frontiers | Frontiers in Blockchain

TYPE Original Research
PUBLISHED 25 September 2023
DOI 10.3389/fbloc.2023.1226892



OPEN ACCESS

EDITED BY
Andrea Pizzoferrato,
University of Bath, United Kingdom

REVIEWED BY
Cesare Fracassi,
The University of Texas at Austin,
United States
Anupama Mishra,
Swami Rama Himalayan University, India

*CORRESPONDENCE
Jack R. Rogers,
j.r.rogers@exeter.ac.uk

RECEIVED 22 May 2023
ACCEPTED 28 August 2023
PUBLISHED 25 September 2023

CITATION
Rogers JR (2023), Bitcoin equilibrium dynamics: a long term approach.
*Front. Blockchain* 6:1226892.
doi: 10.3389/fbloc.2023.1226892



# Bitcoin equilibrium dynamics: a long term approach

Jack R. Rogers*

Economics, University of Exeter Business School, Exeter, United Kingdom

In the long run, Bitcoin transaction fees are the only source of revenue for miners. They compete broadly in two main ways: proof of work effort to win blocks; and transaction processing to gather fee rewards into the blocks they win. This paper contributes to existing literature by developing a dynamic model that separates these two functions, and explores implications for aggregate efficiency outcomes. Specifically, when set by free market forces (unrestricted by artificially imposed block size caps), what happens to overall transaction prices and quantities relative to total energy use? When is it worth Stackelberg-leading miners investing in efficiency-improving R&D? What effect does this have on overall efficiency over time? By explicitly separating specialised capital dedicated to SHA256 hashing (for proof of work) from transaction processing capital (for transaction collection and verification), this paper sheds light on these questions. One key conclusion is that miner innovation lowers energy use per transaction over time for elastic enough transaction demand schedules. The more competitors Bitcoin has (existing fiat and data services, and other new Blockchain-based systems), the stronger is this conclusion.

KEYWORDS

**bitcoin, equilibrium, stackelberg, energy efficiency, transaction fees**

## 1 Introduction

The fact that the transaction fee market is a critical determinant of real outcomes in the long run has been analysed previously (Easley et al., 2019; Houy 2014). In Houy (2014), partial equilibrium outcomes with fixed block sizes are shown to be equivalent to transaction price fixing. Welfare implications in scenarios where these variables are centrally-planned, subject to constraints including a minimum overall hash rate are explored in Houy (2014). In their model, aggregate hash rates have to be above an all-or-nothing threshold, below which the Blockchain totally fails due to lacking enough security. Although the relationship between hash rates and security is not explicitly modelled in this paper, there is scope for exploring this further. For example, it could be that competitive miners with larger revenues and/or profits stemming from transactions fees offer more security by virtue of being better resourced. Easley et al. (2019) assume that users gain less utility, the longer is the delay between submitting their transaction to the network and observing it in a confirmed block. They conclude that block size constraints limit overall growth of the network, and may cause instability. Again though, there is no further analysis of scenarios where transaction volumes and prices are determined in a free market with no artificial constraints. Although this institutional structure is consistent with the block size cap implemented on the BTC Blockchain today (which effectively acts as a quota on ledger-auditable transaction volumes), there are other systems more in line with Satoshi's original proposals (like Bitcoin SV). Furthermore, as touched on in Easley et al. (2019), it could be argued that versions of Bitcoin that do not adapt over time (e.g., by relaxing block quotas or transaction price controls) may

not even survive in the long run. This was presumably what Satoshi Nakamoto meant when they suggested that in 2030 there would 'either be very large transaction volume, or no volume at all'[1]. Bitcoin as a system competes particularly intensively with any others that use SHA256 hashing in proof of work, because the switching costs involved in redirecting equipment are negligible (a miner with equipment specialised in SHA256 hashing does not need to physically relocate to mine on a different chain). Overall then, dynamic competition unfolds on the supply side, between, as well as within specific Blockchain systems. This paper therefore seeks to better understand the nature of long term equilibria in the context of unrestricted transaction fee markets.

The paper is organised as follows. Section two uses the same basic framework as in Dimitri (2017), with explicit dynamic structure as in Ma et al. (2018). This simple two-player Cournot-type game provides the foundation for contributions in the later sections. Strategic interactions known as Tullock contests (Tullock et al., 1980; Fonseca, 2009) repeat and occur during 2-week time horizons, via the channel of Bitcoin's exogenously imposed difficulty adjustment algorithm. Dynamic equilibrium outcomes are presented in which each miner's efforts spill over to others in the form of negative externalities (one miner's efforts increase difficulty, which in turn lowers optimal effort responses overall). As expected, when underlying cost structures are heterogeneous, relatively lower unit energy costs, or higher mining equipment efficiency, result in relatively high hash rates for individual miners.

Although the static results presented in Dimitri (2017) are frequently extended into a dynamic setting (e.g., Alsabah and Capponi 2020; Cong et al., 2020), this paper explores intra-difficulty period competition in more detail. For example, in Fiat et al. (2019), miners' effort levels are fixed for the duration of difficulty periods (referred to as 'epochs'). Instead, this paper allows observation and effort to vary within difficulty periods, and includes original analysis and discussion of specific proposals for how such equilibria are likely to emerge in practice. Again, in contrast to the literature, an explicit parameter separation of underlying energy (typically electricity) costs, distinct from mining equipment efficiency (typically measured in Joules per Gigahash) is included. This latter feature is then exploited in section 3, where fixed investment costs are introduced, and a speed of hash capital parameter is endogenised, leading to a richer description of equilibria. A specific contribution to understanding the nature of overall outcomes in Bitcoin over these longer time horizons is provided by considering an individual firm's optimal spending on R&D designed to improve the energy efficiency of its operation. The conditions under which it is worth investing are formally derived, and equilibrium Stackelberg outcomes presented. In cases where it is worth the leader investing, the extent to which aggregate energy use falls is derived for the case where the Stackelberg follower does not invest. In the calibrated example, the leading miner's optimal strategy lowers aggregate energy use by 30%.

The final section 4 provides an original analysis that builds further on the previous sections by including transaction fee revenues. Transactions have to be gathered, checked, and verified before inclusion inside proposed blocks, a process that is very different from the way blocks are won from hashing. As such, transaction capital is introduced into the model, alongside fee revenues determined by a demand function with an explicit elasticity parameter. The framework outlined here also includes the previous Stackelberg structure, with some novel results. Adoption of more efficient hash equipment (or any change in this) has no effect on aggregate energy use. This is interesting, because it means that given the assumptions outlined here, mining firms naturally incentivised to seek such improvements will increase the aggregate security of the Bitcoin Blockchain without increasing aggregate energy use. Another novel result is derived for transaction processing efficiency improvements. In this analysis, the demand for transactions is exogenous in the sense that the elasticity of demand is fixed. In cases where the elasticity of demand for a typical transaction is higher than one (demand is relatively elastic), improvements in how efficiently miners process transactions unambiguously reduce aggregate energy use per transaction over time. The analysis on whether it is worth investing in R&D in this paper assumes no spillovers of knowledge to competitors, which contrasts with Alsabah and Capponi (2020). Neither does it endogenise the positive externality that comes from proof of work mining: a by-product of individual miner efforts is that they enhance the overall Blockchain security for other users and miners (Houy, 2014). To the extent that consumers of transaction and data services benefit from this, inclusion of these utility benefits would increase demand, presumably lowering aggregate energy use per transaction more than the results presented here. Further work could attempt to endogenise these other effects, and include welfare analysis.

