible, however smaller than the $R^2 = 0.969$ obtained by Hayes (2019). Additionally, a Vector autoregression model (VAR) is derived to test whether the relationship between the time series involved is bi-directional, which can also not be statistically verified.

Underlying Hayes' model is the assumption of perfect competition from small homogenous miners, the treatment of Bitcoin as a commodity, and that electricity costs are the only cost driver. Originally, the mining market may have been characterized by such conditions, however these assumptions no longer hold as will be discussed in Part 3.

A detailed discussion on CPM as well as the output of the empirical analysis that back tests the model with data over the sample period from March 2020 until September 2022 can be found in the Appendix.

2. The market reality of Bitcoin production: Investment race & technological lock-in

Increased competition has systematically caused the blockchain to increase the difficulty of mining. Rajendra & Gear (2019) note, that the relative change in the difficulty of mining versus the rate of change in average hashing power of equipment, may become a bottleneck for new participants and a 'critical contributor to the centralization of consensus power towards commercial and large-scale entities'. Notably centralization can occur across various layers of the blockchain system (Sai, Buckley, Fitzgerald, et al., 2021). On the consensus level, this trend has been widely studied and identified throughout the literature (Beikverdi & Song, 2015; Gervais et al., 2014; Sai, Buckley, & le Gear, 2021; Sai, Buckley, Fitzgerald, et al., 2021). The current Bitcoin production market may therefore better be modelled as one of oligopolistic competition. The number of miners entering the market depends on necessary fixed cost investments and level of expected renumeration. In a symmetric equilibrium of homogenous producers where each exerts $q^* = \frac{n-1}{n^2} \cdot \frac{p_{btc}(t) \cdot R}{c}$, each producer can expect a profit of:

$$E\pi_i = \frac{p_{btc}(t) \cdot R}{n^2} - C$$

[8] According to de Vries (2022), approximately 60% of operational expenditures in Bitcoin are electricity costs.

Under the assumption of perfect competition producers compete for market share until $E\pi_i = 0$, then the number of miners to enter the market may be amounts to:

$$n^* = \sqrt{\frac{p_{btc}(t) \cdot R}{C}}$$

The number of Bitcoin producers n^* increases in the size of the blockchain-native reward R, the (expected) market value of Bitcoin, and decreases in fixed cost investments. At the onset of Bitcoin, when R was relatively high and necessary capital investments C low, entry into the Mining Game increased significantly. In line with the model, the number of active nodes, namely computers participating in the Bitcoin consensus mechanism, almost doubled from 5000 in September 2016 to approximately 10,000 reachable nodes in September 2018 (Bitnodes, 2022). Over time however, the necessary capital investments to enter the mining game have increased significantly, whilst the reward halving have made participation less lucrative, and the market has consolidated.

(Arnosti & Weinberg, 2022) have shown that asymmetric costs and economies of scale inevitably lead to market power concentration even though mining rewards exhibit decreasing marginal gains. The economic incentives of Bitcoin mining seem to inevitably lead to the concentration of production and ownership of Bitcoin mining hardware.

These developments explain the failure of CPM which relies largely on an outdated assumption of small, homogenous miners; At the onset of Bitcoin, when the difficulty of mining was still low, players were able to use standard CPUs and GPUs, often part of standard gaming equipment, for their mining activities, enabling rapid entry into the Mining Game. However, annualized average annualized difficulty in the network has increased exponentially since 2016, when technologists began developing ASIC miners with higher mining efficiency (Bedford Taylor, 2017). Due to their outstanding hash rate and subsequent success in mining, miners raced to invest in ASIC mining equipment. The investment race caused the blockchain to systematically adjust the difficulty upwards, increasing total hashing power in the network by roughly $3 \cdot 10^{13}$ that of 2009[9].

Relying on data from btc.com, which monitors the success in discovering new blocks, it can be inferred that 80% of the relative hashing power in the Bitcoin network are allocated to approximately 10 mining pools over the sample period. Between January 2020 and September

[9] Figure 2 and 3, and Table 3 in the Appendix showcase the development of network difficulty and hashrate.

2020[2], the share of hashing power attributable to these pools amounted to >90%. In response to increased levels of competition, individual miners have begun to pool their resources in mining pools. Mining pools provide as valuable tool for risk-sharing among individual miners (Cong et al., 2018) and mitigate relatively higher variance (Lewenberg et al., 2015) that disadvantages small solo miners (Gencer et al., 2018; Sai, Buckley, Fitzgerald, et al., 2021). The observed dominance of large pools is not a passing fad but expected to continue for the foreseeable future given the current market dynamics (Arnosti & Weinberg, 2022). This also means that the philosophy underlying PoW and Bitcoin as an equitable, competitive market among miners is unlikely to be realized.

The investment race can also be regarded as constant repetition of the Prisoner's Dilemma, where the dominant strategy of each player yields to the collectively worse outcome for all players involved. Namely, by acting in their self-interest, each miner aims to maximize input quantity q, thereby raising network difficulty δ and making participation in the Mining Game more costly overall by systematically raising system-wide costs of production. The emergence of centralized mining pools for risk sharing does not necessarily undermine the decentralization requirement for public blockchains (Cong et al., 2018). Mining pools as a financial innovation however significantly escalate the arms race among competing miners and thereby increases the energy consumption of PoW-based blockchain even further.

Unlike the network difficulty, which can adjust back down, capital investments are less easily reversed because the machines are optimized for the SHA-256 algorithm of Bitcoin and have no outside use beyond the mining market (Prat & Walter, 2021). Thus, the lower-bound network difficulty δ is systematically increased, without reversibility due to technological lock-in. Industry practitioners see the high hashrate level as beneficial because the security of the network increases when more miners work on sustaining the network against outsiders and raise the costs required to run a 51% attack on the network (Bitcoin Mining Council, 2022). These viewpoints suggest that the production market cares not only for market share, but also market size in general. Thus, the security of the Bitcoin network seems diametrically opposed to environmental sustainability.

3. Externalities of Bitcoin mining

A key sustainability issue is the use of tangible resources in the production process, which are irretrievably lost (sunk) after the currency has been generated, even though there is no protection against depreciation. Increased competition has intensified these externalities. The next paragraphs discuss the technique, difficulties, and results of analyzing the amount of Bitcoin production externalities.

3.1. Systematic estimation of externalities in Bitcoin production

A top-down mathematical approach[10] relies on calculating electricity consumption from the networks' hashrate, using estimates of mining rig efficiency (Krause & Tolaymat, 2018). Since energy consumption is not equivalent to carbon emissions, the average energy mix used to fuel operations as well as the location of mining operations is often assessed to derive emission factors (EF)[11] based on the chosen production inputs and process characteristics (Goodkind et al., 2020; Jones et al., 2022; Krause & Tolaymat, 2018). The corresponding damage coefficient, often referred to as the social cost of carbon (SCC) can then be used to derive an economic quantification of e.

Exact localization of mining activities has generally rendered difficult due to a lack of reliable data (Goodkind et al., 2020; Krause & Tolaymat, 2018) as well as the utilization of routing services and virtual private networks (VPNs) (Gencer et al., 2018). Self-contributed, geolocational mining data collected by the Cambridge Centre for Alternative Finance (CCAF) indicates that between March 2020 and September 2022, mining activity can be allocated to China (38.0%), the US (21.6%), Kazakhstan (9.1%), Russia (5.2%), Canada (4.2%), Germany (2.4%), Ireland (2%), Iran (2%), Other (11.7%)[12]. The data shows significant variation: Kazakhstan, for instance, became an important site for Bitcoin miners following China's June 2021 ban on cryptocurrency mining (de Vries et al., 2022; John et al., 2022). Before that, China was responsible for 65%–75% of Bitcoin's processing power. Following the ban, the recorded hashrate plummeted to zero during July and August 2021, yet by September 2021 China again made up slightly over 22% of the Bitcoin mining industry again (Cambridge Judge Business School, 2022).

[10] Other Approaches include extrapolation from individual transaction footprints or experimental setups that are then used to generalize (Platt et al., 2021)

[11] An EF is 'a representative value that attempts to relate the quantity of a pollutant released to the atmosphere with an activity associated with the release of that pollutant' (EPA, 2022)

[12] Monthly data collected from March 2020 to January 2022 (Cambridge Centre for Alternative Finance, 2022b). Values from January 2022 deemed representative for the remainder months in 2022. Results represent averages. Note, that values may not add up to 100% due to rounding. Compare Appendix Figure 4 and 5

The observations highlight fundamental regulatory issues in competition policy when the subject transcends national borders and accountability; Since production of q is constraint by the efficient production frontier, the global Bitcoin production market is characterized by a high level of migration for the cheapest or otherwise optimal combination of production inputs or favorable regulation. Unless global taxation and regulatory frameworks are harmonized, geographical arbitration by the miner network will likely continue.

