An Equilibrium Model of the Market for Bitcoin Mining

Julien PRAT* Benjamin WALTER†

September 20, 2020

Abstract

We propose a model which uses the exchange rate of Bitcoin against the US dollar to predict the computing power of Bitcoin network. We show that free entry places an upper-bound on mining revenues and we devise a structural framework to measure its value. Calibrating the model's parameters allows us to accurately forecast the evolution of the network computing power over time. We find that at most one third of seigniorage income was dissipated in electricity consumption. The model indicates that a slowdown in the rate of technological progress will significantly increase Bitcoin's carbon footprint.

*CNRS, CREST, Ecole Polytechnique. Contact details: CREST, 5 avenue Henry Le Chatelier, 91120 Palaiseau, France, julien.prat@ensae.fr.

†CREST, Université Paris-Saclay. Contact details: CREST, 5 avenue Henry Le Chatelier, 91120 Palaiseau, France, benjaminjwalter@gmail.com. We are grateful to Daniel Augot, Giuseppe Bertola, Bruno Biais, Christophe Bisière, Vincent Danos, Hanna Halaburda, Joshua Miller, Harald Uhlig as well as three anonymous referees for their insightful suggestions and feedback. We also thank seminar participants at the University of Paris Dauphine, University of Nottingham, BlockSem seminar, University of Basel, University of Zurich, Cerg-talks, University of Chicago, New-York University, European University Institute and CREST for their comments. We acknowledge the support of the Investissements d'Avenir grant (ANR-11-IDEX- 0003/Labex Ecodec/ANR-11-LABX-0047) and of the the Chair Blockchain and B2B Platform.

1 Introduction

Bitcoin is the first payment system that operates without a central authority. Its protocol replaces trusted third parties with a network of computers, commonly referred to as "miners", that guarantees the immutability of past transactions. Miners compete for the right to add blocks of new transactions to the public ledger. Winners are rewarded with freshly minted bitcoins. Hence, as the value of Bitcoin skyrocketed, so did the resources devoted to mining. What started as a hobby for a few miners using their personal computers, eventually blossomed into an industry which consumes around 0.3% of the world's electricity through its network of mining farms, each one of them operating thousands of machines specially designed for mining.[1]

The runaway growth of Bitcoin's carbon footprint is widely perceived as one of the most convincing argument against its long-run sustainability. Since the amount of electricity allocated to mining is increasing in Bitcoin price, it seems that the currency cannot appreciate much further without causing intolerable environmental damage.[2] Assessing the robustness of this prediction requires a proper understanding of the factors that shape the relationship between Bitcoin price and miners' investment in computing power. For instance, if price stability discourages miners entry, Bitcoin could very well stabilize at a higher price than today without triggering an increase in energy consumption. To rule out this scenario, a structural model of the mining industry is needed.

We provide such a framework by devising a dynamic model that accurately captures the evolution of miners' computing power. Our model builds on the following two key elements. First, investment in mining hardware cannot easily be reversed: hardware have little to no resale value because they become obsolete very quickly, and, from 2014 onward, have no use outside of the market for Bitcoin mining since they have been optimized for this task only. Second, miners face a lot of uncertainty about future revenues due to the tremendous volatility of Bitcoin price. This combination generates a range of inaction where expected revenues are too low to justify entry, yet still sufficient to prevent incumbents from exiting the market.

The main challenge for our analysis is that we cannot consider the problem of each

[1] See, among other sources, digiconomist.net/bitcoin-energy-consumption .

[2] In one of the most pessimistic forecast, **?** (**?**) argue that, if Bitcoin adoption continues unabated, it could push global warming above 2 Celsius degrees within the next three decades.

miner in isolation or treat revenues as exogenous. Instead, we have to take into account how returns are endogenously determined by the number of active miners. A key insight of our model is that Bitcoin protocol generates revenues functions that are decreasing in aggregate capacity, thereby ensuring that the market for mining behaves as a competitive industry.

Combining the exchange rate of Bitcoin against the US dollar (₿/$) with the total computing power of Bitcoin network, we construct a new measure for miners' payoffs. Our model predicts that miners buy hardware only when this measure reaches a reflecting barrier. Payoffs never exceed the barrier because new entries push them down by triggering additional increases in mining costs. The characterization of the equilibrium is complicated by the fact that mining hardware benefits from a high rate of embodied technological progress. We show how one can adapt the canonical model of **?** (**?**) to account for this trend, and prove that the entry barrier decays at the rate of technological progress.

We calibrate the model and find that it forecasts remarkably well how miners respond to changes in the price of Bitcoin. The accuracy of our simulations is a testament to the fact that miners operate in an environment where perfect competition is a good approximation of reality, whereas trade in most industries is usually impeded by regulations, local oligopolies and search frictions.[3] By contrast, the market for Bitcoin mining verifies many properties that are often assumed but rarely verified in practice. First, free entry holds because mining is an unregulated activity with a streamlined set of tasks. Anyone can buy the appropriate hardware online and join the mining race. Second, there is little heterogeneity among miners since they all face the same problem and earn the same rewards. Third, the mining technology exhibits returns to scale that are constant by nature because Bitcoin protocol ensures that the odds of finding new coins remains proportional to the size of one's investment. Fourth, the elasticity of revenues with respect to the network computing power is commonly known because it is encoded in Bitcoin protocol, and is therefore observable by all parties. The conjunction of all these features is extremely rare, if not unique. It makes the market for Bitcoin mining a perfect laboratory for models of industry dynamics, especially since all transactions are public, giving anyone access to perfectly clean and exhaustive data.

[3]See, for instance, **?** (**?**) for an analysis of local oligopolies in the ready-mix concrete industry and how they respond to demand fluctuations; or **?** (**?**) for a characterization of the dynamic spatial equilibrium of taxicabs in New-York city.

Although our baseline model is fairly accurate in the medium to long run, it sometimes temporarily deviates from the data. To identify the origins of these deviations, we devise and calibrate a series of extensions. First, we allow for discontinuities in miners' rewards that take into account the reductions in the monetary creation rate which are triggered by Bitcoin protocol every four years. Second, we introduce a time-to-build and show that it explains the sluggish response of miners to sudden surges in Bitcoin price. Third, instead of assuming that investment is completely irreversible, we endow miners with the options to mothball or scrap their hardware. This extension enables us to match the rare instances where the network's computing power decreases. Most importantly, it also allows us to disentangle the investment costs from the operating costs, indicating that at most one third of seigniorage income was dissipated in electricity consumption. Comparing our calibrated costs to available data about the price of mining hardware, we find that they are consistent. Finally, we allow for congestion effects and non-linearities in the adjustment cost function at the industry level. This extension is required to fit the data during Bitcoin's 2017 bubble. It shows that the increase in the demand for mining hardware triggered by the bubble was so massive that it stretched the manufacturing capacity of hardware producers. This resulted in a spectacular increase in the price of hardware which prevented entrants to flood the market.

Having established the accuracy and robustness of our framework, we use it to investigate the impact of monopoly power, and to build forecasts about the energy consumption of Bitcoin. Studying the impact of each parameter, we find that Bitcoin's carbon footprint is likely to increase, principally because of a slowdown in the rate of progress of the mining technology.

Since Bitcoin clears and settles transactions through the organization of a two-sided market, our analysis is relevant to the study of platform adoption. On one side of the market, users hold and exchange bitcoins while, on the other side of the market, miners maintain the functionality of the decentralized ledger. From the standpoint of service providers, Bitcoin and, for instance, Uber fulfill a similar function: they both organize competition among Bitcoin miners or Uber drivers.

Calibrating our structural model enables us to identify which actors have been able to extract most of the rents, or seignorage income, generated by Bitcoin. In contrast to platforms that charge monopoly fees for their intermediation, Bitcoin ensures that revenues are passed on to miners.[4] Since we find that the behavior of miners is consistent with free entry, our results substantiate the notion that two-sided platforms can create competitive conditions among service providers by relying solely on price signals. Hence miners channel the income generated by Bitcoin towards the producers of their input factors, namely hardware manufacturers and electricity suppliers. We find that the manufacturers of mining hardware were able to extract most of the rents due to their monopoly power. The distribution of rents from Bitcoin mining therefore followed a similar pattern as that from the Californian gold rush during which, according to **?** (**?**), most of the profits were reaped by individuals who pursued other occupations than mining. Moreover, the rents of hardware manufacturers have recently been eroded by the entry of new competitors. According to our model, this loss of market power did not benefit miners who continued to operate in a competitive environment. Instead, it reallocated part of the seignorage income towards electricity providers, and so resulted in an increase in the energy consumption of Bitcoin.

Related literature.— Our paper uses insights from the literature on irreversible investment to contribute to the nascent field of *cryptoeconomics*. Bitcoin was created a decade ago when Nakamoto's paper (**?**, **?**) was made public on October 31st 2008. It did not immediately attract much attention and it took a few years for Bitcoin to become the focus of academic research. Early works analyzed the reliability of Bitcoin network (**?**, **?**; **?**, **?**). **?** (**?**) examined the anonymity of users, which enabled **?** (**?**) to quantify the different ways bitcoins are used and **?** (**?**) to precisely identify illegal Bitcoin users. **?** (**?**) and **?** (**?**) both corrected mathematical approximations made by Nakamoto in his seminal paper.

It is only recently that papers studying the economic implications of cryptocurrencies have started to emerge. Most articles focus on the monetary implications of Bitcoin. **?** (**?**), **?** (**?**) and **?** (**?**) study the interactions between fiat money and Bitcoin, providing formulas for the fundamental value of Bitcoin and testing their implications. Observing the plethora of existing cryptocurrencies, **?** (**?**) characterize the conditions under which currency competition is economically viable and efficient. **?** (**?**) analyze exchange rate manipulations, while **?** (**?**) assess the calibration of the parameters that underlie Bitcoin's design. **?** (**?**) question the disclosure of information which results from the use of public blockchains.

A series of recent papers is more closely related to our research since they study the

[4] See **?** (**?**) for a thorough description of Bitcoin protocol as a "monopoly without a monopolist".

market for mining. **?** (**?**), **?** (**?**) and **?** (**?**) investigate miners' incentives to behave cooperatively, as expected in Bitcoin protocol, or to play "selfish". **?** (**?**) model the market for mining as a game between miners. **?** (**?**) study the rise of mining pools which allow miners to share their computing power in exchange of a fair allocation of the mining rewards. Although **?** (**?**) find that mining pools do not necessarily undermine the decentralization of Bitcoin's network, they stress that risk sharing significantly escalates the arms race among miners. We bypass risk diversification by considering that miners are risk neutral, a specification which can be rationalized as describing the current state of the industry where pooled mining has become the norm. **?** (**?**) identify another force that intensifies the arms race: When R&D is endogenous, higher investments in research translate into a more aggressive mining game. Even though we take the evolution of the mining technology as given, we characterize in Section 6.1 the impact that market concentration has on the computing power deployed by miners. Finally, **?** (**?**) analyze how users set their fees and how their decisions impact electricity consumption. They raise concerns about the sustainability of Bitcoin in the long-run, when miners will be rewarded in transaction fees only.

Our paper also models the market for mining but unlike aforementioned articles, we focus on miners' entry decisions. We show that their behavior can be captured using real options theory. Since it would be impossible to cover all the major contributions to this field, we refer to **?** (**?**) for a broad overview, as well as to **?** (**?**), **?** (**?**) and **?** (**?**) for more recent surveys of the literature on industry dynamics. Our model being devised in an equilibrium setting, it builds on the seminal work of **?** (**?**) and **?** (**?**). We find that, despite its apparent novelty, the market for Bitcoin mining behaves very much like a standard industry. Our analysis illustrates that it is a perfect laboratory for real options theory because miners solve a common problem, whose parameters are publicly observable.

Structure of the paper.— The article is organized as follows. Section 2 lays out the baseline model along with two extensions. Section 3 presents the data and explains how we calibrate the models described in the previous section. Section 4 relaxes the irreversibility assumption and shows how the investment costs can be disentangled from the operating costs. The 2017 bubble is analyzed in Section 5. The implications of our findings are discussed in Section 6, while Section 7 concludes. The proofs of the Propositions and some additional results are relegated to the Appendix.

2 Equilibrium Models

We propose a framework that takes the demand for bitcoins as given. We use the trajectory of Bitcoin exchange rate against the US dollar, i.e. the dollar nominal price of Bitcoin, to predict the computing power of the network. Explaining how Bitcoin achieves decentralization is beyond the scope of this paper. Hence we only cover the elements that are required for the understanding of our model, namely the tasks accomplished by miners and the rewards they get in return. We refer readers interested in a more comprehensive treatment to **?** (**?**) and **?** (**?**).

2.1 Baseline Model

The mining technology.— The main challenge for a decentralized currency is to maintain consensus among all participants in order to prevent double spendings. To avoid such conflicts, transactions are bundled together into blocks which are then incrementally appended to the public ledger. Producing a valid block is made so difficult, that the average time it takes to build a block is much longer than the time it takes for a block to propagate across the network. This ensures that, in most instances, the whole network agrees on which transactions are included in the ledger.

The resulting data structure is called a Blockchain because blocks are cryptographically chained according to their dates of creation. Bitcoin miners continuously compete for the right to add the next block of transactions. To win the competition, miners have to stamp the header of their block with a "proof-of-work".[5] Generating a valid proof-of-work boils down to finding an integer, known as nonce, such that $S(header) \leq \underline{s}$, where $\underline{s}$ is an arbitrary threshold and S is a hash function. Hash functions are such that the only way to find a valid nonce is to randomly hash guesses until the above condition is met.[6]

The value of the threshold $\underline{s}$ determines the difficulty of finding a valid block, which we denote by D. The target $\underline{s}$ can be adjusted so that *every computed hash* will lead to a valid block with probability $1/D$. The probability that a hash yields a valid block is, for all practical purposes, independent of the number of trials already done. This memory-less property implies that the event of mining a block is captured by a Pois-

[5]Each block possesses a header, which contains both a nonce and a set of statistics that summarizes the transactions contained in the block, the time the block was built and the header of the previous block.
[6]This property is often referred to as puzzle-friendliness in the cryptographic literature.

son process.[7] The Poisson arrival rate $\lambda(h, D) = h/D$ is linear in the number, h, of computed hashes per period or *hashrate*, a requirement known as fairness in the computer science literature.

We normalize the length of a period to 10 minutes and set the hashrate of each miner equal to one hash per period. Let Q_t denote the *total hashrate* of the network, i.e. the overall number of mining units currently competing for the next block. Since fairness implies that the mining technology exhibits constant returns to scale, the average waiting time between blocks is equal to $\lambda(Q_t, D_t)^{-1} = D_t/Q_t$. To ensure that block generation proceeds at a steady pace, the difficulty of the hashing problem is adjusted by the network until new blocks are created on average every ten minutes. Given our normalization, this objective is attained when $\lambda(Q_t, D_t) = 1$, so that $D_t = Q_t$.

In practice, the hashrate of the network Q_t is not observable. Bitcoin circumvents this problem by relying on an adaptive expectation algorithm. Every two weeks on average, Bitcoin protocol uses the block generation rate over the last 2016 blocks to infer the average value of Q during the previous period. Then the difficulty parameter is adjusted until it matches the estimated value of Q. This updating procedure guarantees that, if the network hashrate does not deviate too much from its estimated average, the block generation rate will remain close to its target of 10 minutes. Since we devise our model in continuous time, assuming that difficulty is adjusted periodically would greatly complicate the analysis, making it impossible to derive tractable results. This is why we slightly idealize the actual protocol by assuming that D_t is continuously adjusted.[8] We verify in the Technical Appendix D that the number of blocks mined every day mostly remained within the confidence interval centered on the protocol's target. In other words, the block generation rate was not significantly different from one block every 10 minutes, and so did not deviate much from the idealized state that would prevail under Assumption 1.

Assumption 1. *The difficulty parameter D_t is continuously updated and set equal to the current network hashrate Q_t, so that $D_t = Q_t$ for all t.*

Miners' revenues.— Building a valid block is costly in terms of hardware and electricity. Miners are compensated when they win the competition: The first miner who finds a valid block earns a predetermined amount of new coins (12.5 bitcoins at the

[7]See the Technical Appendix A and **?** (**?**) for a derivation.

[8]From a formal standpoint, this hypothesis is equivalent to assuming that Q_t is observable and that D is set equal to Q with a delay ε, so that $D_{t+\varepsilon} = Q_t$. Our model arises in the limit as ε converges to zero.

time of writing), and the sum of the fees granted by the transactions included in the block. Whereas the amount of new bitcoins is fixed by the protocol, fees are freely chosen by users. So far transaction fees have accounted for only 2.1% of average block rewards. We use R_t to denote the block rewards in dollars, i.e. the ₿/$ exchange rate multiplied by the sum of new coins and fees. Then, as shown in the Technical Appendix A, the *flow payoff* P_t of a miner is equal to the block rewards, R_t, times the Poisson arrival rate, $1/D_t$, of a valid block[9]

$$P_t = R_t/D_t. \tag{1}$$

Under Assumption 1, the flow payoff is given by an isoelastic function of the network hashrate

$$P_t = R_t/Q_t. \tag{2}$$

The microfoundation of (2) is rather unique since the decreasing relationship between revenues and industry capacity does not stem from the satiation of consumers' demand, but is instead generated by the increase in mining costs encoded in Bitcoin protocol.

We do not attempt to endogenize the demand for bitcoins, and thus take its exchange rate against the dollar as given. Following much of the literature on irreversible investment, we assume that revenues follow a Geometric Brownian Motion (GBM hereafter).

Assumption 2. *The block rewards $(R_t)_{t\geq 0}$ follow a Geometric Brownian Motion so there is an $\alpha \in \mathbb{R}$, and a $\sigma \in \mathbb{R}_+$, such that*

$$dR_t = R_t\left(\alpha dt + \sigma dZ_t\right), \tag{3}$$

where $(Z_t)_{t\geq 0}$ is a standard Brownian motion.

Given that newly minted coins account for the bulk of block rewards, changes in R are almost fully proportional to changes in Bitcoin price. The GBM specification is

[9]We implicitly assume that miners value the block rewards at the current market price of Bitcoin. This premise is consistent with **?** (**?**) since they show that agents should be indifferent between holding bitcoins or dollars. Actually, miners are more likely than other agents to favor dollars because they have already tied up the value of their investment to that of Bitcoin. Hence, converting their Bitcoin rewards into fiat currency allows them to hedge part of their investment risk. In practice, miners have to wait on average 16 hours and 40 minutes, i.e. 100 blocks, before being able to transfer their newly earned coins.

consistent with the equilibrium pricing formula for bitcoins of **?** (**?**). The stochastic term captures the martingale component arising from the "exchange rate indeterminacy result" of **?** (**?**); while the deterministic trend is proportional to the correlation between the pricing kernel and the price of Bitcoin. As we will see below, the estimated α are always positive, which indicates that the pricing kernel and Bitcoin price were negatively correlated. Additional factors were probably at work during our period of study because **?** (**?**) focus on the equilibrium situation where Bitcoin is used as a medium of exchange. Whether or not this is true today remains open to debate, but most people would agree that Bitcoin was not widely used as a medium of exchange during its adoption phase. Then, as shown by **?** (**?**), the rate of return on Bitcoin was compensating investors for the risk of hacks. **?** (**?**) also provide a justification for our geometric specification as transactional benefits are proportional to the price of Bitcoin, a property that distinguishes cryptocurrencies from other assets and which yields a pricing equation with a multiplicative structure.

The GBM specification narrows down the class of equilibrium prices, by requiring that they exhibit independently and normally distributed returns with constant variance. Assessing these requirements, we do find that returns are not linearly autocorrelated, and that their distribution is well approximated by a normal distribution (see Technical Appendix E). However, we also find that tail events are too common, and that the volatility of returns varies over time. These shortcomings of the GBM model are not specific to Bitcoin but common to most financial assets. Yet, GBM processes are still widely used to price assets because they provide a reasonable first-order approximation, while being much more convenient to handle than Lévy processes. We adopt this pragmatic approach, and leave the study of more complex price processes to further research.

Knowing the law-of-motion followed by the reward process is not sufficient to compute the expected payoffs because they also depend on the hashrate of the network Q, whose level is endogenously determined. To solve for the equilibrium, one has to simultaneously derive the process followed by Q and the entry policy of miners.

Market entry.— Mining is a costly activity. To operate a unit of hashpower bought at time τ, miners incur the flow operating cost C_τ.[10] The electricity consumption of mining hardware accounts for the bulk of the operating costs.[11] The costs vary with the

[10]The hashpower measures the number of hashes that can be performed per period.

[11]We implicitly assume that the price of electricity remains constant. It is easy to relax this restriction by

vintage of the hardware because they benefit from embodied technological progress, as newer machines are able to perform more hashes with the same amount of energy. We assume that investment in mining hardware is irreversible, and explain why this is a reasonable premise in Section 3.1. As a first approximation, we also assume that miners cannot turn their hardware off, a simplifying assumption that will be relaxed in Section 4.

Assumption 3. *Once installed, mining hardware cannot be switched off so as to save on operating costs.*

Assumption 3 implies that the value of a unit of hashpower of vintage τ reads

$$V(P_t, \tau) = \mathbb{E}_t \left[\int_t^{\infty} e^{-r(s-t)} P_s ds \right] - \frac{C_\tau}{r}, \tag{4}$$

where r is the yearly discount rate and $t \geq \tau$.[12] We consider that all the miners of a given vintage face the same problem. In practice, operating costs may differ across locations but only those miners that have access to the cheapest sources of electricity will find it profitable to enter the market.

Entrants have to buy a unit of hardware whose price we denote by I_t. Both investment and operating costs decrease over time because hardware becomes more efficient. Let A_t measure technological efficiency, so that buying A_t units of hashpower at date t costs the same amount than buying one unit of hashpower at date 0. For the reasons explained below, we assume that technological improvements accrue at a constant pace, i.e. $A_t = \exp(at)$ with $a > 0$.

Assumption 4. *Machines become more efficient at the constant rate $a > 0$. Hence the investment and the operating costs satisfy $I_t = I_0/A_t = \exp(-at)I_0$ and $C_t = C_0/A_t = \exp(-at)C_0$.*

Anyone can enter the mining race: All that is required is to buy the mining hardware, and to connect it to a steady supply of electricity. Hence free entry is likely to

letting C also depend on the current date t. However, changes in electricity costs can be safely ignored in the empirical analysis because they are dwarfed by variations in Bitcoin exchange rate.

