Economic Modelling of the Bitcoin Mining Industry

Charles Bertucci∗ Louis Bertucci† Jean-Michel Lasry‡ Pierre-Louis Lions‡§

December 7, 2021

Abstract

We propose a parsimonious homogenous framework for analyzing the production industry of Bitcoin. Due to miners’ competition and the Bitcoin protocol transparency, computational power suppliers extract all the mining surplus and receive most of miners expenses. Despite a constant growth environment, the revenue per hashrate unit follows a mean reverting process. We quantify the stability and the strength of the bitcoin transactional system which is the public good created by the Bitcoin protocol. Empirically, our model fits the data well. In the long run, innovation spending, blockchain security and bitcoin energy consumption, are proportional to the miners reward.

Keywords: Blockchain ; Bitcoin ; Proof-of-work ; Mining Hardware ; Innovation

JEL Codes: C51, D41, L10

∗CMAP, Ecole Polytechnique, UMR 7641, 91120 Palaiseau, France
†Institut Louis Bachelier, 75002 Paris, France
‡Université Paris-Dauphine, PSL Research University,UMR 7534, CEREMADE, 75016 Paris, France
§Collège de France, 3 rue d’Ulm, 75005, Paris, France
1 Introduction

In April 2021, the market capitalisation of all cryptocurrencies reached $2 trillion for the first time, with Bitcoin representing around half of it. The production industry of Bitcoin, the miners, also in charge of maintaining the blockchain, have taken a significant economic weight. At time of writing, the revenue generated from mining the Bitcoin blockchain is around $16 billion per year. In economic terms, the bitcoin protocol creates both private goods (units of cryptocurrency) as well as a public good (the transactional system i.e. the blockchain), which support one another. A goal of this paper is to shed light on this interaction and show that it relies solely on a strong form of large population equilibrium which gives the Bitcoin blockchain a high stability and resilience.

Bitcoin is unlike any other industries, in many ways. First, all the production effort is devoted to creating, at a constant production rate, a single common good. Second, there are no barriers to entry or to exit, and the producers as well as the consumers cannot be constrained beside what the consensus protocol prescribes. Third, the quantity produced is constant regardless of the investment and spendings of producers, while the growth rate of the total revenue has been tremendous (around 65% per year for the past 5 years on average). Moreover, this high revenue has fuelled innovation on mining hardware, in a process close to Schumpeter’s creative destruction except users do not benefit from this high innovation rate.

The revenue sharing among producers is also quite unusual in an international competitive industry. The winning miner gets rewarded with newly created bitcoins and transaction fees. However, the protocol is designed in such a way that regardless of the number of miners searching for solutions, the block rate is, on average, constant over time. In other words, the number of newly produced bitcoins and of newly registered transactions is independent of the production of hashes. Miners are competing to get a share of the total revenue generated by the bitcoin blockchain, while this total revenue is independent of miners’ spendings and investment to produce more hashes. It is this fierce competition among miners that discourage potential

---

1The are 144 blocks mined per day and 6.25 bitcoins mined each block, so with a USD 50,000 bitcoin price, the value of all the bitcoin mined is USD 16.425 billion in annual terms.
2In other terms, the public good is here of high quality, which is crucial for representing value and for a currency in particular.
3We will come back later on what exactly is this single common good.
4There may exist local regulations but they can only be local and cannot affect the protocol itself. Also, the physical location of the miners does not matter for the quality or quantity of bitcoin production so miners always have the possibility to move to a country that has different local rules.
5Because more efficient mining hardwares can be used both to secure and to attack the blockchain, users do not benefit from this increased efficiency. Note that even if users had a preference for security, an upper security bound should exist at which users are indifferent to more security.
attackers from trying to step in this game thereby contributing to the quality of the public good, i.e. the transactional system.

All those characteristics make Bitcoin, and blockchains in general, the world’s largest real-life experiment of game theory for a continuum of players, the rules of the game being listed in the bitcoin blockchain protocol. The strength of the Bitcoin blockchain is that it is supported by a pure form of large population equilibrium, which makes it highly stable and resilient. Indeed, by opposition to an equilibrium resulting from a small number of players, large population equilibria are less affected by the particular behavior of some actors.

The contribution of this paper is threefold. First, based on facts and homogeneity assumptions and despite the high level of growth and volatility of the mining industry (both around 65% per year), we construct a recursive, time independent, parsimonious model of partial equilibrium. Second, we show that the model fits the data well. Note that the laboratory-like conditions of the mining industry provide extensive data to calibrate models. Furthermore, we explore the resulting joint dynamics of bitcoin value and hashrate, and more specifically we quantify the mean reversion of the revenue to hashrate ratio\(^6\). We also analyse the dynamics of this ratio after several shocks on the bitcoin price and how fast it converges to its long term value and study the mining cost structure associated to several shocks. Lastly, we focus on the three main consequences of our model. First, we analyse the consequence of the equilibrium hashrate dynamics on the security of the blockchain\(^7\). We find a linear relationship between the blockchain security and the bitcoin price. Then we show that the bitcoin miners energy consumption is also a linear function of the bitcoin price. And finally we quantify miners contribution to R&D spendings of hardware manufacturers. This investment is also proportional to the bitcoin price. Note that due to homogeneity assumptions we make, those three quantities of interest are impacted linearly by the bitcoin price in the long run.

The remaining of the introduction is devoted to explaining in more details the main mechanics and results of our paper, to discuss some of the most important assumptions together with a review of the literature, and to introduce the rest of the paper.

The bitcoin blockchain uses proof-of-work to generate consensus over the ordering of bitcoin blocks. With proof-of-work, miners are competing to brute-force the solution of a hash-based puzzle\(^8\). In the mining activity, there are only two factors of

\(^6\)To be more precise the ratio revenue to hashrate discounted at the rate of technological progress is mean reverting. We will explain this in more detail further.

\(^7\)Security is defined as resistance to external 51% attacks.

\(^8\)The puzzle consists in finding the pre-image of a cryptographic hash function that is designed to be resistant to pre-image attack. A cryptographic hash function is a one-way function that transforms a variable-length input into a fixed-length output (called a hash). The solution can only be found by trial-and-error, so miners must compute a lot of hashes before they find a block.
production, computing hardware and energy. Miners transform those two production factors into hashes. One specificity of the blockchain mining industry is that all hashes produced are identical regardless of when and how they were produced as well as who produced them. Miners are directly rewarded by the bitcoin protocol depending on the number of hashes produced, however the value they get per hash is a decreasing function of the total number of hashes produced.

Based on this simple description of the blockchain mining industry, we see that miners express very naturally a demand for mining hardware, and for an ever increasing efficiency (i.e. technical innovation). The total production, i.e. the number of hashes produced - also called the hashrate - can be observed on the blockchain. Moreover, because the incentives are well defined, and as there are no side-rewards that miners get from the mining activity, the demand function for innovation is a direct and explicit consequence of the bitcoin protocol. As a consequence, everyone is able to form expectations on the current and future demand of computing chips, including the chips manufacturers themselves. We would like to insist on this statement as this is very unique to blockchain. Moreover, together with the free entry and exit conditions, the decision is clearly on the computing chips manufacturers’ side. Miners are simply passive agents that are here to take a profit opportunity that anyone can see. In other terms, mining hardware manufacturers are able to extract all the surplus from miners through prices, and miners will make a zero expected profit.

Our model features a continuum of infinitely small miners. It has been documented that the bitcoin miners community is rather concentrated around a few big mining pools (e.g. Cong, He, and Li (2019)) but here we abstract from such concentration issues and consider a well diversified mining community. The important aspect is that we assume no returns of scale, as a consequence of the competitive environment. It is as if all miners were to be part of the same large mining pool.

9 Other costs like security cost or administrative cost can be neglected given the importance of electricity and hardware costs.
10 The hashes are then transformed into blocks and blocks generate bitcoins when they are created.
11 They differ however in cost depending on the efficiency of the mining hardware used. This is central to our model and will be detailed later.
12 In practice there are a number of reasons why all hashes are not valued equally. However, this is true under the perfect diversification assumption, that is that x% of the computing power yields x% of the blockchain revenue. This is an assumption that we make throughout the paper, and that will be discussed later.
13 To be more precise, it can be infer from the actual inter block time and the current difficulty of the hash-based puzzle.
14 The demand function for innovation is the flow of machines at a given efficiency level that miners want to buy.
15 In reality there might be some small returns of scale, due to efficient energy usage, security and administrative costs for big mining farms.
without additional governance issues.

The competition among miners framed by the proof-of-work consensus protocol can be described as a Mean Field Game (MFG hereafter). But as the goal of this paper is to present a framework as simple as possible, we will use only standard mathematical tools: namely our model will boil down to a one dimensional equilibrium equation (a PDE). Moreover, we will show that despite the lack of any possible definition of consumer surplus (as the production flow is kept constant by the protocol) this equilibrium is equivalent to a benevolent social planner problem. Such simplicity is the consequence of strong homogeneity assumptions which will prove to have a good fit to the data. With complementary objectives, we show in Bertucci, Bertucci, Lasry, and Lions (2020) how to deal with heterogeneities of the mining industry using the MFG machinery.

On a PoW blockchain, the miners’ total computational power is called the hashrate, and is expressed in hashes computed per second. This hashrate is directly linked to the security of the blockchain. Indeed, a straightforward attack scenario, referred to as a 51% attack, occurs when a malicious miner owning more hash power than the honest community of miners is able to grow the blockchain faster. This could lead to a double-spend thereby breaking consensus. The usual idea is that the higher the hashrate, the more expensive it is to own 51% of it, and the more secure the blockchain. However, the actual relationship between hashrate and security is more complex.

A key feature of our analysis is the assumption of a constant rate of technological progress for the mining machines. We denote by nominal hashrate the actual hashrate measured in hashes per second computed by the whole miners community, and we let the real hashrate be the hashrate discounted at the rate of technological progress. As a consequence of the constant rate of progress, the relevant metric when considering the computational power is the real hashrate. As machines become more efficient at transforming electricity into hashes, it becomes cheaper to rebuild a given constant nominal hashrate which translates to a decreasing real hashrate.

\footnote{Double spending refers to situation in which an agent is able to spend the same unit of money twice. An attacker with more hashrate than the rest of the network could in principle rewrite part of the chain and perform a double spending. For more information on 51% attacks see: Grunspan and Pérez-Marco (2018).

\footnote{In reality there are 2 types of 51% attacks: the internal and the external 51% attack. The external attack refers to a situation in which an external agent is able to build up more hash power than the current honest hashrate. The cost is therefore straightforward as the malicious miner would have to buy enough machine to reproduce at least the current hashrate. In the internal attack, existing miners collude such that they collectively own more hashrate than the community of honest miner. Since we do not consider collusion issues we are abstracting from the internal 51% attack and focus on the external ones for which the blockchain hashrate is an indication of security.

\footnote{While this may seem like a simplifying assumption we show that this is a fair approximation. See section 3.2.3.}
Throughout our paper, we will consider the real hashrate unless explicitly mentioned. The mining technology indeed became more efficient since the early days of mining, although the rate of progress was not constant. There were several major phases with structural breaks: CPU-mining, GPU-mining, FGPA-mining and ASIC-mining. However, since the start of our sample period (January 1st 2015), ASIC-mining has been dominant without any substantial structural breaks. We refer to Bendiksen and Bibbons (2019) for more details on the mining technology used on the bitcoin blockchain.