The behavior further impedes a reliable assessment of the average energy mix used to fuel operations for developing an accurate and consistent image of the magnitude of externalities. The CCAF for example estimated that renewable energy sources powered 39% of mining operations between 2020 and 2021 (Blandin et al., 2020). The Bitcoin Mining Council even posits, that 58.4% of mining operations in 2021 utilize sustainable energy sources (Bitcoin Mining Council, 2022). Recent estimates however rather indicate a reduction in renewable energy sources from over 40% in 2020 to 28% in 2021 (de Vries et al., 2022).

Lastly, a monetary equivalent for the damages of production must be derived. International institutions are developing taxation frameworks for the adequate pricing of carbon dioxide emissions (CO2e) (International Monetary Fund., 2019; OECD, 2021). While several estimates have been developed to quantify the 'right' externality price for a ton of CO2e, there is no clear consensus amongst political, economic, and scientific stakeholders (compare Table 1).

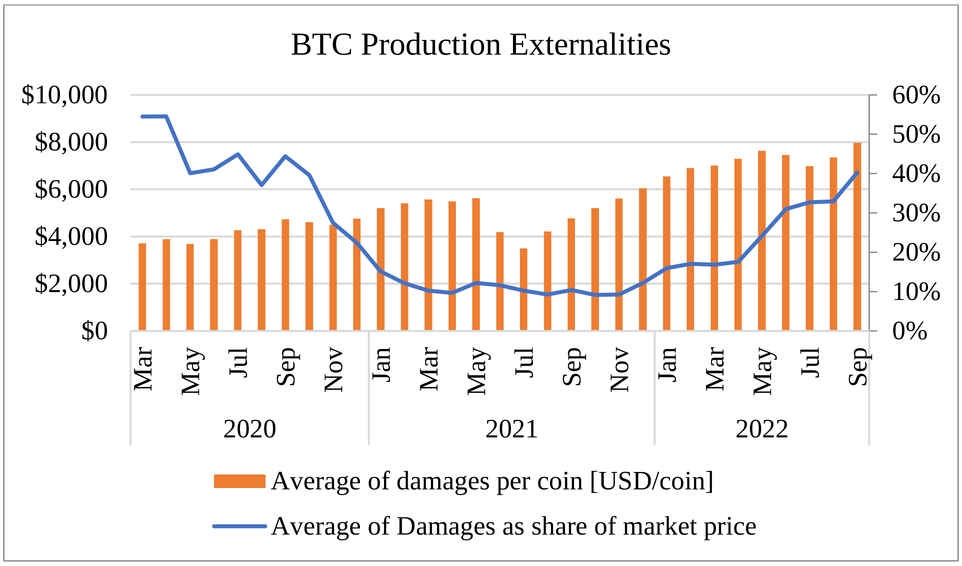
Table 1: Monetary estimation of SCC per ton of CO2

Estimated SCC per ton of CO2	**Source**
USD 51	US Government Working Group (2021)
USD 185 (mean) (range USD 44-413)	Rennert et al. (2022)
USD 171-310	Pindyck (2019)
USD 202	Umweltbundesamt (2021)

3.2.Quantification of damages

Using a damage coefficient of USD 100 per ton, Jones et al. (2022) estimated that between 2016-2021, Bitcoin amassed USD 12 billion in damages. The authors highlight, that climate damages associated with Bitcoins energy demand seem to increase with industry maturity and estimate, that a bitcoin mined in 2021 is responsible for emitting 126 times the CO2e as one mined in 2016. The situation is attributable to market price appreciation and the industry's increasing industrialization discussed (de Vries, 2021). Following the methodology set forth by Jones et al (2022) and using the estimated average Emission Factor (EF) of 557.8 CO2e/tkWh, as well as a conservative damage coefficient of USD 51/tCO2 over the sample period, we can estimate that damages amount to USD 5.6 billion or 34% of the market price on average over the sample period between March 2020 and September 2022. Though based on average EFs and absent considerations for additional side effects, such as pressure on local grid systems, the magnitude is alarming[13].

Figure 2: Bitcoin Production Externalities between March 2020 and September 2022



Even though Bitcoin mining is based on the principle of developing the most advanced and effective computational infrastructure possible, at this point in time, the effectiveness of its infrastructure can be most accurately compared to that of conventional, antiquated production methods that are remnants of the manufacturing industry. Cryptocurrency mining has been found to consumer more energy than the mining of copper, platinum, gold, and rate earth oxides to produce an equivalent market dollar value (Krause & Tolaymat, 2018). Recent estimates compare the Bitcoin production process to that of other energy-intensive or heavy-polluting commodities such as beef, or gasoline from crude oil (Jones et al., 2022). This calls into question the innovative character of the use of the technology and has resulted in significant retraction of public support. Ultimately, the physical damages seem incompatible with merely virtual value-creation, given, that they cannibalize the very tangible basis they rely on.

3.3. Reduction Targets

Given the rising trend of observable emissions in comparison to evident carbon reduction goals, the debate remains as to how severe the damages may be permitted to become. To keep global warming to no more than 1.5°C – as called for in the Paris Agreement – emissions need to be

[13] Compare Appendix Table 4 for estimated emission reduction targets based on various assumptions of SCC

reduced by 45% by 2030 and reach net zero by 2050. According to the Intergovernmental Panel on Climate Change (IPCC), we must remove 5 to 16 Gigatons (Gt) of CO_2 per year until 2025 from the atmosphere (European Environment Agency, 2022)[14] in addition to further slowing down emission growth. This gives a required reduction in global CO_2 emissions until the end of the century of 1,000 Gigatons of CO2. In theory, assuming 1458 days between each halving, the last Bitcoin should be created in April 2044[15]. Ceteris paribus, if the network continues to utilize electricity at the current rate and absent significant energy efficiency improvements (or their offsetting due to higher competition) it will produce approximately 1,250 Megatons of CO_2e until then. Halting Bitcoin now would already safe 0.12% of the required emission reductions until 2100.

3.4. Other externalities in Bitcoin production

A second environmental concern less frequently discussed is an increasing amount of electronic waste that is amplified with investment racing (de Vries & Stoll, 2021). Due to a doubling in energy efficiency of mining equipment roughly every 18 months machines become obsolete after 1.57 years (Koomey et al., 2011). In an empirical analysis, de Vries & Stoll (2021) find, that the average time of a Bitcoin mining machine to become unprofitable sums up to less than 1.29 years, even. By constantly replacing less efficient machines with new ones the Bitcoin mining industry is amassing substantial electronic waste (de Vries & Stoll, 2021) that is estimated to amount to 43 kilotons annually (Cambridge Centre for Alternative Finance, 2022a). Investments in such equipment cannot easily be reversed as they have little to no resale value once they become obsolete. Additionally, since the built-in chips are optimized for the SHA-256 algorithm of Bitcoin, they have no use outside use beyond this market (Prat & Walter, 2021). The dependence on special-purpose machines also creates market power for producers. Bitmain Inc. is the leading mining machine producers, domiciled in China, it stopped disclosing sales information upon its IPO in 2018 and has since been criticized for a lack of transparency and customer support (Bedford Taylor, 2017; de Vries & Stoll, 2021).

[14] The goal of carbon dioxide removal is to remove excess CO2 from the atmosphere and store it for the long term, thereby assisting in the restoration of our climate. Carbon dioxide removal serves three climate aims: in the near term, carbon removal helps to keep the globe within its carbon budget and stabilizes the climate by reducing CO2 levels in the atmosphere. In the medium term, it helps to zero out emissions from difficult-to-abate industries, so assisting the globe in reaching net-zero emissions and in the long term, it may support to reverse global warming.

[15] Compare Appendix Table 2

4. Is evolution towards sustainable Bitcoin production possible?

Effectively achieving climate goals will require new approaches to governance that Mark Bevir (2012) describes as hybrid between market, private and public stakeholders, multi-jurisdictional and plural. Cryptocurrency networks are part of our economy and must acknowledge their role in shaping global economic and social outcomes. The current incentive scheme of Bitcoin mining seems fundamentally non-compatible with environmental concerns and forces to think the trade-off between technological innovation and environmental sustainability.

4.1. Maintain PoW but divest wasted energy to productive use

4.1.1. Auction

An essential problem in PoW is that most of the networks' work is inevitably wasted. Recall that during the Mining Game miners are incentivized to invest their maximum input quantity q under uncertainty, taking the current production price as given. The probabilistic nature of the algorithm as well as the winner-takes-all mentality cause most of these resources to be invested in vain - drawing an analogy to a rent-seeking contest akin to Tullock (1991).