[12] See the Technical Appendix A for a derivation of (4). It is straightforward to generalize (4) to include an exogenous rate at which hardware breaks down. We do not take it into account because its calibration returns non significant values. Intuitively, failures seem to occur at a much slower rate than technological obsolescence since we do not observe that the network hashrate decreases in the absence of market entry.

prevail, ensuring that

$$I_t \geq V(P_t, t) = \mathbb{E}_t \left[\int_t^\infty e^{-r(s-t)} P_s ds \right] - \frac{C_t}{r}, \text{ for all t.} \tag{5}$$

When new miners enter the market, (5) holds with equality. Since the exchange rate follows a Markov process, it is natural to conjecture that miners' decisions will only depend on the current realization of P: Whenever payoffs reach some endogenously determined threshold $\overline{P}_t$, a wave of market entries will ensure that the free entry condition (5) is satisfied.

To see why such a mechanism defines a competitive equilibrium, it is helpful to decompose the law of motion of P. Reinserting (3) into (2) and using Ito's lemma, we find that

$$d\log(P_t) = \left(\alpha - \frac{\sigma^2}{2}\right) dt + \sigma dZ_t - d\log(Q_t). \tag{6}$$

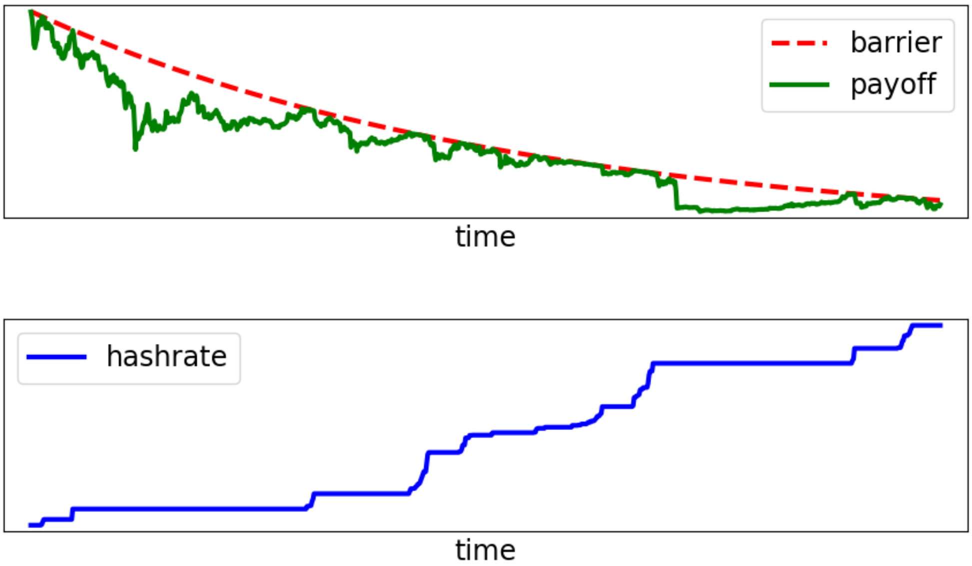
Payoffs are decreasing in Q because the response of the protocol to an increase in total hashrate is to raise the difficulty parameter, thus making it less likely for each miner to earn a reward. This is why free entry places an upper bound on payoffs. Their value can never exceed a threshold $\overline{P}_t$ as more miners would find it profitable to enter the market, which would push payoffs further down.

Industry equilibrium.— So far, the main takeaway from our analysis is that the market for mining can be described as a standard industry because Bitcoin protocol generates a cost function that is increasing in aggregate capacity. We define a competitive equilibrium as a symmetric Nash equilibrium in entry strategies. If all other miners follow a policy of entry at $\overline{P}_t$, no individual miner can find it optimal to follow any other policy.

Definition 1 (Industry equilibrium)**.**
An industry equilibrium is a payoff process P_t and an upper barrier $\overline{P}_t$ such that:
(i) $P_t \in [0, \overline{P}_t]$.
(ii) The network hashrate Q_t increases only when $P_t = \overline{P}_t$.
(iii) The free entry condition (5) is satisfied at all points in time, and it holds with equality whenever $P_t = \overline{P}_t$.

Conditions (i) and (ii) ensure that entry keeps P_t below the entry barrier $\overline{P}_t$; while condition (iii) ensures that no individual miner will find it profitable to deviate from the entry policy. Conjecturing the properties of the equilibrium greatly simplifies the

Figure 1: Industry Equilibrium



analysis since we only have to verify that they are indeed satisfied by the entry strategies. From a formal standpoint, the fundamental difference between our equilibrium and the one studied by **?** (**?**) is that, due to embodied technological progress, the investment and the operating costs decrease over time. Hence the entry barrier $\overline{P}_t$ cannot remain constant. However, if we impose Assumption 4, so that mining efficiency improves at a constant rate, we can solve for the equilibrium in the space of detrended payoffs and recover a flat barrier.

Proposition 1. *Assume that assumptions 1, 2, 3 and 4 hold. Then there exists an industry equilibrium* $(P_t, \overline{P}_t)$ *such that* P_t *is a GBM reflected at* $\overline{P}_t = \overline{P}_0 / A_t$ *where*[13]

$$\overline{P}_0 = \frac{(r-\alpha)\beta}{\beta - 1}\left[I_0 + \frac{C_0}{r}\right], \text{ and } \beta = \frac{\frac{\sigma^2}{2} - \alpha - a + \sqrt{\left(\alpha + a - \frac{\sigma^2}{2}\right)^2 + 2\sigma^2 (a + r)}}{\sigma^2} > 0. \tag{7}$$

A typical equilibrium is illustrated in Figure 1. The upper-panel reports an arbitrary sample path for the payoff process $(P_t)_{t \geq 0}$. Payoffs follow the changes in block rewards and thus behave as a GBM until they hit the reflecting barrier $\overline{P}_t$. Such events trigger market entry, as shown in the lower-panel. The resulting increase in hashrate raises the difficulty of the mining problem, and so pushes payoffs down until market entry is not anymore profitable. The entry barrier decreases at the rate of technological

[13] Note that, when $\alpha = r$, $\overline{P}_0 = \left(I_0 + \frac{C_0}{r}\right)\left(\alpha + a + \frac{\sigma^2}{2}\right)$.

progress because it corresponds to the pace at which both investment and operating costs fall over time.

Comparative statics.— To get some intuition about the impact that each parameter has on the entry barrier, it is useful to consider the hypothetical situation where further entries are precluded. Then the marginal miner is also the last one to ever enter the market. Provided that $r > \alpha$, the value of the last entrant is positive whenever $P_0 > \overline{P}_0^{last} \equiv (r-\alpha)\,[I_0 + C_0/r]$.[14] Comparing the thresholds with and without entry, we see that $\overline{P}_0 = [\beta/(\beta-1)]\overline{P}_0^{last} > \overline{P}_0^{last}$. The break-even payoff is higher under free entry because the arrival of new miners ensures that future payoffs are reflected downwards when they reach the entry barrier $\overline{P}_0$. The term $\beta/(\beta-1)$ measures the negative impact that entries have on the value of the marginal incumbent.

Differentiating the expression of $\overline{P}_0$ in (7), we find that $\partial\overline{P}_0/\partial a > 0$ and $\partial\overline{P}_0/\partial r > 0$. If technological progress accelerates, miners' revenues shrink more rapidly because there will be even more entries in the future. Hence entrants have to earn more early on, which raises the entry barrier. A similar mechanism explains the impact of r since future revenues are discounted at a higher rate when r goes up. Not surprisingly, an increase in the average growth rate α of the block rewards incentivizes entry as $\partial\overline{P}_0/\partial\alpha < 0$. Finally, the volatility of payoffs σ discourages entry since $\partial\overline{P}_0/\partial\sigma > 0$. Note that this is not due to an increase in the value of waiting because the perfectly competitive structure of the industry rules out such an option: Competitors would preempt any procrastination beyond the zero expected profit threshold. Instead, the negative impact of σ on entry is mechanical. Given that payoffs are truncated from above by the reflecting barrier, an increase in their spread automatically lowers their expected value. Quantitatively, the rate of technological progress a has, by far, the largest effect on $\overline{P}_0$.

2.2 Extensions

We now generalize our model so as to take into account the delivery lags for mining hardware, and the halving of block rewards every four years.

[14] If market entry is forbidden, P_t obeys the same law of motion as R_t so that

$$V_0^{last} = \int_0^{\infty} e^{-rs}\mathbb{E}_0\left[P_t\right]dt - \left[I_0 + \frac{C_0}{r}\right] = \frac{P_0}{r-\alpha} - \left[I_0 + \frac{C_0}{r}\right].$$

Time-to-build.— We have assumed that miners can enter the market immediately. In practice, however, new hardware have to be delivered and installed. Each step increases the lapse of time separating entry from actual production. When it requires δ years to effectively become operational, prospective entrants at date t have to forecast their revenues starting from $t+\delta$. Hence they have to take into account the price fluctuations that may ensue during the delivery period, as well as the amount and arrival times of hardware in the delivery pipeline.

To reduce the dimensionality of the state space, we follow the approach proposed by **?** (**?**). Let H_t denote the amount of "committed hashrate", that is all the mining units which are either already operational, or on their way to being delivered. Given that all orders will be installed δ years from now, the hashrate of the network when today's orders become operational will be equal to the current amount of committed hashrate, i.e. $Q_{t+\delta} = H_t$. Hence the relevant state variable from the standpoint of entrants is not anymore $P_t = R_t/Q_t$, but instead $P_t^\delta \equiv R_t/H_t$. We show in the Technical Appendix L that equilibrium strategies are functions of P_t^δ only, and that the mining market is in equilibrium when P_t^δ is a reflected GBM.

Proposition 2. *Assume that assumptions 1, 2, 3 and 4 hold. Furthermore, assume that market entry is delayed by the time-to-build δ. Then there exists an industry equilibrium $\left(P_t^\delta, \overline{P}_t^\delta\right)$ such that $P_t^\delta = R_t/H_t$ is a GBM reflected at $\overline{P}_t^\delta = \overline{P}_0^\delta/A_t$. The entry barrier is related to that of the model without time-to-build by the following equation*

$$\overline{P}_t^\delta = e^{(r-\alpha)\delta}\overline{P}_t\left[K_t/K_t^\delta\right], \tag{8}$$

where $K_t \equiv I_t + C_t/r$ denotes the overall costs of entry in the model without delay, and $K_t^\delta \equiv K_t - (1-e^{-r\delta})C_t/r$.

Proof. See the Technical Appendix L. □

The expression of the entry barrier with time-to-build differs from that of the baseline model in two respects. First, overall costs of entry K_t^δ are slightly lower because they are evaluated at the time of the entry decision. Since entrants have to wait δ years to start mining, their operating costs C_t/r are multiplied by the discount factor $e^{-r\delta}$. Second, the barrier without delay is rescaled by $e^{(r-\alpha)\delta}$ because it is optimal to enter when the expected value of payoffs in δ years is equal to the discounted threshold, $e^{r\delta}\overline{P}_t$. Since $\mathbb{E}_t\left[P_{t+\delta}\right] = e^{\alpha\delta}P_t^\delta$, setting $\mathbb{E}_t\left[P_{t+\delta}\right] = e^{r\delta}\overline{P}_t$ indeed implies that

$P_t^\delta = e^{(r-\alpha)\delta}\overline{P}_t$.[15]

Note, however, that the models with and without delays are not as similar as their descriptions might suggest. The solution of the baseline model is Markovian since knowing the current hashrate and Bitcoin price is enough to forecast the evolution of the network hashrate. By contrast, the solution of the model with time-to-build is path dependent since forecasts over the next δ years are conditional on all the purchase orders that were placed over the previous δ years.

Halvings.—Another limitation of our baseline model is that it ignores the inclusion in Bitcoin protocol of a feature which divides by two the number of coins issued per block. These so-called *halvings* are triggered every 210,000 blocks to ensure that the supply of bitcoins converges to a finite limit, namely 21 millions. Halvings generate discontinuities in the paths of R_t that are inconsistent with the GBM specification. To take them into account, one has to replace Assumption 2 with Assumption 5 according to which block rewards are halved every four years.

Assumption 5. *The block rewards are given by $R_t = h_t \tilde{R}_t$. $\tilde{R}_t$ follows a GBM while $h_t = \left(\frac{1}{2}\right)^{\lfloor t/4 \rfloor}$, where t measures the number of years elapsed since the inception of Bitcoin, and $\lfloor x \rfloor = \max_{n \in \mathbb{N}}\{n \leq x\}$.*

Assumption 5 slightly simplifies the halving process. First, the reward a miner gets when she finds a block is not exactly divided by two after each halving because it includes transaction fees on top of new coins. But the discrepancy is not very important in practice, as transaction fees account for a residual share of block rewards. Second, halvings do not occur every four years, but instead every 210,000 blocks. Counting years is a way to approximate elapsed time because Bitcoin protocol adjusts the difficulty of the hashing problem every two weeks on average. It is shown in the Technical Appendix D that, indeed, the updating rule manages to keep the block generation rate close to one every 10 minutes.

Halvings render the optimization problem of miners non-stationary: the closer they are to the halving date, the lower their expected payoffs. This implies that we have to rely on numerical methods because the entry barrier does not anymore admit a

[15]The relationship between the expectation of $P_{t+\delta}$ and P_t^δ holds true because $Q_{t+\delta} = H_t$, so that

$$\mathbb{E}_t\left[P_{t+\delta}\right] = \mathbb{E}_t\left[\frac{R_{t+\delta}}{Q_{t+\delta}}\right] = \frac{\mathbb{E}_t\left[R_{t+\delta}\right]}{H_t} = e^{\alpha\delta}P_t^\delta.$$

closed-form solution. Starting from the analytical solution derived in the proof of Proposition 1, we proceed by backward induction and use a finite-difference procedure to approximate the entry rule. As the horizon increases, our algorithm quickly converges towards an entry barrier that is independent of the number of future halvings.[16]

3 Calibration

3.1 Data

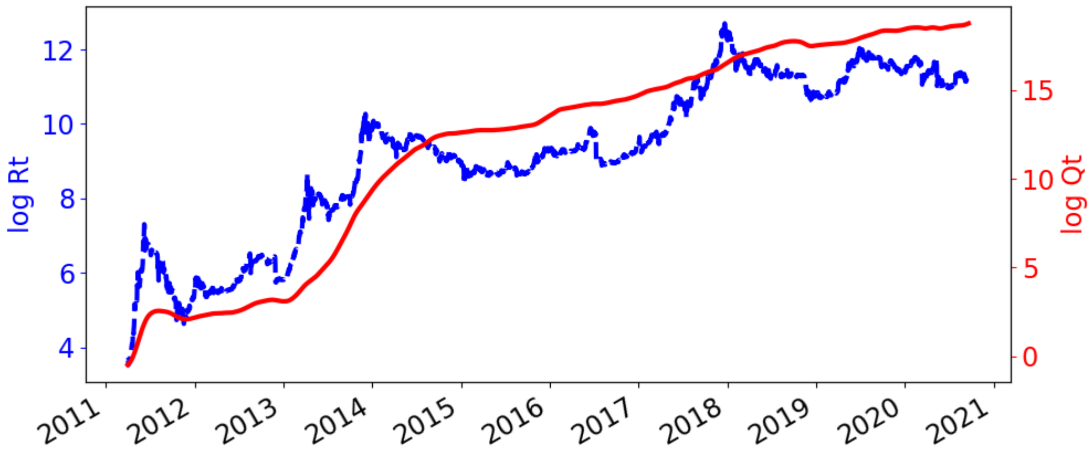
We now show that feeding our model with exchange rate data allows one to accurately predict the evolution of the network hashrate. For this purpose, we need to infer the miners' payoffs $P_t = R_t/Q_t$. Remember that the numerator, R_t, is equal to the value of new coins plus the transaction fees. The number of created coins per block is specified by the protocol while Bitcoin exchange rate against the dollar is directly available from coindesk.com.[17] The transaction fees are recorded in Bitcoin's blockchain and can easily be retrieved from btc.com. Thus all the components of R_t are readily available. By contrast, the network hashrate Q_t is not directly observable. It must be estimated using the theoretical probability of success and the number of blocks found each day. Given that we are not primarily interested in statistical inference, we relegate the description of our estimation procedure to the Technical Appendix F and save on notation by using Q_t to denote our estimate, although its time series only approximates the true hashrate. We show in the Technical Appendix F that the approximation is accurate. We update the value of Q_t on a daily basis and, since there are on average 144 blocks mined every day, the expected payoffs per day are given by $P_t = 144 \times R_t/Q_t$.

We report the series followed by R_t and Q_t in Figure 2. There is a clear correlation between the two variables. Our model suggests that their structural relation should

[16]More precisely, the entry barrier turns out to be stable after four iterations. We use finite-difference methods to approximate the Hamilton-Jacobi-Bellman equations satisfied by the value functions of miners. We rely on the implicit Euler scheme in order to ensure that the approximation is stable. The system of linearized equations is solved using a generalization of the Gauss-Seidel iterative method known as the successive-over-relaxation method.

[17]There are many different exchanges and the exchange rate varies a bit across them. In the Technical Appendix C, we check the validity of coindesk data by comparing them to a weighted average measure over 17 exchanges. Since the two series are virtually indistinguishable, we select the one that is most easily accessible.

Figure 2: Miners Revenues R and Network Hashrate Q



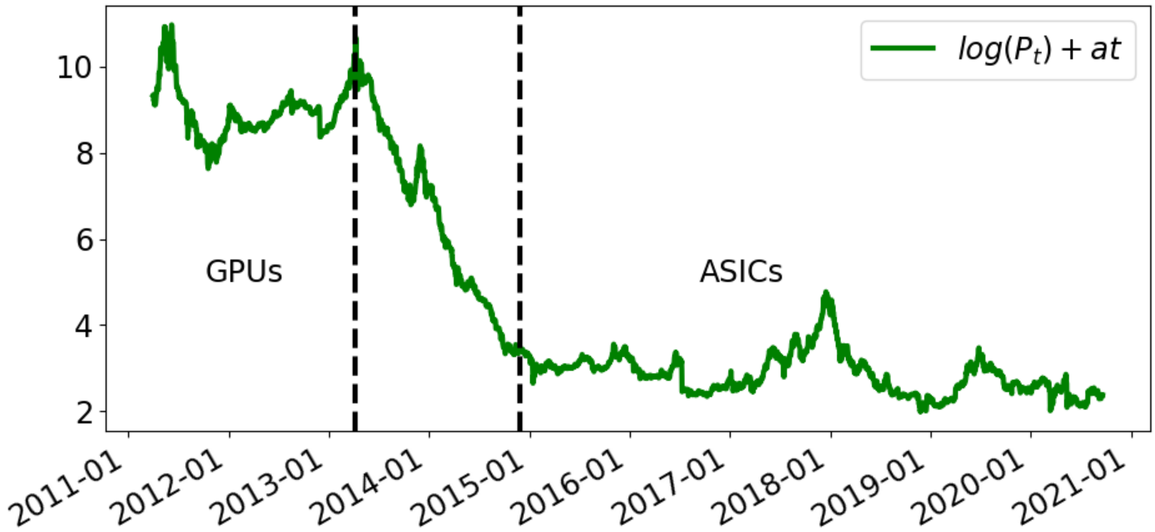
NOTE: R_t IS COMPUTED USING INFORMATION COLLECTED ON COINDESK.COM AND BTC.COM. Q_t IS MEASURED IN TERAHASH PER SECOND. ITS VALUE IS INFERRED USING THE PROCEDURE DESCRIBED IN APPENDIX F.

become apparent if one takes the ratio of the two series and detrend it at the rate of technological progress a. Then the resulting series should behave as a reflected GBM. For many years, improvements in the processing industry have followed Moore's law, according to which processor speed doubles every two years. We expect improvements in the mining technology to outpace those in processing speed because miners came up with a series of innovations which allowed them to leverage their computing power. Thus, at this stage we pick a rate of techological progress slightly faster than Moore's law (1.5 times faster). We will refine our guess later on by calibrating the value of a.

The payoff series detrended at the rate implied by Moore's law is reported in Figure 3. It exhibits two stationary regimes, with a break in the middle where payoffs decreased regularly until they reached a lower plateau. At first, this pattern does not seem to square with our model. But if we focus on the date at which the break initiates, we realize that it coincides with a fundamental change in the mining technology.

Early on, miners used to mine with their own computers. Around mid-2010, they realized that Graphical Processing Units (GPU) were much more efficient. One year later, miners started to use Field Programmable Gate Arrays (FGPA) and, since 2013, they mostly mine with Application Specific Integrated Circuits (ASIC). ASICs are also

Figure 3: Detrended Payoff Series



NOTE: P_t IS EQUAL TO THE DAILY NETWORK REVENUES $144 * R_t$ DIVIDED BY Q_t.

called mining rigs because their sole purpose is to solve Bitcoin's hash-puzzle.

The first ASIC was delivered to Mr. Jeff Garzik on January 30th 2013.[18] Since this revolution in the mining technology boosted the rate of technological progress well above its long-run trend, its propagation among miners violates Assumption 4, and so, one should not expect the predictions of our model to be verified during the transitory phase. We therefore leave aside the lapse of time where miners switched from GPUs and FPGAs to ASICs, and focus instead on the two subperiods where miners used the same technology. More precisely, during the first period, which ranges from 2011/04/01 to 2013/01/31,[19] miners mainly mined with GPUs; while they mostly relied on ASICs from 2014/10/01 onwards. Our second subperiod ranges from 2014/10/01 to 2017/03/31. It does not include our most recent data because they cover an episode of trading frenzy during which Bitcoin experienced a giant bubble followed by a sudden burst. We will analyze this event and its aftermath in Section 5.

Buying an ASIC is an irreversible decision because it can be used for cryptocurrency mining only. Hence, if the price of Bitcoin falls, ASICs cannot be resold for profit be-

[18] See https://bitcoin.stackexchange.com/questions/40944/when-did-the-asic-mining-era-begin

[19] We excludes the very early history of Bitcoin because it features an unstable block generation rate (see the Technical Appendix D).

cause all miners face the same returns. The irreversibility assumption is less obvious for GPUs. Yet, the calibrated values of a reported below in Table 1 show that GPUs were facing a very high rate of obsolescence. This suggests that irreversibility is also a sensible approximation for GPUs, as nobody would buy them second hand without a tremendous discount. The conjecture is confirmed by the analysis in the Technical Appendix I, where we calibrate a model with reversible investment and find that it fails to match the data.