Our goal is to build a homogenous model for understanding the bitcoin hashrate. There is both a temporal and a spatial heterogeneity issue. We solve the spatial heterogeneity by simply assuming that miners have access to the exact same mining technology, and that the cost they pay for electricity is the same whatever their location. We refer the reader to Bertucci, Bertucci, Lasry, and Lions (2020) for a discussion on how to integrate population heterogeneity in this framework. Regarding temporal heterogeneity, the issue is that the quantities of interest tend to be non-stationary. Both the bitcoin price (hence the miners’ revenue) and the hashrate have increased substantially since the early days of bitcoin. To obtain a stationary model we specifically assume that both the miners revenue and the real hashrate grow at the same pace. We can then reconsider the whole model in terms of the revenue per mining unit, which is shown to vary around a long term average. This allows us to keep a stationary model, with the state variable being only the revenue per machine, even in the presence of an unbounded price process. All other things being equal, the higher the cryptocurrency price, the higher the profit and the higher the incentive to mine. However, in equilibrium miners decide to increase the hashrate at the same growth rate on average. On the one hand, the revenue per machine is constant on the long run. On the other hand, the hashrate reacts imperfectly to changes in mining reward due to the supply function of hardware manufacturers, therefore the revenue per machine follows a mean reverting process.

We define the blockchain security as the value of the real hashrate\footnote{For a technical view of the security of proof-of-work blockchains see Garay, Kiayias, and Leonardos (2015).}. As explained, in equilibrium the revenue per machine is constant on the long run. Moreover, in our model the only state variable is the revenue per machine and the value of one unit of real hashrate is an increasing function of the revenue per machine. So, the value of one machine is also constant in the long run. Therefore, the security of the blockchain increases with the real hashrate which in turn increases with the revenue from mining\footnote{It is important to note that in our model, we assume a constant bitcoin reward per block and the price of bitcoin to follow a random process. In reality, the supply of new bitcoins (i.e. the number of bitcoins created per block) is decreasing over time and at some point it will be zero.}. On the long run the value of one machine stays constant but as
the mining reward increases the number of mining machines increases, and therefore the security increases. In our homogenous setup, we show that this relationship is in fact linear, i.e. security grows linearly with the bitcoin price.

Given the above remarks, our empirical strategy goes as follows. We postulate a given form for the supply function of mining hardware, then we solve the game and numerically compute the value function. We then use the bitcoin blockchain public data (hashrate and total miners revenue) between January 1st 2015 and February 1st 2021 to calibrate the parameters of the supply function by selecting the ones that produce a hashrate dynamics that best matches the actual hashrate dynamics. All other parameters can be either estimated independently from the data (drift and variance of the random reward process) or are calibrated based on external data (electricity consumption and machine efficiency). To support our modelling choices we show that our model is able to explain around 63% of variations in the hashrate with a parsimonious model.

Due to homogeneity assumptions, the only state variable is the revenue per machine and we also study its equilibrium dynamics. First, we also provide further support for our calibration with Monte Carlo simulations and moments comparison for the distribution of the revenue per machine of which the first two moments are well represented by our model. Second, we provide impulse responses analysis after shocks of different sizes on the bitcoin price. We show that given the mining hardware manufacturers’ production constraints, it takes some time for a shock on the revenue per machine to resorb but it is faster the higher the shock. This supports the idea that the equilibrium resulting from Proof-of-Work is highly stable and reliable. We also study the mining cost allocation between hardware buying and electricity and show by opposition to the common conception, electricity costs only accounts for a small portion of the total mining costs. This proportion decreases with the size of the shock on the bitcoin price. This supports the idea that the critical aspects of mining is access to fast and efficient computing devices.

Our model allows us to analyze the dynamics of the bitcoin energy consumption. We show that, in equilibrium, the average energy consumption of bitcoin mining is linear in the bitcoin price. Moreover we show that our estimate of energy consumption based on a constant rate of technological progress is aligned with other estimates in the literature. In particular, it is consistent with the Cambridge Bitcoin Energy Consumption Index (CBECI) which estimates the energy consumption by gathering specific data on the energy efficiency of each mining hardware unit. This suggests that the constant rate of technological progress approximation is consistent at that time, the revenue of miners will only be composed of transaction fees. We leave to future research such an analysis.

\[\text{See } \text{http://cbeci.org}\text{ for more info.}\]
with actual data. We also show that the energy consumption is proportional to
the security of the blockchain. Our model allows us to quantify the intuitive result
that it is not possible to have a Proof-of-Work blockchain with high security and
low energy consumption.

Lastly we analyze miners contribution to technological progress. We show that
the revenue of the mining chips manufacturers is a linear function of the total miners
revenue on the long run. Once again, the total miners revenue (mostly driven by the
bitcoin price) drive linearly this quantity. This arises because the manufacturers’
revenue is also proportional to the energy consumption and the blockchain security.
If we assume that a constant part of the manufacturers’ revenue is invested in R&D
we get that R&D spendings are linearly affected by miners reward. So far, the bitcoin
price (hence the total miners reward) has increased exponentially, so have the R&D
spendings. However, this exponential increase in R&D seems to have produced a
constant rate of technological progress. This suggests that it is exponentially more
difficult to maintain a given rate of technological progress.

This paper builds on the growing blockchain literature. Since Nakamoto (2008),
blockchains have attracted more and more interest from academia (see for instance
Halaburda, Haeringer, Gans, and Gandal (2022) for a recent survey). Some papers,
like Biais, Bisiere, Bouvard, Casamatta, and Menkveld (2020), Schilling and Uhlig
(2019), Pagnotta and Buraschi (2018) and Pagnotta (2020) study the underlying
economics of bitcoin and analyze the implied valuation for cryptocurrencies. We
rather focus on the economics of the consensus algorithm and take the price of the
cryptocurrency as exogenous.

There is a literature studying frictions that can arise on a blockchain. Easley,
O’Hara, and Basu (2019) build a model for analysing the emergence of transaction
fees, and Huberman, Leskno, and Moallemi (2017) study the cost structure of a
blockchain based transactional system. Transaction fees do not play a great role in
our analysis and we only consider the total blockchain reward. As of early 2021,
transaction fees are a small proportion of the block reward. In the future, as the
supply of new coins will decrease, it is possible that transaction fees represent a
higher share of the block reward, our model is still expected to work well except
that an additional risk factor beside the price of cryptocurrency would have to be

\[22\] We also provide an analysis of the actual efficiency of each miners (with the CBECI data). The
constant rate of technological progress indeed seems to be a good approximation except for a couple
of structural break (introduction of GPU mining and ASIC mining with specialized hardware.
Those structural breaks are outside our sample period.

\[23\] There are of course other consensus algorithms of which the most promising is Proof-of-Stake
for which this claim is not valid. It raises however other concerns. See Saleh (2021) for an analysis
of Proof-of-Stake.

\[24\] Of course, this fact can be due to R&D fragmentation and/or delay in the research process but
the effect seems to be quite consistent over time suggesting that the costs for R&D development
are indeed convex.
introduced. Some authors have studied optimal contracting under mining pools in which miners gather to mitigate the risk of not finding a block (see for instance Schrijvers, Bonneau, Boneh, and Roughgarden (2016), Fisch, Pass, and Shelat (2017), and Cong, He, and Li (2019)). In general, they show how the mining industry will keep getting more centralized. Studying miners investment in R&D, Capponi, Olafsson, and Alsabah (2021) show that the mining industry will indeed tend to be centralized, but less than what might seem in the first place. By opposition to them, we explicitly model the computing chips manufacturers instead of having the miners themselves invest in R&D. With a MFG framework Li, Reppen, and Sircar (2019) also obtain a concentration result. While those questions are an important part of the economics of proof-of-work, we take a more general approach and focus on the fundamental mechanisms. By opposition to this literature, we assume miners are perfectly diversified (or equivalently focus on the long-run) such that a share of $x\%$ of the total hashrate yields $x\%$ of the reward. This is as if every single hash computed was remunerated to its marginal reward. Biais, Bisiere, Bouvard, and Casamatta (2019) study the game theoretic aspects of forks, showing that there are multiple Nash equilibria in which forks may exist. We analyze the mining game from the computational intensity point of view, and in our model there is a single chain miners can mine.

The proof-of-work consensus algorithm is inherently a Mean Field Game but we do not use the MFG literature here. We refer the interested reader to Bertucci, Bertucci, Lasry, and Lions (2020) for the presentation of a complete MFG framework that allows the study of several variations most notably with several populations of miners each facing different electricity prices.

With an analysis closely related to ours, Prat and Walter (2021) build a structural model to estimate the underlying unobserved parameters. Like us, they take a general approach and take miners as diversified risk neutral agents, and the share of the reward they get is strictly proportional to the hashrate they contribute. The main difference with our analysis is that they do not model the manufacturers market, so there is an infinite quantity of mining machine available in equilibrium. On the other hand, we assume that mining hardware manufacturers respond to variations in demand (i.e. revenue per machine) by adjusting their production capacities, so the available quantity of new hashrate is always finite and miners buy all the available quantity. While they calibrate the rate of technological progress, we use our structural model to calibrate the parameters of the supply function of mining hardware manufacturers given a rate of technological progress.

Our framework is flexible enough to allow for a number of risk factors although in this version there is only one risk factor, the cryptocurrency price (or total reward).
The remaining of the paper is organized as follows. Section 2 presents the homogenous model for bitcoin mining. Section 3 presents the data, the empirical strategy and the main results. Section 4 presents some implications of the findings and section 5 concludes.

2 A homogenous model of bitcoin mining

This section introduces a homogenous and parsimonious model for understanding the dynamics of the hashrate on a proof-of-work blockchain. Based on facts that have been presented in the introduction, we will add homogeneity and scale invariance assumption to introduce a homogenous, recursive and scale invariant model, despite the high level of growth and volatility.

Although, the model could be written as a usual social planer problem that goes back to Lucas-Prescott, the path we take is different as will be explained. This way of writing models can be used even when the model cannot be reduced to a social planer problem.

2.1 Nominal and real hashrate

We assume that time is continuous (indexed by $t$). Let $P_t$ be the hashrate measured in hashes computed per second by the whole miner community, at time $t$, that we denote by nominal hashrate\textsuperscript{26}. We let $\delta$ be the constant rate of technological progress of the mining machines. Because of R&D investment of machine manufacturers, new mining hardware can compute more hashes for a given electricity consumption, they are more efficient at transforming electricity into hashes. In other words, with technological progress it becomes cheaper to compute a given number of hashes. The key insight is that we need to consider the progress-adjusted hashrate, which we call the real hashrate, and denote by $K_t$. Both the nominal and the real hashrate are continuous variables, and we have

$$K_t := e^{-\delta t} P_t. \quad (1)$$

The real hashrate is the nominal hashrate deflated by the rate of technological progress. In other words, it is the number of current machines needed to rebuild the entire hashrate. Changes in the real hashrate represent variations in the hashrate not related to the technological progress. The hashrate is often said to represent the security of the blockchain, however the technological progress must be taken into account. We argue that the real hashrate is a lot more relevant when assessing the

\textsuperscript{26}The term nominal, by opposition to the term real, has to be understood in the economical rather than physical sense.
security of the underlying blockchain. We will extend the discussion about security in section 4.1.

### 2.2 Mining revenue dynamics

Miners continuously buys machines to compute hashes. The mining game works as follows. There is a fix number of coins output by the blockchain per unit of time, the reward, and miners compete against each other to get a share of this reward. The share they get is proportional to their relative share of the total computational power.

The random cryptocurrency price will play an important role in miners decisions.\(^{27}\) We define the process \(\{R_t\}_{t \geq 0}\) to represent the instantaneous miners reward. We assume that this process follows a Geometric Brownian Motion, that is

\[
\frac{dR_t}{R_t} = \alpha dt + \sigma dW_t
\]

where \(\alpha > 0, \sigma > 0\) and \((W_t)_{t \geq 0}\) is a standard brownian motion on a probability space \((\Omega, \mathcal{A}, \mathbb{P})\). Note that the actual blockchain reward is composed of newly created coins as well as transaction fees. Here, we model the sum as following the random process \((2)\).