Rather than directly investing q ex ante, miners may bid for the privilege of adding the next block in an auction mechanism based on the current price level of production. The right to mine the next block may be awarded to the miner with the highest valuation, whilst the network difficulty continues to be adjusted based on the overall valuation by the network recorded.

Since the bid must be paid to incentivize true revelation, one may think of divesting all but the winning bid towards an alternative productive use. Notably this proposal underlies the assumption that q is generic, namely that computational effort is not limited to solving the cryptographic algorithm of the Bitcoin blockchain but can be variegated. Further research should be dedicated into investigating the technical feasibility of such a proposal. Bidding may reduce the urgency of solving the cryptographic puzzle, thereby potentially lowering energy demand. At the same time, depending on the purpose of divested usage of computational effort and the utility factors of producers, it may incentivize even higher bids, for example if the losing bids are used to power social energy systems.

4.1.2. Productive insertion into local energy networks

Rather than letting the energy used to sustain and expand the network go to waste innovative solutions for a secondary productive use should be investigated. Bitcoin mining rigs have one crucial advantage over traditional data centers, which is that they are interruptible. Mining plants, often comprised of several hundred individual machines, can react quickly, at low costs, and with high granularity. A challenge in renewable energy development meanwhile is that it brings a unique circumstance of intermittency. It has therefore been proposed that the Bitcoin network may serve as a flexible energy buyer of last resort to balance fluctuations in renewable[16] power generation and demand (Satoshi Energy Corp., 2020). The excess heat generated as a byproduct of running mining machines could also be used to heat houses and apartment building, a system already being tested with traditional data centers. By hosting mining operations in private locations such as business building or logistic centers, the costs of setting up traditional mining farms could potentially be reduced, while the hosting households or businesses can save on electricity costs, creating a mutually beneficial incorporation of Bitcoin production into society. Further research should be dedicated to quantifying the potential long-term benefits and risks of integrating Bitcoin mining operations into local energy networks. One should be especially careful that mining operations do not crowd out other more productive use of sustainable energy.

4.2. Control market size and internalize competitive externalities

4.2.1. Multilateral cooperation

A common method to overcome the aforenamed mentioned Prisoner's Dilemma is multilateral cooperation. In the prisoner's dilemma, the failure of achieving the socially best outcome is attributable to a lack of trust between the agents in question (the prisoners). PoW approaches this problem from a technical implementation standpoint, but results in a costly and competitive arms race. If cooperation could be achieved, the competitive externality of choosing computational input could be internalized, leading to lower computational input for each Bitcoin producer and overall, a lower level of energy consumption[17].

In order to mitigate the investment racing, the Bitcoin production market could (directly or indirectly) agree on a certain level of total hashrate (market size) and relative contribution (market share) to each mining firm. Multilateral cooperation would demand proper governance to manage who joins the production market and to agree on and adhere to market share agreements. Such limitations to participation contradict the philosophy of truly public blockchains. Nonetheless, the market reality already contradicts the intentions of decentralization for which PoW was selected. When a market reality outgrows the ideas upon which it was founded, it may be time to reconsider those ideals. Such cooperative agreements

[16] While technological progress has made solar and wind farms relatively cheap, these renewable energy sources are prone to suffer from grid bottlenecks due to their unstable energy supply.
[17] Compare Appendix for an analysis of break-even electricity prices given various assumptions on market price and total network hashrate (market size)

are only enforceable if neither party has a motive to stray from them, which is contingent on the production rent that may be obtained. It will also likely necessitate constraints on the process for speculative price formation, which are difficult to enforce. Any amount of network hashrate might be sustained, though, if producers received a greater benefit from collusion. Further study should be devoted to identifying the set of oligopolistic equilibria or competitive regimes under which such a collusive conclusion is enforceable.

One additional benefit of holding computational input of the Bitcoin mining network fixed would be a stable level of difficulty. Podhorsky (2019) has shown, that difficulty adjustments inevitably lead to welfare losses. The change in the difficulty level acts akin to an ad-valorem tax on the production price of Bitcoin imposed by the blockchain. Instead of accruing tax revenue however the adjustment alters electricity costs for miners and while a higher price is obtained, the rents that would have arisen from limiting the supply are wasted, as they benefit neither a government, not the miner network. Thus, one may also think about an evolution towards a more efficient difficulty adjustment mechanism, for example one that anticipates input quantities and reacts accordingly, thereby reducing distortion (Feng et al., 2021). The scenario is theoretic.

4.2.2. Permissioned blockchain

In addition to the polar cases of completely centralized ledgers and decentralized blockchain systems however, a third type of ledger called a ‘permissioned’ blockchain exists, which has shown promise across application. Permissioned blockchains can break the blockchain trilemma by allowing for fork competition but eliminating the waste of resources that characterized PoW (Abadi & Brunnermeier, 2022). Moving from a permissionless to permissioned type of blockchain means that participants of the consensus process become known agents rather than anonymous miners. This would restrict free, anonymous entry into the consensus participation but could also allow to make entry into the consensus scheme conditional on miners meeting certain sustainability criteria.

4.3. Change of consensus mechanism

A common call in the literature concerned with the environmental footprint of cryptocurrency mining is to change the consensus mechanism from PoW which relies on outdated notions of efficiency and competition, to one that is decoupled from any energy-intensive production processes (de Vries & Stoll, 2021; Goodkind et al., 2020; Jones et al., 2022). Changing the core protocol and thereby changing the consensus method is possible if the community deems them necessary. In this regard, blockchain-based economies are a prime example of self-governed systems. Other public cryptocurrencies provide illustrations: Monero for example has decided to pursue a strategy to hard-encode ASIC resistance, relying on random code execution and memory-hard techniques that prevent specialized mining hardware from dominating the network (Cho, 2018). Thereby it effectively avoids investment racing and aims to maintain low market entry barriers by changing the algorithm when the network observes a critical level of centralization[18].

Ethereum, the second largest cryptocurrency by market capitalization (Bitinfocharts, 2022) has also decided to change from PoW to Proof-of-Stake (PoS). PoS substitutes competitive validation by single entities with randomized selection and group-based behavior. In PoS blocks are verified by a group or committee of so-called validators that must each stake a specific amount of their own coins, thereby changing the cost structure of incentives (Gui et al., 2018). A change would shift market power in Bitcoin production from those with the most production capacity to those with the highest holdings. PoS achieves security through community control and potential ex-posts costs, should a malicious validator be detected. It thereby decouples completely from a resource-intensive security mechanism and avoids the ex-ante waste of resources as well as the incentive to engage in a computational arms race (Saleh, 2018).

Ethereum, which previously ran on PoW, has exemplified, that the transfer is technologically feasible whilst using 99.99% less energy than PoW (Beekh, 2021). Other advantages of POS include faster block generation speed, as well as transaction confirmation time (Gui et al., 2018). Various other consensus algorithms exist, that do not require to tap into tangible resources are Proof-of-Elapsed-Time (PoET), Proof-of-Burn (PoB), Proof-of-Activity (PoA) etc. Ultimately, the choice of consensus algorithm depends on the desired application.

Changing the Bitcoin production algorithm would undoubtedly render vast amounts of expensive infrastructure worthless. Nonetheless, Bitcoin producers must be careful not to fall victim to the Sunk Cost Fallacy, particularly considering the future costs of maintaining the existing scheme.

4.4. Natural Market Correction

While not an active solution, it is likely that the Bitcoin mining market may correct itself, if not cannibalize itself. The market capitalization of the crypto industry fell from more than USD 3tn at the height in 2021 to less than USD 1tn in September 2022 in a protracted downturn. At the time of writing, Bitcoin has already lost more than 65% of its all-time market high of 67,000

[18] Notably the success of such a strategy has been called into question (de Vries & Stoll, 2021), as it may lead to even shorter life cycles of equipment which could in the worst case amplify the generation of electronic waste

USD/BTC in November 2021, trading at around 17,000 USD/BTC. Additional pressure on Bitcoin producers comes from rising energy prices. The World Bank's energy price index grew by 26.3 percent between January and April 2022, following a 50 percent increase from January 2020 to December 2021 (World Bank, 2022). This combination puts operating margins of mining companies significantly under pressure. The Nasdaq-listed mining hosting company Core Scientific recently warned investors of bankruptcy threats, citing the 'prolonged decrease in the price of Bitcoin, the increase in electricity costs, the increase in the global Bitcoin network hash rate and the litigation with' a large global bankrupt cryptocurrency lending company (Core Scientific, 2022). The development aligns with other bankruptcies in the ecosystem that are tangent to Bitcoin mining operations. Speculative bubbles rely on new money flowing in, yet this money is also the most sensitive to exit in times of economic downturns. Bitcoin's price has been artificially inflated and is currently being adjusted downwards which will likely result in a large number of miners leaving the market permanently[19]. The correction may reset the mining industry to a more modest level.