## 2 Short run competition

Two miners $A$ and $B$ compete to earn revenue from block rewards from hashing, which is costly. They seek to maximise the expected value of their profits, by choosing hash rates $h_A$ and $h_B$. With only two miners, the probability a specific miner wins a block competition is only determined by their relative hash rate. Defining the aggregate hash rate $H = h_A + h_B$, then:

$$P(\text{Miner A wins a particular block competition}) = \frac{h_A}{H}. \quad (1)$$

Costs for a particular block competition are $\gamma \times h_A$ for miner $A$, so their expected profit is:

$$E[\Pi_A] = \omega \frac{h_A}{H} - \gamma h_A \tau, \quad (2)$$

where $\omega$ is the block subsidy reward, and $\gamma$ captures the average cost of conducting one hash. Section 3 later describes a scenario where a leading miner has the opportunity to invest in new hashing equipment. This investment improves efficiency, as distinct from any lowering of variable costs that mainly derive from having to supply power to mining rigs. As such, this parameter is defined as:

$$\gamma = \frac{c}{e}, \quad (3)$$

1 Nakamoto, S. (2010, February 14). I'm sure that in 20 years there will either be very large transaction volume or no volume. [Online forum post]. https://bitcointalk.org/index.php?topic=48.msg329#msg329.

where $c$ is the cost (normally of electricity, here denominated in bitcoins) of 1 joule of energy, and $e$ is the efficiency of the hashing capital equipment (commonly referred to as 'rigs') deployed by the miner. As an example calibration, Kristoufek (2020) includes a list of different chip manufacturers specified by the number of Joules (J) required to execute a gigahash (one Gh, or one billion hashes) ranging from the least efficient 0.95 J/Gh down to the most efficient 0.09 J/Gh. If a miner has equipment capable of 0.1 J/Gh, this is equivalent to a capability of running 10 billion hashes from 1 J of energy (note that the way efficiency is expressed in this paper as the inverse of this, a higher number means more efficient). If the cost of 1 J of electricity translates to $8.7 \times 10^{-4}$ bitcoins then the overall average cost per hash is $\gamma = 8.7 \times 10^{-14}$ bitcoins. Here is a complete summary of this numerical example:

$$\begin{aligned} J/Gh &= 0.1, \text{so } Gh/J = \frac{1}{0.1} = 10 \\ e &= h/J = 10 \times 1 \text{ billion} = 10 \times 1^9 = 10^{10} \\ c &= 8.7 \times 10^{-4} \\ \gamma &= \frac{c}{e} = \frac{8.7 \times 10^{-4}}{10^{10}} = 8.7 \times 10^{-14} \end{aligned}$$

Individual block rewards $\omega$ are denominated in bitcoin and directly observable. They consist of two sources - a bitcoin subsidy that started at 50 bitcoins, halving every 4 years, currently to 6.25 bitcoins per block. In the long run the only source sustaining all miner activities are the transactions fees accumulated within each block.

It is important to note that while $\gamma$ costs are typically borne in fiat currencies, $\omega$ revenues are received directly in bitcoins, so real miner profits are directly affected by Bitcoin's famously volatile exchange rate. However, to the extent that miners are able to exchange recently won bitcoin rewards into fiat and/or other more stable assets quickly, and able to forecast average bitcoin exchange rates in the short and medium run, profit maximising decisions are underpinned by the fundamental analysis set out in this paper. In practice, this means two things: treating speculative trading activity as a separate function, even though this may naturally occur; and assuming rational expectations so that exchange rate forecast errors are not systematically biased in any way. Whilst these are heavy assumptions, they are argued to provide a useful benchmark from which to develop more complex theory. Miners will have to decide when to trade their accumulated bitcoins for fiat (after the approximate 17 h time window when they cannot, as defined by Bitcoin's 100 block 'cooling off period'). The model presented here does not include the exchange rate, and generally abstracts away from risk by assuming risk neutrality. Instead, it turns this issue around on its head, by focusing on economic fundamentals, towards future scenarios where speculative hype is no longer a factor, offering logical reasoning behind potential stability and forecastability of the bitcoin/fiat exchange rate. In terms of economic costs, for now this analysis also ignores overheads and assumes constant marginal costs - other cost function types and features, including capital investment, can be added without altering the main conclusions set out here (Section 3 develops this further).

Approximately every 2 weeks, Bitcoin difficulty adjusts according to a formula. In the following analysis, each discrete time period corresponds to the 2016 block competitions that make up a difficulty period. Each block competition lasts approximately 10 min, and hence a difficulty period is $10 \times 2016 = 20,160$ min, or 2 weeks on average. As already noted, transaction fee revenue is the only source that sustains miners in the long term, and this is absolutely fundamental to sustainable economic behaviour, but the focus here is on the intra-difficulty-period game theoretic forces steering competitive miners towards equilibrium behaviour. Hence, expected revenue derives directly from the expected proportion $\frac{h_A}{H}$ of fixed block subsidies won by miner $A$ instead of miner $B$. Costs rise and fall in proportion to $\tau$, the time duration during which the miners apply their hash rates. In practice the duration of each block competition, and hence the 2016-block difficulty-period, is a stochastic variable drawn from a geometric or exponential distribution, depending on how this is expressed mathematically. With the assumption that miners are profit maximisers with risk-neutral preferences, they only care about difficulty-period time duration expected values (not variances or higher moments). The time duration $\tau$ increases and decreases in expectation, inversely to the aggregate hash rate relative to a benchmark $\bar{H}_0$ that is defined by the current difficulty. Conventionally, difficulty is expressed as a number that defines how much harder it is to find a valid block solution compared to the genesis block (the first ever block created), but depending on the type of analysis, it can be specified relative to any chosen benchmark.

$$\tau_t = \frac{\bar{H}_{t-1}}{H_t} \tag{4}$$

In the following, hash rates are defined as the number of hashes during a 2 week difficulty period, and the benchmark $\bar{H}_{t-1}$ as the expected number of hashes required to find a valid solution. In practice, each single hash is a random integer draw from 0 to $M = 2^{256}-1$, and difficulty is a target range from 0 to a target number $T_0$. For example, if the current target is $T_0 = 2^{200}$, the probability that one particular hash will land in the success region is $p = \frac{2^{200}}{2^{256}} = 2^{-56}$ and the benchmark hash rate is $\bar{H}_0 = \frac{1}{p} = 2^{56}$ for a particular block. With $2^{56}$ hashes required on average to find a valid block, $2016 \times 2^{56}$ hashes will be required on average to complete a difficulty period. Bitcoin's difficulty adjustment algorithm aims to ensure that difficulty periods last $\bar{\tau} = 2$ weeks, so if a particular duration $\tau_t$ turns out to be shorter (longer) than 2 weeks, the target for the next difficulty period is reduced (increased) in proportion, according to[2]:

$$T_{t+1} = T_t \frac{\tau_t}{\bar{\tau}} \tag{5}$$

The corresponding benchmark hash rate updates according to:

$$\bar{H}_{t+1} = \bar{H}_t \frac{\bar{\tau}}{\tau_t}$$

In the example, if $\tau_1$ turned out to be 1 week, block solutions would have been found twice as fast as they should have been, so the target in the next period would have been halved:

2 In practice, due to a bug, Bitcoin's difficulty adjustment protocol bases new targets on activity during the previous 2015, not 2016 blocks. This analysis ignores the negligable difference this makes for simplicity, and without loss of generality, but empirical and other work can adjust this as needed.

$$T_1 = T_0 \frac{1\text{ week}}{2\text{ weeks}} = 2^{200} \times \frac{1}{2} = 2^{199}$$

Accordingly, with the difficulty now doubled, the benchmark number of hashes required would double:

$$\bar{H}_1 = (\bar{H}_0)\frac{2\text{ weeks}}{1\text{ week}} = (2016 \times 2^{56}) \times 2 = 2016 \times 2^{57}$$

In summary then, given an initial condition specified for the benchmark target value $T_0$, and hence $\bar{H}_0 = \frac{M}{T_0}$, and defining the total block subsidy available during the 2 week difficulty period $\Omega = 2016 \times \omega$, at the beginning of difficulty period 1 the expected profits for miner $A$ are:

$$E_1[\Pi_A] = E_1[\Pi_{A1} + \Pi_{A2}] = \Omega\frac{h_{A1}}{H_1} - \gamma h_{A1}\tau_1 + \Omega\frac{h_{A2}}{H_2} - \gamma h_{A2}\tau_2$$

Where expected durations are $E_1[\tau_1] = \frac{\bar{H}_0}{H_1}$ and $E_1[\tau_2] = \frac{\bar{H}_1}{H_2}$, hence (dropping the bar notation for expected values, except for $\bar{H}_0$ which is given at the beginning of time $t = 1$):

$$E_1[\Pi_A] = \Omega\frac{h_{A1}}{H_1} - \gamma h_{A1}\frac{\bar{H}_0}{H_1} + \Omega\frac{h_{A2}}{H_2} - \gamma h_{A2}\frac{H_1}{H_2} \tag{6}$$

Collecting revenue and cost terms together, and defining the cost of a hash denominated in bitcoins relative to the difficulty period block reward as $\kappa = \frac{\gamma}{\Omega}$, this can be rearranged as:

$$E_1[\Pi_A] = \Omega\left[\left(\frac{h_{A1}}{H_1} + \frac{h_{A2}}{H_2}\right) - \kappa\left(h_{A1}\frac{\bar{H}_0}{H_1} + h_{A2}\frac{H_1}{H_2}\right)\right]$$