As we will see in section 3.2.1, the actual growth rate of the mining revenue has been quite high at around \(\alpha \approx 0.652\) over the last 5 years. Throughout the paper we make the assumption that this expected growth rate of the mining revenue is constant. Therefore our model could be understood as a transitory model. Indeed, it is not realistic that the mining revenue will keep growing at such a rate.\(^{28}\) On the other hand, this constant growth rate assumption is still relevant in this model as miners’ time horizon is quite short. Indeed, due to the high technological rate of progress, as well as the high cost of capital (that would be introduced in the next section), miners have a time horizon of about a couple of years.\(^{29}\) On such a short horizon, miners can expect the total revenue to keep growing at the same constant growth rate. We leave for future research the study a model in which \(\alpha\) is a decreasing function of time.

---

\(^{27}\)While we express all values in traditional fiat currency, we could also have denominated everything in cryptocurrency, in which case the cost of computing hashes would have random.

\(^{28}\)If the Bitcoin price keeps growing at such a rate, in 9 years the market capitalisation of Bitcoin would be higher than the world GDP (USD 84 T).

\(^{29}\)See section 3.2.3 and section 3.2.2 for calibration of those parameters and the discussion on miners’ horizon.
2.3 Investment in machines: demand and supply function

Let $u$ be the value of one unit of real hashrate. By value, we mean the discounted sum of expected profits generated by one unit of real hashrate. We assume there are no barriers to entry or to exit in the mining market, however there is a limited quantity of mining devices available in equilibrium. The free entry condition means that there will always be someone ready to buy the mining devices available on the market as long as its price is below $u$, and conversely no machine will be sold if their price is higher than $u$. The demand is perfectly elastic and the price of the mining devices has to be $u$. On the other side of this market, we have mining hardware manufacturers that face a cost for producing mining devices and are represented by a supply function, $Q(p)$.

As previously stated, we make homogeneity assumptions on the supply function of mining hardware. We assume space homogeneity, that is the mining hardware is at the same price for all miners regardless of their location. We also assume time homogeneity, as a scale invariance assumption: we assume mining hardware manufacturers develop as the demand increase, and that this scale upgrade happens at the simplest way, that is by homothety. One of the simplest supply function that satisfies those homogeneity properties is given by $Q(K, p) = K\lambda(p - \bar{p})$, with $(\lambda, \bar{p}) \in \mathbb{R}^2$, and this is the one we chose.

We assume that the price of the mining devices is always given by $p = u$. The underlying assumption, which is key in our analysis, is that the mining hardware are able to extract all the surplus from the mining activity. Indeed, Bitcoin mining is a very specific industry in the sense that all the incentives, the reward and the cost are completely defined from within the protocol itself\textsuperscript{30}. Miners do not possess any idiosyncratic technology that make them more efficient than others miners. Therefore anyone, including mining hardware manufacturers, can derive and solve miner’s optimization problem. In other terms, miners’ demand for mining devices comes from the Bitcoin protocol, so hardware manufacturers know that miners would demand an infinite quantity if the price was $p < u$ and demand no quantity if the price was $p > u$. This is why the price in equilibrium must be $p = u$, and we have that in equilibrium a quantity $Q(u)$ is available on the market for mining devices.

$$Q(u) = \lambda K(u - \bar{p}) \quad (3)$$

Note that the parameter $\lambda$ is the elasticity of the supply function with respect to the price. For simplicity we assume that miners can decrease the quantity of real hashrate they provide but they can do so only with the exact same constraint.

\textsuperscript{30}To be more precise, the only parameter that is defined from outside the protocol itself is the price of electricity, but it is fairly easy to make assumptions on its value.
In practice, miners only reduce the hashrate when the bitcoin price (hence their revenue) drops significantly. We assume that scaling down, like scaling up, is costly for them. Another argument could be that they are averse to scaling down because of the scale-up cost. Indeed, if they scale down in response to a shock on the price they might miss an opportunity if the price quickly recovers.\footnote{As a simplification, our model assumes that the mining chips are always up and running. Being able to switch them off does not change the equilibrium quantity as in equilibrium all machines are running (the stopped machines would not be replace). However, it does change the dynamics.}

In addition to that, because of the technological progress, the real hashrate continuously depreciates at rate $\delta$. Therefore, we have the following dynamics for the real hashrate:

\[
\frac{\dot{K}}{K} = -\delta + \lambda (u - p)
\] (4)

### 2.4 The value function and the equilibrium equation

We now need to understand the value of one unit of real hashrate $u$. On the one hand, the total revenue from mining is shared among all miners and as $K$ is the real hashrate, one unit of real hashrate yields $R/K$ in revenue. An important assumption is that miners are perfectly diversified. The actual blockchain reward is paid out in discrete time and there is always the risk of not finding a block because of bad luck. A relatively small miner would get lump sum payment once in a while and he would have to be able to sustain the mining cost in the meantime.\footnote{The average inter-block time on the Bitcoin blockchain is 10 minutes, which yields 52,560 blocks per year. This means that a miner with 0.01% of the hashrate would only get about 5/6 block rewards per year, with potentially long series without reward. To hedge this risk, miners use mining pools, in which they share the computational power and the reward. In our model all happens like if all miners use a large mining pool, although we do not consider the associated risks and issues of mining pools. For more details see e.g. Fisch, Pass, and Shelat (2017).}

On the other hand, miners must pay a cost $c$ for running one unit of real hashrate. Because of the technological progress, the number of hashes that can be computed with the same amount of energy increases, therefore the cost of running the real hashrate is constant over time. Note that as the machine gets older the energy consumption required to provide one unit of real hashrate increases. This creates some heterogeneity between machines. We do not take this into account and instead assume that the cost $c$ is the average electricity cost during the lifetime of the machine. Without this assumption we would need to keep track of the number of machine of each generation, and because machines continuously arrive on the market, we would have a problem with infinite dimension. We leave such analysis for future research.

We assumed that the cost of capital for miners is $r$.\footnote{In section 3.2.2 we will see that this cost of capital is relatively high as it encompasses all other risks including the risk of a structural change in the revenue dynamics.} Therefore the value function
The value of one unit of real hashrate is given by
\[
u(K, R) := \mathbb{E} \left[ \int_0^\infty e^{-(r+\delta)t} \left( \frac{R_t}{K_t} - c \right) dt \right], \tag{5}
\]
where \((K_t)_{t} \text{ and } (R_t)_{t}\) are the process satisfying
\[
\begin{align*}
  dK_t &= [-\delta K_t + \lambda (u(K_t, R_t) - p) K_t] dt, \\
  dR_t &= \alpha R_t dt + \sigma R_t dW_t, \\
  K_0 &= K, \\
  R_0 &= R.
\end{align*}
\tag{6}
\]

Here we use a standard no arbitrage argument to write the equilibrium equation. The value of one unit of real hashrate at time \(t\) is the value at time \(t + dt\) plus the profit generated during this period, that is
\[
u(K_t, R_t) = \mathbb{E} \left[ e^{-(r+\delta)t} u(K_{t+dt}, R_{t+dt}) + \left( \frac{R_t}{K_t} - c \right) dt \right]. \tag{7}
\]

Using Ito's Lemma on the revenue random process and the assumed dynamics of the hashrate, \(K\), we obtain the following equilibrium equation of which the solution is the value function \(u\)
\[
0 = -(r + \delta) u + (-\delta + \lambda (u - \overline{p})) K \partial_K u + \alpha R \partial_R u + \nu R^2 \partial^2_{RR} u + \frac{R}{K} - c \text{ in } [0, \infty) \times \mathbb{R},
\tag{8}
\]
with \(\nu = \frac{\sigma^2}{2}\).

### 2.5 Scale invariance

Before we fit this equation to the data we need to make a couple of changes. Based on our assumptions, the value function becomes homogenous of degree 0, i.e. \(\forall c \in \mathbb{R}, u(cK, cR) = u(K, R)\). We can then introduce a new function \(v(\cdot)\) such that \(u(K, R) = U(1, \frac{R}{K}) = v(\frac{R}{K})\). This allows us to keep the idea of a stationary model for the agents, that is the behavior of the unitary producer only depends on the average return per machine, \(\frac{R}{K}\), and a producer of size \(Q\) behaves like \(Q\) producers of size 1.

We now reduce the number of variables by using the function \(v(\frac{R}{K}) = u(1, \frac{R}{K})\). With \(x = \frac{R}{K}\), the equilibrium equation associated to this new \(v\) function is then
\[
0 = -(r + \delta)v(x) - xv'(x) (-\delta + \lambda (v(x) - \overline{p}) - \alpha) + \nu x^2 v''(x) + x - c \text{ in } \mathbb{R}. \tag{9}
\]

We then introduce a new variable \(z = \ln(x) = \ln(\frac{R}{K})\), and the associated value
function $\tilde{v}(\ln(R)) = v(R)$. The equilibrium master equation becomes

$$0 = -(r + \delta)\tilde{v}(z) - \tilde{v}'(z)(-\delta + \lambda(\tilde{v}(z) - \bar{p}) - \alpha + \nu) + \nu\tilde{v}''(z) + e^z - c \text{ in } \mathbb{R}. \quad (10)$$

### 2.6 Benevolent planer equation

As we can see, the equilibrium equation (10) is the derivative of a standard Hamilton-Jacobi-Bellman equation. With $U'(z) = \tilde{v}(z)$, we can integrate equation (10) and obtain the following HJB equation

$$0 = -(r + \delta)U(z) + U'(z)(\delta + \alpha - \nu) + \nu U''(z) - \frac{\lambda}{2}(U'(z) - \bar{p})^2 + e^z - c \text{ in } \mathbb{R}. \quad (11)$$

This is the main equation of our paper. Before looking for numerical solutions we present the following theorem.

**Theorem 2.1.** There exists a unique solution of equation (11).

**Proof.** As the proof of this Theorem is at the same time rather standard and tedious, we only sketch it here.

First of all, let us state that, if this has not been for the fact that the equation is set on the whole $\mathbb{R}$, equation (11) would fall under the classical theory of quasi-linear elliptic equation with a comparison principle. This can be observed since the sign of the terms in front of the second order derivative and the function itself are of constant and opposite signs. Thus should equation (11) be set on an interval with usual boundary conditions, existence and uniqueness of a solution is standard.

The fact that this result can be extended to the whole $\mathbb{R}$ is a consequence of the property that (11) has to characterize the behavior of its solutions at $\pm \infty$. Indeed, a solution of (11) necessary grows like $e^z$ at $+\infty$ and like $c(r + \delta)^{-1}|z|$ at $-\infty$.

To conclude the proof, one has then to adapt the usual proof for equations in an interval, by replacing the boundary conditions by the knowledge of the behavior of the solution at $\pm \infty$. $\square$

To fit the parameters to the data, we need to solve numerically the equation satisfied by the value function. The value of one unit of real hashrate is computed by solving the HJB equation (11). To recover the value function $u$, the solution to HJB $U$ has to be differentiated and essentially all the transformation and dimension reduction steps should be reversed.$^{34}$

$^{34}$ To solve the HJB equation, we restrict our attention on a subdomain $z \in (z_{\min}, z_{\max})$, where $z_{\min}$ and $z_{\max}$ are two real numbers. We impose a Neumann condition at both boundaries. This condition means that the value $z$ is reflected at the boundary. If the bounds $z_{\min}$ and $z_{\max}$ are far enough from reasonable values for $z$ then this condition do not really affect the important range of the value function. To solve (11), with the Neumann boundary conditions, we use a standard Godunov’s scheme to discretize the HJB equation and a Newton’s method to solve it numerically.
We are indeed in a traditional setup with a standard HJB equation. What might be surprising is the path we took. We started from the no arbitrage equilibrium equation written on a single unit of real hashrate, from which we derived the equation associated to the social planner. We argue that this is a general approach useful to solve problem for which the HJB is not a priori obvious. In this specific case, the equilibrium equation was indeed easier to write than the HJB of the social planner.