3.2 Calibration strategy

We calibrate the parameters for each subperiod. The baseline models is parsimonious enough to rely on six parameters only: the deterministic trend α of rewards and their volatility σ^2, the rate of technological progress a, the discount rate r, the price I_0 of one unit of hashpower bought at time 0, and the operating cost C_0 of that same unit. The first two parameters can be directly estimated using R_t only. Under Assumption 2, the log returns are independent and follow a normal distribution with mean $\mu \equiv \alpha - \sigma^2/2$, and variance σ^2, which we estimate by maximum likelihood (see Technical Appendix E).

The rate of technological progress, a, and the reflecting barrier, $\overline{P}_0$, are set to minimize a (pseudo)distance between the observed and the simulated paths of the hashrate. A direct consequence of our equilibrium definition is that $Q_t = \max\left(Q_{t-1}, \frac{R_t A_t}{\overline{P}_0}\right)$ for all t. This condition provides us with a straightforward way to simulate the hashrate for any sample with T observations:

1. Set the initial value of the simulated hashrate Q_0^{sim} equal to its empirical counterpart, i.e. $Q_0^{sim} := Q_0$.
2. Update the simulated hashrate as follows $Q_t^{sim} := \max\left(Q_{t-1}^{sim}, \frac{R_t A_t}{\overline{P}_0}\right)$, for $t = 1, \ldots, T$.

Since $(R_t)_{t\geq 0}$ and Q_0 are observed, the minimization procedure boils down to finding the value of a and $\overline{P}_0$ such that

$$(\hat{a}, \hat{\overline{P}}_0) \in \underset{(a,\overline{P}_0)\in\mathbb{R}\times\mathbb{R}_+}{argmin} \sum_{t=1}^{T} \left(\frac{Q_t - Q_t^{sim}(a, \overline{P}_0)}{Q_t}\right)^2. \tag{9}$$

Unfortunately, the other three parameters $\{r, I_0, C_0\}$ cannot be separately identified. We will describe in Section 4 a model where investment is reversible, and explain how it enables us to separate the investment cost, I, from the operating cost, C. At this stage, the best we can do is to fix r, and recover the overall costs of entry at the beginning of each subperiod, $K_0 \equiv I_0 + C_0/r$, by equating the expression for $\overline{P}_0$ in (7) with the calibrated $\hat{\overline{P}}_0$. The arbitrary choice for the discount rate, r, turns out to be relatively unimportant because the term $(r-\alpha)\beta/(\beta-1)$ in (7), and thus the entry costs, are rather inelastic with respect to r.[20]

3.3 Results

Calibrated parameters.— The parameters resulting from our calibration strategy are reported in Table 1, their values expressed as yearly rates whenever applicable.[21] The standard errors are obtained using block bootstrap, an estimation technique that is more suited to time series than standard bootstrap.[22]

We first present the trend and volatility of the reward process. Both coefficients are independent of the modelling strategy since they are directly estimated by maximum likelihood on the rewards series R_t. The average growth rate of rewards, μ, decreased a lot between the two periods of study. As one would expect, early buyers of bitcoins earned higher returns. Information about their profits pushed the demand for bitcoins which raised the exchange rate even more. But the extremely high returns observed at the beginning became harder to sustain as the market capitalization grew from a negligible amount, to nearly $ 20 billions by the end of our sample. In spite of this cooling process, investing in Bitcoin remained extremely profitable. These tremendous returns have led many observers to announce the imminent collapse of Bitcoin.[23] Whether or not such predictions will eventually be vindicated is beyond the scope of this paper, but our estimates for the volatility coefficient σ indicate that there was no obvious arbitrage opportunity; investors willing to bet on Bitcoin also had to bear a huge risk. Even though the volatility of rewards was divided by three in the second period, its value remained an order of magnitude higher than its counterpart for the S&P 500.[24]

[20] In the second period, setting $r = 0.2$ yields $K_0 =$ \$1639, while $r = 0.05$ yields $K_0 =$ \$1934.

[21] For example, the calibrated values of a means that the price of a new hardware has been on average divided by $\exp(a)$ every year during each subperiod.

[22] The block bootstrap procedure is described in the Technical Appendix G.

[23] According to the website bitcoinobituaries, by August 2019, 371 opinion pieces had predicted the death of Bitcoin.

[24] We find that, for the S&P 500, $\sigma^2 = 0.053$ for the first period and $\sigma^2 = 0.027$ for the second period

According to Moore's law, the price of one unit of hashpower should be divided by two every two years. Hence it implies that the rate of technological progress a should be close to $\log(2)/2 \approx 0.35$, a number well below the calibrated values of a reported in Table 1. The mining technology progressed at a faster pace than the one predicted by Moore's law because miners were able to implement innovations specific to the hash-puzzle on top of the raw increase in computing power. Our calibrated parameters also indicate that the rate of technological progress slowed down considerably in the second period, thus suggesting that improvements specific to the mining problem became harder to unearth as the technology matured.

Comparing the parameters across models, we see that introducing halvings lowers the overall costs of entry, K_0, but raises the rate of technological progress, a. The decrease in K_0 is quite intuitive: Since halvings lower expected revenues, free entry holds when mining costs are smaller. The reason why a increases is more subtle. The adjustment corrects the misspecification of the baseline model that leads to an overestimation of the hashrate around the halving dates. This is why the minimization procedure, when applied to the baseline specification without halvings, generates a negative bias for a because it uses this parameter to reduce the discrepancies around the halving date.

The delivery lags of the model with time-to-build are relatively modest: 11.5 days during the first period, and 46.5 days during the second period. As expected, the lags are smaller during the first period since GPUs are more commonly available than ASICs. The total costs are lower with time-to-build than without, a finding that is in line with Proposition 2 and the impact of discounting on future profits. We also notice that the impact of delays on the calibrated rate of technological progress is negative in the first period, but positive in the second period. Without further data, it is difficult to tell whether this ambiguity is structural, or simply specific to our samples.

Finally, note that the parameters are identified with much higher precision in the second period. Three factors explain why the first period calibration is so fuzzy. First, Bitcoin price was extremely volatile. Second, Bitcoin experienced a long slump, a period known as the first crypto winter within Bitcoin community. This resulted in a nearly flat hashrate for most of the sample, as can be seen in Figure 4. From the standpoint of our calibration strategy, this means that there are relatively few data points where free entry binds, making it difficult to pin down the structural parameters. Finally, the technology was less homogenous during the first period. In particular, it witnessed the emergence of mining pools. **?** (**?**) explain why market entry was incentivized by this new opportunity to share risk, thus generating a positive bias in our calibration of the rate of progress. For all these reasons, we henceforth treat the second period as our sample of reference.

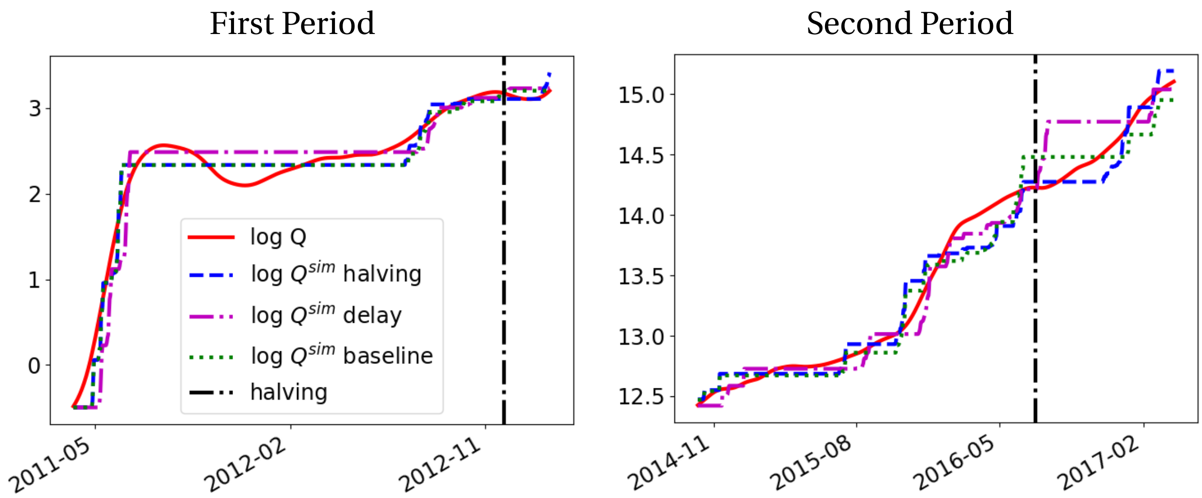
Predicted vs actual hashrate.— The calibration procedure provides us with an estimate for the reflecting barrier, $\overline{P}_0$, as well as for its trend, a. Using these two values, we can run the two-step algorithm described above to simulate the network hashrate Q^{sim}. We report the simulated series against their empirical counterpart in Figure 4. In spite of its very parsimonious structure, the baseline model tracks the actual hashrate remarkably well.

We nonetheless notice some temporary discrepancies. The most striking is around the second halving date (2016/07/09). This should not be surprising since miners do not anticipate halvings in the baseline specification while they certainly do in reality. Figure 4 shows that this shortcoming is solved by the extended model with halvings. However, besides this specific period, the paths generated by the three models remain very close to each other. Due to the extreme volatility of the exchange rate, halvings affected miners' behavior only a couple of months ahead. It is actually more intriguing that such a disconnect between the simulation of the baseline model and the data is not apparent around the first halving date (2012/11/28). According to our model, miners had a very short investment horizon during the first period because the rate of technological progress was extremely high.

Another noticeable difference between the actual and simulated hashrates is that the former sometimes decreases, especially during the first period, while the latter never does. Our models cannot generate any decrease in hashrate because they are based on the premise that investment is totally irreversible. We will address this shortcoming in Section 4 where we allow miners to mothball and scrap their hardware.

These discrepancies do not invalidate our approach because its objective was to capture medium to long run adjustments in hashrate, and it largely succeeds in this respect. Yet one may argue that such a conclusion is too generous because our procedure minimizes the distance between the simulation and the data, and so would fit the data fairly well even if the model were misspecified. Remember, however, that the baseline model uses only two parameters to fit times series of 608 and 913 data points. For each simulation, we start from the initial hashrate and then let the model run without using intermediate realizations to correct its output. Hence, any funda-

Figure 4: Simulated vs Observed Hashrates



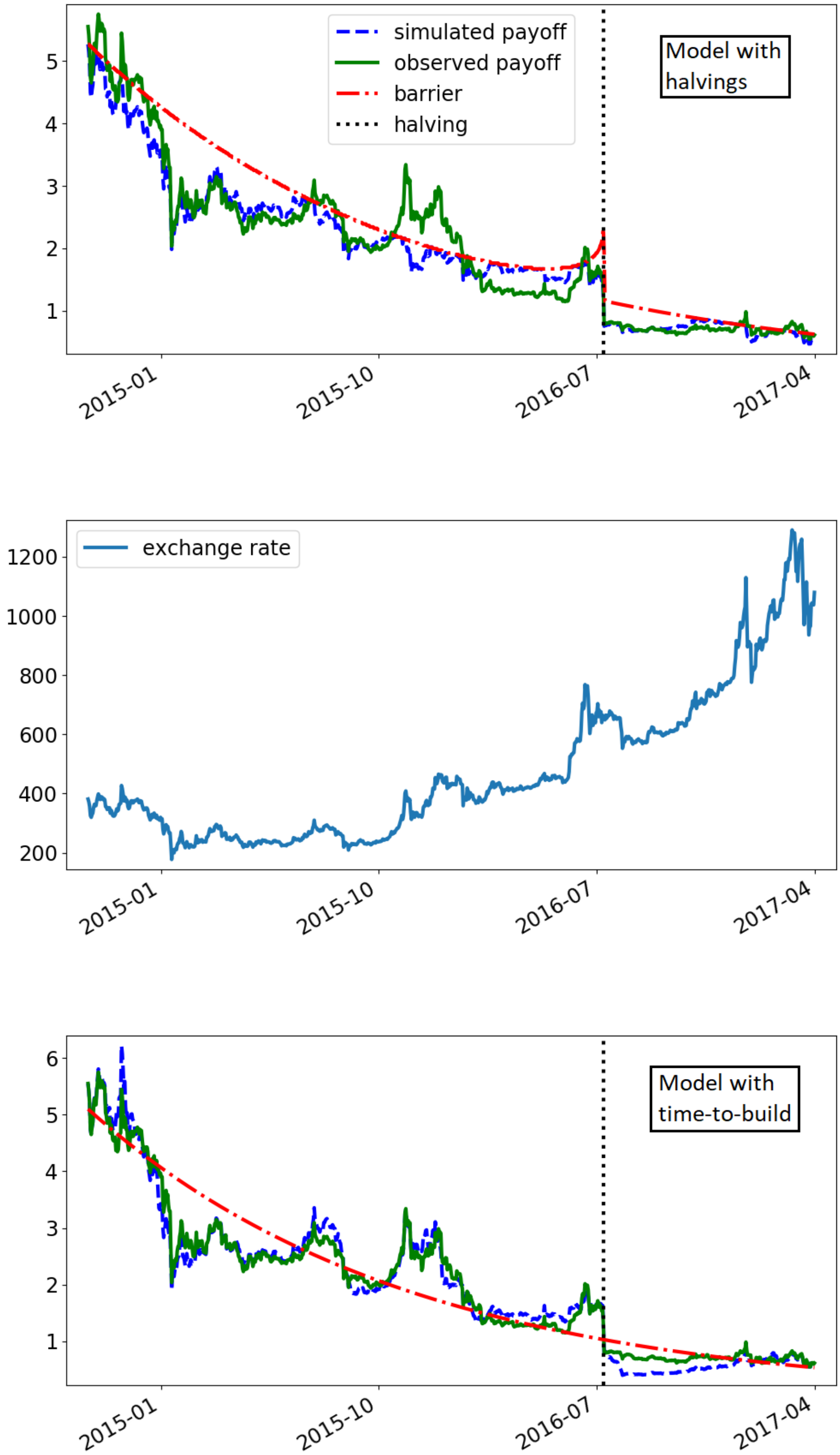
mental misspecification would generate a noticeable gap between the simulation and the data, at least over some time intervals. The fact that there is no deterioration of the models' accuracy is therefore a convincing argument in favor of their validity. We now provide additional evidence in favor of this interpretation by performing out-of-sample experiments, and by comparing the entry rules generated by the models with the ones prevailing in the data.

We assess the model's ability to match out-of-sample data by dividing the second period into a fit period and a test period. We calibrate a and $\overline{P}_0$ on the fit period only and find that, even when the fit period is short, the calibrated values remain close to the ones based on the full sample. Hence the predicted hashrate stays accurate several years after the end of the fit period, as shown in the Technical Appendix H.

Inspecting the entry rule.—Besides assessing the accuracy of the simulated hashrate, we can also check whether the behavior of payoffs is consistent with the entry rule. For this purpose, we report in Figure 5 the simulated and observed payoffs series, as well as the ฿/ $ exchange rate to ease interpretation. For the sake of conciseness, we only report the payoff series of the second period.[25] The upper-panel of Figure 5 focuses on the model with halvings whose barrier shifts down by 50% on the halving date. This drop is preceded by a period where the barrier slopes up because miners anticipate the fall in future revenues, and so, procrastinate further before entering the market. But the increase in the barrier becomes noticeable only a few months before the halving

[25]We show in the Technical Appendix B that the fit of the payoff series during the first period is also very convincing.

Figure 5: Simulated vs. Observed Payoffs



and is therefore not relevant for most of the preceding period. This might be surprising given that a division by two of revenues seems like a huge loss; yet one has to put it into perspective by comparing it to the very rapid obsolescence of hardware, and to the extreme volatility of Bitcoin price. These two forces imply that a loss of 50% in rewards over a few months was not an implausible event. Accordingly, as can be seen comparing the two panels of Figure 4, the lower the rate of technological progress and the volatility of Bitcoin, the more noticeable halvings are.

As predicted by our model, observed payoffs remain below the barrier most of the time and tend to reflect downwards when they reach its vicinity. This is remarkable since $\overline{P}_t$ was calibrated regardless of this requirement, fitting the hashrate only. Although the observed and simulated payoff series are often superimposed, they differ over some short time intervals. These discrepancies are usually triggered by extreme increases in the exchange rate, as can be seen comparing the upper-panel of Figure 5 with the middle-panel that contains Bitcoin price series. Quite intuitively, when the exchange rate goes up by 10% or more in one day, miners cannot enter the market as quickly as the model predicts because they are facing, among many other frictions, delivery and manufacturing delays.

This conjecture is confirmed by the lower-panel of Figure 5 which reports the payoff series with time-to-build. The simulation now almost perfectly tracks the data. In particular, sudden price increases do not anymore drive a wedge between the model and the data. Instead, they push both series above the entry barrier for a short amount of time. This is possible in the model with time-to-build because the entry threshold acts as a reflecting barrier for the committed hashrate, H_t, and not for the actual hashrate, Q_t. Hence, a sudden increase in the price of Bitcoin triggers a jump in H_t, as new miners decide to enter the market, but the impact of their decision is delayed by the time-to-build. This explains why the payoff series tends to revert after a big price surge: On impact, it follows the price trajectory, and then decreases a few weeks later, once the mining hardware has been delivered.

To take stock, out-of-sample experiments and inspecting the entry rule confirm that the baseline model reliably predicts the evolution of the network hashrate. Yet, its accuracy temporarily deteriorates around halving dates and after big price surges, two shortcomings that can be addressed by the introduction of halvings and time-to-build. These adjustments do not strongly affect the calibrated values of the parameters which remain rather stable across the three specifications. Having established the soundness of our approach, we now consider two extensions. The first one will allow us to separate the investment from the operational costs, while the second one will enable us to match the 2017 bubble and its aftermath.

4 Reversible Investment

4.1 Mothballing and scrapping options

The network hashrate never decreases in our simulations because they hinge on the assumption that miners always keep their hardware in mining mode. In practice, miners have the option to switch off their hardware, and they can switch them back on should mining become profitable again. We now generalize our approach to take these options into account. We assume that mining hardware can be kept idle at zero costs. Then the mothballing decision is fully reversible, and as such does not involve any forward-looking component: Machines are mining whenever their flow revenues are higher than their operating costs. Hence the per-period profits at time t of a miner entered at time τ are equal to $\max(P_t - C_\tau, 0)$, and her value function reads

$$V(P_t, \tau) = \mathbb{E}_t \left[\int_t^{+\infty} e^{-r(s-t)} \max(P_s - C_\tau, 0)\, ds \right]. \tag{10}$$

If there is no technological progress, all miners pay the same operating costs (C_τ is constant) and thus face the same problem. Then the industry equilibrium features two reflecting barriers: an upper-barrier generated by the entry of new miners which pushes payoffs downwards until free entry is satisfied again, and a lower barrier generated by the exit of incumbents which pushes payoffs upwards until miners are indifferent between operating and stopping their hardware.[26] With technological progress, however, the structure of the industry is much more intricate. Then miners cannot all be indifferent since they bear different operating costs. The least productive miners are the first to mothball their hardware, and they do so until the marginal miner makes zero flow profits. This endogenous cutoff depends on the distribution of vintages among incumbents. Thus the law of motion of P_t is not anymore a function of current revenues only, but also of the vintage distribution. This in turn greatly complicates the decision of prospective entrants who now have to solve a problem which includes a distribution function among its state variables.

[26]See **?** (**?**) for a model with two reflecting barriers generated by workers entry and exit.

Instead of following this direct approach, we take the view that prospective entrants do not have access to the data required to solve the full information problem. Finding the vintage of all hardware is an extremely tedious, if not impossible, task. It is therefore quite unlikely that miners actually looked for this information before investing and, even if they did, they would only have observed a very noisy measure of the actual distribution. We assume instead that potential entrants make their decisions considering only the current value of their flow payoffs. We establish below the plausibility of this restriction by showing that mothballing and scrapping have very little impact on the hashrate, so that entrants cannot significantly benefit from solving the full information problem. From a formal standpoint, we assume that miners' expectations satisfy the following Markov property.

Assumption 6. *Let $\mathcal{F}_t \equiv \sigma(P_s; 0 \leq s \leq t)$ denote the filtration generated by P. We assume that, for all measurable set $A \in \mathbb{R}_+$ and all $s > t$, $\mathbb{P}^e\left(P_s \in A | \mathcal{F}_t\right) = \mathbb{P}^e\left(P_s \in A | P_t\right)$, where $\mathbb{P}^e(\omega)$ is the probability of event ω as evaluated by potential entrants, and $\mathcal{F}_t$ is the filtration generated by P_t.*

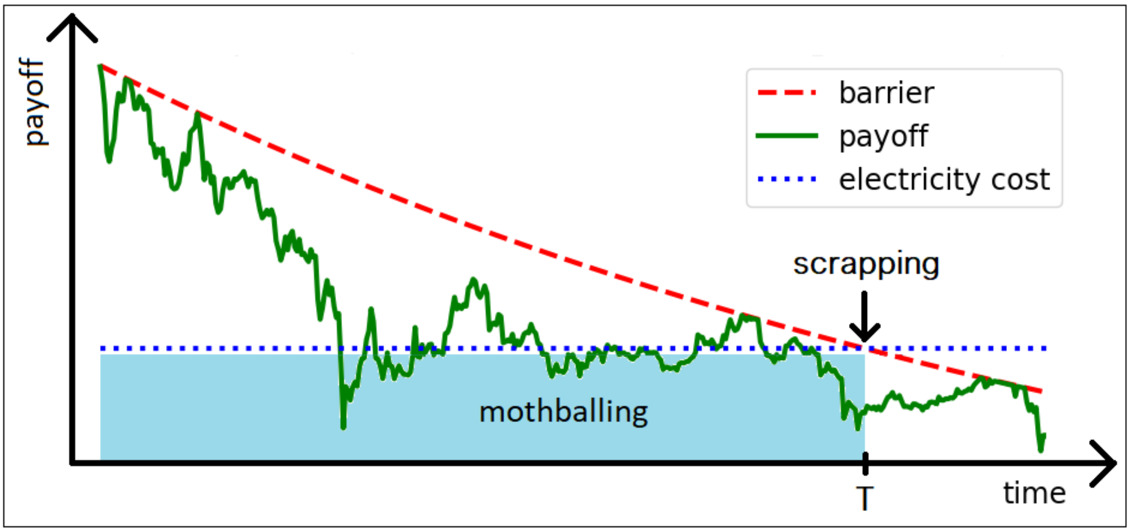
We show in the proof of Proposition 3 that, replacing Assumption 3 with Assumption 6, does not fundamentally alter the structure of the equilibrium. It remains characterized by an entry barrier $\overline{P}_t$ which decays at the rate of technological progress. Since payoffs are reflected downwards when they hit the barrier, it will never be profitable to operate a piece of hardware which is so obsolete that its operating costs exceed the entry barrier. A typical mining cycle is illustrated in Figure 6: Hardware are mothballed whenever payoffs fall below its operating costs, as indicated by the colored area; and they are scrapped when the entry barrier crosses the operating costs.