This shows explicitly that given miner $B$'s chosen hash rate path $\bar{h}_{B1}$ and $\bar{h}_{B2}$, as miner $A$'s chosen hash rates rise, on the one hand they expect to win a larger proportion of the block subsidies $\Omega$, while on the other their costs rise in proportion to the relative cost of a single hash $\kappa = \frac{\gamma}{\Omega}$, and the benchmark difficulty contained inside $\bar{H}_0$. Crucially though, if $A$ chooses to increase $h_{A1}$, not only do their expected costs rise in period 1, as defined by the first cost term $\kappa\bar{H}_0\frac{h_{A1}}{h_{A1}+h_{B1}}$, their period 1 choice also increases expected costs in period 2 as defined by the second cost term $h_{A2}\frac{H_1}{H_2}$ that contains $\frac{\kappa h_{A2}}{h_{A2}+h_{B2}}h_{A1}$. The expected revenue part of the profit function varies with $h_{A1}$ according to $\frac{\delta E[\text{Revenue}_A]}{\delta h_{A1}} = \Omega\frac{\delta E[h_{A1}H_1^{-1}]}{\delta h_{A1}}$, while the cost part varies according to:

$$\frac{\delta E[\text{Cost}_A]}{\delta h_{A1}} = -\gamma\left[\frac{\bar{H}_0}{H_1} - h_{A1}\frac{\bar{H}_0}{H_1^2} + \frac{h_{A2}}{H_2}\right]$$

Symmetric Nash equilibrium implies $h_{A1} = h_{B1} = h_1 = \frac{H_1}{2}$ and $h_{A2} = h_{B2} = h_2 = \frac{H_2}{2}$, so

$$\frac{\delta E[\text{Cost}_A]}{\delta h_{A1}} = -\gamma\left[\frac{\bar{H}_0}{2H_1} + \frac{1}{2}\right].$$

Assuming expected outcomes will be close enough to the Nash equilibria, and that being close enough to a steady state implies $H_1 \approx \bar{H}_0$, this means:

$$\frac{\delta E[\text{Cost}_A]}{\delta h_{A1}} \approx -\gamma,$$

So when miner $A$ is considering their choice of period 1 hash rate $h_{A1}$, every extra hash conducted in period 1 has an approximate overall extra expected linear cost of $\gamma$ accumulated across the two periods, whereas the effect on total expected revenue is clearly non-linear and strategically dependent on miner $B$'s choice:

$$\frac{\delta E[\text{Revenue}_A]}{\delta h_{A1}} = \Omega\left[\frac{1}{h_A + h_B} - \frac{h_{A1}}{(h_A + h_B)^2}\right]$$

## 2.1 Short run profit maximisation

The miner $A$ profit Equation 6 from earlier can be re-written as:

$$E_1[\Pi_A] = (\Omega - \gamma\bar{H}_0)\frac{h_{A1}}{H_1} + (\Omega - \gamma H_1)\frac{h_{A2}}{H_2},$$

or, using the average cost of a hash relative to the rewards defined earlier ($\kappa = \frac{\gamma}{\Omega}$):

$$E_1[\Pi_A] = \Omega\left((1 - \kappa\bar{H}_0)\frac{h_{A1}}{H_1} + (1 - \kappa H_1)\frac{h_{A2}}{H_2}\right)$$

The profit maximisation problem can therefore be determined from the following objective function, $\Omega$ removed,

$$\max_{h_{A1}}\left\{(1 - \kappa\bar{H}_0)\frac{h_{A1}}{H_1} + (1 - \kappa H_1)\frac{h_{A2}}{H_2}\right\} \tag{7}$$

Defining auxiliary variables $W = 1 - \kappa\bar{H}_0$ and $V = \kappa\frac{h_{A2}}{H_2}$, leaves just:

$$\max_{h_{A1}}\left\{Wh_{A1}H_1^{-1} + \frac{h_{A2}}{H_2} - VH_1\right\}$$

Differentiating this with respect to $h_{A1}$ and setting to zero gives:

$$W(H_1^{-1} - h_{A1}H_1^{-2}) - V = 0,$$

Which can be rearranged as follows:

$$\begin{aligned} W(H_1 - h_{A1}) - VH_1^2 &= 0 \\ Wh_{B1} - V(h_{A1}^2 + 2h_{A1}h_{B1} + h_{B1}^2) &= 0 \\ -Vh_{A1}^2 - 2Vh_{B1}h_{A1} - Vh_{B1}^2 + Wh_{B1} &= 0 \end{aligned}$$

In any symmetric equilibrium where $h_{A1} = h_{B1} = h_1$, the last equation becomes:

$$\begin{aligned} -Vh_1^2 - 2Vh_1^2 - Vh_1^2 + Wh_1 &= 0 \\ h_1^* &= \frac{W}{4V} = \frac{1 - \kappa\bar{H}_0}{4\kappa\frac{h_{A2}}{H_2}} \end{aligned} \tag{8}$$

This last equation pins down the optimal hash rate for miner $A$ (and symmetrically the same for miner $B$), for assumed period 2 hash rates. If this 'game' is only played for these two periods, the same cannot be derived for period 2. However, as shown in section 3 later, assuming the same type of Nash equilibrium behaviour in period 2 is consistent with maximisation of an infinite discounted stream of future profits. In the special case where the initial conditions are set up to ensure a steady state where $\bar{H}_0 = H_1 = H_2$, and where the same symmetric outcome in period 2 ($h_{A2} = h_{B2} = h_2$) is assumed (so that $\frac{h_{A2}}{H_2} = \frac{1}{2}$), from the earlier definitions of $W$ and $V$, this implies:

$$h_1^\star = \frac{1-\kappa\bar{H}_0}{2\kappa} = \frac{1}{4\kappa} = \frac{\Omega}{4\gamma} \tag{9}$$

which also implies the aggregate hash rate $\bar{H}_0 = H_1^\star = 2h_1^\star = \frac{\Omega}{2\gamma}$ and from earlier definitions $\bar{H}_0 = \frac{M}{T_0}$, $\kappa = \frac{\gamma}{\Omega}$ and $\Omega = 2016 \times \omega$, so:

$$\frac{\Omega}{2\gamma} = \frac{2016 \times \omega}{2\gamma} = \frac{M}{T_0}$$
$$T_0 = \frac{\gamma}{1008\omega} 2^{256}$$

With a block reward subsidy worth $\omega = 6.25$ bitcoins, and using the calibration example where the average cost of a single hash is $\gamma = 8.7 \times 10^{-14}$ bitcoins, the target will be approximately the same as earlier:

$$T_0 = \frac{8.7 \times 10^{-14}}{1008 \times 6.25} 2^{256} \approx 2^{200}$$

Note that at the Nash equilibrium, the profit function simplifies to:

$$E_1[\Pi_A] = \Omega - 2\gamma h = \Omega - 2\gamma\left(\frac{\Omega}{4\gamma}\right) = \frac{\Omega}{2}, \tag{10}$$

So with the tailored steady state initial conditions (equivalent in a multi period model to assuming dynamic equilibrium), and Nash equilibrium outcomes, each miner expects to earn half of this, or $\frac{\Omega}{4}$ in terms of profit each period. In Nash equilibrium, their total expected profits are independent of hash costs. Although this result is present in Dimitri (2017) and others, it is worth briefly reflecting on what drives this. It is unintuitive, in the sense that in equilibrium, the total level of profits made by the miners are completely unrelated to the underlying cost of a hash $\gamma$. It is explained by the fact that by design, the Bitcoin system changes the unit cost of hashing systematically, depending on miners' collective behaviour. Even if $\gamma$ is astronomically high, the two miners both end up contributing negligible hash effort in equilibrium, so difficulty, and hence their average costs fall to appropriate levels until each miner is back to expecting $\frac{\Omega}{4}$. Any increase in average cost per hash (indicated by the left hand $\gamma$ in the representation below) is exactly offset by miners lowering their optimal choice $h_1^\star = \frac{1}{4\frac{\gamma}{\Omega}} = \frac{\Omega}{4\gamma}$, which lowers difficulty, and hence costs:

$$\Omega - (2\gamma\uparrow)\left(\frac{\Omega}{4\gamma}\downarrow\right)$$

This mechanism also implies that ignoring investment costs, profits stay positive in equilibrium for arbitrarily large numbers of competing miners. As others enter this competition, expected profits fall at a decreasing rate, approaching zero as $n \to \infty$ where $n$ is the total number of miners. Specifically with $n$ miners, each miner expects a profit of $\frac{\Omega}{2n}$. The introduction of a fixed overhead cost to the profit equation, along with a zero profit condition defines $n$.