The fact that we can take the integral of the equilibrium equation written on a single unit of real hashrate means that the solution can be written as the solution of an optimal control problem, the one of the social planer. The equation (11) is the HJB equation of the following optimal control problem

\[
\min_{(a_t)_t} \mathbb{E} \int_0^{+\infty} e^{-(r+\delta)t} \left[ e^{z_t} - cz_t + \bar{p}^2 \frac{\lambda}{2} + \frac{a_t^2}{2\lambda} \right] dt,
\]

\[
dz_t = \left( \alpha + \delta - \frac{\sigma^2}{2} + \lambda \bar{p} \right) dt + a_t dt + \sigma dW_t.
\]

which can be rewritten as

\[
\min_{(a_t)_t} \mathbb{E} \int_0^{+\infty} e^{-(r+\delta)t} \left( f(z_t) + \frac{a_t^2}{2\lambda} \right) dt,
\]

\[
dz_t = (c_0 + a_t)dt + \sigma dW_t.
\]

with \( f(z) = e^z - cz + \frac{\lambda \bar{p}^2}{2} \) and \( c_0 = \alpha + \delta - \frac{\sigma^2}{2} + \lambda \bar{p} \). Note that the class \( A \) of the possible controls is \( A = C^0(\mathbb{R}) \) (where \( C^0(\mathbb{R}) \) is the set of continuous functions on \( \mathbb{R} \)), i.e. closed-loop controls that are processes of the form

\[
a_t = a(z_t).
\]

Recall that \( z_t = \ln(\frac{R_t}{K_t}) \), but as the miners total revenue is taken as exogenous and given by (2), we can rewrite this program as an optimal control problem for the value \( K \). We replace the control of \( z_t \) by \( a_t \) with the control of \( K_t \) by \( b_t \). More precisely we have

\[
dz_t = \frac{dR_t}{R_t} - \frac{dK_t}{K_t},
\]

\[
dz_t = \alpha dt + \sigma dW_t - \frac{dK_t}{K_t}.
\]

As written in (13), recall that \( z_t \) is defined by

\[
dz_t = (c_0 + a_t)dt + \sigma dW_t.
\]
from which we deduce

\[
\frac{dK_t}{K_t} = (\alpha - c_0 - a_t)dt. \tag{17}
\]

We let \((b_t)_{t \geq 0}\) be defined as \(b_t = \alpha - c_0 - a_t\). We can now rewrite the optimal control problem as

\[
\min_{(b_t)} E \int_0^{+\infty} e^{-(r+\delta)t} \left( g(K_t, R_t) + \frac{(b_t - \alpha)^2}{2\lambda} \right) dt,
\]

\[
\frac{dR_t}{R_t} = \alpha dt + \sigma dW_t,
\]

\[
\frac{dK_t}{K_t} = b_t dt \tag{18}
\]

with \(g(K, R) = f(\ln(\frac{R}{K})) = \frac{R}{K} - c \cdot \ln(\frac{R}{K}) + \frac{\lambda R}{2}\). This is a control problem in which the state of system is \((K_t, R_t)\) and in which we seek any closed-loop optimal controls of the form \(b_t = b(\frac{R_t}{K_t})\). If we open for all possible closed-loop controls \(\beta(K_t, R_t)\), it won’t change anything because the optimal control is of the form \(\beta(K_t, R_t) = b(\frac{R_t}{K_t})\). The benefit of (18) is that it really shows that the social planner problem is to manage the size of the flow of the real hashrate.

This shows that the competitive equilibrium of miners is equivalent to the solution of the social planner optimal control problem. This is a result of the type Lucas-Prescott : the social planner minimizes the producers’ surplus. The context here is original in three ways. First, the goal is to control the dynamics of the production capacity \(K\). Second, this control happens in a situation in which the miners total revenue increases at a constant expected rate \(\alpha\). Lastly, the demand of the consumers is very special as they are indifferent to the quantity produced (regardless of the quantity of hash produced the total revenue is the same). It is therefore very interesting that the equivalence between a competitive equilibrium and the social planner problem holds despite the previous remarks.

By opposition to Lucas Jr and Prescott (1971), we can’t write the surplus of the consumer for this industry. This is due to the very specifics of Bitcoin mining, that is that miners always get the same surplus regardless of the price they pay for hardware. On the other hand, the program (18) is equivalent to a social planner that would minimize the producer surplus.

Given that, we find that it is easier to explicitly write the problem in term of the equilibrium equation and then to transform it into an optimal control problem than trying to guess the optimal control problem of the social planner.
3 Data, Calibration and Analysis

This section describes the data used and details the calibration procedure. It also analyses the solution and its equilibrium behavior.

3.1 Data

We use publicly available data on the Bitcoin blockchain. To estimate our model we require the hashrate and the total revenue from mining. Both are publicly observable directly on the blockchain[18], however we take this data from the public website http://blockchain.com. An alternative could have been to download the blockchain and estimate those quantities ourselves.

3.1.1 The Bitcoin hashrate

The hashrate represents the number of hashes per second that are collectively computed by miners. From January 1st 2015 to February 1st 2021, we have 1 data point every 3 days which makes 741 points. Figure 1 represents those data points, and table 1 presents some descriptive statistics on the hashrate. Note that this corresponds to the nominal hashrate, \((H_t)_t\), we will see in section 3.2 how to transform this series into the real hashrate, \((K_t)_t\).

3.1.2 The Bitcoin total mining reward

The total miners revenue in bitcoin can be directly observed on the blockchain. For each block, the total revenue is composed of the (deterministic) newly created bitcoins in addition to the sum of the transaction fees of all transactions included in that block. Both of those information can be read directly from the blockchain itself.

From January 1st 2015 to February 1st 2021, we have 1 data point every 3 days which makes 741 points. This corresponds to the series \((R_t)_t\). Figure 2 represents those data points, and table 1 presents some descriptive statistics on miners revenue.

<table>
<thead>
<tr>
<th>Hashrate (in (10^{10}) h/s)</th>
<th>count</th>
<th>mean</th>
<th>stdev</th>
<th>min</th>
<th>25th</th>
<th>50th</th>
<th>75th</th>
<th>max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>741</td>
<td>38.948</td>
<td>45.294</td>
<td>0.289</td>
<td>1.491</td>
<td>8.56</td>
<td>43.123</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Miners revenue (in mUSD)</th>
<th>count</th>
<th>mean</th>
<th>stdev</th>
<th>min</th>
<th>25th</th>
<th>50th</th>
<th>75th</th>
<th>max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>741</td>
<td>9.345</td>
<td>8.381</td>
<td>0.945</td>
<td>1.66</td>
<td>8.56</td>
<td>43.123</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Descriptive Statistics for the Bitcoin Hashrate and miners revenue between January 1st 2015 and February 1st 2021

\[\text{Note that the hashrate actually needs to be estimated from the block difficulty and the actual inter-block time. We don’t detail the full procedure here, but it is fairly standard.}\]
3.2 Calibration of the exogenous parameters

We first discuss the calibration of the parameters of the diffusion process of the miners revenue, $\alpha$ and $\sigma$, as well as the other parameters $\delta$ and $c$. Then, in section 3.3, we detail the calibration of the remaining parameters, those associated with the mining chips manufacturers’ supply function.

3.2.1 Calibration of the revenue dynamics parameters

As the parameters of the diffusion process of the total miners revenue are independent of everything else, we can estimate them separately. Based on the assumed dynamics for the miners revenue process (6), we estimate the drift and the deviation parameters using a standard maximum likelihood method. Under the log-normality assumption, we have that $\sigma$ is the standard deviation of the log returns of the series $(R_t)_t$, and the drift parameter is given by $\alpha = \overline{\mu} + \frac{1}{2} \sigma^2$, where $\overline{\mu}$ is the empirical average log return. The results of this estimation are presented in table 2. As expected the miners revenue, being heavily correlated with the bitcoin price, is very volatile, with a standard deviation of 68%. On the other hand the average return over the period is also quite high at 65%. Those values seem like reasonable expectations that miners can form about the diffusion process of their revenue.
Figure 2: Daily total revenue (in mUSD) from the bitcoin blockchain between January 1st 2015 and February 1st 2021

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Estimation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha$</td>
<td>Drift</td>
<td>0.652</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>Diffusion</td>
<td>0.679</td>
</tr>
</tbody>
</table>

Table 2: Parameter calibration of the total miners revenue process

3.2.2 Cost of capital

The model also features the rate at which agents discount time, $r$, that we take equal to 20%. As a risky activity, a cost of capital for the miners at $r = 20\%$ seems reasonable. In the model, only the sum of this discount rate and the rate of technological progress matters. Moreover, as the technological progress is quite high, the precise value of the cost of capital $r$ is not critical. Note that there can be some heterogeneity in the cost of capital, once again as the technological progress is high compare to the cost of capital, this will not be critical.

As mentioned in section 2.2, our model has to be a transitory model due to the assumption that the growth rate of the miners revenue is constant. Let us mention here that a high discount rate could also encompass a small probability of the revenue growth rate to suddenly drops. To avoid making assumption on the crash probability, we do not provide more details here and simply sum up this risk
in the the 20% discount rate.

3.2.3 Calibration of the technological progress

We then turn to the $\delta$ parameter, the rate of technological progress. We will take this rate of technological progress as exogenous and constant. For its calibration we rely on previous studies. Bendiksen and Bibbons (2019) measure the efficiency of different specialized machines based on their shipping date. Based on their data, we estimate a rate of technological progress of 0.57. The issue is that they cannot know how much machines are available for each level of efficiency, so this is more like the maximum rate of technological progress. The Cambridge Bitcoin Energy Consumption Index (CBECI) have a similar dataset of several mining hardware units with their associated efficiency and shipping dates. We present the efficiency data from CBECI in figure 3. We fit an exponential function to this dataset and we estimate an average rate of technological progress of 0.383. This rate has to be taken carefully as it represents the average efficiency increase of all machines, not only the most efficient hardware. It is therefore likely to undervalue the actual rate of technological progress whereas Bendiksen and Bibbons (2019) seem to be more conservative on the hardware included in their dataset.

On the other hand, Moore’s law (doubling every two years) yields a rate of technological progress of 0.35. It makes sense that the actual rate of technological progress is higher than Moore’s law given the high incentives to innovate provided by the high demand.

Given all those information, we choose a rate of technological progress of 0.42 which stands in between Moore’s law, the mean efficiency increase estimated by Bendiksen and Bibbons (2019) and the estimation based on CBECI data.

For comparison, Prat and Walter (2021), in a study very similar to ours, estimate the rate of technological progress to be 0.76. They essentially estimate a version of our model in which the elasticity of the mining hardware manufacturers’ supply function is infinite. This means that there are no constraint to the available quantity in equilibrium and miners increase the hashrate whenever it is profitable to do so.

Table 3 presents a summary of the calibration value for the rate of technological progress. In the following, we made all the calculations with $\delta = 0.42$.