Proposition 3. *Assume that assumptions 1, 2, 4 and 6 hold true. Then there exists a $\overline{P}_0 > 0$ such that $\left(P_t, \overline{P}_t = \overline{P}_0/A_t\right)$ is an industry equilibrium that satisfies the requirements of Definition 1.*

Simulating the hashrate.— The addition of an exit threshold makes it impossible to analytically solve for the entry barrier $\overline{P}_t$. Moreover, simulating the hashrate is more complicated than for the baseline model because one must keep track of the operating costs, as well as of the activity status of all miners. The inputs of the algorithm are the block rewards R_t, the rate of technological progress a, the initial hashrate, the operating costs and the entry barrier $\left(Q_0, C_0, \overline{P}_0\right)$.[27]

[27]We also need to initialize the vintage distribution of all active miners. In line with Assumption 6, we

Figure 6: Mothballing and Scrapping Regions

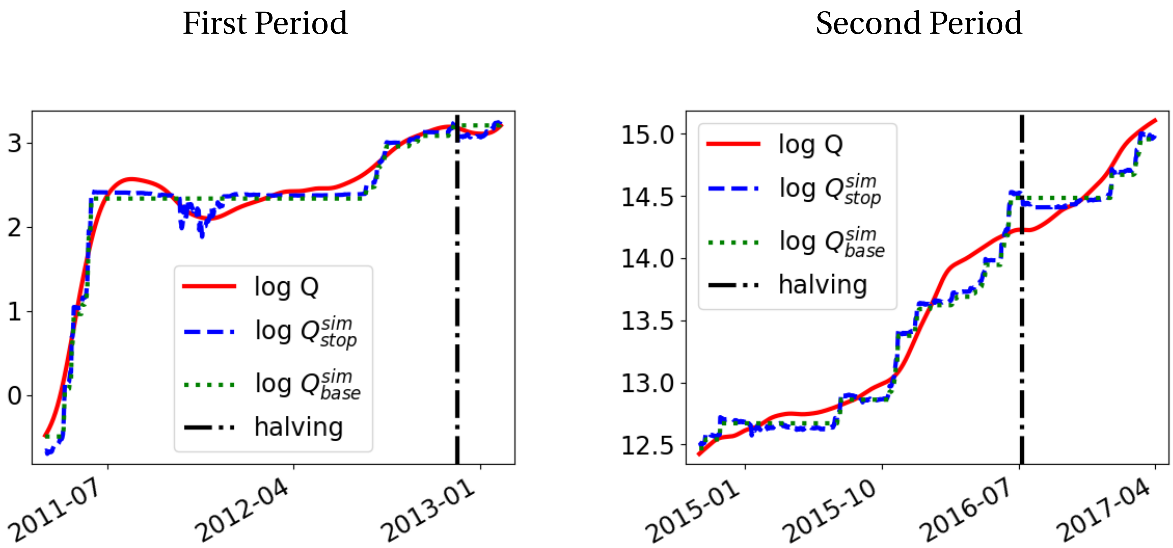


The simulation procedure works as follows. For each day, we start by deleting from the database all miners whose operating costs are bigger than the entry barrier since they will never find it profitable to mine in the future. Then, given the new value of R_t, we compute the temporary payoff faced by miners if the hashrate remains constant. Depending on its value, two configurations may arise. First, if this temporary payoff is smaller than the operating costs of the least efficient–i.e. oldest–active miner, we know that some miners should switch off their hardware. Thus we let the least efficient miners mothball their hardware, and update the temporary payoff until no active miner prefers to remain idle. Alternatively, if the temporary payoff is higher than the operating costs of the most efficient inactive miner, we know that some miners should switch on their hardware. Finally, if all incumbents are active and the temporary payoff is still bigger than the entry barrier, we let new miners enter the market until the temporary payoff is equal to the entry barrier.

Predicted vs actual hashrate.—As before, we calibrate a, $\overline{P}_0$ and C_0 so as to minimize the distance between the simulated and actual hashrates. Figure 7 reports the resulting series along with the prediction of the baseline model. As expected, the model with exit fits the data better whenever the hashrate falls. But the improvement is rather

find that knowing the true distribution of miners' vintages does not significantly improve forecast accuracy. A series of robustness checks demonstrates that the initial choice of vintages hardly affects the simulated paths after a couple of days. We therefore pick a distribution for which the mass of miners of any vintage is inversely proportional to the price of their hardware, as would have happened if the environment were deterministic.

Figure 7: Simulated vs Observed Hashrates



marginal because significant decreases were exceptional. Most of the time the predictions of the two models coincide, thus substantiating our claim that Assumption 3 is a reasonable benchmark. Adding reversibility does not fundamentally affect the hashrate trajectory because of the very high rate of technological progress. Scrapping is profitable for mining rigs that were purchased a few years ago, but they have become so obsolete that they only account for a negligible share of the network hashrate. Yet, pretending that investment is irreversible is not totally innocuous. It leads to an overestimation of the lifetime operating costs since, in practice, all mining rigs are eventually turned off. Having a framework that takes this option into account makes it possible to correct the cost bias.

4.2 Disentangling investment from operating costs

We now explain how one can use the model with reversible investment to disentangle the price of mining hardware from their operating costs. The simulations reported in Figure 7 show that miners who ignored the impact of mothballing and scrapping decisions were nonetheless able to make accurate predictions about the network hashrate. Thus we strengthen Assumption 6 and consider that entrants disregard the rare instances where the hashrate shrinks.

Assumption 7. *When forming their expectations, potential entrants ignore the impact that mothballing and scrapping have on the network hashrate.*

Entrants who base their expectations on the premise that incumbents will remain operational can disregard the vintage of the technology operated by other miners. Thus Assumption 7 implies Assumption 6, although the converse is not true. Assumption 7 ensures that agents expect payoffs to follow a reflected GBM as in the baseline model. Knowing the distribution of P allows us to infer the expectations of prospective entrants. In particular, equation (10) is compatible with free entry if and only if

$$I_t \geq \int_t^{+\infty} e^{-r(s-t)} \left(\int_0^{\overline{P}_s} \max\left(y - C_t, 0\right) f^e_{P_s|P_t}(y)\, dy \right) ds, \text{ for all t,} \tag{11}$$

where $f^e_{P_s|P_t}(\cdot)$ denotes the distribution, as anticipated by entrants, of P_s conditional on P_t. For brevity, we relegate the explicit expression of f^e to the Technical Appendix J. Using the calibrated values of a, $\overline{P}_0$ and C_0 to evaluate the integral on the right-hand side of (11) yields the investment cost I_0 consistent with free entry. Moreover, condition (11) also places an upper bound on the overall costs of entry paid by miners. Let T denote the time it takes for the entry barrier to reach the operating costs of entrants. Given that the entry barrier decays at the rate of technological progress, we have $T = \log\left(\overline{P}_0/C_0\right)/a$. The total costs paid by miners who entered at time 0 must necessarily be inferior to $K_0 = I_0 + \int_0^T C_0 e^{-rt} dt$ because they will never find it profitable to mine after date T.

Table 2 contains the parameter values resulting from these computations along with their counterparts for the baseline calibration. The overall costs of entry are lower in the model with exit than in the baseline model. This is not surprising because miners now have a finite horizon. Given that costs are smaller, entries happen sooner, which translates into a lower entry barrier.

Comparing calibration to price data.— Overall costs are made of two components: the initial purchase of mining hardware and the daily operating costs. Assumption 7 allows us to disentangle them. Their values are reported in the fourth and fifth lines of Table 2.[28] In both subperiods investment costs amount to around two thirds of the overall costs of entry. Hence all seignorage income was not spent on electricity, as often argued, but instead largely captured by mining rigs producers.

The plausibility of our calibrated parameters can be assessed by comparing them

[28]The calibrated value for I_0 depends on r which we set equal to 0.1. However, our results are not very sensitive to the choice of r because the obsolescence process is so fast that miners do not operate their hardware for a very long time. For example, $r = 0.05$ yields $I_0 = \$1033$ in the second period, while $r = 0.2$ yields $I_0 = \$943$.

to online data on the selling price of mining hardware. To the best of our knowledge, there is no official source for hardware characteristics and availability dates. We therefore retrieved our data from different websites, selecting those which offered the most reliable information, namely Bitcoin wiki and the Bitcoin forum. We collected data on state-of-the-art mining hardware at the time they were put on the market.[29] We focused on the post-2014 period because there is too much uncertainty around the type of hardware that was used before the introduction of ASICs.

Figure 8 reports the electricity consumption and market price of hardware, along with the price series predicted by the model.[30] It indicates that our calibration of the cost of investment and of the rate of technological progress are consistent with online data. Besides supporting the parameters resulting from our calibration strategy, Figure 8 also validates Assumption 4 according to which the price of mining hardware and their energy consumption should decrease at the same rate. There is, however, a specific time window where the assumption fails to hold: Between August 2017 and February 2018, the price of mining rigs skyrocketed from around $2,000 to $5,200. This temporary increase was triggered by the concurrent bubble in Bitcoin price. We now explain how our model can be modified to capture this temporary deviation from the long-run trend.

5 The 2017 Bubble and its Aftermath

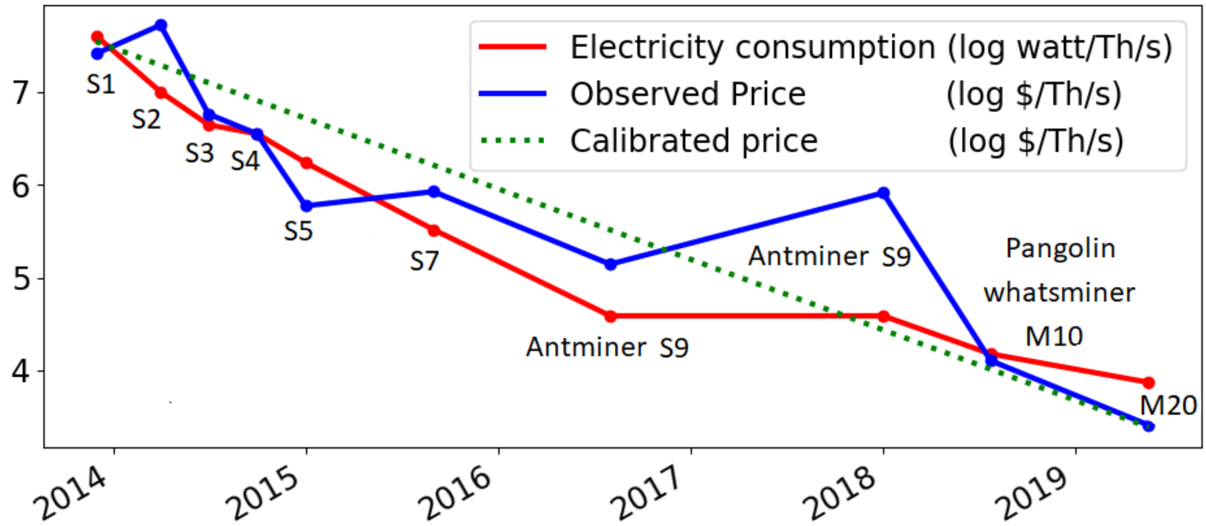
So far we have restricted our attention to pre-2018 data. We have excluded recent observations because Bitcoin experienced a period of trading frenzy during the winter of 2017: From three thousand dollars in September 2017, Bitcoin exchange rate shot up to nearly twenty thousand in December, and then, dropped back to six thousand in February 2018. This bubbly episode raises a significant challenge because it led to a structural break in the relation between the exchange rate and the network hashrate. As shown in Figure 9, if the relation had remained stable, the hashrate should have been five times higher than its actual value at the peak of the bubble. The discrepancy between the observed hashrate and the one that would have resulted from our frictionless model is explained by three different factors.

First, market entry was constrained by the manufacturing capacity of ASICs pro-

[29] The online data and their sources are reported in the Technical Appendix K.

[30] We extrapolate the model's prediction to cover all the sample where online price data are available.

Figure 8: Calibrated vs Observed Rate of Technical Progress



ducers. In May 2017, there were approximately 230,000 active mining rigs. Between May and December 2017, the ฿/$ exchange rate was multiplied by 12. To keep up with this pace, approximately 2,700,000 new mining rigs would have had to be installed within eight months only. Such a dramatic increase was bound to stretch the capacity of Bitmain, the main manufacturer of ASICs for Bitcoin mining. Second, Bitmain exercised his monopoly power and decided not to flood the market with new hardware in order to raise their selling price. Indeed, the price of an Antminer S9 mining rig was multiplied by three between the beginning and the climax of the bubble, and then divided by around four during the following crash.[31] Third, as the bubble collapsed within a few months only, prospective miners simply cancelled their orders or backtracked on their decision to enter the market.

We take these constraints into account by assuming that investment costs are not constant but increasing in aggregate investment. More precisely, let q_t denote the *flow of entrants* at date t, so that $Q_t = Q_0 + \int_0^t q_s ds$. The investment costs for the marginal entrant are now given by

$$I(q_t; Q_t, A_t) = \frac{I_0}{A_t}\left[1 + \left(\frac{q_t}{bQ_t}\right)^{\eta}\right], \text{ for } I_0, b \in \mathbb{R}_+, \text{ and } \eta > 1. \tag{12}$$

Congestion externalities are captured by the convex function on the right-hand side of (12): An increase in the flow of entrants, q_t, stretches manufacturing capacities, thus raising the cost of entering the market. The parameter η controls the convexity of the

[31] See Technical Appendix K.

cost function.[32] As η increases, I converges towards an hyperbolic function with an asymptote at bQ_t. Hence, one can think of bQ_t as the production capacity of ASICs manufacturers, which is assumed to be proportional to the number of operational units.

For brevity, the derivation of the optimal entry rule under (12) is relegated to the Technical Appendix M. We demonstrate that, as in the baseline model, entry is a function of P_t only, and that there exists a threshold $\overline{P}_0$ such that $dQ_t = 0$ whenever $P_t < \overline{P}_t = e^{-at}\overline{P}_0$. However, $\overline{P}_t$ is not anymore a reflecting barrier. Due to the convexity of the cost function, aggregate investment is now absolutely continuous with respect to time.[33] Whenever $P_t > \overline{P}_t$, an Hamilton-Jacobi-Bellman equation, whose solution can be numerically approximated, pins down the positive relationship between q_t and P_t.

We include the most recent observations and select, as before, the parameters that minimize the distance between the simulated hashrate series and its empirical counterpart. We also include online price data for mining hardware in our set of targeted moments. This enables us to identify the convexity parameter η since it controls the elasticity of the hardware price with respect to aggregate investment.[34]

Figure 9 shows that the baseline model vastly overestimates entry during the bubbly episode, and then, due to the irreversibility of past investment, remains well above the actual hashrate for the rest of the sample. By contrast, calibrating the model with convex costs enables us to match the hashrate over the full sample. The lower-panel which reports the normalized price series, $\tilde{I}_t = A_t I_t$, indicates that the simulated investment costs are also in line with the data. As predicted by the baseline model, the investment costs decrease at the rate of technological progress, thus generating a flat profile when they are normalized. There is, however, a notable exception during the height of the 2017 bubble, where the investment costs increased dramatically. This means that the marginal cost function (12) is essentially flat until it nears the threshold bQ_t, and starts to increase exponentially.

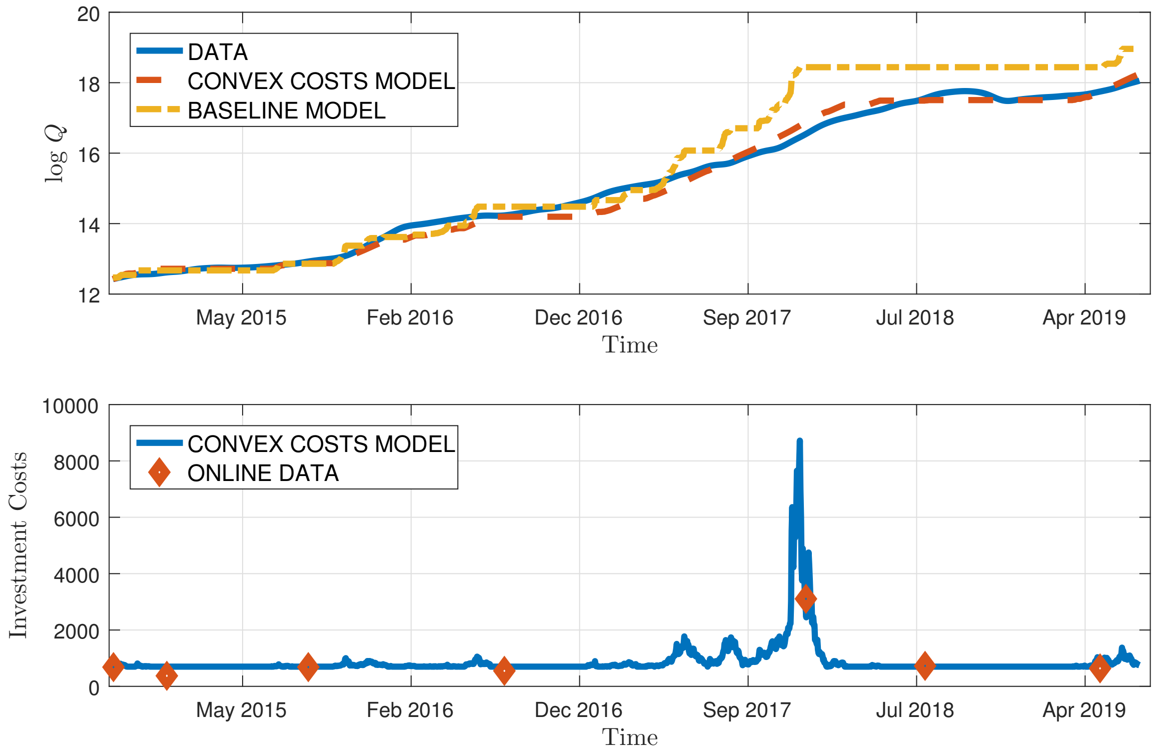
The calibrated parameters are reported in the legend of Figure 9. The value $b = 3$ implies that the congestion externality becomes relevant solely at very high rates of investment amounting to a twentyfold annual increase in the network hashrate. The

[32] In particular, note that $I(q_t; Q_t, A_t)$ is isomorphic to our baseline specification when $\eta = 0$.

[33] By contrast, aggregate investment was a singular control process in the baseline model with dQ_t being (infinitesimally) positive only on a measure-zero set of time points.

[34] See the Technical Appendix M for further details on the calibration procedure.

Figure 9: Model with Convex Costs



PARAMETERS: $r = .1$, $a = 0.65$, $\eta = 14.1$, $b = 3$.

NOTE: INVESTMENT COSTS ARE MULTIPLIED BY THE EFFICIENCY COEFFICIENT A_t.

calibration $\eta = 14.1$ confirms that the cost function is indeed extremely steep in the vicinity of bQ_t. This explains why the bubble triggered a sudden burst in the cost of entry which prevented miners to flood the market during the bubbly episode. Interestingly, our calibration demonstrates that, even in the face of an event as extreme as Bitcoin bubble, one does not to need to abandon the efficient market hypothesis by assuming, for instance, that miners refrained from investing because they anticipated the incoming crash. Instead, we find that their behaviour is explained by large variations in the price of their main input factor.

6 Discussion

Having established the accuracy of our framework, we use it to address the questions that motivate our analysis. First, is Bitcoin design really generating a competitive environment for its mining industry and, if so, which actors were able to appropriate Bitcoin's seigniorage income? Second, what forecasts can we draw about the evolution of Bitcoin's carbon footprint?

6.1 Revenues allocation

Oligopolistic industry.— Although we cannot reject the premise that miners operate under perfect competition, our results do not prove that the premise is true either. One should be careful when interpreting our findings because, as first established by **?** (**?**), a similar entry rule can hold even when the industry is oligopolistic. More precisely, assume that, instead of being populated by a continuum of atomistic miners, the market is controlled by n symmetric firms. Then, provided that assumptions 1, 3, 2 and 4 hold, there exists a symmetric Nash equilibrium where each firm increases its mining power when P_t reaches the trigger level $\overline{P}_t^n = e^{-at}\overline{P}_0^n$. As in the baseline model, P_t is a GBM reflected at $\overline{P}_t^n$, where

$$\overline{P}_0^n = \frac{n}{n-1}\frac{\beta(r-\alpha)}{\beta-1}K_0^n, \text{ and } K_0^n = I_0 + \frac{C_0}{r}. \tag{13}$$

Given that we identify the entry barrier without relying on the model, our calibration strategy returns the same threshold independently of whether the industry is competitive or not. The degree of competition matters at the second stage, when we infer the cost parameters that are consistent with the barrier. Setting (7) equal to (13), we find that the costs in the oligopolistic and competitive models are proportional as $K_t^n = [(n-1)/n]\,K_t$. Calibrated costs are lower when the industry is oligopolistic because firms are able to extract some rents.

We can easily construct an intuitive measure for the oligopolistic rents. First, note that the net present value of an additional unit of hashpower is equal to $W(P_t) - K_t^n$, where $W(P_t) \equiv \mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)}P_s ds\right]$ denotes the expected value of discounted payoffs. The expectation operator for P does not depend on the degree of competition because it does not affect the calibrated barrier. Hence, free entry is satisfied in the baseline model if and only if $W(\overline{P}_t) = K_t$. It follows that if we evaluate the net present value of entrants and divide it by the overall costs of entry, we find that the option premium reads[35]

$$\text{Option Premium} = \frac{W(\overline{P}_t) - K_t^n}{K_t^n} = \frac{1}{n-1}.$$

[35]Given that the mining technology exhibits constant returns to scale at the aggregate level, the option premium is not well defined when $n = 1$, that is when the market for mining is controlled by a monopolist.