## 2.2 Best response functions

Nash equilibria described in the previous sub-section can be thought of as fully rational forward looking behaviour. Both miners know that in both periods, they will be able to respond to each other strategically, and that their choices in period 1 will affect difficulty in period 2. With varied hash rates, competition can unfold even within difficulty periods. When two large miners interact during a difficulty period, they can estimate each others' hash rates by observing each others' block successes in real time. However this is done (as a Bayesian learning process, for example), this strengthens the assumption of forward-looking rational behaviour, with each miner responding to each others' hash rate choices in real time. This sub-section first derives the best response functions from the perspective of period 1, for each miner $A$ and $B$, before briefly considering how miners could best-respond to each other in real time, during a difficulty period.

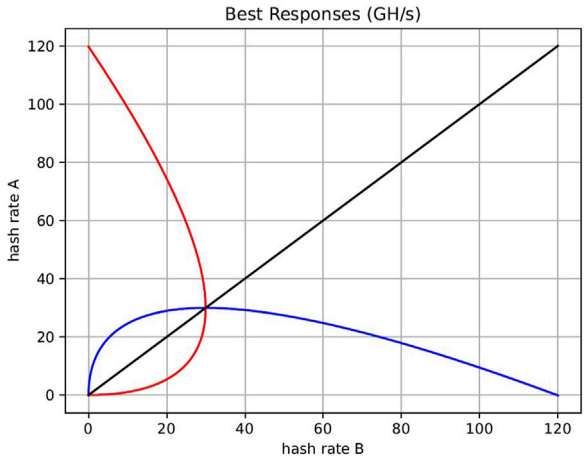


FIGURE 1
Best response functions (Gigahashes per second).

From earlier, miner $A$'s best response function is:

$$Vh_{A1}^2 + 2Vh_{B1}h_{A1} + Vh_{B1}^2 - Wh_{B1} = 0$$

This is solved and rearranged as follows:

$$h_{A1}^\star = \frac{-2Vh_{B1} \pm \sqrt{(2Vh_{B1})^2 - 4(V)\left(Vh_{B1}^2 - Wh_{B1}\right)}}{2V}$$
$$h_{A1}^\star = -h_{B1} \pm \left(\frac{W}{V}\right)^{\frac{1}{2}} h_{B1}^{\frac{1}{2}}$$

Assuming non-negative costs and hash rates, the negative root is dropped:

$$BRF_A\colon h_{A1}^\star = -h_{B1} + \left(\frac{W}{V}\right)^{\frac{1}{2}} h_{B1}^{\frac{1}{2}} \tag{11}$$

where $W = 1 - \kappa\bar{H}_0$ and $V = \kappa\frac{h_{A2}}{H_2}$, and as before, with the selected initial condition $\bar{H}_0 = H_1$, and at the equilibrium $h_{A1} = h_{B1} = h_1$, then the $(\frac{W}{V})^{\frac{1}{2}}$ term simplifies down to $\theta = \kappa^{-\frac{1}{2}} = (\frac{\Omega}{\gamma})^{\frac{1}{2}}$ leaving:

$$BRF_A\colon h_{A1}^\star = -h_{B1} + \theta h_{B1}^{\frac{1}{2}} \tag{12}$$

Miner $B$ will optimally respond to $A$, in the same way to give $B$'s best response function:

$$BRF_B\colon h_{B1}^\star = -h_{A1} + \theta h_{A1}^{\frac{1}{2}}$$

Rearranged as the inverse function for comparison on the same plane this is:

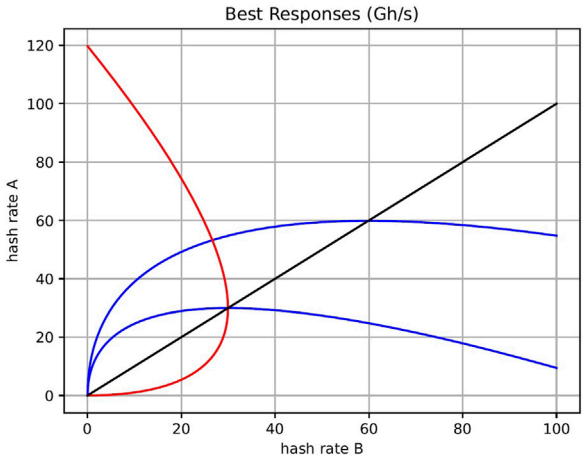


FIGURE 2
Best response functions (Heterogenous marginal hash costs).

$$BRF_B\colon h_{A1} = \frac{\theta^2}{2} - h^\star_{B1} \pm \theta\sqrt{\frac{\theta^2}{4} - h^\star_{B1}} \tag{13}$$

The two best response functions together provide each miner's optimal response to the other's hash rate choice in period 1. On its own, forward-looking rational reasoning could be used to justify this outcome as an assumption from the perspective of the start of period 1. Compared to many other real world settings though, the fact that during a difficulty period, miners can observe each others' activity only strengthens these rationality assumptions. Figure 1 shows the unique Nash equilibrium.

The blue line in Figure 1 shows miner $A$'s best hash rate response (in numbers of billions of hashes, or Gigahashes, per second, GH/s) on the $y$ -axis, to $B$'s choice on the $x$-axis. To recalibrate from hashes per 2 week period in the *BRF* equations above, the following conversion of parameter $\theta$ was required (there are 1,209,600 sec during 2 weeks): $\frac{\Omega/(1{,}209{,}600)}{\gamma \times (1\text{ billion})}$. As already established, at the Nash equilibrium where the two *BRFs* intersect, each miner maximises their profit given the others' hash rates when they both choose $h^\star_{A1} = h^\star_{B1} = \frac{\Omega}{4\gamma}$, which in the numerical example here is $\frac{6.25/(10\times 60)}{4\times 8.7\times 10^{-5}} =$ 30 GH/s. If they both choose this hash rate in periods 1 and 2, total expected profits for each miner are $\frac{\Omega}{2} = 6,300$ bitcoins.

## 2.3 Comparative cost advantage

Again, just as in Dimitri (2017) and others, unit hash costs may be heterogeneous. If, for example, miner $A$ has more expertise, or entered the competitive environment with more efficient hashing technology (e.g., better specialised ASICs), it could be that $\gamma_A < \gamma_B$ (and from earlier, $\kappa = \frac{\gamma}{\Omega}$ and $\theta = \kappa^{-\frac{1}{2}}$ so $\theta = \sqrt{\frac{\Omega}{\gamma}}$). With this definition, the Nash equilibrium comes from solving the following simultaneous equations:

$$BRF_A:\ h^\star_{A1} = -h_{B1} + \theta_A h^{\frac{1}{2}}_{B1}$$
$$BRF_B:\ h_{A1} = \frac{\theta_B^2}{2} - h^\star_{B1} \pm \theta_B\sqrt{\frac{\theta_B^2}{4} - h^\star_{B1}}$$

The solution to this system is:

$$h^\star_{A1} = \theta_B^2\left(\frac{\theta_A^2}{\theta_A^2+\theta_B^2}\right)^2 = \left(\frac{\theta_B}{\left(\frac{\theta_B}{\theta_A}\right)^2+1}\right)^2$$
$$h^\star_{B1} = \theta_A^2\left(\frac{\theta_B^2}{\theta_A^2+\theta_B^2}\right)^2 = \left(\frac{\theta_A}{\left(\frac{\theta_A}{\theta_B}\right)^2+1}\right)^2$$

And given $\theta_A = \sqrt{\frac{\Omega}{\gamma_A}}$ and $\theta_B = \sqrt{\frac{\Omega}{\gamma_B}}$

$$h^\star_{A1} = \Omega\frac{\gamma_B}{(\gamma_A+\gamma_B)^2} = \frac{\kappa_B}{(\kappa_A+\kappa_B)^2} \tag{14}$$
$$h^\star_{B1} = \Omega\frac{\gamma_A}{(\gamma_A+\gamma_B)^2} = \frac{\kappa_A}{(\kappa_A+\kappa_B)^2} \tag{15}$$

Figure 2 shows the same numerical example as earlier, with the upper blue line indicating miner $A$'s best response function when its marginal hash cost $\gamma$ halves in value. As its unit hash costs fall, its equilibrium $h^\star_{A1}$ increases substantially, while the fall in $B$'s hash rate $h^\star_{B1}$ in equilibrium is relatively modest.