Note that, as mentioned in section 2.2, the combination of a high rate of tech-

---

36 This maximum rate could be undervalued if the miners manufacturers were to keep the most efficient miners for proprietary mining, but to the best of our knowledge no such a behavior is documented.
37 At the time of writing, the CBECI data on efficiency are available at http://sha256.cbeci.org.
38 We refer the reader to Bertucci, Bertucci, Lasry, and Lions (2020) for more details on how to integrate an infinitely elastic supply function in our framework.
Table 3: Calibration of the rate of technological progress $\delta$

<table>
<thead>
<tr>
<th>Paper</th>
<th>Method</th>
<th>Value of $\delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moore’s law</td>
<td>-</td>
<td>0.35</td>
</tr>
<tr>
<td>CBECI data</td>
<td>intrinsic characteristics</td>
<td>0.38</td>
</tr>
<tr>
<td>Bendiksen and Bibbons (2019)</td>
<td>intrinsic characteristics</td>
<td>0.57</td>
</tr>
<tr>
<td>Prat and Walter (2021)</td>
<td>estimation from blockchain data</td>
<td>0.76</td>
</tr>
<tr>
<td>Our paper</td>
<td>-</td>
<td>0.42</td>
</tr>
</tbody>
</table>

Table 3: Calibration of the rate of technological progress $\delta$

nological progress ($\delta = 0.42$) as well as a high cost of capital ($r = 0.2$), makes the time horizon a miners quite short. Indeed, miners discount time at rate $\delta + r$, so their horizon does not exceed a couple of years.

### 3.2.4 Hashrate normalization

We now discuss the calibration of the normalization parameter for the real hashrate, and present some associated descriptive statistics. In section 3.1.1, we presented the data for the nominal hashrate, which was defined by $(H_t)_t$, that is the actual number of hashes per second produced by the bitcoin blockchain. In this paper, we consider the real hashrate expressed in number of most efficient machines, $(K_t)_t$. In other words, $K_t$ is the number of machines that require 1kW of energy, with the best efficiency available at time $t$, needed to rebuild the entire hashrate. The real hashrate is the deflated actual hashrate, that we normalized by a constant to make sure we are measuring the number of machines that consumes 1kW so that figures
are more meaningful. Let’s consider the Antminer S19, one of the most efficient mining hardware as of early 2021, manufactured by Bitmain which is one of the largest mining hardware manufacturers. We see on figure 3 that the Antminer S19 is indeed among the most efficient miners since 2020. The Antminer S19 produces around 95TH/s for a power of 3250 W. Therefore, we assume the normalization factor to be $95/3.25 = 29.23$. Figure 4 presents the series $\{K_t\}_t$. To compute this series, we assume that all machines running at the time of the last data available in our dataset (February 1st 2021) are Antminers S19. We then run backward the constant rate of technological progress to compute the number of time $t$ machines needed to rebuild the entire hashrate.

![Figure 4: Real Hashrate $K_t$, with a rate of technological progress $\delta = 0.42$, between January 1st 2015 and February 1st 2021 - unit is discounted hashes per second](image)

### 3.2.5 Comments on the revenue per machine - $R/K$

In this paper, we present a homogenous model in which both the total miners revenue and the real hashrate grow at a constant rate. As this allows us to write the whole model in terms of the average revenue per machine, $\frac{R}{K}$, we now present this series. Figure 5 presents the plot of this quantity over time. The huge peak corresponds to when the price of bitcoin increased rapidly to around 20,000 USD/BTC at the end of 2017. We can see that the ratio $\frac{R}{K}$ tends to decrease a little over our sample
period. We interpret this as being due to more competition in the mining industry. However, it is important to keep in mind that in our model the ratio $\frac{R}{K}$ has a constant long term value. Indeed, on the long run, if the miners revenue increases, this will increase the profitability for mining, which will in turn incentivize miners to increase the real hashrate, and bring the ratio $\frac{R}{K}$ down to its long term target. Figure 6 presents the time series of the growth rate of the real hashrate. The average value for the growth rate of the real hashrate is 0.61, which is quite close to the estimated value of the miners revenue growth, we see however an extremely high volatility. Table 4 extends table 1 to include statistics about the real hashrate dynamics and the annualized revenue per machine.

![Figure 5: Annual revenue in USD per machines of 1kW, between January 1st 2015 and February 1st 2021](image)

3.2.6 Cost of electricity

Lastly, we calibrate the cost of electricity $c$. The analysis in this section is performed on an annual basis. Moreover, as explained above, the reference mining hardware is the machines that consumes 1kW of power at the current efficiency level, that is at time $t$. The assumption made is that with the same amount of electricity consumed, a more recent machine will be able to produce more hashes per second, so the cost

\[39\] We explore this statement in section 3.4.
of electricity in our model, \( c \), is constant. As previously stated, this constant cost of electricity \( c \) is the average over the lifetime of the machine. Therefore, the cost \( c \) represents the average annual cost of 1kW of power. Of course, different miners will have access to different electricity prices, which will be a huge determinant of their incentives to mine and their profit. We assume an average electricity price of 0.04 USD/kWh, which yields \( c = 350 \).

We have detailed the calibration of the main models parameters. Table 5 summarizes the selected values. In the next section we explain how we can use the data to calibrate the remaining parameters that are associated to the supply function of the mining hardware manufacturers.

### 3.3 Calibration of the supply function

So far the parameters have been exogenously calibrated. We now use the model to calibrate the supply function.

The goal is to estimate the parameters of the supply function for the mining hardware, which are the only two parameters that couldn’t be calibrated exogenously. Recall that, in equilibrium, this supply function is assumed to be like \( \bar{\lambda} \). We will pick \( (\lambda, \bar{p}) \) such that the model prediction best fit the real hashrate data. We
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r$</td>
<td>Opportunity cost of capital</td>
<td>0.2</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Drift of the miners revenue process</td>
<td>0.652</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>Volatility of the miners revenue process</td>
<td>0.679</td>
</tr>
<tr>
<td>$\delta$</td>
<td>Rate of technological progress</td>
<td>0.42</td>
</tr>
<tr>
<td>$c$</td>
<td>Average annual cost of electricity for a 1kW machine</td>
<td>350</td>
</tr>
</tbody>
</table>

Table 5: Summary of parameters calibration

denote by $\gamma_t$ the function that represents the difference between the actual change in the real hashrate and the one expected by the model, which corresponds to the model error at time $t$. We have

$$
\gamma_t(\lambda, \bar{p}) = \frac{\dot{K}_t}{K_t} + \delta - \lambda \left[ v_{\lambda, \bar{p}} \left( \frac{R_t}{K_t} \right) - \bar{p} \right]
$$

(19)

where $v_{\lambda, \bar{p}}$ is the function $v()$ as defined in (9) parametrized by $\lambda$ and $\bar{p}$. In other words, if the model was perfect, $\gamma_t$ would be equal to zero for each time $t$. Therefore, we pick the parameters $(\lambda, \bar{p})$ that minimize the $L^2$ norm of $\gamma_t$, that is

$$(\lambda^*, \bar{p}^*) = \arg\min_{\lambda, \bar{p}} \int_{t_1}^{t_2} (\gamma_t(\lambda, \bar{p}))^2 dt.$$

(20)

with $t_1$ and $t_2$ the start and the end of our sample period respectively. We then use a gradient descent optimization method to minimize the discretization of (20). We replace $\gamma_t$ by the discrete approximation $\Gamma$,

$$
\Gamma(t, \lambda, \bar{p}) = \frac{K_{t+\tau} - K_t}{K_t} + \delta - \lambda \left[ v_{\lambda, \bar{p}} \left( \frac{R_t}{K_t} \right) - \bar{p} \right],
$$

(21)

and we have

$$(\lambda^*, \bar{p}^*) = \arg\min_{\lambda, \bar{p}} \sum_t \Gamma(t, \lambda, \bar{p})^2,$$

(22)
where $\tau$ is a positive integer that represents the lag at which our model can predict the future hashrate. Indeed, in practice there are a number of logistic and financial considerations that can make the hashrate not immediately sensitive to variations in the miners revenue. In the following we take $\tau = 30$ which corresponds to a 3-month lag.

Recall that in order to get the value of $v$, we solve numerically for $U$ using the associated HJB equation (11), and then we take the derivative of the solution and apply all the transformations presented in section 2 to get back the value of $v$.

Table 6 presents the main result. We find that the values that best matches the data are $(\lambda, p) = (7 \times 10^{-4}, 775)$. With those values the correlation between the actual real hashrate and the prediction by the model is 0.629. Figure 7 presents the graph of those two quantities over time. With those values for $(\lambda, p)$, we can compute the value function $v_{\lambda, p}$, the solution of the master equation (9). Figure 8 presents this value function $v_{\lambda, p}(x)$ with $x = \frac{R}{K}$ for $x \in [400, 8100]$, as well as the histogram of the observed values of $x$ within our data sample. Within this sample, we can see that $v$ is not far from a linear approximation. However, the convexity is in the region of interest that is for low values of $x$.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda$</td>
<td>$7 \times 10^{-4}$</td>
</tr>
<tr>
<td>$p$</td>
<td>775</td>
</tr>
<tr>
<td>Correlation between</td>
<td>0.629</td>
</tr>
<tr>
<td>actual real hashrate and</td>
<td></td>
</tr>
<tr>
<td>prediction by the model</td>
<td></td>
</tr>
</tbody>
</table>

Table 6: Main results from the model with parameters $(\alpha, \sigma, \delta, c) = (0.652, 0.679, 0.42, 350)$

Note that our model do not take into account the halving in the number of coins created per block. In practice, every 210,000 blocks - roughly 4 years - the number of new coins is divided by two, which translates to an almost division by two of the miners revenue\(^{40}\). During our sample period, there were 2 halvings, on July 9th 2016 and on May 11th 2020\(^{41}\). Those events tend to decrease the real hashrate, which might cause a discrepancy from our model that does not take this into account. To see this effect, we have added vertical lines on figure 7 on the halving dates\(^{42}\). We can see that within those time windows, the actual real hashrate growth rate decreases while our model fails to predict this drop. Moreover, the real hashrate is now lower that what the model would expect so it actually predicts an increase in

---

\(^{40}\)This is due to the fact that newly created bitcoins constitute the major portion of the total miners revenue as transaction costs are still relatively low.

\(^{41}\)The first halving happened on November 28th 2012, outside of our sample period.

\(^{42}\)There are two lines because we have estimated the growth rate of the real hashrate over a 3-month period, so the halving effect starts to show up on the real hashrate growth data series 3 months before the actual date.
Figure 7: Comparison between the actual annualized real hashrate growth rate (blue) and the model prediction (orange); Second halving (July 9th, 2016) in red and third halving (May 11th, 2020) in green.

the real hashrate growth during this exact time. We leave for future research the introduction of the halving in the model.

In figure 7, we can also see that our model does not pick up well decreases in the real hashrate growth rate. This is a direct consequence of the fact that we do not give miners the ability to turn off their mining devices. In our model, after a sudden drop in the total revenue, miners discard mining devices at rate \( \lambda(v(x) - \bar{p}) \), instead of turning them off. Therefore our model cannot pick up sharp decrease in the real hashrate. On the other hand, if the bitcoin price recover after a sharp decrease, miners would not necessarily buy new machines but simply turn back on the mining devices that were previously turned off. Therefore our model would catch back the real hashrate when all mining devices are turned back on. For instance, we see that on figure 7 the low point in the fall of 2018 was not picked up by our model but because this sharp decrease in only temporary, our model can recover accurate values afterwards.