As expected, when n goes to infinity, the option premium converges to zero so that free entry holds. The option premium rapidly decreases in the number of competitors. For instance, the option premium is below 10% of expected revenues if, as suggested by **?** (**?**), more than 10 mining firms are competing. Incidentally, our model unambiguously rejects high degrees of concentration, with n equal or smaller than 4, since they would imply that the overall costs of entry are smaller than the market price of mining hardware.

Input producers.— Since miners are not able to extract significant rents, they channel most of their income towards the producers of their input factors, namely hardware manufacturers and electricity suppliers. As large mining farms are scattered around the globe (with major hubs in China, North-America, and Scandinavian countries), evaluating their impact requires a geographic analysis that would go well beyond the scope of this paper. **?** (**?**) provide the most comprehensive survey of mining locations but, as far as we know, no study has yet used their data to assess the effect that mining has on the revenues of local electricity providers.

By contrast, the production of ASICs was, until recently, a very concentrated activity, with Bitmain claiming a market share of 74.5% of 2017 sales revenues. In their 2018 application proof for an IPO on the Hong Kong Stock Exchange,[36] Bitmain indicated that it had been able to generate $\$952.6$ million in profits out of $\$2.5$ billion in revenues, thus reporting an healthy profit margin of 37.8% in 2017. To put these numbers into perspective, the overall seigniorage income generated by Bitcoin over the same year was equal to $\$3.18$ billion. Hence, in line with our findings, all seignorage income was not spent on electricity, but instead largely captured as a monopoly rent by ASICs manufacturers. The quasi-monopolistic position enjoyed by Bitmain was finally contested in 2018 by the arrival of new competitors. In particular, Halong Mining, which uses chips produced by Samsung, entered the market in March 2018, proposing a mining rig called DragonMint 16T that was 30% more efficient than the previous state of the art. The entry of this new competitor triggered a dramatic drop in the price of Bitmain's product, as can be seen in Figure 19 in the Technical Appendix K.

[36]Prospectus available at http://templatelab.com/bitmain-ipo-prospectus/. Note that Bitmain was drawing part of its revenues from proprietary mining and mining services. Yet hardware production accounted for the bulk of Bitmain's activity, namely 90% of its overall revenues.

6.2 Electricity consumption of Bitcoin

The erosion of Bitmain's dominant position is lowering the cost of entering the mining market. At the same time, price data indicate that Bitcoin is providing lower returns and not exhibiting as much volatility as in the past. We also expect the rate of technological progress to slow down and converge, in the best case scenario, to the value predicted by Moore's law. What will be the impact of these ongoing changes on Bitcoin's electricity consumption? Having a structural model enables us to answer this question in a quantitative manner.

The entry barrier fully characterizes the industry dynamics for any price trajectory. Most of the time, however, payoffs will be below the barrier. Thus we need to evaluate the payoffs probability distribution in the no-entry region. Fortunately, the ergodic distribution of reflected Brownian motions admits a closed-form solution. In order to apply it to our setting, we first notice that the detrended payoff, $\tilde{P}_t \equiv P_t A_t$, is a GBM reflected at $\overline{P}_0$. Then it is well known (see for instance **?** (**?**)) that $\tilde{P}_t$ has a long-run stationary distribution whenever $\alpha + a > \sigma^2/2$, a condition which is comfortably satisfied by our calibrated parameters. Using $f_{\tilde{P}}$ to denote the ergodic density of $\tilde{P}$, we find that, for all $y \in (0, \overline{P}_0]$,

$$f_{\tilde{P}}(y) = \frac{\gamma}{y}\left(\frac{y}{\overline{P}_0}\right)^{\gamma}, \text{ where } \gamma \equiv \frac{2\left(\alpha + a - \sigma^2/2\right)}{\sigma^2}.$$

In contrast to $\tilde{P}$, the network hashrate, Q, follows a non-stationary process, and thus fails to have long-run distribution. Yet, a simple change-of-variable allows us to compute the steady-state distribution of Q conditional on R and A, as

$$\begin{aligned} f_Q(Q; R, A) &= f_{\tilde{P}}\left(\tilde{P}(Q, R, A)\right)\frac{\partial \tilde{P}(Q, R, A)}{\partial Q} \\ &= -\gamma Q^{-(\gamma+1)}\left(\frac{RA}{\overline{P}_0}\right)^{\gamma}. \end{aligned}$$

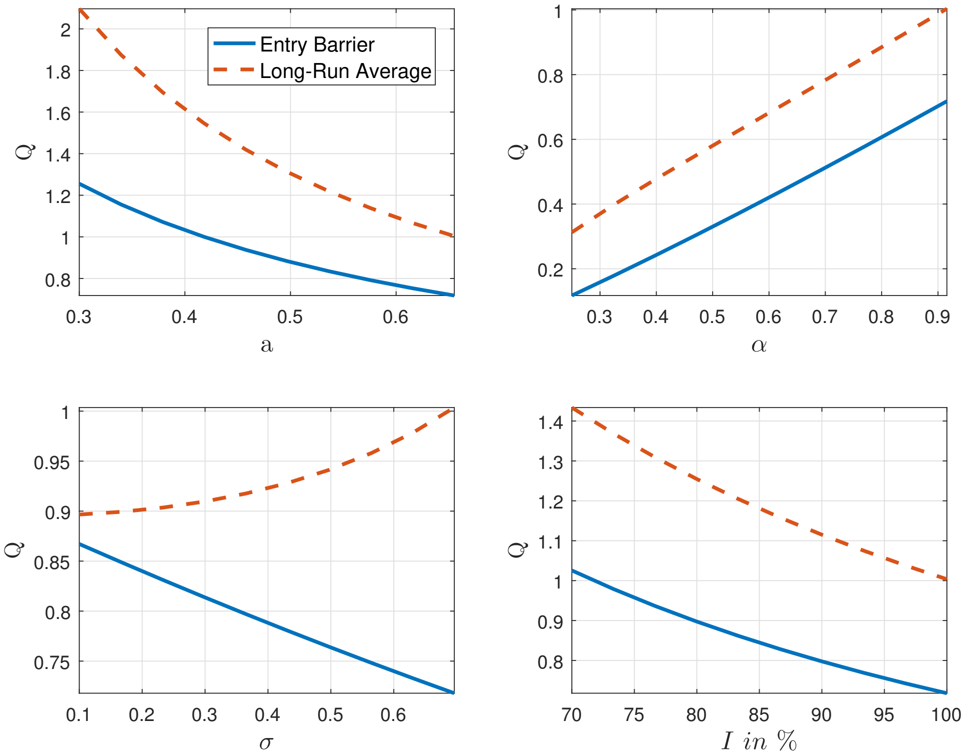
Integrating f_Q over the consistent values of Q finally yields its conditional mean

$$\mathbb{E}[Q; R, A] = \int_{\infty}^{\frac{RA}{\overline{P}_0}} Q f_Q(Q; R, A)dQ = \left(\frac{\gamma}{\gamma - 1}\right)\frac{RA}{\overline{P}_0}. \tag{14}$$

The electricity consumption of the network is inversely proportional to the efficiency parameter A. Hence

$$\frac{\mathbb{E}[Q; R, A]}{A} = \left(\frac{\gamma}{\gamma - 1}\right)\frac{R}{\overline{P}_0} \tag{15}$$

Figure 10: Impact of Parameters on Hashrate



is the best guess one can make about the long-run energy requirements of Bitcoin. Since (15) is linearly increasing in block rewards, our model confirms the widely held belief that halvings will lower Bitcoin's electricity consumption. Our contribution consists in characterizing the slope of the relation between R and Q. Figure 10 reports the impact of the parameters on the conditional expectation of Q, as well as on its value at the entry barrier. For readability, we set R and A equal to one. We also normalize to one the average value of Q generated by the calibrated parameters. Hence, all changes can be interpreted as percentage deviations from the calibrated model.

First we lower a from its calibrated value to the one consistent with Moore's law. The results reported in the north-west panel of Figure 10 show that a decrease in the rate of technological progress significantly raises the average hashrate. As hardware becomes obsolete at a lower pace, miners are able to devote a greater share of their income to operating costs. Not surprisingly, the growth rate of block rewards, α, has a positive impact on the level of investment as more miners find it attractive to enter the market. The impact of the volatility coefficient, σ, is more intriguing since it has opposite effects on the entry barrier and average hashrate. When σ increases, miners are more reluctant to enter the market because they anticipate that large negative shocks are more likely to leave them burdened with excess mining power.[37] This added dispersion is what drives apart the conditional expectation and entry barrier in the southwest panel of Figure 10. As these opposite effects partially compensate each other, σ has a positive but relatively modest effect on the average hashrate. Finally, we report the impact of a decrease in the selling price of mining hardware I. We use Bitmain's 2017 profit margin of around 30% as an upper-bound on the price correction. When hardware become cheaper, miners enter the market in greater numbers and devote more of their resources to electricity consumption.

Finally, our framework predicts that energy requirements are increasing in the degree of competition among miners. Let $\mathbb{E}^n[Q; R, A]$ denote the conditional expectation of Q when the mining market is oligopolistic with n symmetric firms. Reinserting (13) into (14), we find that an increase in the number of competing firms n raises the network hashrate since $\mathbb{E}^n[Q; R, A] = (1 - 1/n)\,\mathbb{E}[Q; R, A]$. Given that normative studies conclude that Bitcoin hashrate is too high (see for instance **?** (**?**)), encouraging concentration in the mining market is likely to increase welfare.

What lessons can be drawn from these experiments regarding the future of Bitcoin's electricity consumption? The increased competition between hardware producers and, most notably, the decrease in the rate of technological progress will worsen Bitcoin's carbon footprint. For these trends to be contained, Bitcoin price will have to stabilize, thus suggesting that the carbon footprint may eventually place a hard cap on the price of Bitcoin.

7 Conclusion

One of the most enticing promise of Blockchains is their ability to support the maintenance of their infrastructure through a decentralized network. Decentralization has received a lot of attention, becoming a byword for Blockchains and their capacity to dislodge traditional intermediaries. Yet, the extent to which Blockchains truly achieve decentralization remains open to debate. We address this issue by assessing whether Bitcoin is indeed able to create a competitive market for intermediaries. To the best of our knowledge, our paper is the first to use a structural model to answer this question, and our conclusion is mostly positive: the confirmation and immutability of Bitcoin

[37] Note that Q and P are negatively correlated, hence a decrease in the value of Q at the entry barrier is equivalent to an increase in the entry barrier $\overline{P}$.

transactions is guaranteed by a market that operates under competitive conditions.

Our findings should be of interest beyond the community of economists working on Bitcoin and Blockchains. They demonstrate that Bitcoin is a remarkable example of mechanism design on a wide scale. Bitcoin protocol encodes several features that are rarely observed. Agents mostly face aggregate uncertainty. They operate a common technology which exhibits constant returns to scale at the micro-level, and earn revenues that are decreasing in aggregate capacity. All these characteristics make the mining market a perfect laboratory for models of industry dynamics, all the more so since data are exhaustive, clean and publicly available. In particular, we show how one can observe the entry barrier using industry-level data only. As far as we are aware, no other industry has yet been used to construct such a direct measure, and it is therefore reassuring that the canonical model of industry dynamics convincingly replicates the evolution of mining capacity.

Our analysis also has normative implications that go well beyond the scope of model testing. It supports the view that Blockchains provide a meaningful alternative for the design of online platforms and marketplaces. The surge of the digital economy is raising ever more pressing concerns about the predatory behavior of platform owners. We find that their market power could be mitigated through the introduction of tokens, and the creation of markets for infrastructure maintenance. Scores of companies are trying to emulate Bitcoin design across various sectors of the digital economy. Our results indicate that, when properly harvested, market forces and price signals are indeed able to coordinate agents, thus avoiding the emergence of a monopolistic owner in favor of a market allocation of revenues among the many stakeholders.

Finally, we believe that our findings will be of interest to Bitcoin practitioners since our model provides a forecasting tool for investors willing to enter the mining industry. From a practical standpoint, it has three main implications. First, the hashrate of the network is closely related to the exchange rate and, in the event of a significant market crash, the hashrate barely moves in the short run due to the irreversibility of past investments. This is good news for the security of Bitcoin transactions but bad news for their carbon footprint. Second, around two thirds of all seigniorage income was not dissipated in electricity consumption, as often argued, but was instead spent on mining hardware. Third, we expect the energy efficiency of the network to deteriorate if the rate of technological progress decelerates from the high pace it has experienced so far.

Although our model is fairly accurate in the medium to long run, it assumes that the environment is stationary. Since this restriction is hard to maintain over a long horizon, a promising direction for further research would be to embed our framework into a non-stationary environment, and allow agents to update their priors. Future research should also strive to improve our granular understanding of the mining industry by building on the growing amount of geographical data. Finally, our modeling strategy is likely to apply to other cryptocurrencies. Taking into account the ability of miners to concurrently mine multiple cryptocurrencies would bring us closer to a proper understanding of the ecosystem built around Bitcoin.

8 Appendix

8.1 Proof of Propositions

Proof of Proposition 1 Let $W\left(P_t, \overline{P}_t, A_t\right) \equiv V\left(P_t, t\right) + C_t/r$ denote the value of an entrant net of operating costs as a function of the payoff P_t, the entry barrier $\overline{P}_t$ and the efficiency of the technology A_t. Assumption 4 requires that $dA_t = -aA_t dt$. Assumptions 1 and 2 imply that $dP_t = P_t\left(\alpha dt + \sigma dZ_t\right)$ whenever $P_t < \overline{P}_t$ because Q_t remains constant in that region of the payoff space. Finally, the law-of-motion of the entry barrier $\overline{P}_t$ is endogenous, and it is precisely the aim of this proof to show that the market for mining satisfies the equilibrium requirements stated in Definition 1 when $\overline{P}_t$ decreases at the rate of technological progress. Thus we conjecture that $\overline{P}_t = \overline{P}_0/A_t$, with $\overline{P}_0$ as in Proposition 1, and proceed to show that it is indeed optimal for entrants to wait until $P_t = \overline{P}_t$.

Having specified the law of motion of the three state variables allows us to use Ito's Lemma to derive the Hamilton-Jacobi-Bellman equation satisfied by the value function

$$\begin{aligned} rW\left(P_t, \overline{P}_t, A_t\right) &= P_t + \alpha P_t W_1\left(P_t, \overline{P}_t, A_t\right) - a\overline{P}_t W_2\left(P_t, \overline{P}_t, A_t\right) + aA_t W_3\left(P_t, \overline{P}_t, A_t\right) \\ &\quad + \frac{\sigma^2}{2} P_t^2 W_{11}\left(P_t, \overline{P}_t, A_t\right), \end{aligned}$$

when $P_t < \overline{P}_t$. Assume that $\alpha \neq r$,[38] then the general solution of the Hamilton-Jacobi-Bellman equation reads

$$W\left(P_t, \overline{P}_t, A_t\right) = \frac{P_t}{r-\alpha} + \frac{D_1}{A_t}\left(\frac{P_t}{\overline{P}_t}\right)^{\beta_1} + \frac{D_2}{A_t}\left(\frac{P_t}{\overline{P}_t}\right)^{\beta_2},$$

where D_1 and D_2 are constants whose values will be chosen so as to match some boundary conditions, while β_1 and β_2 are the two roots of the following quadratic equation

$$\mathcal{Q}(\beta) \equiv \frac{\sigma^2}{2}\beta(\beta-1) + (\alpha+a)\beta - a - r = 0.$$

Since $\mathcal{Q}(0) = -a - r < 0$ and the coefficient associated to the second order term is strictly positive, we know that one root, β_1 for instance, is strictly positive while the other root, β_2, is strictly negative.

[38] As r tends to α, $\overline{P}_0$ converges to $\left(I_0 + \frac{C_0}{\alpha}\right)\left(\alpha + a + \sigma^2/2\right)$ and $W\left(P_t, \overline{P}_t, A_t\right)$ tends to $\frac{I_0+\frac{C_0}{\alpha}}{A_t}\left(\frac{P_t}{\overline{P}_t}\right)\left[1 - \log\left(\frac{P_t}{\overline{P}_t}\right)\right]$.

The function W has to satisfy the following three boundary conditions. First, since $P_t = 0$ is an absorbing state, we must have $W(0, \overline{P}_t, A_t) = 0$. This implies that $D_2 = 0$, as otherwise the value function would diverge to either minus or plus infinity when P goes to zero. Second, the left continuity of the value function at the entry threshold $\overline{P}_t$ implies that there can be no arbitrage opportunity solely if the value function is flat at the contact point. This requirement, known as the smooth-pasting condition, is satisfied when $W_1\left(\overline{P}_t, \overline{P}_t, A_t\right) = 0$, i.e. when $D_1 = -\frac{\overline{P}_0}{\beta_1(r-\alpha)}$. Finally, the entry barrier is pinned down by the free entry condition $W\left(\overline{P}_t, \overline{P}_t, A_t\right) = I_t + C_t/r$, which implies that $\overline{P}_0 = (I_0 + C_0/r)\frac{(r-\alpha)\beta_1}{\beta_1 - 1}$.[39] Thus we have found a solution which satisfies all the requirements laid-out in Definition 1 for the existence of a competitive equilibrium.

Proof of Proposition 3 We proceed as in the proof of Proposition 1. We assume that $\overline{P}_t = \overline{P}_0/A_t$, for some $\overline{P}_0$, and show that it is indeed optimal for miners to enter the race when $P_t = \overline{P}_t$. The value function of an active miner entered at time τ reads $W\left(P_t, \overline{P}_t, C_\tau\right) = \int_t^{+\infty}\left(\int_0^{\overline{P}_s} \max(x - C_\tau, 0) f^e_{P_s|P_t}(x)dx\right) e^{-r(s-t)}ds$, where $f^e_{P_s|P_t}$ denotes the density of the payoff variable at time s as anticipated by entrants at time t. Under the equilibrium rule, the barrier $(\overline{P}_s)_{s\geq t}$ is deterministic. This is why we do not account for the dependency on the whole future trajectory of the barrier when defining W. We only need to show that $W\left(\overline{P}_t, \overline{P}_t, C_t\right) = W\left(\overline{P}_0, \overline{P}_0, C_0\right)/A_t$ because then the condition $W\left(\overline{P}_t, \overline{P}_t, C_t\right) = I_t = I_0/A_t$ will be met for all t whenever $\overline{P}_0$ is chosen such that $W\left(\overline{P}_0, \overline{P}_0, C_0\right) = I_0$.

According to Assumption 6, potential entrants make their entry decisions based on P_t and $\overline{P}_t$ only. Multiplying the two variables by the rate of technological progress, this implies that potential entrants make their entry decisions based on A_tP_t and $\overline{P}_0$ only. In this detrended space, the barrier is flat. Hence, under the conjectured rule for entry, the process A_tP_t anticipated by potential entrants is Time-Homogeneous Markov, meaning that for all t, s, $\delta > 0$, we have: $f^e_{A_tP_t|A_sP_s}(y) = f^e_{A_{t-\delta}P_{t-\delta}|A_{s-\delta}P_{s-\delta}}(y)$.

[39] Alternatively, we could have solved the planner's problem and used the "super contact" condition $W_{11}\left(\overline{P}_t, \overline{P}_t, A_t\right) = 0$.

Reinserting this equality into the definition of W, we find that

$$
\begin{aligned}
W\left(\overline{P}_t, \overline{P}_t, C_t\right) &= \int_t^{+\infty}\left(\int_0^{\overline{P}_s} \max\left(x - C_t, 0\right) f^e_{P_s|P_t=\overline{P}_t}(x)dx\right) e^{-r(s-t)}ds \\
&= \int_0^{+\infty}\left(\int_0^{\frac{\overline{P}_u}{A_t}} \max\left(x - C_t, 0\right) f^e_{P_{u+t}|P_t=\overline{P}_t}(x)dx\right) e^{-ru}du \\
&= \int_0^{+\infty}\left(\int_0^{\overline{P}_u} \frac{1}{A_t}\max\left(\frac{y}{A_t} - \frac{C_0}{A_t}, 0\right) f^e_{P_{u+t}|P_t=\overline{P}_t}\left(\frac{y}{A_t}\right)dy\right) e^{-ru}du \\
&= \frac{1}{A_t}\int_0^{+\infty}\left(\int_0^{\overline{P}_u} \max\left(y - C_0, 0\right) f^e_{P_{u+t}A_t|A_tP_t=\overline{P}_0}\left(y\right)dy\right) e^{-ru}du \\
&= \frac{1}{A_t}\int_0^{+\infty}\left(\int_0^{\overline{P}_u} \max\left(y - C_0, 0\right) f^e_{P_u|P_0=\overline{P}_0}\left(y\right)dy\right) e^{-ru}du \\
&= \frac{W\left(\overline{P}_0, \overline{P}_0, C_0\right)}{A_t}.
\end{aligned}
$$

The second equality follows from $u = s - t$ and replacing $\overline{P}_{u+t}$ by $\overline{P}_u/A_t$. The third and fourth equalities use the change of variable $y = A_t x$. The fifth equality is a direct consequence of the Time-Homogeneous Markov property of A_tP_t. The last equality holds by definition, proving that free entry is indeed satisfied when $\overline{P}_t$ decays at the rate of technological progress.