## 2.4 Learning towards equilibrium

Dimitri (2017) assumes complete information about opponents' cost structures, arguing that there are only a few, large miners. This section discusses this a little further. The previous results documented Nash equilibria in the sense that both miners were best-responding to each others' best responses, and $A$'s profit $\Pi_A(h^\star_{A1}, h^\star_{B1}) > \Pi_A(h'_{A1}, h^\star_{B1})$ for all $h'_{A1}$. It can easily be shown however, that if miner $A$ behaves systematically according to $BRF_A$, then miner $B$ receives $\frac{\Omega}{2}$ profit, no matter what hash rate $B$ adopts (to the detriment of $A$, if they, veer away from equilibrium). The threat of punishment strategies can steer both miners to the Nash equilibrium. For example, introducing a dampening parameter $0 < D < 1$ as follows causes a unique profit maximisation point close to $h^\star_{B1}$ even for values of $D$ very close to 1:

$$BRF_A\colon h^\star_{A1} = D\left(-h_{B1} + \theta h^{\frac{1}{2}}_{B1}\right)$$

Miner $A$ could adopt more dramatic responses, like simply matching $B$'s hash rate. Fully rational miners should want to avoid these scenarios in the first place, as it is in their interest to simply land straight on the Nash equilibrium from the outset. Note also that within a difficulty period there is of course a time lag between actual miners' implementation of their hash rates, and the stochastic observed outcomes, so each miner can only approximate their opponents' hash rates, and with a lag. In terms of information, miners are pseudonymous in the sense that when they win a block, they do not have to include a self-identifying label. Even if they attempt to stay private though, very large miners may be easy to identify, not least because it is in all of their interests to build strong network connections with each other (that give them slight time advantages in starting and finishing block races, for example). At scale, large miners are enterprises that require large investment, so again it should be easy to reconcile their public business credentials with observed behaviour on the public Bitcoin blockchain.

Depending on precise assumptions on their information sets though, more complex scenarios may unfold. For example, miner $B$ could be bluffing in the sense of pretending to have more efficient

hashing technology, and hence a higher hash rate. Competitive miners should therefore want to gain intelligence on the underlying lowest real cost of conducting a hash, as well as testing their competitors by incorporating the probability of bluffing tactics, which in practice will mean raising their hash rates higher than the equilibria derived above. A Bayesian learning approach to both intra-difficulty period competition, and also longer term estimation of competitor cost structures and behaviour makes sense. With free entry, at the margin of profitability, miners that bluff in this way may not survive in the sense that they become unprofitable for long enough to go bankrupt.

Finally, just as in the classic Prisoners' Dilemma, miners can gain from collusion, so what forces might prevent this? If both miners could agree to arbitrarily lower their hash rates, their combined profits would approach the full value of block rewards available with negligible hash costs as difficulty falls. Apart from regulator enforcement, the threat of new entrants limits this possibility. Compared to many other real world economic settings, again, in the case of Bitcoin miner competition, cost and revenue structures are fully transparent, and any drop in difficulty should immediately encourage new entrants.

# 3 Medium run competition

Garratt and van Oordt (2020) show that the fixed costs associated with capital investment make Bitcoin more resilient to attack. This section builds on the intra difficulty period competition outlined up to now by introducing the cost of investing in equipment. Similar to the previous simplifying assumption that the marginal cost of one hash is constant, investment costs are assumed to be linear, again without compromising general conclusions laid out here. In practice, mining rigs are 'lumpy' in the sense that they cannot be purchased in tiny fractions, but again to keep analysis simple, it is assumed that conducting 1 single hash every 2 weeks requires a tiny fractional unit of mining rig $k_h$, that costs $p_{kh}$ each, and there is no depreciation. Expanding the numerical example from earlier where the average cost of a single hash is $\gamma = 8.7 \times 10^{-14}$ bitcoins, assume the unit cost of investment is the same $p_{kh} = 8.7 \times 10^{-14}$, and as before this can be expressed relative to the 2 weeks reward as $\kappa_{kh} = \frac{p_{kh}}{\Omega}$. In the two period model this introduces $\kappa_{kh} k_{h1}$ as a one-off cost to the profit equation. In the previous section, the only constraint was $\gamma$ comprised of the cost of energy $c$ and energy efficiency of equipment $e$, but introducing capital exposes the need to explicitly endogenise the speed of hashing equipment denoted as $s$. Specifically, it is assumed that a fractional micro unit of mining rig $k_h$ provides the capability of running $s$ hashes every 2 weeks, placing an upper bound on the number of hashes each period for each miner $\bar{h} = s \times k_h$. With the same dynamic equilibrium assumptions used earlier, defining $K = k_{hA} + k_{hB}$, the profit equation for miner $A$ then becomes:

$$\begin{aligned} E_1[\Pi_A] &= \Omega\left[\left(\frac{h_{A1}}{H_1} + \frac{h_{A2}}{H_2}\right) - \kappa s\left(h_{A1}\frac{\bar{H}_0}{H_1} + h_{A2}\frac{H_1}{H_2}\right) - \kappa_{kh} k_{Ah1}\right] \\ E_1[\Pi_A] &= \Omega\left[2k_{Ah1}K^{-1} - (2\kappa s + \kappa_{kh})k_{Ah1}\right] \end{aligned} \tag{16}$$

Defining auxiliary variables $W = 2$ and $V = 2\kappa s + \kappa_{kh}$, leaves just:

$$\max_{k_{Ah1}}\{W k_{Ah1} K_1^{-1} - V K_1\}$$

Differentiating this with respect to $k_{Ah1}$ and setting to zero gives:

$$W\left(K_1^{-1} - k_{Ah1}K_1^{-2}\right) - V = 0,$$

which assuming symmetrical outcomes with miner $B$ rearranges to:

$$k^{\star}_{Ah1} = k^{\star}_{Bh1} = \frac{W}{4V} = \frac{2}{4(2\kappa s + \kappa_{kh})} = \frac{1}{2(2\kappa s + \kappa_{kh})}$$

More generally, the same can be derived for longer time horizons assuming dynamic equilibrium prevails, and for more than two miners. Specifically for $T$ 2-week time periods, and $n$ other miners:

$$k^{\star}_{Ah1} = k^{\star}_{Bh1} = \ldots = k^{\star}_{nh1} = \frac{T}{n^2(T\kappa s + \kappa_{kh})} \tag{17}$$

This is characterised as a Nash equilibrium, in the sense of being the unique choice of hash capital purchased by $n$ miners, who each are selecting the best investment given the choices of each of the others. All other things equal, miners invest more, the lower the relative average cost of running a hash $\kappa$, the speed of the hashing equipment $s$, and the fractional unit cost of hash capital $\kappa_{kh}$.

This investment equilibrium is a Stackelberg outcome, in the sense that all the miners make an optimal investment choice, but then during the 2 week difficulty periods these become sunk costs, and only the underlying already-established hash costs determine outcomes. This becomes apparent when considering what happens when the speed $s$ and/or relative price $\kappa_{kh}$ of hashing equipment is low enough, so that

$$k^{\star}_{Ah1} = \frac{T}{n^2(T\kappa s + \kappa_{kh})} > \frac{1}{n^2\kappa}$$

The term on the right hand side $\frac{1}{n^2\kappa}$ is the nash equilibrium from section 2. It is not worth miners investing any more than this amount, because the optimal hash rates within the 2 week difficulty period are:

$$h^{\star}_{A1} = s \times k^{\star}_{Ah1} = s \times \frac{1}{n^2\kappa} \tag{18}$$

Intra-difficulty period competition, without coordination (see previous Best Response Functions section 2.2) steers hash rates towards this outcome, regardless of the sunk investment costs.

## 3.1 Stackelberg leadership as R&D investment

To concretely see how the strategic interactions outlined here are a multi-period multi-player Stackelberg game, consider a scenario where miner $A$ can spend the fiat equivalent of $Z$ bitcoins on research that aims to improve the energy efficiency of their hashing by $Z \times \phi\%$. This process could be stochastic, with $\phi\%$ being the mean of a random variable, in which case assuming risk-neutral miner preferences would still be consistent with the following analysis. The R&D process can be interpreted as costly research time that is expected to improve energy efficiency in various ways. Hashing

equipment could be reconfigured, or rigs could be replaced with newer technology. In the latter case, the following problem would be more complex, but the underlying principle will still be the same for any process that is costly for the leading miner, with expected improvement in efficiency.