Recall that the \((\lambda, \bar{p})\) parameters are components of the producers’ supply function and therefore of the quantity of mining hardware available in equilibrium. When for instance the value of one unit of real hashrate is USD 2,000, it means that the net investment rate is \( \lambda(2000 - \bar{p}) = 7 \times 10^{-4} \times 1.225 \times 10^3 = 85.7\% \). To emphasize this point, figure 9 presents a graph of the miners investment rate in real hashrate as a function of the revenue per machine. From (4), the miners investment rate \( j_i \) is
Figure 8: Value function $v(x)$ resulting from the model (left-scale / orange / USD) and histogram of the observations of $x$ (right-scale / blue) for $x = \frac{R}{K}$ defined as

$$j_t = \frac{\dot{K}}{K} + \delta = \lambda (U_t - \bar{p}).$$

The miners investment rate is higher than the rate of technological progress for a value of the revenue per machine around $x = 765$. Above this value, the miners investment rate produce an increase in the real hashrate, while below this value miners do not invest more than the rate of technological progress and the real hashrate decreases overall.

### 3.4 Equilibrium dynamics and validation through Monte Carlo simulations

In this section we investigate a complementary fit of our model to the data through a moments matching technique.

Our model predicts that the revenue per machine, $\frac{R}{K}$, has a constant long term expected value. It will give a precise quantification to an obvious mechanism: when the revenue per machine is too low, mining is not so profitable, investment decreases and the real hashrate $K$ tends to decrease, while when the revenue per machine is very high, mining is highly profitable, investment increases and the real hashrate $K$
Figure 9: Miners investment rate as a function of the revenue per 1kW-machine tends to increase. Indeed, our model gives a precise equation for this mean reversion.

We consider here the log of the revenue per machine, \( z = \ln \left( \frac{R}{K} \right) \). From (10), we have that the dynamics of \( z_t \) is given by the following

\[
\frac{dz_t}{dt} = (\delta - \lambda(\tilde{v}(z) - \bar{p}) + \alpha - \nu) dt + \sigma dW_t. \tag{24}
\]

Replacing \( \tilde{v} \) in equation (24) by its linear approximation, we see that \( (z_t)_t \) is a mean reverting process. As the function \( \tilde{v} \) is almost linear in the observed range of values of \( z_t \), the dynamic of \( z_t \) is approximately an Ornstein-Uhlenbeck mean reversion process around the equilibrium value \( z^* \) defined by

\[
\delta - \lambda(\tilde{v}(z^*) - \bar{p}) + \alpha - \nu = 0. \tag{25}
\]

For an Ornstein-Uhlenbeck process, the equilibrium \( z^* \) is also the long run mean value. As \( \tilde{v} \) is close to linear in the range of fluctuations of (24), it is still true for (24) that the equilibrium \( z^* \) is also almost equal to the long run mean value.\(^{43}\)

As it is possible to explore this mean reversion by simulating trajectories for the revenue per machine, \( \frac{R}{K} \), using (24) and the value of the function \( \tilde{v} \), we can compute the distribution of states \( (z_t)_t \) and the associated distributions of other variables like the revenue per machine. We can then compare the moments of these distributions.

\(^{43}\)The small bias between an Ornstein-Uhlenbeck process and our slightly non-linear diffusion process (24) is illustrated by the histogram of figure 10: an Ornstein-Uhlenbeck process would generate a Gaussian while our process generates a lightly asymmetric gaussian-like distribution.
to the moments of the observed data. This gives a complementary check of the fit of our model to the observed data.

We use the values of the parameters that we calibrated in the previous sections. With (24) we simulate 10,000 trajectories over 100 years. To remove the dependance to the initial condition, we only take into account the values for the last 80 years of each simulated trajectory. With 100 points for each year, this is a total of 8,000,000 simulated data points. Figure 10 presents the distribution of the simulations of the log of the revenue per machine, while figure 11 presents the distribution of the actual values for the log of the revenue per machine. It is important to keep in mind that we simulated a total of 1,000,000 years of trajectories while our data sample cover only about 6 years. This greatly explains why the histogram of the simulated data is so smooth compared to the actual data. We see qualitatively that the distributions are quite close. Table 7 presents a comparison of the first few moments of each distribution: the simulations and the actual values.

![Figure 10: Distribution of the simulated values of the log of the revenue per machine](image)

There are a few remarks to make. First, as can be seen on figure 11, the actual distribution of $z$ is clearly truncated for low values. This is due to the fact that in practice, miners can simply turn off their machines if the revenue per machine decreases too much. This implies a minimum value for $z$ that corresponds to a no profit condition. This model does not take that effect into account so when...
the miners revenue drops to low values, $K$ will also drop due mainly to machine’s depreciation, the rate of technological progress, but at a lower pace than when miners can turn off their machines. Second, we have obviously a lot more data points in the simulation than in the actual data. Moreover, a number of different assumptions like the log-normality of the increment of the miners revenue process may not particularly hold in practice.

With those remarks in mind, we can see in table 7 that the mean and the variance of the actual distribution are close to the ones predicted by our model. However, higher order moments do not really match and would require additional assumptions in our model. To help better understand how the theoretical moments of the distribution of the revenue per machine varies across all trajectories, we present in figure 12 the distribution of the mean and the moments up to order 4.

### Table 7: Comparison of the log of the revenue per machine: Actual values VS Simulated values

<table>
<thead>
<tr>
<th></th>
<th>Actual $z$</th>
<th>Simulated $z$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>7.43</td>
<td>7.19</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>0.31</td>
<td>0.3252</td>
</tr>
<tr>
<td>3rd moment</td>
<td>0.068</td>
<td>-0.136</td>
</tr>
<tr>
<td>4th moment</td>
<td>0.25</td>
<td>0.5851</td>
</tr>
</tbody>
</table>

Figure 11: Distribution of the actual values of the log of the revenue per machine.
across all trajectories. The red lines corresponds to moments from the actual data. To account for the fact that our data sample only covers about 6 years, we also use 6 years to compute each moment. This corresponds to 130,000 data points for each moment. This shows that our model can in some cases, be very close the actual data. The first two moments are quite close to the actual mean and variance in the data. We also see that our model does not explain well higher order moments.

![Figure 12: Distribution of the moments of \((z_t)\) per trajectory; red lines correspond to values for the actual distribution.](image)

### 3.5 Equilibrium responses to shocks on the bitcoin price

The previous analysis has shown that despite the high observed volatility the revenue per machine has a long run target equilibrium value. Indeed, although the miners’ revenue volatility moves the revenue per machine around, economic forces resulting from the mining game keep pushing the revenue per machine toward a long term target. This section further improves this analysis and show how the revenue per machine responds to shocks on the mining reward.

With the set of parameters considered in this analysis, as presented in table (5), we can use (25) to compute the log of the long run target value for the revenue per machine \(z^* = 7.2813\), which gives a revenue per machine of USD 1,453.
To study the speed of convergence of the revenue per machine in response to a shock we remove noise in (24), by setting $dW_t = 0$ for all $t$, and compute the associated dynamics after several shocks\footnote{Indeed, the deterministic part is what is explained by our model, therefore to really understand what is going on, we remove the noise.}. Figure 13 presents the dynamics of the revenue per machine after 3 shocks of $1\sigma$, $2\sigma$ and $4\sigma$, with $\sigma$ the diffusion parameter in (24). This figure also presents the half-life of shocks, that is how long it takes for the revenue per machine to be half-way to the long term target value. With a half-life between 5 and 8 months, shocks take some time to resorb. This is entirely due to the constraint of the mining hardware manufacturers, and in particular comes from the supply function on the mining hardware market.

![Figure 13: Dynamics of the revenue per machine after a shock on the Bitcoin price (without noise)](image)

As can be seen on figure 13, the half-life varies quite a bit depending on the size of the shock. To further study this relationship, figure 14 presents the half-life of a shock as a function of the initial value of the revenue per machine (i.e. the size of the shock). Large shocks can have a half-life around 4 months while it can take up to 10 months for small shocks.

In economic terms, a sharp increase in the bitcoin price creates profitable mining opportunities that can last for several months due to constraints on how much mining power is available in equilibrium. An arbitrage opportunity only exists for a miner
(or a mining hardware manufacturer) that would have access to efficient mining hardware, while regular miners simply wait for mining hardware to be produced and sold, which takes some time due to industrial constraints.

There is an important remark to make at this point. If the model was linear (i.e. the value function was linear), the half-life would be the same regardless of the size of the shock. We have shown that the model is slightly non-linear and it turns out that the non-linearity decreases the half-life for high shocks (up to 38% shorter between a $4\sigma$ and a $1\sigma$ shock).

To further study this non-linearity, we compute the miners’ investment in mining hardware, denoted by $\Lambda(x_t)$ with $x_t = \frac{R_t}{K_t}$. Based on equation (23), we have that

$$\Lambda(x_t) = j_t K_t U_t = \lambda (U(x_t) - \bar{p}) K_t U(x_t). \tag{26}$$

Table 8 presents the miners’ investment after several shock on the bitcoin price, which is defined as $\int_0^{1Y} \Lambda(\frac{R_t}{K_t}) dt$ for different $R_0$. We see that the non-linearity in the value function yields an increase in the mining hardware investment that is more than proportional to the increase in the bitcoin price. If the bitcoin price goes to USD 120k from USD 40k, this corresponds to a 4-quarterly-standard-deviation increase. In this table, we see that if the bitcoin/USD price doubles from USD 40k to USD 80k, this corresponds to USD 50b being invested on the year following
this price increase. With approximately 18 million bitcoins in circulation, a USD 40k bitcoin price corresponds to a market capitalisation of USD 720b. Therefore those USD 50b invested in mining hardware represents around 7% of the increase in market capitalisation that is invested in mining hardware by miners.

<table>
<thead>
<tr>
<th>Bitcoin/USD Price after the shock</th>
<th>Miners’ investment in hardware (for first year in USD b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>40,000 (no shock)</td>
<td>21.17</td>
</tr>
<tr>
<td>60,000</td>
<td>35.4</td>
</tr>
<tr>
<td>80,000</td>
<td>50.05</td>
</tr>
<tr>
<td>100,000</td>
<td>65.01</td>
</tr>
<tr>
<td>120,000</td>
<td>80.13</td>
</tr>
</tbody>
</table>

Table 8: Miners’ total investment in mining hardware for the year following several shocks and an initial Bitcoin/USD price of 40,000

There are a couple of remarks to make. First, we do not study the impulse response to a downside shock on the revenue per machine as our model does not include the ability for miners to switch off their computers. As mentioned in section 3.4, in the case of a drop in the bitcoin price, miners would simply turn off their machine when it is not profitable for them to do so, and the hashrate will adjust much quicker. Second, the fact that the real hashrate converges faster to its long term target value for larger shocks should also be interpreted in terms of high security. Indeed, this supports the idea that the equilibrium resulting from miners’ interactions is strong and resilient to perturbation. Section 4.1 extends the discussion about security.

3.6 Analysis of the mining costs

Our model and calibration also allows to shed light on a common misconception which is that the major cost to mining is electricity. It turns out that investment in mining hardware is a lot larger than electricity spendings.

Table 9 presents the blockchain revenue as well as the electricity cost and the investment in mining hardware for different initial value of the bitcoin price. As in the previous section, we do not consider the noise, and we set \( dW_t = 0 \) for all \( t \). Different initial bitcoin prices can be interpreted as shocks, there are meant to give a better understanding of the underlying dynamics. The investment in mining hardware is defined, as in section 3.5, by \( \int_0^Y \Lambda(\frac{f_t}{K_t})dt \) while the electricity spending is defined by \( \int_0^Y cK_t dt \).

Even in the absence of shocks (the first line of table 9), we can see that the total electricity spendings represent only around 21% of the total miners investment.