5. Summary of key results and implications for further research

Bitcoin has undoubtedly trailblazed a new era of digitally enabled finance and exemplified the potential reach of blockchain-based system. There are a lot of promising applications of blockchain for coordinating small, decentralized multi-agent machine systems (Nguyen et al., 2019; Tang et al., 2022). However, the use of a promising technology is not a sufficient condition for an added value of a product that is based on it. In the case of Bitcoin, the use of blockchain technology for coordinating production decisions has created limited value for society but rather exemplifies how a market falls subject to technological lock-in by historical randomness. The network is conducive to complex anticompetitive strategies that evade regulatory oversight, which wouldn't be a problem if it didn't assist the formation and maintenance of exceptionally durable market power, which violates its initial premise. Perhaps most importantly, the digital-market conduct tends to lack significant offsetting inefficiencies and is not efficiently self-correcting, calling for alternative forms of governance.

From an environmental standpoint, there are several alternative mechanisms existent, virtually all of which perform better in terms of resource-efficiency. As blockchain-based market and cryptocurrency networks are becoming an integrated part of our global financial and economic

[19] Compare also Figure 1, which indicates that the market is converging back towards its production bound after having been heavily inflated throughout 2020 and 2021

system, they must acknowledge their capability and role in reducing net emissions. The imperative is for the mutual benefit: The future of Bitcoin is no longer dependent on exemplifying the effectiveness of its design. The future of Bitcoin depends on whether it can lower its energy demand. Not just in anticipation of power shortages that threaten the vary basis the virtual currency depends upon, but also because the financial landscape of the 21st century requires to uphold Ecological, Social, and Governance (ESG) factors. It is highly unlikely that investments in PoW-based assets can be part of an ESG investment strategy. Even so-called 'green crypto mining' would crowd out other, likely more productive uses of renewable energy. Ultimately, the Bitcoin community should shift from using a mechanism that is doing things (technically) right, to doing the right thing.

6. Limitations and room for further research

Since this thesis is part of a master's thesis dissertation, it is vital to be aware of all of its limits. Blockchain, Bitcoin, and cryptoassets are a developing and highly interdisciplinary field of study that relies on insights from finance, economics, computer science, organizational engineering, and other disciplines. This makes the work project prone to practical challenges in inter-disciplinary research, such as a lack of a shared language and divergent perspectives on the same topic. Challenges inherent to comprehending dynamic systems, such as their ongoing change and inability to perceive the system as a whole, also complicate the study. The integration of blockchain-based economies into global value chains is poorly understood and scientific consensus is lacking in most models. Consequently, the approach is overly simplistic and likely fails to represent the intricacies that characterize the Bitcoin production network on a worldwide scale. It does not analyze, for instance, the impact of transaction fees on production decisions, nor does it investigate other variables that may impact the utility of Bitcoin miners and subsequent mining decisions. Other limitations include limited time, as well as limited financial resources.

References

Abadi, J., & Brunnermeier, M. (2022). *Blockchain Economics*.

Akram, S. V., Malik, P. K., Tanwar, S., Singh, R., & Gehlot, A. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy*, *3*.

Alabi, K. (2017). Digital blockchain networks appear to be following Metcalfe's Law. *Electronic Commerce Research and Applications*, *24*, 23–29. https://doi.org/10.1016/j.elerap.2017.06.003

Arnosti, N., & Weinberg, S. M. (2022). Bitcoin: A Natural Oligopoly. *Management Science*, *68*(7), 4755–4771. https://doi.org/10.1287/mnsc.2021.4095

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

Beekh, C. (2021, March 18). *Ethereum's energy usage will soon decrease by ~99.95%*. EF Blog. https://blog.ethereum.org/2021/05/18/country-power-no-more

Beikverdi, A., & Song, J. (2015, August 3). Trend of centralization in Bitcoin's distributed network. *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2015 - Proceedings*. https://doi.org/10.1109/SNPD.2015.7176229

Bitcoin Mining Council. (2022). *Global Bitcoin Mining Data Review Q1 2022*.

Bitinfocharts. (2022, December 1). *Cryptocurrency statistics*. https://bitinfocharts.com/

Bitnodes. (2022, October 17). *Reachable nodes in the Bitcoin Network*. https://bitnodes.io/dashboard/7y/

Blandin, A., Pieters, G., Wu, Y., Eisermann, T., Dek, A., Taylor, S., & Njoki, D. (2020). *3 RD GLOBAL CRYPTOASSET BENCHMARKING STUDY*.

btc.com. (2022, October 1). *Pool Distribution*. https://btc.com/stats/pool

Cambridge Centre for Alternative Finance. (2022a, October 10). *Bitcoin Mining Index*. https://ccaf.io/cbeci/index

Cambridge Centre for Alternative Finance. (2022b, November 10). *Bitcoin Mining Map*.

Catalini, C., Gans, J. S., al Roth, to, Ali, M., Ravikant, N., Greco, N., Simcoe, T., Stern, S., Tucker, C., & Wu for helpful discussions, J. (2019). *Some Simple Economics of the Blockchain*. https://ssrn.com/abstract=2874598

Cho, H. (2018). ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols. *IEEE Access*, *6*, 66210–66222. https://doi.org/10.1109/ACCESS.2018.2878895

Cong, L. W., He, Z., & Li, J. (2018). Decentralized Mining in Centralized Pools. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3143724

Core Scientific, Inc. (2022). *SEC Form 8-K*.

Davidson, S., de Filippi, P., & Potts, J. (2016). *Economics of Blockchain*. http://ssrn.com/abstract=2744751

de Vries, A. (2019). Renewable Energy Will Not Solve Bitcoin's Sustainability Problem. In *Joule* (Vol. 3, Issue 4). Cell Press. https://doi.org/10.1016/j.joule.2019.03.006

de Vries, A. (2021). Bitcoin boom: What rising prices mean for the network's energy consumption. *Joule*, *5*(3), 509–513. https://doi.org/10.1016/j.joule.2021.02.006

de Vries, A., Gallersdörfer, U., Klaaßen, L., & Stoll, C. (2022). Revisiting Bitcoin's carbon footprint. *Joule*, *6*(3), 498–502. https://doi.org/10.1016/j.joule.2022.02.005

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

EPA. (2022, January 4). *Basic Information of Air Emissions Factors and Quantification*. United States Environmental Protection Agency. https://www.epa.gov/air-emissions-factors-and-quantification/

European Commission. (2019). *The European Green Deal*.

European Environment Agency. (2022). *Trends and projections in Europe 2022.*

Feng, W., Cao, Z., Shen, J., & Dong, X. (2021). RTPoW: A Proof-of-Work Consensus Scheme with Real-Time Difficulty Adjustment Algorithm. *2021 IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS)*, 233–240. https://doi.org/10.1109/ICPADS53394.2021.00035

Gencer, A. E., Basu, S., Eyal, I., van Renesse, R., & Sirer, E. G. (2018). *Decentralization in Bitcoin and Ethereum Networks*. http://arxiv.org/abs/1801.03998

Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is Bitcoin a Decentralized Currency? *IEEE Security and Privacy*, *12*(3), 54–60. https://doi.org/10.1109/MSP.2014.49

Goodkind, A. L., Jones, B. A., & Berrens, R. P. (2020). Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. *Energy Research and Social Science*, *59*. https://doi.org/10.1016/j.erss.2019.101281

Gschossmann, I., von der Kraaij, A., Benoit, P.-L., & Rocher, E. (2022). *Mining the environment – is climate risk priced into crypto-assets?* Https://Www.Ecb.Europa.Eu/Pub/Financial-Stability/Macroprudential-Bulletin/Html/Ecb.Mpbu202207_3~d9614ea8e6.En.Html.

Gui, G., Hortacsu, A., & Tudon, J. (2018). *A Memo on the Proof-of-Stake Mechanism*. http://arxiv.org/abs/1807.09626

Hayes, A. S. (2015). *A Cost of Production Model for Bitcoin*. http://en.wikipedia.org/wiki/Bitcoin_network#Bitcoin_mining

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

International Monetary Fund. (2019). *Fiscal Monitor, October 2019*. International Monetary Fund.