In the 2 period model, in dynamic equilibrium, $A$'s profits are as follows, where $x = f(z) = 1 + Z\phi\%$ and $A$'s underlying costs $\kappa_A = \frac{\kappa}{x}$ compared to $B$'s that will remain at $\kappa_B = \kappa$.

$$E_1[\Pi_A] = 2\Omega\left[\frac{h_A}{H} - \frac{\kappa}{x}h_A\right] - Z$$
$$\frac{E_1[\Pi_A]}{2\Omega} = \Pi = \frac{h_A}{H} - \frac{\kappa}{x}h_A - z, \text{ where } z = \frac{Z}{2\Omega}$$

The Comparative cost advantage section 2.3 showed that when $A$'s underlying hash costs $\kappa_A$ differ from $B$'s, equilibrium hash rates are determined by $h^*_{A1} = \frac{\kappa_B}{(\kappa_A+\kappa_B)^2}$ and $h^*_{B1} = \frac{\kappa_A}{(\kappa_A+\kappa_B)^2}$. These can be substituted into the profit equation, and rearranged as follows:

$$\begin{aligned} h_A &= \frac{\kappa_B}{(\kappa_A+\kappa_B)^2} = \frac{\kappa}{\left(\frac{\kappa}{x}+\kappa\right)^2} = \frac{1}{\kappa}\left(\frac{x}{1+x}\right)^2 \\ \frac{h_A}{H} &= \frac{\kappa_B}{\kappa_A+\kappa_B} = \frac{\kappa}{\frac{\kappa}{x}+\kappa} = \frac{x}{1+x} \\ \Pi &= \frac{x}{1+x} - \frac{1}{x}\left(\frac{x}{1+x}\right)^2 - z \\ \Pi &= \left(\frac{x}{1+x}\right)^2 - z \end{aligned} \tag{19}$$

The earlier definitions together mean $x = 1 + 2\Omega\phi z$, so defining $\alpha = 2\Omega\phi$, $x = 1 + y$, where $y = \alpha z$

$$\Pi = \left(\frac{1+y}{2+y}\right)^2 - \frac{y}{\alpha} \tag{20}$$

then the choice of $y$ that maximises profit is:

$$\max_z\left\{(1+y)^2(2+y)^{-2} - \frac{1}{\alpha}y\right\} \tag{21}$$

This has solutions defined by:

$$2\alpha(1+y) - 8 - 12y - 6y^2 - y^3 = 0, \tag{22}$$

which only has a positive root if $\alpha > 4$.

To illustrate what this can mean in practice, here is an example. Up to this point, the investment time horizon has been limited to only an approximate month (two 2-week periods). The two period model can be expanded to an infinite horizon where each miner maximises the expected discounted sum of future profits enjoyed from the efficiency boost. Although such net present values are very sensitive to precise assumptions over the rate of time preference as a theoretical concept, such analysis provides a logical approach to understanding the decisions forward-looking miners face. A natural approach is to interpret the discount rate as the entrepreneur/investors' access to funds in the form of the interest rate they can borrow at (or compare different projects with). If some investors have better access, this will give them an advantage that expands their relative size and profits. Here the discount rate is assumed to be $\beta$ for all miners, and the net present value of profits for miner $A$ is defined by the following equation:

$$E_t\sum_{s=t}^{\infty}\beta^{s-t}E[\Pi_{As}] = \Omega\left[\begin{array}{c}\left(\frac{h_{At}}{H_t} + \beta\frac{h_{At+1}}{H_{t+1}} + \beta^2\frac{h_{At+2}}{H_{t+2}} + \cdots\right) \\ -\kappa\left(\frac{h_{At}\bar{H}_{t-1}}{H_t} + \beta\frac{h_{At+1}H_t}{H_{t+1}} + \beta^2\frac{h_{At+2}H_{t+1}}{H_{t+2}} + \cdots\right)\end{array}\right] - Z_t \tag{23}$$

Assuming dynamic equilibrium ($\frac{h_{At}}{H_t} = \frac{h_{At+1}}{H_{t+1}} = \ldots$ and $\bar{H}_{t-1} = H_t = \ldots$), the discounted summed stream (now labelled $\Pi$) becomes:

$$\Pi = (1 + \beta + \beta^2 + \cdots)\Omega\left(\frac{h_A}{H} - \kappa h_{At}\right) - Z_t$$
$$\Pi = \frac{1}{1-\beta}\Omega\left(\frac{h_A}{H} - \kappa h_{At}\right) - Z_t$$

This looks similar to the 2 period analysis earlier, except $\alpha = \frac{1}{1-\beta}\Omega\phi$ instead of $\alpha = 2\Omega\phi$. Given that the approximate length of one period is only 2 weeks, if, for example, the annual interest rate is $r = 1\%$, then $\beta \approx \frac{1}{1+\frac{0.01}{24}} = 0.99958$ and $\frac{1}{1-\beta} \approx 2401$. Earlier it was established that in equilibrium $(\frac{h_A}{H} - \kappa h_A) = \frac{1}{4}$, so with a 2-week reward of 12,600 bitcoins, the profit equation is:

$$\Pi = 2401 \times 12,600 \times \frac{1}{4} - Z_t,$$

which means the R&D spending $Z_t$ would be compared to much larger net present values, approximately 7.5 million bitcoins in this example. Here, there is no depreciation, and the time preference rate is relatively low, but it illustrates the important principle clearly that, with longer time horizons, it is of course much more likely that a forward-looking miner will find it worth investing in R&D.

Taking this example a little further, assume that a 10,000 bitcoin spend on R&D is expected to increase energy efficiency by 10%. In the example used in the short run section 2, this would mean the equivalent of mining rigs running at 0.1 J/Gh, improving down to 0.09 J/Gh, and all else equal, that would also lower average hashing costs $\kappa$ by 10%. So what would be the optimal R&D investment spending for the leader miner? If 10,000 bitcoins improve efficiency by 10%, then each bitcoin spent improves efficiency by $\phi = 0.001\%$. This means $\alpha = \frac{1}{1-\beta}\Omega\phi = 2401 \times 12,600 \times 0.001 = 30,252.6$, so $y^* = 243.477$, and therefore $Z'_t = \frac{y^*}{\phi} = \frac{243.477}{0.001} = 243,477$ bitcoins. This amount of spending would be expected to lower miner $A$'s underlying costs from $\kappa$ to:

$$\kappa^*_A = \frac{\kappa}{1+x} = \frac{\kappa}{1 + 243,477^* \times 0.001\%} = \frac{\kappa}{3.43477}$$

In equilibrium without R&D spending, $\kappa_A = \kappa_B = \kappa$ so hash rates are the same $h^*_A = h^*_B = 0.25\frac{1}{\kappa}$. After the optimal spending, the lower costs that miner $A$ is expected to enjoy will shift equilibrium to:

$$h^*_A = \frac{1}{(2+x^*)^2}(1+x^*)^2\frac{1}{\kappa} = 0.60\frac{1}{\kappa}$$
$$h^*_B = \frac{1}{(2+x^*)^2}(1+x^*)\frac{1}{\kappa} = 0.17\frac{1}{\kappa}$$

This means the aggregate hash rate $H = h_A + h_B$ is expected to change from $H = 0.5\frac{1}{\kappa}$ to $H^* = (0.60 + 0.17)\frac{1}{\kappa} = 0.77\frac{1}{\kappa}$, so approximately a 53% increase in aggregate hash rates. On the other hand, each hash conducted by the leading miner will be more efficient - in this example, the baseline efficiency measured

as hashes per Joule is $e = 10^{10}$ (expressed conventionally, the inverse of this, per billion hashes, is $0.1J/Gh$). The optimal R&D spending above means an improvement in efficiency by the same factor $\frac{1}{1+x^*}$, so efficiency increases to $e^* = (1 + x^*) \times e = 3.43477 \times 10^{10}\ h/J$ (so Joules per gigahash fall down to $0.029J/Gh$). The leader in the new equilibrium conducts $\frac{1+x^*}{2+x^*} = 77.5\%$ of the hashes, the follower $\frac{1}{2+x^*} = 22.5\%$, so the aggregate energy efficiency changes by a weighted factor from $e$ to: $(\frac{2}{2+x^*} + x^*)e$.