---

45This is directly linked with analysis of section 3.5 except we consider here the repartition between hardware investment and electricity.
<table>
<thead>
<tr>
<th>Bitcoin/USD Price after the shock</th>
<th>Hardware investment (for first year in USD b)</th>
<th>Electricity spendings</th>
<th>Total Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>40,000 (no shock)</td>
<td>21.17</td>
<td>4.46</td>
<td>18.51</td>
</tr>
<tr>
<td>60,000</td>
<td>35.4</td>
<td>5.14</td>
<td>27.77</td>
</tr>
<tr>
<td>80,000</td>
<td>50.05</td>
<td>5.77</td>
<td>37.02</td>
</tr>
<tr>
<td>100,000</td>
<td>65.01</td>
<td>6.34</td>
<td>46.28</td>
</tr>
<tr>
<td>120,000</td>
<td>80.13</td>
<td>6.9</td>
<td>55.54</td>
</tr>
</tbody>
</table>

Table 9: Mining costs for one year following an increase in the bitcoin price with an initial bitcoin/USD price of USD 40,000

over the same period. The incentives in the bitcoin protocol are defined in such a way that miners are racing to obtain the most efficient mining hardware. Moreover, a central assumption to our model is that the mining hardware manufacturers are able to extract all the value from the mining activity. In fact in equilibrium, the price is such that they are indifferent between buying new hardware and not mining at all. If we assume that the electricity cost is an incompressible cost, all the surplus from mining (after electricity spendings) will be transferred to the hardware manufacturers through the miners’ investment.

This effect is even more striking when we consider variation in the miners’ revenue (i.e. the bitcoin price). When the bitcoin price jumps, this creates a profitable mining opportunity that will be fully extracted by hardware manufacturers who would increase the quantity they produce as well as the price at which they sell the mining machines. Indeed, the revenue per machine increases which affects the price of machines right away (recall that in equilibrium $p = U$). This also increases the quantity available in equilibrium but with some lag due to the elasticity of the supply function, represented by $\lambda$. Then as more machines are being produced, the real hashrate increases and the revenue per machine decreases which decreases the price of each machine. Moreover, because the quantity available in equilibrium is proportional to the current stock of real hashrate, the overall effect is that the miners’ investment increases. However, in the meantime, the electricity cost is directly proportional to the real hashrate in place, therefore it increases at a slower pace and the ratio of total electricity spendings to total miners’ investment in mining hardware decreases. This effect is illustrated by figure 15 which presents how the hashrate and the miners’ investment in mining hardware evolve after shocks of several sizes. The left panel presents the real hashrate which first increases more for larger shocks but its growth rate will decrease over time to reach the long term target of the growth rate. The electricity cost is directly proportional to this real hashrate. The right panel of figure 15 presents the miners’ daily total investment. We can see than the daily total miners’ investment jumps due the price effect, whereas the real hashrate (on the left panel) of which the electricity price is proportional does not
Table 9 also presents the total revenue that miners get from the blockchain over the same period (one year). It may seem surprising that the miners’ revenue is lower than even just the hardware investment over the same period (without even taking into account the electricity cost). However, this is not how miners’ profit would be computed. In fact, because miners transfer all the surplus to mining hardware manufacturers, they pay the mining hardware exactly the discounted value of the future profits so they make a zero expected profit on each machine. However, they are continuously buying new machines to remain competitive so they are constantly spending more than what they receive over a given period. Our model does not take into account any liquidity constraint for the miners and we assume that they would find a way to finance mining hardware investment. We leave for future research the introduction of liquidity constraints in our framework.

4 Implications of the model

In this section we analyze our model’s implications in terms of: i) blockchain security, ii) mining energy consumption, and iii) mining hardware manufacturers R&D expenses. In our model, all of them are indeed intrinsically linked and the miners revenue positively drives them all. Our model provides a dynamic view on the evolution of those quantities. As such, it would be delicate to make predictions because they would strongly rely on assumptions on the miners revenue evolution,
i.e. the bitcoin price. For an analysis of the limit case, when the expected growth rate of miners revenue is $\alpha = 0$ see appendix [6.1].

4.1 The blockchain security

In this model the security of the underlying blockchain is directly linked to the long term average value of the revenue per machine. Recall that the value function $v(x)$ (with $x = \frac{R}{K}$) is the value of the reference machine that consumes 1kW of energy, which corresponds to the price at which miners will be ready to buy it. More precisely, the demand will be infinite if the price of the unitary machine was lower than this value. We define the security as being the total value of the real hashrate in place at a given point in time,$^{46}$ Formally, at any given time $t$, the security of the blockchain is given by $K_t v(\frac{R_t}{K_t})$.

Recall that in this homogenous model, the real hashrate is expected to grow at the same expected growth rate as the miners total revenue. To make this clearer we can multiply and divide by the total revenue and we get that the long term total value of mining machines, i.e. the security, denoted by $\xi$, is given by

$$\xi = \xi(R_t) = \frac{v(x^*)}{x^*} R_t$$  \hspace{1cm} (27)

Therefore the security of the underlying blockchain will grow with the total miners revenue. Also because, the miners total revenue is directly linked to the price of bitcoin, we have that the security of the blockchain is proportional to the price of bitcoin.$^{47}$ This is an intuitive idea but our model allows us to study the sensitivity of the security to changes in the miners revenue, i.e. the bitcoin price.

The security of the blockchain is therefore a function of the long term value of the unitary machine, as well as the long term average of the revenue per machine.

Let’s measure those quantities. First, from the dynamics of $z = \ln(\frac{R}{K})$, as expressed in (24), we can obtain the equilibrium long term value of the reference machine. By definition, the long term value of the reference machine is given by

$$v(x^*) = \frac{\delta + \alpha - \sigma^2}{\lambda} + \overline{p} \approx 1977.$$  \hspace{1cm} (28)

Second, from this we can deduce the long term target of $x = \frac{R}{K}$, denoted by $x^*$. We have that $x^*$ is uniquely defined by (28). We can inverse (either graphically or

---

$^{46}$This is directly linked to outside 51% attacks. Indeed, performing an external 51% attack would require to buy at the very least the hashrate in place. Therefore the higher the price of each machine, the higher the cost of a 51% attack. Even considering selfish mining (see Eyal and Sirer (2014)) does not change the analysis as there is still a threshold that an attacker must control, even if it is lower than 50%.

$^{47}$See Ciaian, Kancs, and Rajcaniova (2021) for similar results.
through a simple optimization procedure) the value function $v(x)$ to get the target value for the revenue per machine. We obtain

$$x^* = 1451.$$  \hfill (29)

We therefore have that the long term security is given by

$$\xi(R_t) = \frac{v(x^*)}{x^*} R_t \approx 1.3628 \times R_t.$$  \hfill (30)

Conveniently, the proportionality constant in the value of the long term security is also the long term price of the reference machine, $v(x^*)$, divided by the long term value of the revenue per machine, $x^*$. Recall that this revenue per machine, $x = \frac{R}{K}$, is not the actual revenue generated by a machine over its lifetime but rather the annualized instantaneous revenue per machine for one reference machine that consumes 1kW of energy.

It could be tempted to study the sensitivity of the security with respect to model’s parameters like $\delta$, $\alpha$, $\sigma$, $\lambda$ or $p$ but recall that the parameters $\lambda$ and $p$ are determined from the data and the other parameters. It is therefore not a straightforward analysis and it requires more assumptions, for instance on the cost function of the mining chips manufacturers.

### 4.2 Energy consumption

The debate on bitcoin mining energy consumption is intense. One reason for this is the fact that the bitcoin energy consumption is quite easy to get. As we have explained throughout this paper, the hashrate can be observed directly on the blockchain and with proper assumptions on the rate of technological progress, it is possible to measure the real hashrate, that is the number of reference machines, i.e. machines that consume 1kW of energy\textsuperscript{48}. As previously mentioned, figure 4 presents this series. Each of these machines consumes 1kW of energy, so assuming they are always running, this is equivalent to an annualized electricity consumption of 8,766 kWh each\textsuperscript{49}.

The Cambridge Bitcoin Electricity Consumption Index (CBECI) presents an estimation of Bitcoin miners energy consumption\textsuperscript{50}. The methodology is to construct three time series: theoretical upper and lower bounds as well as an educated guess about the actual energy consumption. The lower bound assumes all miners run on

\textsuperscript{48}As already explained, to be more precise, the hashrate can be inferred from the current mining difficulty and the actual inter-block time. We do not detail this method here as there are little debate on the method itself.

\textsuperscript{49}This is by considering 24 hours a day and 365.25 days a year.

\textsuperscript{50}This index is available at \url{https://cbeci.org}.
the most efficient hardware technology. The upper bound estimate assumes that all miners run the lowest efficient hardware technology that is still profitable. By opposition to our methodology, their rely on the precise introduction date of each new hardware generation as well as their actual efficiency. Figure 16 presents our estimated energy consumption as well as the three data series from CBECI. We see that we get a decent estimate with our constant rate of technological progress assumption. Our estimate is in fact closer to the lower bound of CBECI.

The point of our paper is not to focus on a precise estimate of energy consumption like CBECI, nor is it to address the bitcoin energy debate in a normative way. We rather want to highlight the underlying dynamic mechanisms behind bitcoin energy consumption and in particular its source, which is the bitcoin price. In our model, the revenue per reference machine has a long term target denoted by $x^* = \frac{R}{K}$ which is constant. The reference machine being the machine that requires 1kW of energy, the total energy consumed by bitcoin miners is directly proportional to the real hashrate $K_t$. Therefore, on the long run, the energy consumption will grow with miners revenue. For example, if the bitcoin price grows by less than the decrease in the bitcoin revenue of miners, so that the dollar revenue of mining decreases, the energy consumption will also decrease. In our model we assumed the miners revenue process to follow an unbounded brownian motion so this will not strictly
show up. There is a growing literature tackling the bitcoin valuation problem (see Pagnotta (2020), Chevallier, Guégan, and Goutte (2021) or Zimmerman (2020)) but this unsurprisingly does not allow to form a precise long term target price for bitcoin. However, in the limit we can assume that the bitcoin price and therefore miners revenue will stop growing at more than 60% per year, which will stabilize the energy consumption. See appendix 6.1 for a discussion on this limit case.

As a side note, we would like to highlight that energy consumption per se is not bad for the environment. The carbon footprint of bitcoin mining is the main environmental concern. Estimation of this carbon footprint can be made considering estimated miners location and energy mix in each location (see Stoll, Klaaßen, and Gallersdörfer (2019) or Bendiksen and Bibbons (2019)) or through more complicated methods (Calvo-Pardo, Mancini, and Olmo (2020) use machine learning to estimate the bitcoin’s carbon footprint). First, miners can be assumed to be rational risk neutral agents so they will simply follow the cheapest source of electricity. The price of energy given its source, in addition of being an important matter for the world, will also be detrimental to bitcoin’s carbon footprint. Second, as explained we contribute to this debate with a long run dynamic view of energy consumption and the fact that bitcoin’s electricity consumption will not grow more than the bitcoin price on the long run.

4.3 Miners contribution to the technological progress

We now study the revenue generated by mining hardware manufacturers. Recall that, by assumption, their supply function is of the form $Q(p) = \lambda (p - \bar{p})$. But because the demand is infinite if the selling price is higher than the value of the machine $u$ (equivalently $v$ or $\tilde{v}$), we know that the price paid by the miners per machine will be $u$. Recall also that by assumption, miners contribute to the real hashrate at rate $I_t$ with

$$I_t = \lambda [u (R_t/K_t) - \bar{p}].$$  \hspace{1cm} (31)

Based on (24), we know that on the long run, the investment rate $I_t$ is a mean-reverting process. Its long term target value, $I^*$, is therefore given by

$$I^* = \delta + \alpha - \frac{1}{2} \sigma^2.$$  \hspace{1cm} (32)

Note that, as already stated, the average value of the investment rate may be different than its target value but the bias is small here, as the value function is close to a linear function.