TECHNICAL APPENDIX

A Derivation of equations (1) and (4)

Let D denote the difficulty of the hashing problem, so that every computed hash will lead to a valid block with probability $1/D$. Consider a machine that performs on average a hash per period. Let $(T_n, n \geq 0)$ be a strictly increasing sequence of random variables–$T_0 = 0 < T_1 < ... < T_n$, which measures the dates at which the machine has generated a valid block. To keeps track of the number of mined blocks within $[0, t]$, we also introduce the counting process associated with T_n

$$N_t \equiv \sum_{n \geq 1} \mathbf{1}_{\{T_n \leq t\}}, \text{ and } N_0 = 0.$$

The Poisson distribution is obtained breaking up each period into tiny intervals of size δ, so that there is a very large number, $n = 1/\delta$, of subintervals in each period. The probability that the machine computes a hash in each subinterval is proportional to their length δ. Hence, the probability that the machine generates a block in each subinterval is equal to δ/D, and the machine will find k valid blocks in $[0, t]$ with probability

$$\mathbb{P}\left(N_t = k \middle| \mathcal{F}_0\right) = \binom{nt}{k} \left(\frac{\delta}{D}\right)^k \left(1 - \frac{\delta}{D}\right)^{nt-k},$$

where $\mathcal{F}_t = \sigma\left(N_s, s \leq t\right)$ is the filtration generated by N_t. Replacing $n = 1/\delta$ and $\lambda\left(x, D\right) \equiv x/D$ into the previous equation, we finally find that, when δ converges to zero,

$$\begin{aligned}
\mathbb{P}\left(N_t = k \middle| \mathcal{F}_0\right) &= \binom{t/\delta}{k} \left(\lambda\left(1, D\right)\delta\right)^k \left(1 - \lambda\left(1, D\right)\delta\right)^{t/\delta - k} \\
&\approx \frac{\left(t/\delta\right)^k}{k!} \left(\lambda\left(1, D\right)\delta\right)^k \left(1 - \lambda\left(1, D\right)\delta\right)^{t/\delta} \\
&= \frac{\left(\lambda\left(1, D\right)t\right)^k}{k!} \left(1 - \lambda\left(1, D\right)\delta\right)^{t/\delta} \\
&\approx \frac{\left(\lambda\left(1, D\right)t\right)^k}{k!} e^{-\lambda(1,D)t}.
\end{aligned}$$

Note that considering h units of hashpower simply rescale the Poisson arrival rate. The memory-less property of the hashing problem implies that the number of computed hashes per subintervals is equal to h/D instead of $1/D$. Following the sames steps as before, one finds that the Poisson arrival rate $\lambda\left(h, D\right) = h/D$.

Having established that the probability of finding a block is captured by a Poisson process, we now derive the flow revenues of miners. It is given by a compound process whose jumps of random sizes are proportional to the exchange rate R. Hence, the revenues generated in $[0,t]$ read

$$\Pi_t = \sum_{i=1}^{N_t} R_{T_i} = \int_0^t R_s dN_s.$$

Fix a t small enough such that the expectation of Π_t is finite. Then we have

$$\begin{aligned}
\mathbb{E}_0\left[\Pi_t\right] &= \mathbb{E}_0\left[\int_0^t R_s dN_s\right] \\
&= \mathbb{E}_0\left[\int_0^t R_s \lambda\left(1, D_s\right) ds\right] - \overbrace{\mathbb{E}_0\left[\int_0^t R_s\left(\lambda\left(1, D_s\right) ds - dN_s\right)\right]}^{=0} \\
&= \mathbb{E}_0\left[\int_0^t \frac{R_s}{D_s} ds\right],
\end{aligned}$$

where the third equality follows from the fact that the compensated process $M_t \equiv N_t - \int_0^t \lambda\left(1, D_s\right) ds$ is a martingale–see **?** (**?**), and that R_t and M_t are independent. Finally, letting t converge to 0, we find that the flow payoff of the miner is indeed equal to $P_t = R_t \lambda\left(1, D_t\right) = R_t / D_t$, as stated in eq. (1).

The value function of miners is by definition equal to

$$\begin{aligned}
V\left(R_t, \tau\right) &= \mathbb{E}_t\left[\sum_{i: T_i \geq t} e^{-r\left(T_i - t\right)} R_{T_i}\right] - \int_t^\infty e^{-r(s-t)} C_\tau ds \\
&= \mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)} R_s dN_s\right] - \frac{C_\tau}{r}.
\end{aligned}$$

As before, we can use the martingale property of the compensated process M_t to express the expectation as a function of the payoff process. Following similar steps, we find that

$$\begin{aligned}
V\left(R_t, \tau\right) + \frac{C_\tau}{r} &= \mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)} R_s dN_s\right] \\
&= \mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)} R_s \lambda\left(1, D_s\right) ds\right] - \overbrace{\mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)} R_s\left(\lambda\left(1, D_s\right) ds - dN_s\right)\right]}^{=0} \\
&= \mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)} P_s ds\right],
\end{aligned}$$

as stated in eq. (4). Note that since we cannot arbitrarily choose the upper-bound of the integral, we also to need to make sure that the expectation is bounded. But this will hold true in equilibrium, as otherwise the investment process would violate free entry.

B Entry rule during the first period

Figure 11 displays the simulated and observed payoffs series for our first period, along with the Bitcoin/US Dollar exchange rate. As explained in the main text, the baseline model fails to match the payoff series when the exchange rate suddenly increases. This is particularly noticeable at the beginning of the first period. Yet the model with time-to-build manages to correct this shortcoming and fir the data over the whole sample.

C Exchange rate data for Bitcoin

There is no single Bitcoin price as each exchange has its own exchange rate, which can sometimes be significantly different from another exchange's. The data we use in the article comes from the blockchain information website Coindesk. To make sure that we use high quality data, we compare them with the exchange rate series constructed by **?** (**?**). They rely on the Kaiko dataset, and use all transaction prices from 17 major exchanges: Bitfinnex, bitFlyer, Bitstamp, Bittrex, BTCe, BTCChina, CEX.IO, Coinbase-GDAX, Gatecoin, Gemini, hitBTC, Huobi, itBit, Kraken, Mt.Gox, OKCoin and Quoine. Figure 12 plots the two series and shows that they are almost always superimposed.

Figure 11: Simulated vs. Observed Payoffs

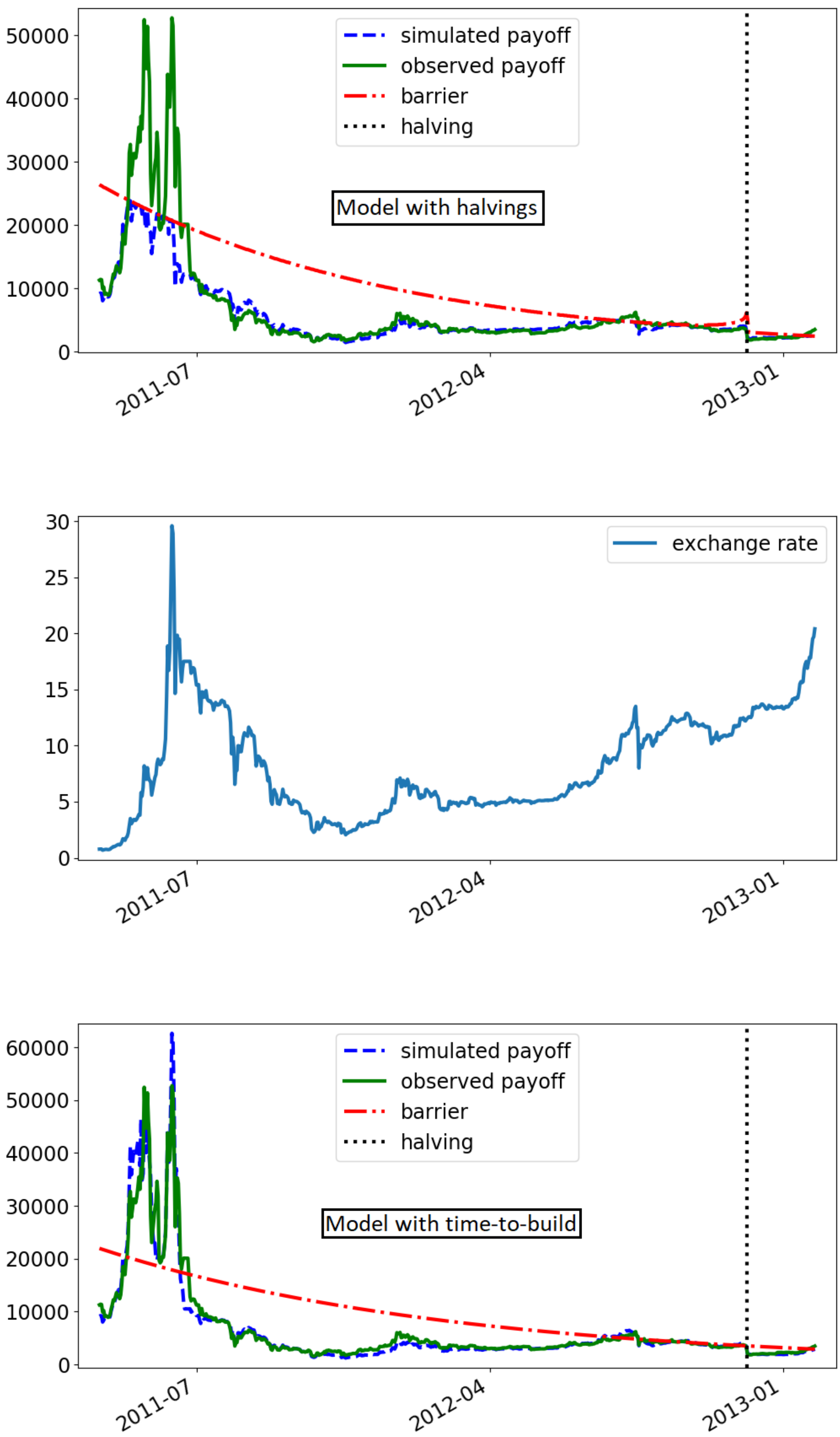
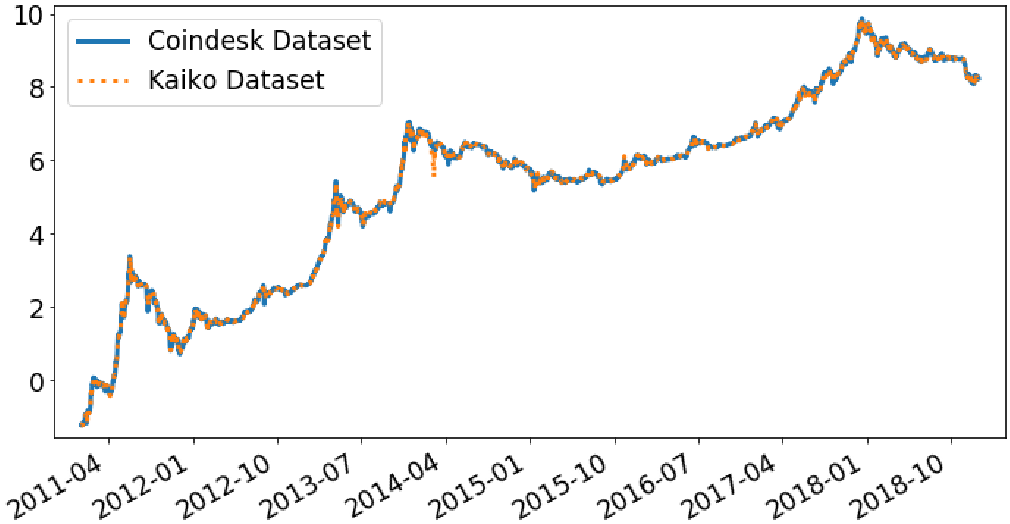


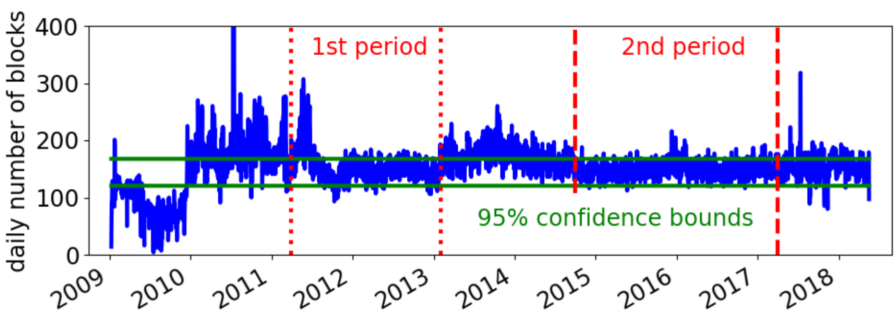
Figure 12: Comparison of Exchange Rate Data



D Block generation rate

According to Assumption 1, the expected value of the block generation rate would always be equal to 10 minutes. Hence it implies that the daily number of generated blocks should not be statistically different from 144. Figure 13 plots the daily number of blocks found along with the two 95% confidence bounds. For our periods of interest, the results are satisfying except for the beginning of the first period. According to this graph, it is sensible not to consider the interval separating our two periods of study. Then, due to the introduction of ASICs, technological progress was so fast that the hashrate significantly exceeded the target of one block every ten minutes.

Figure 13: Number of Blocks Found per Day



Note: The number of blocks found per day has been retrieved from coindesk.com.

E Law-of-motion of block rewards

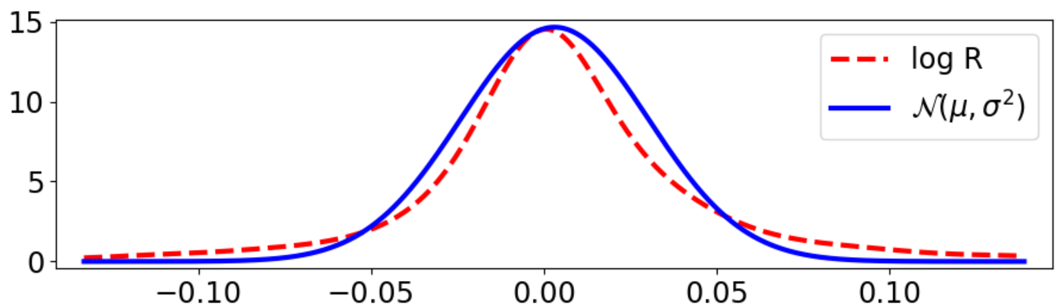
The GBM assumption implies that the log-increments of block reward should be both independent and normally distributed. For all $t \geq 0$, we have $R_t = R_0 e^{\left(\alpha - \frac{\sigma^2}{2}\right)t + \sigma Z_t}$, where $(Z_t)_t \geq 0$ is a standard Brownian motion. Hence we get

$$\log\left(\frac{R_{t+1}}{R_t}\right) = \left(\alpha - \frac{\sigma^2}{2}\right) + \sigma\left(Z_{t+1} - Z_t\right).$$

According to the definition of Brownian motions, $Z_{t+1} - Z_t$ should follow a $\mathcal{N}(0,1)$ distribution, independent from $Z_{s+1} - Z_s$ for all $s \neq t$. Letting $\mu = \alpha - \sigma^2/2$, we see that the log-increments, $\log\left(\frac{R_{t+1}}{R_t}\right)$, are i.i.d and follow a $\mathcal{N}(\mu, \sigma^2)$ distribution.

Figure 14 compares the nonparametrically estimated density of log-increments with their normal density estimated by maximum likelihood under the GBM assumption. It show that if we exclude tail events by discarding the 5% most extreme increments on each side, the empirical distribution is well approximated by a normal distribution. Hence although log-increments are most of the time normally distributed, they exhibit fat-tails as often observed with financial data.

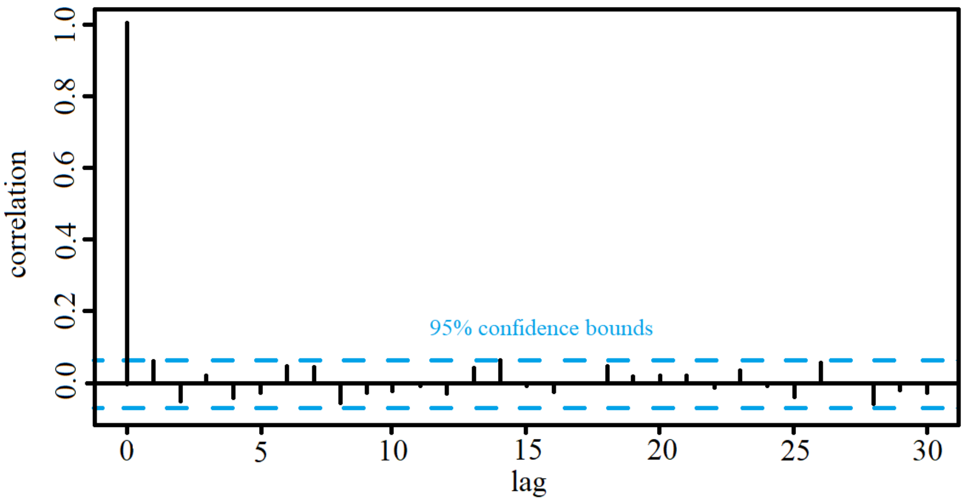
Figure 14: Normality of Log-Increments



Note: Estimation of log-increments excluding tail events.

As for the independence property, Figure 15 shows that log-increments are not linearly autocorrelated. We obtain similar results composing the log-increments with non-linear functions. However, statistical tests indicate that the variance of the block rewards does not remain constant over time, and goes instead through periods of high and low volatility. Although the issue is strongly alleviated by our division of the sample into two subperiods, it suggests that a more realistic specification should allow the variance coefficient σ to vary over time. We leave this extension to further research because it would render the entry barrier state dependent, and thus greatly complicates the characterization of the equilibrium.

Figure 15: Independence of Log-Increments



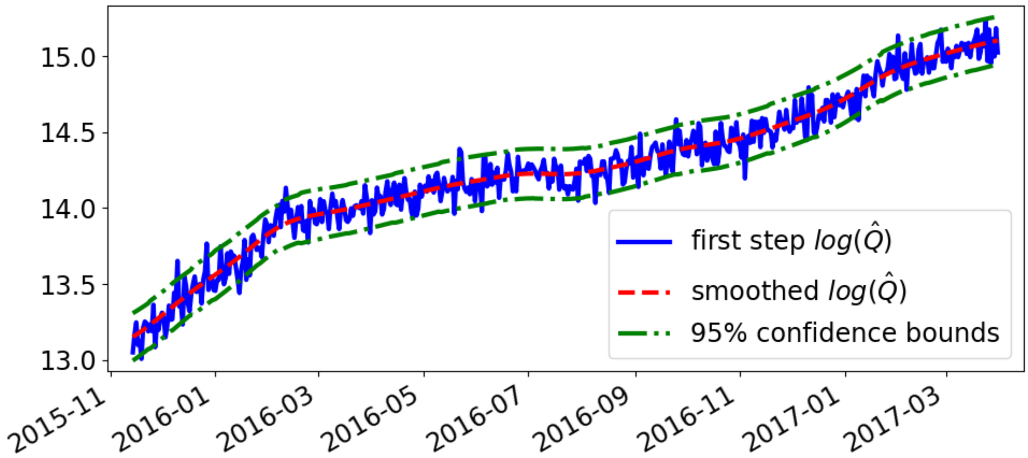
Note: This autocorrelogram has been obtained using the second period log-increments.

F Estimation of Q

The network's hashrate $(Q_t)_{t\geq 0}$ is not observable but can be estimated using a two-step procedure. First, for each day t, let $\hat{Q}_t \equiv N_t/\tilde{\Pi}_t$, where N_t is the number of blocks found for day t and $\tilde{\Pi}_t$ is the probability to find a valid block with a single hash. Both are directly observable in the blockchain. Since N_t follows the binomial distribution with parameters Q_t and $\tilde{\Pi}_t$, $\hat{Q}_t$ is a very natural estimator of the daily hashrate. This estimator is non biased and it can easily be shown that it is asymptotically equivalent to the maximum likelihood estimator. Given that there is a lot of variation across daily estimates, we smooth this new time series using a local linear regression. Figure 16 shows that we are not losing much information performing a local linear regression over $\hat{Q}$.

The two green curves are confidence bounds for the first step estimation if the true $(log\,(Q)_t)_{t\geq 0}$ were the red curve (the second step estimate). If the erratic variations of the first step estimation captured not only the first step estimation variance, but also some real variations of the hashrate not captured by the second step estimation, then its variance should be bigger than the one resulting from the first step estimation error only. Thus it should cross the green bounds much more often than 5% of the time, which does not happen in our data. For the sake of clarity, we do not show the whole series but the test works very well over the whole period.

Figure 16: Estimation of Network's Hashrate Q



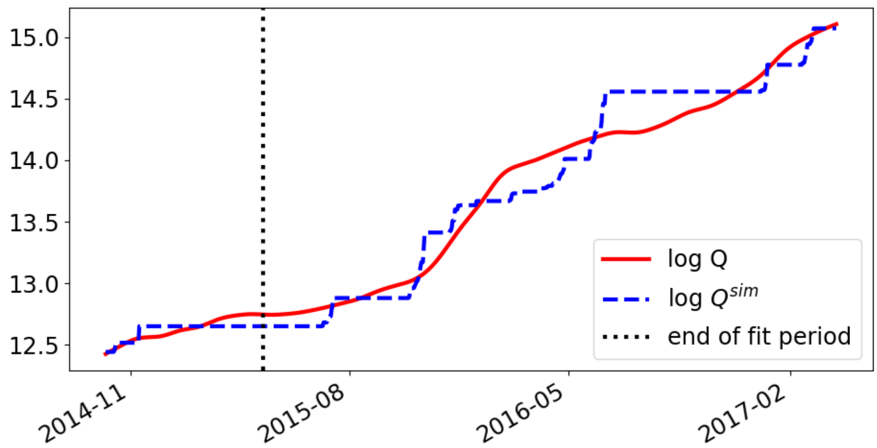
G Block bootstrap

Since our data are time series, we resort to block bootstrap to estimate the standard deviations of our estimates. We follow the following procedure. Then, we compute the returns dR and dQ of the series R and Q. Second, we divide those series of returns into blocks. A bootstrap random draw consists in the drawing with replacement of a series of blocks, which has the same length as the series observed in the data. For instance, if we divide our data in five blocks [1|2|3|4|5], then [2|4|2|3|4] or [5|5|2|1|5] could be bootstrap series. For a bootstrap draw b, we then obtain two series dR_b and dQ_b. Starting with fixed initial values for R and Q, we create series R_b and Q_b from the series of returns. Note that applying the bootstrap procedure on R and Q directly instead of the series of returns would not make any sense since the two series are not stationary. We finally estimate the parameters using our minimization procedure, with R_b and Q_b as input, and repeat the drawing and estimation 100 times in order to estimate the parameters' standard deviations. It is important to note that for a given change in the exchange rate, miners' behavior crucially depends on how far P is from the barrier. As a result, for our procedure to make sense (that is to say, to create bootstrap series which could have happened in the real life), the ratio of P and the barrier must have the same value at the beginning of each block. We pick our blocks under this constraint.

H Out-of-sample experiments

We assess the model's ability to match out-of-sample data by dividing the second period into a fit period and a test period. We calibrate a and $\overline{P}_0$ on the fit period only and find that, even when the fit period is short, the calibrated values remain close to the ones based on the full sample. Hence, as illustrated in Figure 17, the predicted hashrate stays accurate several years after the end of the fit period.