Putting all this together, aggregate energy use $J$ will change from $J = \frac{H}{e}$ to $J^* = \frac{h_A^*}{e^*} + \frac{h_B^*}{e}$, as follows:

$$J = \frac{1}{2\kappa e}$$
$$J^* = \frac{2}{\kappa e}\left(\frac{(1+x^*)}{(2+x^*)^2}\right),$$

which means aggregate energy use changes by a factor of:

$$\frac{J^*}{J} = 4\frac{(1+x^*)}{(2+x^*)^2} \tag{24}$$

In the numerical example here, with $x^* = 3.43477$ this is 0.7. In other words, the action of the leading miner is expected to reduce overall energy use by 30%. Moreover, as long as $\phi$ is positive, and hence so is $x^* = \phi Z^* > 0$, then aggregate energy use in the new equilibrium is guaranteed to fall, because $\frac{J^*}{J} = 4\frac{(1+x^*)}{(2+x^*)^2} < 1$ for all $x^* > 0$. In other words, the expected improvement in efficiency $\phi\%$ from R&D is not necessarily guaranteed to be high enough to induce the leader into investing, but if it is, then aggregate energy use is guaranteed to fall.

## 4 Long run competition

In the long run, the only revenue source for miners comes from gathering transactions fees. Previous analysis up to this point only included a fixed subsidy $\Omega$ without consideration of assumptions relating to the demand for transactions over time. To emphasise just how absolute this design feature of Bitcoin is, note that most of the subsidy, and hence its long run total supply (more than 90%) has already been extracted. In 2140 the subsidy will become so relatively tiny, that this year was chosen as a cut-off point: the Bitcoin subsidy will vanish entirely! It is worth just reflecting for a moment on how important this is. It means that in the long run, only two variables prop up the incentive for miners to provide effort, namely the quantity of transactions processed per block, and their price. Their value will always be obtained in the same way, by winning block competitions. They will still compete with each other, and their collective efforts will still be channeled into one single blockchain, giving it value to end users. Economists refer to price and quantity collectively as 'demand', and tend to think of it as being determined by some kind of utility function associated with the end user, in this case of Bitcoin transactions. As the price of individual transactions rises, consumers will tend to substitute towards alternatives (existing and emerging fiat and data management systems that provide similar services). In other words, Bitcoin competes in a marketplace alongside other systems. Up to now, this demand has tended to stem either from strong ideological principles, or relative price speculation (Schilling and Uhlig, 2019). Although the former motive is culturally strong amongst a subset of the global population, restricting the number of transactions per block logically leads only to one of a combination of the following: long run real resources that flow to miners (whose effort in turn secures the system) will be limited; or demand will have to remain inelastic while transactions fees rise. Similarly, there are limits to how long speculative mania can persist in the long run. Previous work (e.g., Easley et al., 2019; Huberman et al., 2021) has taken a queuing approach to this problem by assuming that users lose utility while waiting for their transaction to appear confirmed on the public Bitcoin blockchain. While there is some merit in this reasoning, section 8 of the Bitcoin whitepaper (Nakamoto, 2008) includes methodology referred to as 'simplified payment verification' (SPV), making the payment process more analogous to handing a banknote to a merchant. It is true that for both parties, the more time that passes, the more likely it is that the transaction is final. For example, in the analogy of physical cash, the merchant (who is presumably more concerned about a failed payment) might hand all their banknotes over to a bank later, that scrutinises them more carefully, and finds one forgery. In practical terms, SPV is like physical cash in the sense that once a transaction has occurred, both parties can consider it final, subject to a failure probability. Given that the transaction is broadcast to all miners, depending on wallet software, intermediate service providers and miner policies, both the payer and the payee know that it should be included in a block eventually. The only question is whether or not the person sending the money tried to forge it and/or commit a double spend. SPV offers the merchant some assurance even in the extreme case where both parties are completely offline, let alone in cases where the transaction has been broadcast. Overall then, when Bitcoin is governed without the imposition of block size caps, payments can be thought of as instantaneous, and transaction fees can be determined freely based on the real underlying economic costs of processing transactions. These principles may not apply to how BTC Bitcoin works in practice today, but they are clearly articulated in section 8 of the Bitcoin whitepaper, and some implementations like Bitcoin SV apply them currently.

To get a better sense of how these assumptions shape the long run, this section adds transaction processing demand and capital. First, define $p$ as the average price of one transaction (the average transaction fee), and $q$ as the number of transactions per 2 week difficulty period, so that $R = pq$ is the total transaction revenue available during a difficulty period. Demand is defined by the following equation, where $\varepsilon$ is the elasticity of demand for a transaction (how responsive user demand is to changes in transaction fee charges):

$$p = q^{-\frac{1}{\varepsilon}} \tag{25}$$

To the extent that individual miners are price takers in a competitive fee market, this means that miner revenue can be expressed purely as a function of the number of transactions they decide to process:

$$R = q^{-\frac{1}{\varepsilon}}q = q^{1-\frac{1}{\varepsilon}} \tag{26}$$

As before, the two miners $A$ and $B$ compete within difficulty periods, but with $R$ added to the fixed subsidy. Whereas $\Omega$ is independent of time durations $\tau$, in each difficulty period $R$ expands and contracts proportionately the same way hash costs $\gamma h$ do. The

average cost of a hash is now labelled $\gamma_h$, distinguished from $\gamma_{TX}$, the average cost of processing one transaction - how these two different activities differ is explained later. As before, this analysis abstracts from risk by assuming risk neutral preferences and hence avoiding the complication of having to make specific assumptions about arrival rate distributions of transactions over time. In other words, the overall arrival rate of transactions is assumed to be constant, and captured by $q$. Adding all this to $A$'s profit equation gives:

$$\begin{aligned}&(\Omega + R\tau_1)\frac{h_{A1}}{H_1} - (\gamma_h h_{A1} + \gamma_{tx} q_1)\tau_1 \\ &+(\Omega + R\tau_2)\frac{h_{A2}}{H_2} - (\gamma_h h_{A2} + \gamma_{tx} q_2)\tau_2\end{aligned} \tag{27}$$

Although these extra terms require solving more complex cubic equations, profit maximisation by $A$ and $B$ leads to the same type of symmetric Nash equilibrium as before, as long as dynamic equilibrium is obtained. The number of transactions $q$ that flow to miners will of course affect profits, but this variable here is exogenous, unaffected by the number of hashes conducted. For now this means that $\gamma_{tx}$ does not appear in miners' profit maximising considerations, but it will affect investment decisions later. Overall, these assumptions result in exactly the same equilibrium hash rates as in previous analysis, except for the addition of $R$:

$$\begin{aligned}E_1[\Pi_A] &= 2(\Omega + R)hH^{-1} - 2\gamma_h h \\ h^\star_{A1} &= h^\star_{B1} = h^\star_{A2} = h^\star_{B2} = h^\star = \frac{1}{4\dfrac{\gamma_h}{\Omega + R}} = \frac{\Omega + R}{4\gamma_h}\end{aligned} \tag{28}$$

For now, the only two consequences of including transactions fees are more complex intra-difficulty period equilibrium dynamics, and a higher inter-difficulty period equilibrium hash rate with the inclusion of $R$. Crucially though, miners now require transaction processing capabilities in addition to just plain old hashing. In the previous section, they had to consider how much hash capital, now labelled $k_{Ah}$ to purchase. As before, each micro unit of $k_{Ah}$ releases the miner's constraints by $s_h$ hashes every 2 weeks. Although there are complementarities in the production of hashes on the one hand, and transaction verifying and batching together on the other, they are two very distinct functions. Bitcoin's transaction processing design is based on a UTXO model that is superiour to account based systems, because it allows parallelisation. Double spending attacks are automatically 'checked' by miners as a simple by-product of their need to keep an up-to-date record of the current intra 10 min set of unspent transaction outputs. This may sound complicated, but it can best be thought of as miners having to manage a set of labelled boxes with coins moving from box to box, rather than having to check the global state of every single account, every time a single transaction is checked and verified. Despite this natural advantage, specific hardware and software is still required. The more transactions that have to be gathered, verified, and processed into blocks, the more hardware will be needed, and the higher will be variable costs just as before with conducting hashes. Define transaction processing capital purchased by miner $A$ as $k_{Atx}$, each unit of which is capable of processing $s_{tx}$ transactions during 2 weeks. The price of transaction capital as $p_{tx}$, and its speed (how many transactions a unit of capital can process in 2 weeks) as $s_{tx}$, these can be added to the miner profit maximisation problem from the previous section as follows:

$$\begin{aligned}E_1[\Pi_A] = &\left(\Omega + (s_{tx}k_{Atx1})^{1-\frac{1}{\varepsilon}}\right)\left(\frac{h_{A1}}{H_1} + \frac{h_{A2}}{H_2}\right) \\ &-\gamma_h s_h\left(h_{A1}\frac{\bar{H}_0}{H_1} + h_{A2}\frac{H_1}{H_2}\right) - \gamma_{tx}s_{tx}\left(\frac{\bar{H}_0}{H_1} + \frac{H_1}{H_2}\right) \\ &-p_{kh}k_{Ah1} - p_{ktx}k_{Atx1}\end{aligned} \tag{29}$$