Jiang, S., & Wu, J. (2019). Bitcoin Mining with Transaction Fees: A Game on the Block Size. *2019 IEEE International Conference on Blockchain (Blockchain)*, 107–115. https://doi.org/10.1109/Blockchain.2019.00023

John, A., Shen, S., & Wilson, T. (2022, September 24). China's top regulators ban crypto trading and mining, sending bitcoin tumbling. *Reuters*. https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/

Jones, B. A., Goodkind, A. L., & Berrens, R. P. (2022). Economic estimation of Bitcoin mining's climate damages demonstrates closer resemblance to digital crude than digital gold. *Scientific Reports*, *12*(1). https://doi.org/10.1038/s41598-022-18686-8

Kiayias, A., Koutsoupias, E., Kyropoulou, M., & Tselekounis, Y. (2016). Blockchain mining games. *EC 2016 - Proceedings of the 2016 ACM Conference on Economics and Computation*, 365–382. https://doi.org/10.1145/2940716.2940773

Koomey, J., Berard, S., Sanchez, M., & Wong, H. (2011). Implications of Historical Trends in the Electrical Efficiency of Computing. *IEEE Annals of the History of Computing*, *33*(3), 46–54. https://doi.org/10.1109/MAHC.2010.28

Krause, M. J., & Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. *Nature Sustainability*, *1*(11), 711–718. https://doi.org/10.1038/s41893-018-0152-7

Kroll, J. A. ; D. , I. C. , F. E. W. (2013). *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*.

Kubal, J., & Kristoufek, L. (2022). Exploring the relationship between Bitcoin price and network's hashrate within endogenous system. *International Review of Financial Analysis*, *84*, 102375. https://doi.org/10.1016/j.irfa.2022.102375

Lamport, L., Shostak, R., & Pease, M. (1982). *The Byzantine Generals Problem*.

Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., & Rosenschein, J. S. (2015). *Bitcoin Mining Pools: A Cooperative Game Theoretic Analysis*. www.ifaamas.org

Li, J., Li, N., Peng, J., Cui, H., & Wu, Z. (2019). Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. *Energy*, *168*, 160–168. https://doi.org/10.1016/j.energy.2018.11.046

Li, Z., & Liao, Q. (2019). Toward Socially Optimal Bitcoin Mining. *Proceedings - 2018 5th International Conference on Information Science and Control Engineering, ICISCE 2018*, 582–586. https://doi.org/10.1109/ICISCE.2018.00126

Mark Bevir. (2012). *Governance: A Very Short Introduction (Very Short Introductions)* (Vol. 1).

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

Nguyen, C. T., Thai Hoang, D., Nguyen, D. N., Niyato, D., Tuong Nguyen, H., Dutkiewicz, E., & Ho Chi, V. (2019). *Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities*.

Announcing Approval of FIPS Publication 180-2, Pub. L. No. Federal Register (66 FR 29287) (2002).

OECD. (2021). *Effective Carbon Rates 2021*. OECD. https://doi.org/10.1787/0e8e24f5-en

Penard, W., & van Werkhoven, T. (2017). *On the Secure Hash Algorithm family*. http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf

Pindyck, R. S. (2019). The social cost of carbon revisited. *Journal of Environmental Economics and Management*, *94*, 140–160. https://doi.org/10.1016/j.jeem.2019.02.003

Platt, M., Sedlmeir, J., Platt, D., Tasca, P., Xu, J., Vadgama, N., & Ibañez, J. I. (2021). *The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work*. https://doi.org/10.1109/QRS-C55045.2021.00168

Podhorsky, A. (2019). *Bursting The Bitcoin Bubble: Assessing The Fundamental Value And Social Costs Of Bitcoin*. https://www.adb.org/publications/bursting-bitcoin-bubble-fundamental-value-

Prat, J., & Walter, B. (2021). *An Equilibrium Model of the Market for Bitcoin Mining*. https://digiconomist.net/bitcoin-energy-consumption.

Rajendra, A., & Gear, L. (2019). *Centralization Threat Metric*. https://www.blockchain.com/stats.

Rennert, K., Errickson, F., Prest, B. C., Rennels, L., Newell, R. G., Pizer, W., Kingdon, C., Wingenroth, J., Cooke, R., Parthum, B., Smith, D., Cromar, K., Diaz, D., Moore, F. C., Müller, U. K., Plevin, R. J., Raftery, A. E., Ševčíková, H., Sheets, H., … Anthoff, D. (2022). Comprehensive evidence implies a higher social cost of CO2. *Nature*, *610*(7933), 687–692. https://doi.org/10.1038/s41586-022-05224-9

Sai, A. R., Buckley, J., Fitzgerald, B., & Gear, A. le. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing and Management*, *58*(4). https://doi.org/10.1016/j.ipm.2021.102584

Sai, A. R., Buckley, J., & le Gear, A. (2021). Characterizing Wealth Inequality in Cryptocurrencies. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.730122

Saleh, F. (2018). Blockchain Without Waste: Proof-of-Stake. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3183935

Satoshi Energy Corp. (2020, December 11). *Special Report: Energy Backed Money*. https://research.satoshienergy.com/special-report-energy-backed-money/

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

Tang, X., Lan, X., Li, L., Zhang, Y., & Han, Z. (2022). *Incentivizing Proof-of-Stake Blockchain for Secured Data Collection in UAV-Assisted IoT: A Multi-Agent Reinforcement Learning Approach*. http://arxiv.org/abs/2207.02705

Thum, M. (2018). *The Economic Cost of Bitcoin Mining*. https://digiconomist.

Tullock, G. (1991). Rent Seeking. In *The World of Economics* (pp. 604–609). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-21315-3_81

Umweltbundesamt. (2021, August 10). *Gesellschaftliche Kosten von Umweltbelastungen*. https://www.umweltbundesamt.de/daten/umwelt-wirtschaft/gesellschaftliche-kosten-von-umweltbelastungen#gesamtwirtschaftliche-bedeutung-der-umweltkosten

United Nations. (2021). *Emissions Gap Report 2021*. . https://www.unep.org/emissions-gap-report-2021

United Nations. (2022). *Emissions Gap Report 2022*. https://www.unep.org/emissions-gap-report-2022

US Government. (2021). *Reducing Greenhouse Gases in the United States: A 2030 Emissions Target*.

US Government Working Group. (2021). *Social Cost of Carbon, Methane, and Nitrous Oxide*. https://www.whitehouse.gov/wp-content/uploads/2021/02/TechnicalSupportDocument_SocialCostofCarbonMethaneNitrousOxide.pdf

World Bank. (2022). *Global Economic Prospects, June 2022*. The World Bank. https://doi.org/10.1596/978-1-4648-1843-1

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Table of Abbreviations

This table references abbreviations used throughout this work project.

PoW	Proof-of-Work
PoS	Proof-of-Stake
PoET	Proof-of-Elapsed-Time
PoA	Proof-of-Activity
SHA	Secure Hashing Algorithm
CPU	Computer Processing Units
GPU	Graphical Processing Units
ASIC	Application Specific Integrated Circuit
EF	Emission Factor
GHG	Global Greenhouse Gas
TWh	Terawatt hours
SCC	Social Costs of Carbon
HHI	Herfindahl-Hirschman-Index
CO2	Carbon Dioxide
CO2e	Carbon Dioxide Emissions
GHG	Greenhouse Gases
kWh	Kilowatt hours
J	Joules
GH	Gigahash (= 10^9 hashes)

List of Figures

List of Tables

List of Outputs:

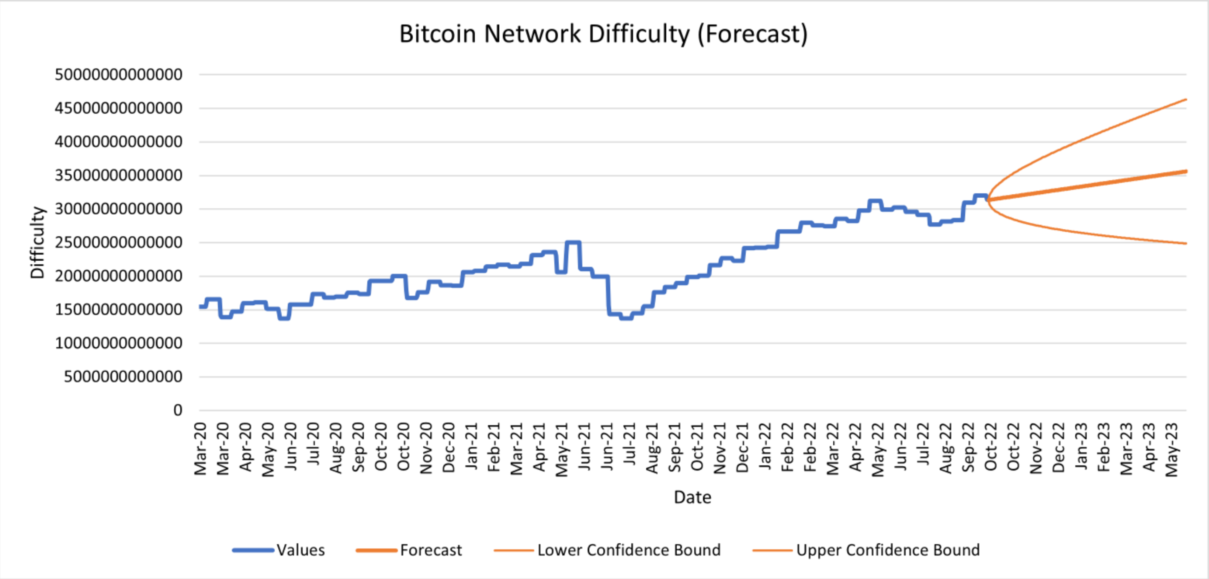
Appendix:

Table 2: Bitcoin Halving Dates

#	halving after block	reward	total BTC per halving frame	Dates of halving
1	210000	50	10500000	3-Jan-09
2	420000	25	5250000	28-Nov-12
3	630000	12.5	2625000	9-Jul-16
4	840000	6.25	1312500	11-May-20
5	1050000	3.125	656250	5/8/2024*
6	1260000	1.5625	328125	5/5/2028*
7	1470000	0.78125	164063	5/3/2032*
8	1680000	0.390625	82031	4/30/2036*
9	1890000	0.1953125	41016	4/27/2040*
10	2100000	0.09765625	20508	4/25/2044*
			20979492.19	

The estimated halving days are based on the assumption that 144 blocks are created per day, which results in 1458 days between halvings.

Figure 3: Bitcoin Network Difficulty and Forecast

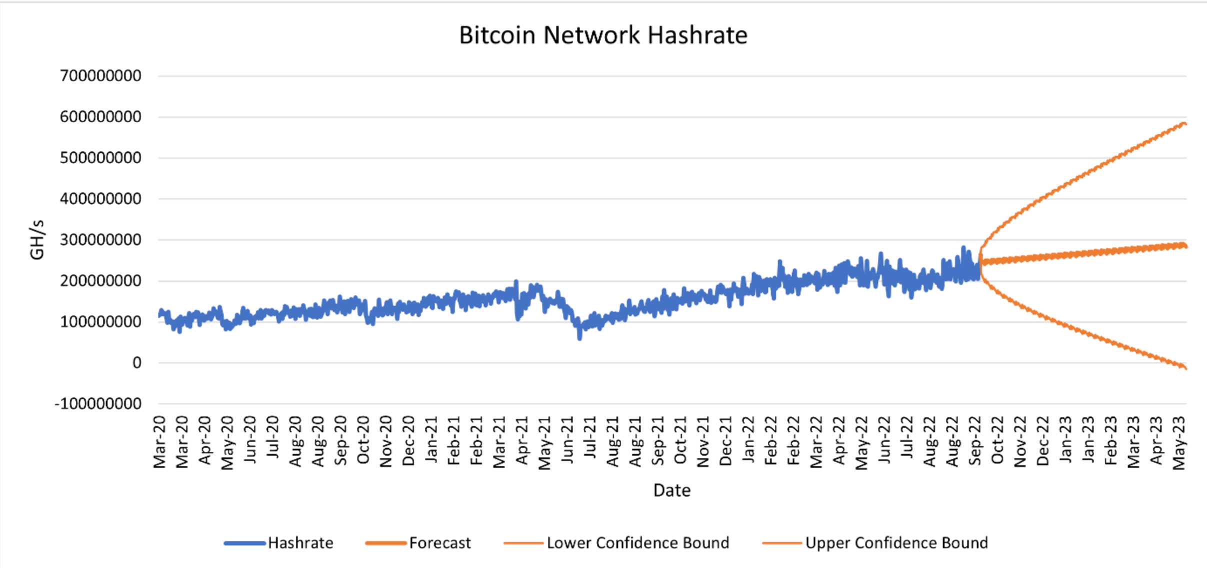


The difficulty is a measure of how difficult it is to mine a Bitcoin block, or in more technical terms, to find a hash below a given target.

Table 3: Bitcoin Network Annualized Average Difficulty

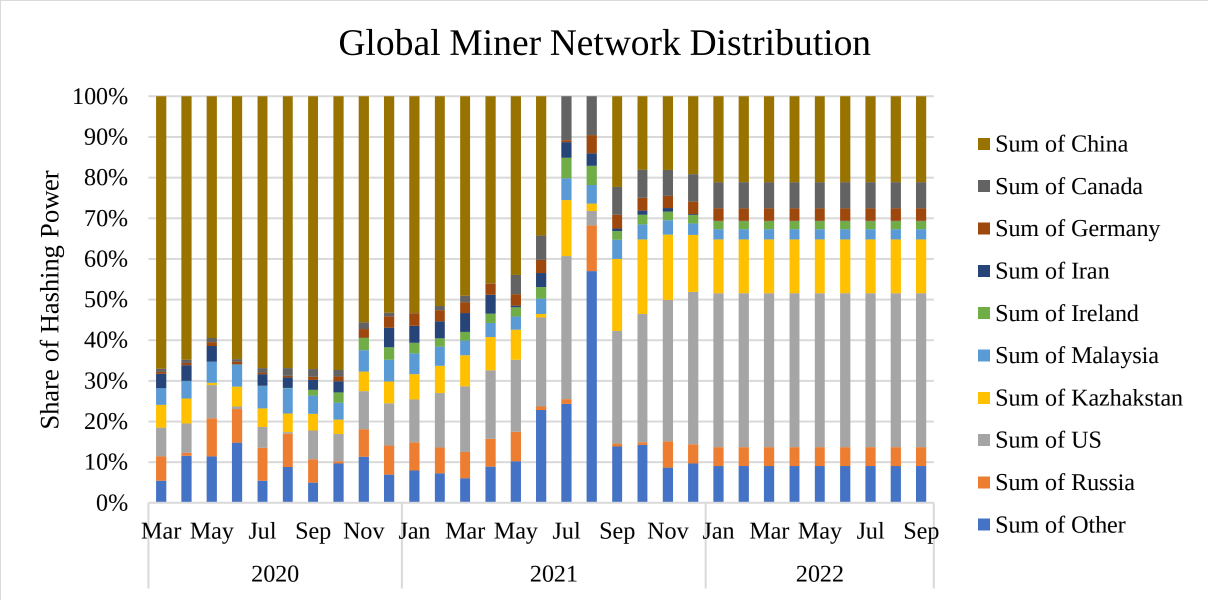
Year	Average Difficulty	% change with base 2019	&´% change with base 2009
2009	1.00	0.00000000001112	100
2010	1691.00	0.00000001879952	169100
2011	867884.00	0.00000964861021	86788400
2012	2125246.00	0.00002362720163	212524600
2013	166886101.00	0.00185533889120	16688610100
2014	18424730866.00	0.20483503138181	1842473086600
2015	54435310097.00	0.60517890508640	5443531009700
2016	204720474534.00	2.27595860860326	20472047453400
2017	828985623427.00	9.21616155072790	82898562342700
2018	4970320545967.00	55.25702233673020	497032054596700
2019	8994912023450.00	100.00000000000000	899491202345000
2020	16589561472466.00	184.43272629255900	1658956147246600
2021	20324906570246.00	225.96003737733500	2032490657024600
2022	29020745958005.00	322.63512841867800	2902074595800500

Figure 4: Bitcoin Network Total Hashrate and Forecast



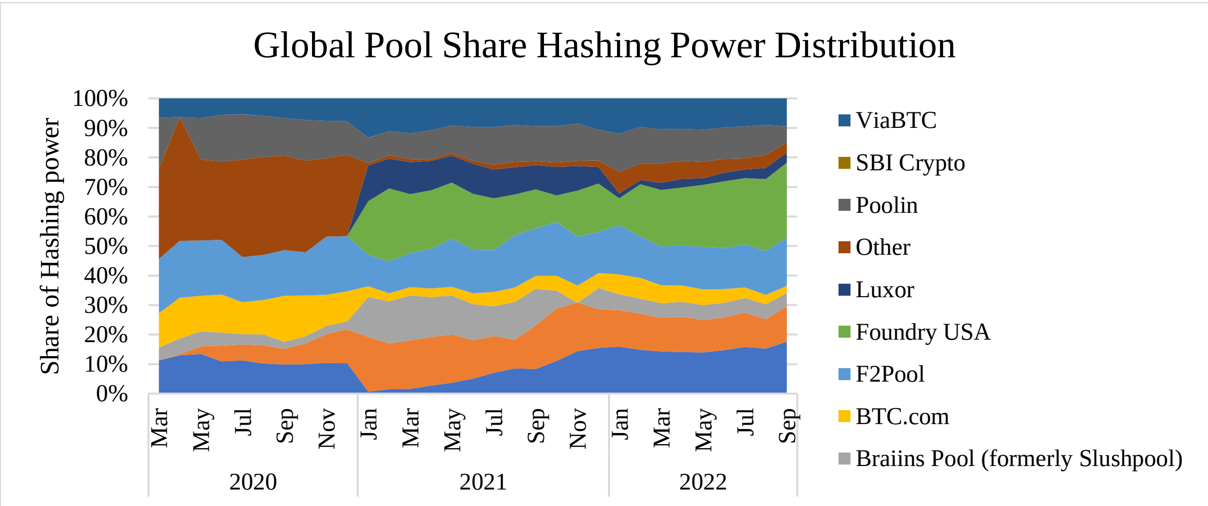
The Bitcoin Network Total Hashrate is a calculated numerical value that specifies an estimate of how many hashes are being generated by Bitcoin miners trying to solve the current Bitcoin block or any given block. It is represented in hashes per second.