Figure 17: Out-of-Sample Experiment



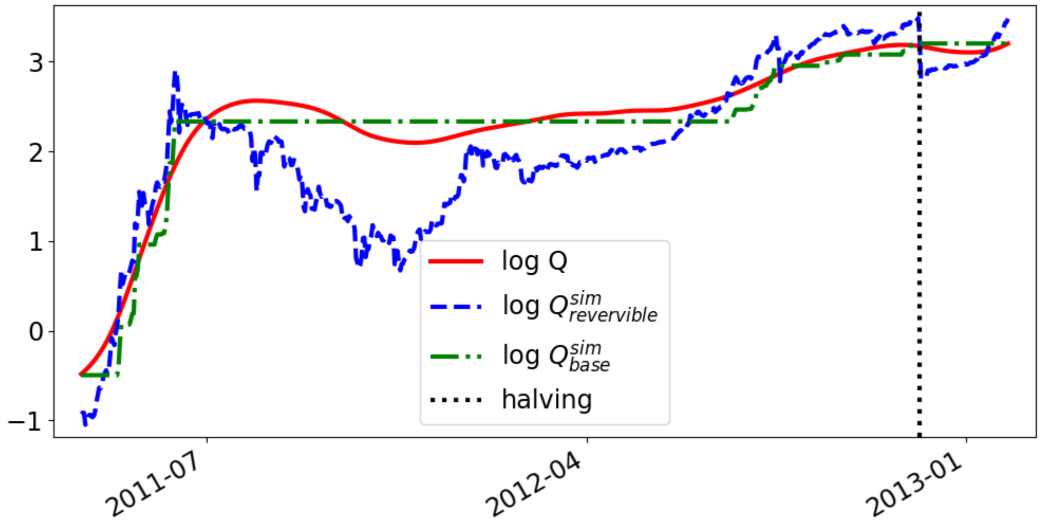
Note: The fit period is the shortest one for which the overall fit remains accurate.

Note, however, that out-of-sample tests are much less conclusive for the first period because the hashrate increases only at the beginning and at the end of that period. Hence, if we split the first data sample into a fit and a test period, the payoffs do not hit the reflecting barrier often enough to deliver a reliable calibration.

I Fully reversible investments

During the first subperiod, miners do not use specific mining hardware. Hence, the assumption that their investment is irreversible is less obvious than for our second period. To assess its accuracy, we estimate here a model with fully reversible investment. Figure 18 shows that the hashrate predicted by the reversible model fail to fits the data.

Figure 18: Model with Totally Irreversible Investment



Note: Reversible model simulated under the free entry assumption. Since miners break even, payoffs are always set equal to the operational costs.

J Derivation of payoffs density f^e

Lemma 1. *Let Assumptions 1, 2, 4 and 7 hold true. Then, for all $t > 0$, the density of P_t conditional on the barrier being reached at time $\tau < t$ reads*

$$
\begin{aligned}
f^e_{P_t|P_\tau=\overline{P}_\tau}(x) = \left(\frac{1}{x}\right) \Bigg\{ & \left(\frac{1}{\sigma\sqrt{t}}\right) \phi\left(\frac{\log(\overline{P}_\tau) - \log(x) + \left(\alpha - \frac{\sigma^2}{2}\right)t}{\sigma\sqrt{t}}\right) \\
& + \exp\left[\left(\log(\overline{P}_\tau) - \log(x) - at\right)\left(1 - 2\left(\frac{a+\alpha}{\sigma^2}\right)\right)\right] \\
& \times \left[\left(2\left(\frac{a+\alpha}{\sigma^2}\right) - 1\right)\Phi\left(\frac{\log(x) - \log(\overline{P}_\tau) + \left(2a + \alpha - \frac{\sigma^2}{2}\right)t}{\sigma\sqrt{t}}\right)\right. \\
& \left.\left. + \left(\frac{1}{\sigma\sqrt{t}}\right)\phi\left(\frac{\log(x) - \log(\overline{P}_\tau) + \left(2a + \alpha - \frac{\sigma^2}{2}\right)t}{\sigma\sqrt{t}}\right)\right]\right\} \mathbb{1}_{]0,\overline{P}_t]}(x),
\end{aligned}
$$

where ϕ and Φ are the density and the cumulative distribution function of the standard normal distribution, respectively.

Proof. Since Assumption 7 implies Assumption 6, Proposition 3 applies and we know that there exists a $\overline{P}_0$ such that $(P_t, \overline{P}_t = \overline{P}_0/A_t)$ is an industry equilibrium. Moreover, Assumption 7 also implies that the anticipated P_t follows a GBM when $P_t < \overline{P}_t$ because the hashrate Q_t remains constant. Hence the anticipated P_t follows a GBM reflected at $\overline{P}_0/A_t$. The density of a positive Brownian motion reflected at 0 and which starts at 0 is given in **?** (**?**). We now show that it can be applied to the logarithm of P.

Without loss of generality, we can set the hitting time $\tau = 0$. Then $R_0/Q_0 = \overline{P}_0$ because we are looking for a density conditional on $P_0 = \overline{P}_0$. Hence the hashrate Q_t is given by $Q_t = \sup\limits_{0\leq s\leq t} A_s R_s/\overline{P}_0$. Replacing this expression into the decomposition of $A_t P_t$, we find that

$$
\begin{aligned}
\log(A_t P_t) &= \log(A_t R_t) - \log(Q_t) \\
&= \log(A_t R_t) - \sup_{0\leq s\leq t} \log(A_s R_s) + \log(\overline{P}_0) \\
&= \log(\overline{P}_0) - \left[-\log(A_t R_t) - \inf_{0\leq s\leq t}(-\log(A_s R_s))\right] \\
&= \log(\overline{P}_0) - Z_t,
\end{aligned}
$$

where Z_t follows a positive Brownian motion with parameters $(\sigma^2/2 - a - \alpha, \sigma)$, reflected at 0 and with initial condition $Z_0 = 0$. We know from **?** (**?**) that, for all $x \geq 0$,

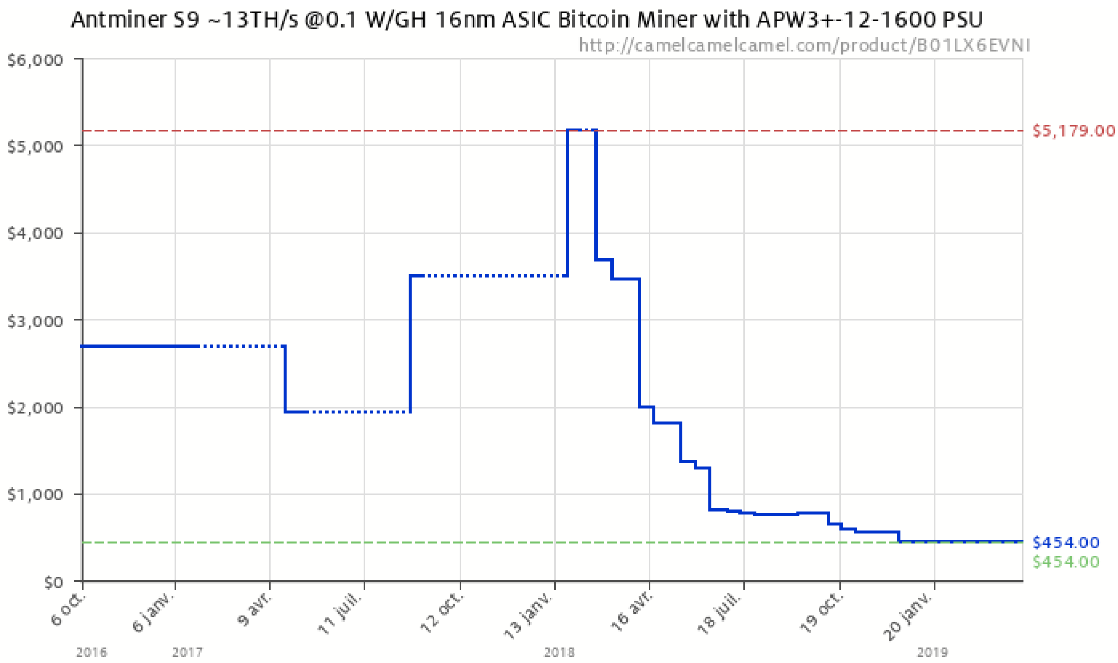
$\Pr\left(Z_t \leq x\right) = \Phi\left(\frac{x-\left(\frac{\sigma^2}{2}-a-\alpha\right)t}{\sigma\sqrt{t}}\right) - e^{\frac{2\left(\frac{\sigma^2}{2}-a-\alpha\right)x}{\sigma^2}}\Phi\left(\frac{-x-\left(\frac{\sigma^2}{2}-a-\alpha\right)t}{\sigma\sqrt{t}}\right)$. Straightforward differentiation of this expression yields the solution for f^e.

$\square$

K Price of mining hardware

Name of rig	available on	hashpower (Th/s)	power (Watts)	price ($)
Bitmain S1	2013/12/01	0.18	360	300
	https://en.bitcoin.it/wiki/Mining_hardware_comparison			
Bitmain S2	2014/04/01	1	1100	2260
	https://en.bitcoin.it/wiki/Mining_hardware_comparison			
Bitmain S3	2014/07/01	0.441	340	382
	https://en.bitcoin.it/wiki/Mining_hardware_comparison			
Bitmain S4	2014/10/01	2	1400	1400
	https://en.bitcoin.it/wiki/Mining_hardware_comparison			
Bitmain S5	2015/01/01	1.15	590	370
	https://en.bitcoin.it/wiki/Mining_hardware_comparison			
Bitmain S7	2015/09/01	4.86	1210	1823
	https://en.bitcoin.it/wiki/Mining_hardware_comparison			
Bitmain S9	2016/08/01	14	1375	2400
	https://en.bitcoin.it/wiki/Mining_hardware_comparison			
Bitmain S9	2018/01/01	14	1375	5179
	https://camelcamelcamel.com/Antminer-S9-~13TH-Bitcoin-12-1600/product/B01LX6EVNI			
Pangolin M10	2018/07/24	33	2150	2000
	https://bitcointalk.org/index.php?topic=4737927.0			
Pangolin M20	2019/05/20	48	2300	1450
	https://bitcointalk.org/index.php?topic=5120959.0			

Figure 19: Price Data for Mining Rigs



L Model with time-to-build

The characterization of the equilibrium with time-to-build is borrowed from **?** (**?**). We outline the logic of the proof and refer readers to the paper for more details. The first step of the proof consists in showing that the equilibrium can be derived solving the problem of a single agent that maximizes a "fictious" objective function. As in **?** (**?**), the decentralized equilibrium maximizes social welfare. Hence it can also be derived as an optima from the social planner's perspective.

Equivalence between central planner and decentralized solutions. Our first task is to define the objective function. The flow benefits are equal to the area under the payoff functions of miners so that $B(R,Q) = \int_0^Q P(R,x)\,dx = \int_0^Q (R/x)\,dx = R\log(Q)$. Since the central planner seeks to maximize benefits net of costs, he solves the following problem

$$\begin{aligned}
J\left(R_t,Q_t,t\right) &= \max_{\{Q_s\}_{s>t}} \mathbb{E}_t\left[\int_t^{\infty} e^{-r(s-t)}\left(\left[B\left(R_s,Q_s\right)-\int_0^s C_\tau dQ_\tau\right]ds - I_s dQ_s\right)\right]\\
&= \max_{\{Q_s\}_{s>t}} \mathbb{E}_t\left[\int_t^{\infty} e^{-r(s-t)}\left(\left[B\left(R_s,Q_s\right)-C_0\int_0^s e^{-a\tau} dQ_\tau\right]ds - e^{-as} I_0 dQ_s\right)\right]\\
&= \max_{\{Q_s\}_{s>t}} \mathbb{E}_t\left[\int_t^{\infty} e^{-r(s-t)}\left(R_s\log(Q_s)ds - e^{-as}\left(I_0+\frac{C_0}{r}\right)dQ_s\right)\right].
\end{aligned}$$

Defining $K_t \equiv e^{-at}\left(I_0+\frac{C_0}{r}\right)$ allows us to rewrite the objective function as

$$J\left(R_t,Q_t,K_t\right) = \max_{\{Q_s\}_{s>t}} \mathbb{E}_t\left[\int_t^{\infty} e^{-r(s-t)}\left(R_s\log(Q_s)ds - K_s dQ_s\right)\right]$$

Hence the value function of the planner satisfies the following differential equation

$$rJ\left(R_t,Q_t,K_t\right) = R_t\log(Q_t) + \alpha R_t J_R\left(R_t,Q_t,K_t\right) + \frac{\sigma^2 R_t^2}{2} J_{RR}\left(R_t,Q_t,K_t\right) - aK_t J_K\left(R_t,Q_t,K_t\right), \tag{16}$$

subject to the value matching and smooth-pasting conditions

$$\begin{aligned}
\frac{\partial J\left(\overline{R}(Q,K),Q,K\right)}{\partial Q} &= K,\\
\frac{\partial J\left(\overline{R}(Q,K),Q,K\right)}{\partial Q\partial R} &= 0.
\end{aligned}$$

Since (16) holds identically along the optimal path, we can differentiate it with respect to Q to obtain

$$rj\left(R_t,Q_t,K_t\right) = \frac{R_t}{Q_t} + \alpha R_t j_R\left(R_t,Q_t,K_t\right) + \frac{\sigma^2 R_t^2}{2} j_{RR}\left(R_t,Q_t,K_t\right) - aK_t j_K\left(R_t,Q_t,K_t\right),$$

where $j\left(R,Q,K\right) \equiv \partial J\left(R,Q,K\right)/\partial Q$ denotes the marginal value of mining capacity. The boundary conditions above are therefore equivalent to

$$\begin{aligned}
j\left(\overline{R}(Q,K),Q,K\right) &= K,\\
\frac{\partial j\left(\overline{R}(Q,K),Q,K\right)}{\partial R} &= 0.
\end{aligned}$$

The differential equation and boundary conditions are verified when (i) $\overline{R}(Q,K) = DQK$, for a constant D that is yet to be determined; and (ii) j reads

$$j\left(R_t,Q_t,K_t\right) = \frac{R_t/Q_t}{r-\alpha} - \left[\frac{DK_t}{\beta(r-\alpha)}\right]\left(\frac{R_t/Q_t}{DK_t}\right)^{\beta}, \tag{17}$$

where β is the positive root of the quadratic equation

$$\mathcal{Q}(\beta) \equiv \frac{\sigma^2}{2}\beta(\beta-1) + (\alpha+a)\beta - a - r = 0,$$

and the constant $D = (r-\alpha)\beta/\left(\beta-1\right)$. Replacing $P_t = R_t/Q_t$, $K_t = K_0/A_t$ and $\overline{P}_t = DK_t$ into (17), we find that the optimal investment strategy of the planner is identical to the entry rule of the decentralized equilibrium.

Industry dynamics with time-to-build. Having shown that we can use a central planner to solve for the equilibrium, we now introduce time-to-build. There is an exogenous delay δ between the time a new unit of hashpower is ordered and when it become operational. Let N_t denote the number of units that are currently in the delivery pipeline because their purchase order occurred within $(t-\delta, t]$, and let $H_t = Q_t + N_t$ denote the "committed hashpower" at date t.

The state of the economy is summarized by the following vector

$$\Omega_t = \{R_t, K_t, Q_t, N_t, \Lambda_t\}, \text{ where } \Lambda_t \equiv \{s \in (t-\delta, t] : Q_t > Q_{t^-}\}.$$

The set Λ_t records all the dates at which hashpower has been committed within the current delivery window $(t-\delta, t]$. Note that the investment cost K_t has to be adjusted to take into account the delivery delay so that $K_t = e^{-at}\left[I_0 + e^{-r\delta}C_0/r\right]$. Since $Q_t = H_{t-\delta}$, $B(R_t, Q_t) = R_t \log(H_{t-\delta})$ and the planner solves the following problem

$$\begin{aligned}
& J^\delta(R_t, K_t, Q_t, N_t, \Lambda_t) \\
= \;& \mathbb{E}_t\left[\int_t^{t+\delta} e^{-r(s-t)} R_s \log(H_{s-\delta}) ds \,\middle|\, R_t, K_t, Q_t, N_t, \Lambda_t\right] \\
& + \max_{\{H_s\}_{s>t}} \mathbb{E}_t\left[\int_{t+\delta}^{\infty} e^{-r(s-t)} \left(R_s \log(H_{s-\delta}) ds - K_s dH_s\right) \,\middle|\, R_t, K_t, Q_t, N_t, \Lambda_t\right] \\
= \;& \mathbb{E}_t\left[\int_t^{t+\delta} e^{-r(s-t)} R_s \log(H_{s-\delta}) ds \,\middle|\, R_t, K_t, Q_t, N_t, \Lambda_t\right] \\
& + \max_{\{H_s\}_{s>t}} \mathbb{E}_t\left[\int_{t+\delta}^{\infty} e^{-r(s-t)} \left(R_s \log(H_{s-\delta}) ds - K_s dH_s\right) \,\middle|\, R_t, K_t, H_t, 0, \emptyset\right] \\
= \;& J^\delta(R_t, K_t, H_t, 0, \emptyset) \\
& + \mathbb{E}_t\left[\int_t^{t+\delta} e^{-r(s-t)} R_s \log(Q_{s-\delta}) ds \,\middle|\, R_t, K_t, Q_t, N_t, \Lambda_t\right] \\
& - \mathbb{E}_t\left[\int_t^{t+\delta} e^{-r(s-t)} R_s \log(Q_{s-\delta}) ds \,\middle|\, R_t, K_t, H_t, 0, \emptyset\right].
\end{aligned} \tag{18}$$

The second equality holds because the flow surplus at date $t+\delta$ only depends on the amount of committed hashpower H_t. Hence the optimized paths are identical under $\Omega_t = \{R_t, K_t, Q_t, N_t, \Lambda_t\}$ and under the assumption that all units currently in the pipeline are delivered, so that $\tilde{\Omega}_t = \{R_t, K_t, Q_t + N_t, 0, \emptyset\} = \{R_t, K_t, H_t, 0, \emptyset\}$. The last equality follows from the definition of J^δ. Note that the last two terms in (18) are beyond the control of the planner at time t. Hence he seeks to maximize $J^\delta(R_t, K_t, H_t, 0, \emptyset)$ which we denote by $V^\delta(R_t, H_t, K_t)$.

Over the range in which H_t remains constant, $V^\delta(R_t, H_t, K_t)$ can be interpreted as the value of an industry with H_t completed units yielding a dividend flow of $R_t \log(H_t)$.

Hence the value function in the no-investment region satisfies the differential equation

$$rV^{\delta}\left(R_t,H_t,K_t\right)=R_t\log(H_t)+\alpha R_tV_R^{\delta}\left(R_t,H_t,K_t\right)+\frac{\sigma^2R_t^2}{2}V_{RR}^{\delta}\left(R_t,H_t,K_t\right)-aK_tV_K^{\delta}\left(R_t,H_t,K_t\right).$$

Since the HJB equation is the same as that of the problem without delay (16), its derivative with respect to installed capacity, $v^{\delta}\left(R,H,K\right)\equiv\partial V^{\delta}\left(R,H,K\right)/\partial H$, also admits a solution of the form

$$v^{\delta}\left(R_t,H_t,K_t\right)=\frac{R_t/H_t}{r-\alpha}+D\left(H_t,K_t\right)R_t^{\beta}. \tag{19}$$

Let $\overline{R}^{\delta}(H,K)$ denote the level of R_t at which market entry is optimal. Then the value-matching condition reads

$$\begin{aligned}
V^{\delta}\left(\overline{R}^{\delta}(H,K),H,K\right) &= J^{\delta}\left(\overline{R}^{\delta}(H,K),K,H,dH,\emptyset\right)-KdH\\
&= V^{\delta}\left(\overline{R}^{\delta}(H,K),H+dH,K\right)-KdH\\
&\quad+\mathbb{E}\left[\int_0^{\delta}e^{-rt}R_t\log(H)dt\,\middle|\,R_0=\overline{R}^{\delta}(H,K)\right]\\
&\quad-\mathbb{E}\left[\int_0^{\delta}e^{-rt}R_t\log(H+dH)dt\,\middle|\,R_0=\overline{R}^{\delta}(H,K)\right].
\end{aligned}$$

Differentiating this condition yields

$$v^{\delta}\left(\overline{R}^{\delta}(H,K),H,K\right)=\frac{\overline{R}^{\delta}(H,K)/H}{r-\alpha}\left[1-e^{-(r-\alpha)\delta}\right]+K. \tag{20}$$

The optimal value of $\overline{R}^{\delta}$ follows from the smooth-pasting condition

$$\frac{\partial v^{\delta}\left(\overline{R}^{\delta}(H,K),H,K\right)}{\partial R}=\frac{1-e^{-(r-\alpha)\delta}}{H\left(r-\alpha\right)}. \tag{21}$$

Combining (20) and (21) with the general solution (19), yields the following solution

$$v^{\delta}\left(R_t,H_t,K_t\right)=\frac{R_t/H_t}{r-\alpha}-\left[\frac{DK_te^{-(r-\alpha)\delta}}{\beta(r-\alpha)}\right]\left(\frac{R_t/H_t}{DK_t}\right)^{\beta},$$

where β is the positive root of the quadratic equation

$$\mathcal{Q}(\beta)\equiv\frac{\sigma^2}{2}\beta(\beta-1)+(\alpha+a)\beta-a-r=0,$$

and the constant D reads

$$D=\frac{\beta(r-\alpha)}{(\beta-1)\,e^{-(r-\alpha)\delta}}.$$

Finally, dividing the block rewards R by H yields the expression of the reflecting barrier, which is indeed decreasing at the rate of technological progress since

$$\overline{P}_t^{\delta}=\frac{\overline{R}^{\delta}(H_t,K_t)}{H_t}=\frac{\beta(r-\alpha)}{(\beta-1)\,e^{-(r-\alpha)\delta}}K_t=e^{-at}\overline{P}_0^{\delta}.$$

M Model with convex adjustment costs

Let q_t denote investment in hashpower so that $Q_t = Q_0 + \int_0^t q_s ds$. Using $c(q,Q,K)$ to denote the overall entry costs as a function of q, the planner's value function must satisfy the following HJB equation

$$\begin{aligned} rJ(R_t,Q_t,K_t) &= \max_{q_t}\{R_t\log(Q_t) - c(q_t,Q_t,K_t) + q_t J_Q(R_t,Q_t,K_t)\} \\ &\quad +\alpha R_t J_R(R_t,Q_t,K_t) + \frac{\sigma^2 R_t^2}{2} J_{RR}(R_t,Q_t,K_t) - aK_t J_K(R_t,Q_t,K_t) \end{aligned} \tag{22}$$

We assume that

$$c(q,Q,K) = \begin{cases} Kq\left[1+\left(\frac{q}{Q}\right)^{\eta}\right], \text{ with } \eta > 1, \text{ for } q \geq 0, \\ g(q) > 0, \text{ with } g'(q) > 0, \text{ for } q < 0. \end{cases}$$

As in **?** (**?**), assuming that reducing Q has a positive cost effectively ensures that investment is irreversible. Hence we have

$$q_t = \max\left\{0, \left(\frac{j(R_t,Q_t,K_t)/K_t - 1}{1+\eta}\right)^{\frac{1}{\eta}} Q_t\right\}, \tag{23}$$

where $j(R_t,Q_t,K_t) \equiv J_Q(R_t,Q_t,K_t)$.