\footnote{As the block reward decreases over time, miners revenue (the true driver of energy consumption) will grow at a lower rate than the bitcoin price.}
Because we know the equilibrium long term price of a machine, which is \( v((R/K)^*) \), we can compute the long term expected revenue for mining hardware manufacturers, \( \Pi^* \). Given a value of real hashrate, the long run quantity of mining chips that manufacturers can expect to sell is given by \( I^* K_t \). Let us rewrite this by multiplying and dividing by \( R_t \) because the exogenous variable is actually the miners revenue \( R_t \), while the revenue per machine is constant on the long run. We have that

\[
\Pi^* = I^* K^* v(x^*) = \frac{I^*}{x^*} v(x^*) R_t.
\]

We see that, on the long run, the revenue generated by the whole mining chips manufacturers industry is proportional to the miners revenue (i.e. the bitcoin price). So far the bitcoin price and miners revenue have increased by more than 60% each year, which translated into the same increase for the mining chips manufacturers revenue. This also means that the R&D spendings have also increased by a significant amount.

However, as can be observed on figure 3 the actual rate of technological progress has been rather constant since 2015.\(^{52}\) This can be due to R&D fragmentation and/or convex cost function. First, R&D is being more and more fragmented as new mining chips manufacturers are entering the market. So there might be some redundancy on the R&D conducted by all those actors. This is not completely satisfying as there are still very large computing chips manufacturers like Bitmain that can produce a lot of research. The other explanation might be that achieving the same rate of technological progress requires exponentially more R&D spendings each year. Indeed, have a 30%+ rate of technological progress on already highly efficient machines requires more and more R&D expenses.

We refer the reader to appendix 6.1 for a discussion on what happens when the bitcoin price stabilizes.

5 Conclusion

The Bitcoin protocol creates both a private good (units of cryptocurrency) and a public good (the payment system). In this context, agents’ preference for the private good depend on the strength of the public good. In this regards, our paper show that the security of the Bitcoin transactional systems is the result of a large population equilibrium which is inherently highly stable. Furthermore, mining incentives create a fierce battle among miners to get access to the most efficient hardware, which dis incentivize potential attackers to step in. We do not tackle other factors that

\(^{52}\)There were some structural breaks before 2015 with the introduction of FGPA and ASIC but since then the progress has been rather constant.
could influence the quality of a currency.

In this paper we have built a homogenous and parsimonious model for understanding the dynamics of the bitcoin hashrate. We have also tested our model with publicly available data and shown that it explains well the hashrate.

This Bitcoin production industry, resulting from the proof-of-work consensus algorithm, is very special in several respects. Anonymous miners engage in a no-skill competition to produce a fix amount of bitcoin. There are no barriers to entry or to exit, and the only thing they can do is to provide computational power, which in turn have a positive effect on the security of the underlying blockchain.

As the hashrate increases exponentially and the miners revenue (directly linked to the bitcoin price) keeps increasing, we have to make the right assumptions to express this problem as a stationary model. In particular, it is clear that the best way to think about the hashrate is in deflated terms, or real terms, which we call the real hashrate. Also, assuming miners decisions to change the real hashrate affect it proportionally to the stock of the current real hashrate (homogeneity assumption), allows to reduce the dimensionality of our model and obtain this stationary equilibrium in which the revenue per machine follows a mean-reverting process. This mean-reversion process for the revenue per machine provide strong stability to the miners’ industry.

In our model miners are quite passive. They see a profitable mining opportunity and they accordingly buy new mining hardware. Moreover the manufacturers of mining hardware are able to extract all the surplus from the mining activity and miners make no expected profit. The intuition behind is that miners’ incentive can be read from the blockchain itself, anyone can compute the value they can extract from mining activity, including mining hardware manufacturers so they set the price of those mining devices so that miners makes no expected profits. This is very particular to the Bitcoin industry as both the revenue and the cost are defined in a protocol that is publicly accessible.

By opposition to the common misconception, our analysis provides evidence that the major cost for miners is hardware buying instead of electricity (which represent only around 20% of total miners investment). This shows that the real battle of miners is the access to fast computing devices.

We also show that the security of the blockchain is directly linked to the bitcoin price (through miners’ revenue). The security of the blockchain is measured as the value of the real hashrate in place, which corresponds to the resistance to external 51% attacks. As the price of bitcoin increases, miners have more and more incentives to mine while the value of one mining machine is moving around a long-term target value, therefore the value of all the machines also increases. This creates a link between the price and the security that remains to be studied in our framework.
Indeed, in our model the price is exogenous but we have seen that higher price translates to a higher security, which may have a positive impact on the price on the long run.

In our homogenous setting, we show that i) the security of the blockchain, ii) miners energy consumption, and iii) the mining chips manufacturers investment in R&D are all linear functions of the total revenue from mining. Indeed, the only exogenous variable is the mining reward (which is heavily affected by the bitcoin price), moreover the homogeneity assumptions create this linear relationship even if the miner’s optimization problem is inherently non-linear. This comes from the fact that the revenue per machine follows a mean reverting process in equilibrium. Even if the price of bitcoin (and therefore the total miners reward) has increased exponentially since its inception, it is likely to stabilize in which case the energy consumption will also stabilize (as well as security and R&D spendings).

The homogeneous model we derived in this paper is very well suited for empirical calibration of the parameters but it has a number of limitations. We leave for further research the study of heterogeneous models of proof-of-work mining.

References

Bendiksen, Christopher, and Samuel Bibbons, 2019, the bitcoin mining network, *CoinShares Research*.


, and Albert J Menkveld, 2020, Equilibrium bitcoin pricing, *Available at SSRN 3261063*.

Calvo-Pardo, Hector F, Tullio Mancini, and Jose Olmo, 2020, Machine learning the carbon footprint of bitcoin mining, *Available at SSRN 3647593*.

Capponi, Agostino, Svein Olafsson, and Humoud Alsabah, 2021, Proof-of-work cryptocurrencies: Does mining technology undermine decentralization?, *Available at SSRN*.


Cong, Lin William, Zhiguo He, and Jiasun Li, 2019, Decentralized mining in centralized pools, Discussion paper, National Bureau of Economic Research.


———, and Andrea Buraschi, 2018, An equilibrium valuation of bitcoin and decentralized network assets, *Available at SSRN 3142022*. 46


Zimmerman, Peter, 2020, Blockchain structure and cryptocurrency prices, *Available at SSRN 3538334*. 


6 Appendix

6.1 Analysis of the limit case when $\alpha = 0$

Since its inception in 2009, the price of bitcoin, and therefore the whole industry, has grown exponentially but such growth is unlikely to last. In this appendix we analyze the situation of a stationary industry, that is when the growth rate of the total revenue from mining bitcoin is set to $\alpha = 0$. Even if it is likely that some expected rate of return remains, given bitcoin’s scarcity property, but we consider here the limit case with no drift at all.

As the only exogenous variable in our analysis, the total miners revenue, $R_t$, drives the security of the blockchain, the energy consumption of miners and the amount invested in R&D by mining hardware manufactures. We will discuss how those three quantities will behave in a world with no exogenous growth.

6.1.1 The security of the blockchain

We defined the security of the blockchain to be the resistance to external 51% attacks. By equation (27) we know that in the long run the security is proportional to the total miners revenue. Let’s write the dynamics of the security, $\xi$, in the general case (with $\alpha > 0$), we have

$$d\xi_t = \frac{v(x^*)}{x^*} \left[ \alpha dt + \sigma dW_t \right].$$

(34)

In the stationary world, the drift $\alpha$ is null and the security of the blockchain $\xi$ is constant on average, we have

$$d\xi_t = C^* dW_t$$

(35)

with $C^* = \frac{v(x^*)}{x^*} \sigma$ a constant. We cannot address the question of whether the long term security is sufficiently high as it would require some definition and objective measure of the benefit of using a blockchain as well as assumptions on the resources of potential attackers. We leave that for future research.

6.1.2 The energy consumption

The long term energy consumption of bitcoin mining is an important matter given the current climate concerns that are raised across the world. Our model shows the long term linear relationship between energy consumption and the bitcoin price (or the total miners revenue to be more precise).

If we consider a stationary world in which the average miners revenue does
not increase, we have that the energy consumption of bitcoin will be constant. Indeed, without any additional incentives to mine blocks, miners just replace the mining hardware due to the increased efficiency (i.e. the technological progress) but this does not change the real hashrate and therefore does not change the total energy consumption. Note that at this level, the nominal hashrate will still increase exponentially because of the technological progress. In other words, exponentially more hashes will be computed by all the miners but with the exact same average energy consumption.

This is of particular importance for anyone willing to make projections on the bitcoin energy consumption. Simply because the nominal hashrate increases exponentially, it does not mean that the energy consumption will also grow exponentially.

6.1.3 Investment in R&D

In the long run, miners contribution to technological progress is proportional to the total reward from mining the blockchain. Therefore, as we have discussed, the expected growth rate of the mining hardware manufacturers’ revenue is also the growth rate of the revenue from mining $\alpha$.

The interactions between the growth rate of miners’ revenue and the hardware manufacturers’ revenue suggest an endogenous relationship between the growth of the bitcoin price and the technological progress. Indeed, when $\alpha > 0$, miners have more and more incentives to buy more hardware which increases the revenue of hardware manufacturers. It therefore also increases their R&D spendings. The main analysis in the paper shows that this exponential increase in R&D spendings tends to produce a constant rate of technological progress. This suggests that if the growth rate of the miners revenue were to vanish (i.e. $\alpha = 0$), the rate technological progress would decrease over time. This assumption is critical for this analysis. If this was true, the R&D spendings would eventually not be enough to produce any technological progress at all. Note that in this case, from the moment $\alpha = 0$, there would still be some R&D investments (on average a constant value each year), as long as this can produce technological progress.

On the other hand, if the technological progress cost function is not convex with respect to R&D spendings, there will still be some residual R&D spendings and some level of technological progress even if the industry stops from growing. We have explained that if there is no expected growth in the total revenue from mining, the real hashrate is constant, i.e. miners only replace old machines by new ones without additional energy consumption and security. So as long as there is still some rate of technological progress, miners will still have a demand for more efficient mining chips. If the cost is indeed not convex, this demand for hardware replacement will be enough for sustaining some level of technological progress. It is
interesting to see that in this case, an industry that is stationary will still produce some level of technological progress in the long run.

To have a more accurate analysis, we would need to make stronger assumptions on the cost function of hardware manufacturers which we leave for future research.

6.1.4 Remark on endogenous Bitcoin price

In this appendix, we analyse the impact of a change in the average growth rate of miners revenue, \( \alpha \), as if it were exogenous. The question of whether this rate \( \alpha \) will ever go to zero and whether it should be endogenized could be raised but it comes down to what determine the price of bitcoin.

In line with Pagnotta (2020), the blockchain security could have a positive impact on the bitcoin price. By assuming users of bitcoin have a preference for security, there can exist an equilibrium in which the bitcoin price increases with security. However, it seems that even if agents have a preference for security, there would be a security level above which agents are indifferent toward more security. In such a case, it is likely that the expected growth rate of bitcoin vanishes over time, making the analysis of the case \( \alpha = 0 \) still relevant.

Having a deeper analysis of the endogeneity of the bitcoin price would require a more formal model of agents preferences which is outside of the scope of this paper.