Figure 5: Bitcoin Miner Network – Global Distribution of self-reported hashing power



Source: (Cambridge Centre for Alternative Finance, 2022b)

Figure 6: Bitcoin Miner Network - Pool Share



Data Source: (btc.com, 2022)

Table 4: Emission Reduction Targets

Reduction of damages to X% of coin price	Required EF [gCO2/kWh] at SCC 51 $/tCO2	Required reduction of CO2e/tkWh in %*	Required EF [gCO2/kWh] at SCC 202 $/tCO2	Required reduction of CO2e/tkWh in %*
25%	410.8	26%	103.7	81%
20%	328.6	41%	83	85%
15%	246.5	56%	62.2	89%
10%	164.3	71%	41.5	93%

Table 4 exemplifies the amount of necessary CO2e reductions given various assumptions on associated SCC over the sample period. * based on the current estimated EF of 557.8 CO2e/tkWh (de Vries et al., 2022), own calculation

Cost of Production Model (CPM) according to Hayes (2015, 2019)

<u>Assumptions and Input Variables:</u>

According to Hayes, the important decision variables for a miner are

a) The cost of electricity ($/kWH)
b) The energy consumption per unit of mining effort (J/GH or watts/GH/s)
c) The market price of Bitcoin (USD/BTC)
d) The current level of mining difficulty

These allow to determine the expected profit per day, as well as associated electricity costs.

I. $$BTC/day^* = \left[\frac{\beta\rho}{\delta 2^{32}} \div 3600\right] \cdot 24$$

II. $$E_{day} = p_e \cdot 24 \cdot \mu) \cdot (\frac{hash\ power\ in \frac{GH}{s}}{1000})$$

Where:

- β is the block reward
- ρ is the hashing power of equipment
- δ is the mining difficulty
- p_e is electricity price per kWh
- 3600 is number of seconds in an hour
- 24 the numbers of hours in a day
- 2^{32} is the probability of any single hash solving the PoW for a given block
- μ is energy efficiency of mining equipment

According to Hayes, the marginal product of mining should theoretically equal its marginal cost in a competitive market and in turn, equal its selling price. Since costs per day are expressed in $/day and mining production as BTC/Day, the USD/BTC represents the ratio of the two p^*. The price p^* serves as a theoretically lower bound for the market price, below which a miner would operate at marginal loss and therefore retract from The Mining Game. It is expressed as:

III. $$p^* = \frac{E_{day}}{BTC/day^*}$$

Empirical Analysis of CPM over the sample period

For our empirical calcilations, the following Assumptions are imposed:

- β stands constant at 6.25 BTC/block over the sample period
- p_e is electricity price per kWh and assumed to amount to 13.5 $/kWh in line with Hayes (2019)
- μ is the energy efficiency of mining equipment.

The estimations follow Jones et al (2021), which derive a non-linear relationship between calculated annual average rig efficiency from sales data between 2016-2018 and leading BTC mining equipment in 2021. The authors fit a declining but flattening rig energy usage per hash for their study period until 31.12.2021 as such:

$$efficiency\left(\frac{J}{GH}\right) = 1.3415 \cdot 10^{9} \exp\{-0.00054\, days\}$$

where days is the number of days since 1/1/1990. Data up until the end of 2021 is directly taken from the supplementary data of the authors, the remainder estimated energy efficiency curve is derived based on the above equation.

We collect data on the observed market price p_{btc} in USD/BTC and the network difficulty δ in Gigahashes per second using The Nasdaq Datalink, which is a reliable source for Bitcoin-data, from 01.03.2020 until 30.09.2022. The dataset has a total of 944 observations, collected at daily frequency. We analyze CPM at the time of difficulty adjustments, thus approximately every two weeks in STATA. When back-testing CPM over the sample period using a conventional OLS regression to obtain a proxy for model fit, which produces an $R^2 = 0.442$, indicating that 44% of the observed market price can be explained by CPM.

<u>*Output 1: OLS Regression Results*</u>

```
. reg mkt_price e_day btc_day

      Source |       SS           df       MS      Number of obs   =       944
-------------+----------------------------------   F(2, 941)       =    375.97
       Model |  1.2488e+11         2  6.2442e+10   Prob > F        =    0.0000
    Residual |  1.5628e+11       941   166082851   R-squared       =    0.4442
-------------+----------------------------------   Adj R-squared   =    0.4430
       Total |  2.8117e+11       943   298162537   Root MSE        =     12887

------------------------------------------------------------------------------
   mkt_price |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
       e_day |  -8.26e+09   3.65e+08   -22.59   0.000    -8.97e+09   -7.54e+09
     btc_day |   2.09e+13   2.93e+12     7.12   0.000     1.51e+13    2.66e+13
       _cons |   131253.5   3691.877    35.55   0.000     124008.2    138498.7
------------------------------------------------------------------------------
```

In line with Hayes (2019) a second OLS regression on the log transformation of each time series is performed, which results in an $R^2 = 0.599$, indicating that roughly 60% of the marginal change in market price can be explained by the change in marginal costs. This is not negligible, however smaller than the $R^2 = 0.969$ obtained by Hayes (2019) between June 2013 and March 2018.

Output 2: OLS Regression Results Log-Transformation

```
. reg log_mkt_price log_e_day log_btc_day

      Source |       SS           df       MS      Number of obs   =       944
-------------+----------------------------------   F(2, 941)       =    703.31
       Model |  267.425624         2  133.712812   Prob > F        =    0.0000
    Residual |  178.902866       941  .190119942   R-squared       =    0.5992
-------------+----------------------------------   Adj R-squared   =    0.5983
       Total |   446.32849       943  .473306988   Root MSE        =    .43603

------------------------------------------------------------------------------
log_mkt_pr~e |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
   log_e_day |  -5.740876   .1889625   -30.38   0.000    -6.111712   -5.370039
 log_btc_day |   .9266675   .0937424     9.89   0.000     .7426991    1.110636
       _cons |  -34.56992   1.357114   -25.47   0.000    -37.23323    -31.9066
------------------------------------------------------------------------------
```

In order to compare the two time-series directly, a multivariate vector autoregression (VAR) is constructed. VAR is a forecasting algorithm that can be used when two or more time series influence each other. It tests whether the relationship between the time series involved is bi-directional considering the two null hypotheses:

$H_0$1: The market price does not cause the model price

$H_0$2: The model price does not cause the market price

VAR models generalize univariate autoregressive models by allowing multivariate time series, where the current values of a model are explained by its lagged values. In essence they test whether changes in the marginal costs of Bitcoin production influence its price with lags and are a coherent and credible approach to predict economic variables.

The formal representation of our VAR(1) model with one lag in Matrix form is as such:

$$\begin{bmatrix} \mathrm{p}_t^{\mathrm{btc}} \\ \mathrm{p}_t^* \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} + \begin{bmatrix} b_{11} b_{12} \\ b_{21} b_{22} \end{bmatrix} \begin{bmatrix} \mathrm{p}_{t-1}^{\mathrm{btc}} \\ \mathrm{p}_{t-1}^* \end{bmatrix} + \begin{bmatrix} u_t \\ v_t \end{bmatrix}$$

The two time-series are represented with $\mathrm{p}_t^{\mathrm{btc}}$ being the market price and p_t^* the CPM model price. Since VAR Models require stationarity in the dependent and independent variables and errors to be i.i.d, meaning that u_t and v_t are white noise terms, we use the Dickey-Fuller and Phillips Peron test to test for unit roots. We find, y_t as well as x_t to be stationary in first difference.

Next, we identify the appropriate lag-length by comparing Akaike, Schwartz, and Hannan-Quinn criteria. It is important to choose lag-length appropriately to not miss-specify the model but also not waste degrees of freedom. Akaike, Schwartz, and Hannan-Quinn criteria all indicate to use 1 lag, thus, a VAR model with one lag is constructed.