The HJB equation (22) can be differentiated with respect to Q since it holds identically. Hence the shadow value of of Q satisfies the following HJB

$$\begin{aligned} rj(R_t,Q_t,K_t) &= \frac{R_t}{Q_t} - c_Q(q_t,Q_t,K_t) + q(j(R_t,Q_t,K_t),Q_t,K_t)\, j_Q(R_t,Q_t,K_t) \\ &\quad +\alpha R_t j_R(R_t,Q_t,K_t) + \frac{\sigma^2 R_t^2}{2} j_{RR}(R_t,Q_t,K_t) - aK_t j_K(R_t,Q_t,K_t) \\ &\quad +\underbrace{[j(R_t,Q_t,K_t) - c_q(q_t,Q_t,K_t)]}_{=0\ if\ q_t>0}\underbrace{q_j(j(R_t,Q_t,K_t),Q_t,K_t)}_{=0\ if\ q_t=0} j_Q(R_t,Q_t,K_t) \end{aligned} \tag{24}$$

In order to reduce the state space, we guess that $j(R,Q,K) = Kj\left(\frac{R}{QK},1,1\right)$. We now verify that this conjecture is indeed correct by proving that it satisfies the HJB equation. Readers interested in a more systematic analysis can read Lemma 2 below, where we prove that j is homogenous of degree zero in (R,Q), and homogenous of degree one in (R,K). Since $j(R,Q,K)=Kj\left(\frac{R}{QK},1,1\right)$, it must hold true that

$$\begin{aligned}
j_R(R,Q,K) &= \frac{1}{Q}j_1\left(\frac{R}{QK},1,1\right),\\
j_{RR}(R,Q,K) &= \frac{1}{Q^2K}j_1\left(\frac{R}{QK},1,1\right),\\
j_Q(R,Q,K) &= -\frac{R}{Q^2}j_1\left(\frac{R}{QK},1,1\right),\\
j_K(R,Q,K) &= j\left(\frac{R}{QK},1,1\right)-\frac{R}{QK}j_1\left(\frac{R}{QK},1,1\right).
\end{aligned}$$

Replacing the four conditions above into the HJB equation (24) yields

$$\begin{aligned}
rj(R_t,Q_t,K_t) &= \frac{R_t}{Q_t}+K_t\eta\left(\frac{q(R_t,Q_t,K_t)}{Q_t}\right)^{1+\eta}+\alpha\frac{R_t}{Q_t}j_1\left(\frac{R_t}{Q_tK_t},1,1\right)+\frac{\sigma^2R_t^2}{2Q_t^2K_t}j_{11}\left(\frac{R_t}{Q_tK_t},1,1\right)\\
&\quad -aK_t\left[j\left(\frac{R_t}{Q_tK_t},1,1\right)-\frac{R_t}{Q_tK_t}j_1\left(\frac{R_t}{Q_tK_t},1,1\right)\right]-q\left(\frac{R_t}{Q_tK_t},1,1\right)Q_t\left[\frac{R_t}{Q_t^2}j_1\left(\frac{R_t}{Q_tK_t},1,1\right)\right], \quad (25)
\end{aligned}$$

where we have used the fact that

$$\begin{aligned}
q(R_t,Q_t,K_t) &= \left(\frac{j(R_t,Q_t,K_t)/K_t-1}{1+\eta}\right)^{\frac{1}{\eta}}Q_t\\
&= \left(\frac{j\left(\frac{R_t}{Q_tK_t},1,1\right)-1}{1+\eta}\right)^{\frac{1}{\eta}}Q_t\\
&= q\left(\frac{R_t}{Q_tK_t},1,1\right)Q_t.
\end{aligned}$$

Replacing $j(R_t,Q_t,K_t)$ with $K_tj\left(\frac{R_t}{Q_tK_t},1,1\right)$ on the left-hand side of (25), and dividing by K_t, yields an equation that depends on $R_t/(Q_tK_t)$ only

$$\begin{aligned}
rj\left(\frac{R_t}{Q_tK_t},1,1\right) &= \frac{R_t}{Q_tK_t}+\eta q\left(\frac{R_t}{Q_tK_t},1,1\right)^{1+\eta}+\alpha\frac{R_t}{Q_tK_t}j_1\left(\frac{R_t}{Q_tK_t},1,1\right)+\frac{\sigma^2}{2}\left(\frac{R_t}{Q_tK_t}\right)^2j_{11}\left(\frac{R_t}{Q_tK_t},1,1\right)\\
&\quad -a\left[j\left(\frac{R_t}{Q_tK_t},1,1\right)-\frac{R_t}{Q_tK_t}j_1\left(\frac{R_t}{Q_tK_t},1,1\right)\right]-\frac{R_t}{Q_tK_t}q\left(\frac{R_t}{Q_tK_t},1,1\right)j_1\left(\frac{R_t}{Q_tK_t},1,1\right).
\end{aligned}$$

We have derived an ODE that only depends on $R_t/(Q_tK_t)$ and which solves the original PDE while satisfying the optimality condition for investment. Replacing q with its expression in (23) and using x_t to denote $R_t/(Q_tK_t)$, we finally obtain the simplified HJB equation

$$(r+a)\tilde{j}(x_t)=\begin{cases} x_t+\eta\left(\frac{\tilde{j}(x_t)-1}{1+\eta}\right)^{\frac{1+\eta}{\eta}}+\left(\alpha+a-\left[\frac{\tilde{j}(x_t)-1}{1+\eta}\right]^{\frac{1}{\eta}}\right)x_t\tilde{j}'(x_t)+\frac{\sigma^2}{2}x_t^2\tilde{j}''(x_t), & \text{when } \tilde{j}(x_t)\geq 1,\\ x_t+(\alpha+a)x_t\tilde{j}'(x_t)+\frac{\sigma^2}{2}x_t^2\tilde{j}''(x_t), & \text{when } \tilde{j}(x_t)<1.\end{cases}$$

For our calibration, we generalize the cost function to take into account the distinction between the investment and the operating costs. More precisely, we assume that, as in the body of the paper, the marginal costs of entry are given by

$$I(q,Q,A) = \frac{I_0}{A}\left[1+\left(\frac{q}{bQ}\right)^{\eta}\right], \text{ for } q \geq 0.$$

Then the overall entry costs read

$$\begin{aligned} c(q_t,Q_t,K_t) &= \int_0^{q_t} I(y,Q_t,K_t)\,dy + q_t\frac{C_t}{r} \\ &= K_t q_t\left[1+\left(\frac{q_t}{\tilde{b}Q_t}\right)^{\eta}\right], \end{aligned}$$

where $K_t = (I_0 + C_0/r)/A_t = e^{-at}(I_0 + C_0/r)/A_0$, and $\tilde{b} \equiv b\left[\frac{(1+\eta)K_0}{I_0}\right]^{1/\eta}$. Given that the optimal entry flow solves

$$q(R_t,Q_t,K_t) = \max\left\{0, \left(\frac{j(R_t,Q_t,K_t)/K_t - 1}{1+\eta}\right)^{\frac{1}{\eta}}\tilde{b}Q_t\right\},$$

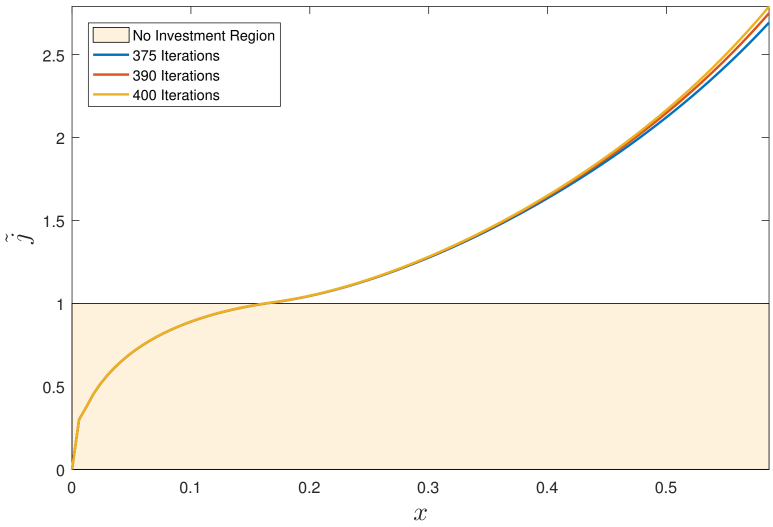
the HJB is now equivalent to

$$(r+a)\,\tilde{j}(x_t) = \begin{cases} x_t + \eta\tilde{b}\left(\frac{\tilde{j}(x_t)-1}{1+\eta}\right)^{\frac{1+\eta}{\eta}} + \left(\alpha + a - \left[\frac{\tilde{j}(x_t)-1}{1+\eta}\right]^{\frac{1}{\eta}}\tilde{b}\right)x_t\tilde{j}'(x_t) + \frac{\sigma^2}{2}x_t^2\tilde{j}''(x_t), \text{ when } \tilde{j}(x_t)\geq 1, \\ x_t + (\alpha+a)\,x_t\tilde{j}'(x_t) + \frac{\sigma^2}{2}x_t^2\tilde{j}''(x_t), \text{ when } \tilde{j}(x_t) < 1. \end{cases} \tag{26}$$

We use a finite-difference method to approximate the HJB equation, using the value function with linear costs as our starting guess. We rely on the implicit Euler scheme in order to ensure that the approximation is stable. The system of linearized equations is solved using a generalization of the Gauss-Seidel iterative method known as the successive-over-relaxation method. Solving for j yields the investment rate q as a function of P, as well as the marginal costs of investment c_q. As for the baseline model, we use the policy function to simulate the trajectory of the network hashrate and also that of the investment costs. The empirical moments are summarized by the vector $\hat{\mathbf{m}}$ which contains the actual hashrate of the network and the online price series described in the Technical Appendix K. Using $\mathbf{m}(\upsilon)$ to denote the simulated moments generated by the vector of parameters $\upsilon \equiv \{a,\eta,b\}$, we compute the quadratic distances $d(\upsilon) \equiv (\mathbf{m}(\upsilon) - \hat{\mathbf{m}})\,\Omega\,(\mathbf{m}(\upsilon) - \hat{\mathbf{m}})$, where Ω is a weighting matrix that places equal weight on the hashrate and price data. Our calibrated vector $\hat{\upsilon} = \arg\min_{\upsilon\in\mathbb{R}^3_+} d(\upsilon)$.

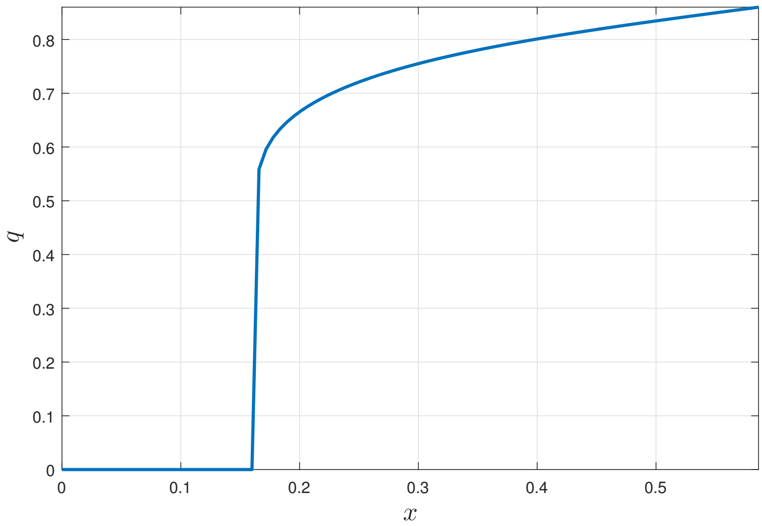
Figure 20 illustrates the convergence of our numerical procedure. It reports the simulated value function $\tilde{j}$ after different number of iterations. One can see that after

Figure 20: Convergence of Numerical Solution



Note: Simulated solutions of the HJB equation (26) at different numbers of iterations.

Figure 21: Policy Function



Note: Calibrated policy function of the model with convex adjustment costs.

400 iterations, the incremental changes in the value function are negligible, especially if one focuses on the region around the investment threshold $\tilde{j}(\overline{x}) = 1$. The policy function $q(x)$ of the calibrated model is reported in Figure 21. Aggregate investment is nearly vertical at the entry barrier $\overline{x}$, but is prevented from reaching an infinite intensity, as would be the case under linear costs, by the convexity of the adjustment cost function.

We conclude our analysis of the model with convex costs with a Lemma that proves the validity of the normalization $j(R, Q, K) = Kj\left(\frac{R}{QK}, 1, 1\right)$.

Lemma 1. *The shadow value of capital* $j(R_t, Q_t, K_t)$ *is homogenous of degree zero in* (R_t, Q_t)*, and homogenous of degree one in* (R_t, K_t)*, i.e.* $j(\lambda R_t, \lambda Q_t, K_t) = j(R_t, Q_t, K_t)$ *and* $j(\lambda R_t, Q_t, \lambda K_t) = \lambda j(R_t, Q_t, K_t)$ *for all* $\lambda > 0$.

Proof. Let $q_\cdot^*(R_t, Q_t, K_t) = \{q_s^*(R_s, Q_s, K_s)\}_{s \geq t}$ denote the optimal investment path starting at (R_t, Q_t, K_t). Consider a planner which faces the initial condition $(\lambda R_t, \lambda Q_t, K_t)$ where $\lambda > 0$, and implements the investment strategy $q_\cdot^\lambda = \lambda q_\cdot^*(R_t, Q_t, K_t)$. Then the hashpower resulting from $q_\cdot^\lambda$ satisfies

$$Q_s^\lambda = \lambda Q_t + \int_s^t q_\tau^\lambda d\tau = \lambda \left[Q_t + \int_s^t q_\tau^* d\tau\right] = \lambda Q_s^*, \text{ for all } s \geq t.$$

Moreover, since R_t follows a geometric Brownian motion

$$\Pr\{R_s \leq x | R_t\} = \Pr\{\lambda R_s \leq \lambda x | \lambda R_t\}, \text{ for all } s > t \text{ and all } x \in \mathbb{R}_+,$$

we have

$$\begin{aligned} V^\lambda(\lambda R_t, \lambda Q_t, K_t) &= \mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)}\left(\frac{\lambda R_s}{\lambda Q_s^*} - \frac{\partial c\left(q_s^\lambda, Q_s^\lambda, K_s\right)}{\partial Q_s}\right) ds\right] \\ &= \mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)}\left(\frac{R_s}{Q_s^*} - \eta K_t\left(\frac{q_s^*}{Q_s^*}\right)^{1+\eta}\right) ds\right] \\ &= \mathbb{E}_t\left[\int_t^\infty e^{-r(s-t)}\left(\frac{R_s}{Q_s^*} - \frac{\partial c\left(q_s^*, Q_s^*, K_s\right)}{\partial Q_s}\right) ds\right] \\ &= j(R_t, Q_t, K_t), \end{aligned}$$

where the second equality follows from $c_Q\left(q_s^\lambda, Q_s^\lambda, K_s\right) = K_s\eta\left(\lambda q_s^* / \left(\lambda Q_s^*\right)\right)^{1+\eta}$, while the third equality holds because $q_\cdot^*$ is the optimal investment policy given (R_t, Q_t, K_t). The mimicking strategy $q_\cdot^\lambda$ being one of the many feasible strategies, it must be the case that $j(\lambda R_t, \lambda Q_t, K_t) \geq V^\lambda(\lambda R_t, \lambda Q_t, K_t) = j(R_t, Q_t, K_t)$.

The reverse inequality is established considering a planner which faces the initial condition (R_t, Q_t, K_t) but implements the investment strategy $q_\cdot^{1/\lambda} = q_\cdot^* (\lambda R_t, \lambda Q_t, K_t) / \lambda$. The same derivations as before yields $j(R_t, Q_t, K_t) \geq V^{1/\lambda}(R_t, Q_t, K_t) = j(\lambda R_t, \lambda Q_t, K_t)$. Putting the two inequalities together, we finally obtain $j(\lambda R_t, \lambda Q_t, K_t) = j(R_t, Q_t, K_t)$.

The proof for the homogeneity in (R_t, K_t) follows a similar logic. Consider a planner which faces the initial condition $(\lambda R_t, Q_t, \lambda K_t)$ and implements the optimal strategy $q_\cdot^*(R_t, Q_t, K_t)$ of a planner facing (R_t, Q_t, K_t). Since both planners share the same initial hashpower and invest the same quantities, $Q_s = Q_s^*$ for all $s \geq t$. The expected returns of this strategy are

$$\begin{aligned}
V(\lambda R_t, Q_t, \lambda K_t) &= \mathbb{E}_t \left[\int_t^\infty e^{-r(s-t)} \left(\frac{\lambda R_s}{Q_s} - \frac{\partial c(q_s, Q_s, K_s)}{\partial Q_s} \right) ds \,\middle|\, q_s = q_s^*(R_t, Q_t, K_t) \right] \\
&= \mathbb{E}_t \left[\int_t^\infty e^{-r(s-t)} \left(\frac{\lambda R_s}{Q_s^*} + \lambda K_s \eta \left(\frac{q_s^*}{Q_s^*} \right)^{1+\eta} \right) ds \right] \\
&= \lambda j(R_t, Q_t, K_t),
\end{aligned}$$

which implies in turn that $j(\lambda R_t, Q_t, \lambda K_t) \geq V(\lambda R_t, Q_t, \lambda K_t) = \lambda j(R_t, Q_t, K_t)$. Homogeneity is again established considering the reverse situation where a planner which faces the initial condition (R_t, Q_t, K_t) implements $q_\cdot^*(\lambda R_t, Q_t, \lambda K_t)$ so that

$$\begin{aligned}
V(R_t, Q_t, K_t) &= \mathbb{E}_t \left[\int_t^\infty e^{-r(s-t)} \left(\frac{R_s}{Q_s} - \frac{\partial c(q_s, Q_s, K_s)}{\partial Q_s} \right) ds \,\middle|\, q_s = q_s^*(\lambda R_t, Q_t, \lambda K_t) \right] \\
&= \frac{1}{\lambda} \mathbb{E}_t \left[\int_t^\infty e^{-r(s-t)} \left(\frac{\lambda R_s}{Q_s^*} + \lambda K_s \eta \left(\frac{q_s^*}{Q_s^*} \right)^{1+\eta} \right) ds \right] \\
&= \frac{1}{\lambda} j(\lambda R_t, Q_t, \lambda K_t).
\end{aligned}$$

Since $j(R_t, Q_t, K_t) \geq V(R_t, Q_t, K_t) = j(\lambda R_t, Q_t, \lambda K_t)/\lambda$, combining the two inequalities yields the required homogeneity $j(\lambda R_t, Q_t, \lambda K_t) = \lambda j(R_t, Q_t, K_t)$. $\square$

Table 1: Calibrated Parameters

Parameters	Interpretation	1st period			2nd period		
A. MAXIMUM LIKELIHOOD							
α	Trend R_t		2.38			0.46	
σ^2	Volatility R_t		1.95			0.54	
B. CALIBRATION		Baseline	Halvings	Time-to-Build	Baseline	Halvings	Time-to-Build
a	Rate of TP	1.18	1.29	1.10	0.76	0.85	0.90
		(0.50)	(0.43)	(0.42)	(0.12)	(0.13)	(0.13)
K_0	Total Costs	\$ 5.6 mn	\$ 5.3 mn	\$ 4.7 mn	\$1, 825	\$1, 655	\$1, 465
		(\$ 16 mn)	(\$ 8.9 mn)	(\$ 17.8 mn)	(\$199)	(\$83)	(\$232)
δ	Time-to-Build			11.5 days			46.5 days
				(9.24 days)			(27.8 days)

Parameters	Interpretation	3rd period		
A. MAXIMUM LIKELIHOOD				
α	Trend R_t		0.27	
σ^2	Volatility R_t		0.80	
B. CALIBRATION		Baseline	Halvings	Time-to-Build
a	Rate of TP	0.76	0.95	0.65
		(0.34)	(0.31)	(0.32)
K_0	Total Costs	\$ 182	\$ 173	\$ 160
		(\$ 203)	(\$ 122)	(\$ 152)
δ	Time-to-Build			43.5 days
				(21.3 days)

Note: Calibrations based on an annual discount rate $r = 10\%$. K_0 is the calibrated total cost per Terahash-second at the first day of each subperiod. All parameters expressed as yearly rates except the time-to-build, δ, which is expressed in days. Standard errors from block bootstrap in parenthesis.

Table 2: Calibration with and without Exit

Parameter	Interpretation	1st period		2nd period	
		Baseline	Exit	Baseline	Exit
a	Rate of TP	1.18	1.15	0.76	0.76
		(0.50)	(0.44)	(0.12)	(0.12)
$\overline{P}_0$	Barrier	25996	23858	5.30	5.05
		(25843)	(19811)	(0.66)	(0.64)
K_0	Overall Costs of Entry	$\$5.6 \times 10^6$	$\$4.8 \times 10^6$	\$1,825	\$1,581
		(1.6×10^7)	(2.6×10^7)	(199)	(220)
C_0	Daily Operating Costs		\$2,767		\$0.68
			(1332)		(0.38)
I_0	Price of Mining Rig		$\$3.1 \times 10^6$		\$1,002
			(2.5×10^7)		(444)
T	Maximal Mining Time		1.87 years		2.65 years

Note: Calibrations based on a an annual discount rate $r = 10\%$. I_0, C_0 and K_0 correspond to a one-Terahash per second hardware at the first day of each subperiod. Standard errors from block bootstrap in parenthesis.