Output 3: Lag order selection statistics

```
varsoc

 Selection-order criteria
 Sample:  3/4/2020 - 9/30/2022                 Number of obs      =       941
```

lag	LL	LR	df	p	FPE	AIC	HQIC	SBIC
0	-14708.1				1.3e+11	31.2648	31.2688	31.2751
1	-14675.9	64.375*	4	0.000	1.2e+11*	31.2049*	31.2167*	31.2358*
2	-14672	7.8766	4	0.096	1.2e+11	31.205	31.2247	31.2566

```
 Endogenous:  d_mkt_price d_cpm_price
  Exogenous:  _cons
```

The estimated VAR is only stable, if all inverse roots of the characteristic AR polynomial have modules less than one and lie inside the unit circle. The command varstable checks the eigenvalue stability condition after estimating the parameters of a vector autoregression.

Output 4: Stability condition

```
varstable

 Eigenvalue stability condition
```

Eigenvalue	Modulus
.1739026 + .2231648*i*	.282922
.1739026 - .2231648*i*	.282922
-.06394274 + .1259761*i*	.141275
-.06394274 - .1259761*i*	.141275

```
 All the eigenvalues lie inside the unit circle.
 VAR satisfies stability condition.
```

Next, we perform residual diagnostics to validate, that errors are homoscedastic, meaning i.i.d. and converge to 0 and test for autocorrelation at lag-order using a Lagrange-multiplier test. The residuals have a mean of 1.12e-06 and appear i.i.d. The Lagrange Multiplier test indicates no autocorrelation at lag order.

Output 5: Lagrange-Multiplier test

```
 Lagrange-multiplier test
```

lag	chi2	df	Prob > chi2
1	0.9780	4	0.91312
2	0.7466	4	0.94546

```
 H0: no autocorrelation at lag order
```

Given that VAR stability conditions are met, and residual diagnostics indicate a correct model-fit, we can perform a Granger causality test to test for our Hypothesis:

H_0: The CPM price does not cause the market price

H_1: The CPM price does not cause the market price

Output 6: Granger Causality Wald Test

```
. vargranger

  Granger causality Wald tests
```

Equation	Excluded	chi2	df	Prob > chi2
d_mkt_price	d_cpm_price	2.8513	2	0.240
d_mkt_price	ALL	2.8513	2	0.240
d_cpm_price	d_mkt_price	1.2489	2	0.536
d_cpm_price	ALL	1.2489	2	0.536

Based on the observed p-values we cannot reject H_0 or H_1. These results differ to Hayes (2019) who finds that H_1 can be rejected, subsequently claiming that the cost of production approach of Bitcoin is capable of explaining price developments in the Bitcoin market.

A Primer on Value Formation

Several techniques have been proposed to value cryptoasset network. Alabi (2017)Alabi (2017)Alabi (2017)Alabi (2017) suggested that the value of certain cryptoasset networks can be modelled using Metcalfe's Law. It states that the value of the network is proportional to the number of its nodes or end users. More concretely, the value of the network is proportional to the square of the nodes of the network. Let V be the network value (market capitalization) and N the number of nodes, then Metcalfe's Law can be formalized as: $V(N) = k \cdot N^2$. In reality new entrants into the network do not add value linearly, as the pair-wise mathematical connection suggest. Another network valuation method could therefore be based on Odlzyko's Law, formalized as $V(N) = k_o N_{log_e}(N)$. The growth rate of the network decreases when new members join because the most valuable links are likely to be formed early on. Unlike in Metcalfe's Law, which assumed homogeneity between the values added for each new node introduced to the network, the latter assumes diminishing returns for value for newer nodes.

Extended production model

We can model the representative profit of a miner by taking into consideration the real mechanics of Bitcoin production. Therefore let $\emptyset$ be the total number of hashes a miner network generates per second, 2^{32} refers to the protocol's set probability of finding the right hash, adjusted by difficulty δ. Let h represent the hours of running his equipment. In 1 hour, he can generate $60^2\emptyset$ hashes.

Thus, his expected number of blocks he can expect to find over h hours:

$$x_{btc}(h) = \frac{h60^2\emptyset}{\delta 2^{32}}$$

Let R be the reward in Bitcoins per block, which sell for p_{btc} on the open market, then his expected profit is:

$$E\pi(h) = \frac{p_{btc}R\emptyset h60^2}{\delta 2^{32}}$$

Which is linear in h, namely in the time of running his equipment.

Noting that the target blocktime is 10 minutes, or 600 second, the **optimal difficulty $\boldsymbol{\delta}$** in the network can be written as

$$\delta^* = \frac{600\emptyset 10^9}{2^{32}}$$

Whereby $\emptyset$ stands for the total hashing power of the network. In a symmetric market with n miners investing q, $\emptyset = nq$ entire

Substituting 1 and 2 in to our equation yields a break-even scenario of:

$$\frac{p_{btc}R\emptyset 10^9 h_i 60^2}{\delta 2^{32}} = \frac{\emptyset\zeta h_i}{1000}p_e$$

Break-even electricity price scenarios

Rearranging for the optimal price of electricity:

$$p_e^* = \frac{p_{btc}R\emptyset 10^9 60^2 1000}{\delta^* 2^{32}\emptyset\zeta}$$

Based on current market conditions, namely assuming that p_{btc}~\$20,000, $R = 6.25\frac{BTC}{block}$, $\zeta \sim \frac{0.046J}{GH}$ (BTC mining council), $\emptyset$ ~ 260,000,000,000 gigahashes per second currently deployed by the network, $\delta^* = 36321580410003.70$, then $p_e^* = 0.0627$ \$/kWh.

Ceteris paribus, only changing the market price for Bitcoin, break-even electricity prices can be estimated.

The following analysis indicate different break-even electricity-prices for various levels of market price and total hashrate contribution. The results illustrate how multilateral cooperation or an overall decline in total market size could re-establish or improve profitability in Bitcoin mining. Own calculation

Baseline Scenario:

Assumptions	**Value**
reward per block [BTC/block]	6.25
Hashing power of miner network [GigaHashes/second]	260000000000.00
energy efficiency of mining hardware [Joules/Gigahash]	0.0460
network difficulty	see Calculation 1
Bitcoin market price [USD/BTC]	20000.00
Calculation 1: optimal network difficulty δ*	36321580410003.70
Calculation 2: optimal electricity price for break-even pe*	$0.06271

Scenario Analysis 1: Changing Bitcoin prices at current network difficulty	
market price (USD/BTC)	pe* (USD/kWH)
10000	0.03135
15000	0.04703
20000	0.06271
25000	0.07839
30000	0.09406
35000	0.10974
40000	0.12542
45000	0.14110
50000	0.15677
55000	0.17245
60000	0.18813
65000	0.20380
70000	0.21948
75000	0.23516

Scenario 1: Total Network Hashrate Reduction by 25%

Assumptions	**Value**
reward per block [BTC/block]	6.25
Hashing power of miner network [Hashes/second]	195000000000.00
energy efficiency of mining hardware [Joules/Gigahash]	0.0460
network difficulty	see Calculation 1
Bitcoin market price [USD/BTC]	20000.00
Calculation 1: optimal network difficulty δ*	27241185307502.70
Calculation 2: optimal electricity price for break-even pe*	$0.0836

Scenario Analysis 1: Changing Bitcoin prices at current network difficulty	
market price (USD/BTC)	pe* (USD/kWH)
10000	0.04181
15000	0.06271
20000	0.08361
25000	0.10452
30000	0.12542
35000	0.14632
40000	0.16722
45000	0.18813
50000	0.20903
55000	0.22993
60000	0.25084
65000	0.27174
70000	0.29264
75000	0.31355

Scenario 2: Total Network Hashrate Reduction by 50%

Assumptions	**Value**
reward per block [BTC/block]	6.25
Hashing power of miner network [Hashes/second]	130000000000.00
energy efficiency of mining hardware [Joules/Gigahash]	0.0460
network difficulty	see Calculation 1
Bitcoin market price [USD/BTC]	20000.00
Calculation 1: optimal network difficulty δ*	18160790205001.80
Calculation 2: optimal electricity price for break-even pe*	$0.1254

Scenario Analysis 1: Changing Bitcoin prices at current network difficulty	
market price (USD/BTC)	pe* (USD/kWH)
10000	0.06271
15000	0.09406
20000	0.12542
25000	0.15677
30000	0.18813
35000	0.21948
40000	0.25084
45000	0.28219
50000	0.31355
55000	0.34490
60000	0.37625
65000	0.40761
70000	0.43896
75000	0.47032