Note that this involves optimally choosing both $k_{Ah}$ and $k_{Atx}$ simultaneously, with the aim of balancing hashing and transaction processing capabilities. In dynamic equilibrium, this becomes (as before, aggregate hash capital is $K = k_{Ah} + k_{Bh}$):

$$\begin{aligned}E_1[\Pi_A] = &\left(\Omega + (s_{tx}k_{Atx})^{1-\frac{1}{\varepsilon}}\right)[2k_{Ah}K^{-1}] \\ &-(2\gamma_h s_h + p_{kh})k_{Ah} - (2\gamma_{tx}s_{tx} + p_{ktx})k_{Atx}\end{aligned} \tag{30}$$

Profit maximisation requires fulfilling two first order conditions (dropping $A$ notation that denotes miner $A$):

$$\begin{aligned}\frac{\delta\Pi}{\delta k_{Ah}} &= 2\left(\Omega + (s_{tx}k_{tx})^{1-\frac{1}{\varepsilon}}\right)(k_h) - (2\gamma_h s_h + p_{kh})4k_h^2 = 0 \\ \frac{\delta\Pi}{\delta k_{Atx}} &= \left(1 - \frac{1}{\varepsilon}\right)s_{tx}^{1-\frac{1}{\varepsilon}}k_{tx}^{-\frac{1}{\varepsilon}} - (2\gamma_{tx}s_{tx} + p_{ktx}) = 0,\end{aligned}$$

Which rearranges to:

$$\begin{aligned}2\left(\Omega + (s_{tx}k_{tx})^{1-\frac{1}{\varepsilon}}\right)(k_h) - (2\gamma_h s_h + p_{kh})4k_h^2 &= 0 \\ \left(1 - \frac{1}{\varepsilon}\right)s_{tx}^{1-\frac{1}{\varepsilon}}k_{tx}^{-\frac{1}{\varepsilon}} - (2\gamma_{tx}s_{tx} + p_{ktx}) &= 0,\end{aligned}$$

Rearranged for the optimal choice of hash and transaction capital as:

$$k_h^\star = \frac{\Omega + (s_{tx}k_{tx})^{1-\frac{1}{\varepsilon}}}{2(2\gamma_h s_h + p_{kh})} \tag{31}$$

$$k_{tx}^\star = \left(\frac{\varepsilon - 1}{\varepsilon}\right)^\varepsilon (2\gamma_{tx}s_{tx} + p_{ktx})^{-\varepsilon}s_{tx}^{\varepsilon-1} \tag{32}$$

The first of these equations shows that as the Bitcoin subsidy $\Omega$ tapers to zero in the future, forward-looking miners invest relatively less and less in energy intensive hash capital (and hence conduct relatively fewer hashes per time period) compared to transaction capital and processing. Just as in the previous section, the hash capital choice, with its corresponding hash rate, represents a 'maximum' in the sense that the $h^\star = \frac{\Omega+R}{4\gamma_h}$ rate derived earlier will be the equilibrium choice if the choice above turns out to be higher (which will be true for a low enough price of hash captial $p_{kh}$, for example).

The volume of transactions is defined by the following equation:

$$Q^\star = 2 \times k_{tx}^\star \times s_{tx} = 2\left(\frac{\varepsilon - 1}{\varepsilon}\right)^\varepsilon (2\gamma_{tx}s_{tx} + p_{ktx})^{-\varepsilon}s_{tx}^\varepsilon \tag{33}$$

This shows clearly that transaction volume rises (and hence transaction prices fall), as the underlying cost of transaction processing $\gamma_{tx}$ falls, as the price of transaction capital $p_{ktx}$ falls, and as the speed of transaction processing $s_{tx}$ rises.

The previous section documented that aggregate energy use was guaranteed to fall, if a Stackelberg leader optimally invests in discovering and using energy efficiency improvement technology, even without followers adopting it. This positive result is partly thanks to the fact that as leaders' hash rates expand, followers with less efficient technology contract. Over time, followers are incentivised to catch up with leaders, reinforcing the adoption of the more efficient technology. Now adding to this, what happens to

aggregate energy in any new equilibria where transaction capital efficiency improves? To keep analysis simple, assume the follower has already caught up with the leader, so $h_A^\star = h_B^\star = h^\star$ and $H^\star = 2h^\star$, and also assume the case of the simpler low hash capital price equilibrium, $h^\star = \frac{\Omega+R}{4\gamma_h}$. So distinguishing hash capital efficiency $e_h$ from transaction processing capital efficiency $e_{tx}$ and defining $Q^\star = 2q^\star$, then the total energy use is the sum $J^\star = J_h^\star + J_q^\star$ where:

$$J_h^\star = \frac{H^\star}{e_h} = \frac{\Omega + R^\star}{2c_h} \tag{34}$$

$$J_q^\star = \frac{Q^\star}{e_{tx}} = \frac{1}{2e_{tx}}\left(\frac{s_{tx}}{2\gamma_{tx}s_{tx} + p_{ktx}}\right)^2, \tag{35}$$

and where $R^\star = q^{\star\frac{\varepsilon-1}{\varepsilon}}$. Notice as well that $\gamma_h$ is replaced by $\frac{c}{e_h}$, which cancels out $e_h$ from $J_h^\star$, so that $\frac{\delta J^\star}{\delta e_h} = 0$. In other words, improvements in hash capital efficiency never increase or decrease aggregate energy use. It is always the case that as miners adopt better hashing technology, the higher hash rates are exactly offset by the lower energy use per hash.

There are many other questions that can be answered from here, which will be better answered with calibration of the various parameters from empirical work. But this section finishes with arguably one of the most important. Users of Bitcoin get utility from the transaction and public ledger services they provide, instead of existing alternatives. So how much energy is used up per transaction? In other words, how useful is Bitcoin, compared to its energy consumption, and what happens over time as technology improves? On aggregate, energy used per transaction is given by $\frac{J^\star}{Q^\star}$. All the various definitions can be combined and rearranged to the following:

$$\begin{aligned}\frac{J^\star}{Q^\star} = \frac{1}{2}\left(\frac{\varepsilon}{\varepsilon-1}\right)^\varepsilon \frac{s_h s_{tx}^{-\varepsilon}\left(2c_{tx}e_{tx}^{-1}s_{tx} + p_{ktx}\right)^\varepsilon}{e_h\left(2\gamma_h s_h + p_{kh}\right)} \\ \times\left(\Omega + \left(\frac{\varepsilon-1}{\varepsilon}\right)^{\varepsilon-1} s_{tx}^{\frac{(\varepsilon-1)^3}{\varepsilon^2}}\left(2c_{tx}e_{tx}^{-1}s_{tx} + p_{ktx}\right)^{1-\varepsilon}\right) + e_{tx}^{-1}\end{aligned} \tag{36}$$

Although this is complex, with many terms, it can easily be shown that for $\varepsilon > 1$, meaning demand for transactions is elastic, and all other normal parameters positive, the differential of this term with respect to transaction processing efficiency $e_{tx}$ is always negative $\frac{\delta \frac{J^\star}{Q^\star}}{\delta e_{tx}} < 0$. In other words, for a reasonable level of responsiveness of demand to changes in the price of transactions (which is more likely, the more alternative systems Bitcoin competes with), improvements in transaction processing efficiency always lead to reductions in energy use per transaction over time.

## 5 Conclusion

In conclusion, this paper has explored the nature of long run competition in Bitcoin by taking a standard dynamic short run model, extending this to a Stackelberg game in the medium run, and then introducing transaction demand and supply in a free market with no artificial volume quotas. Although users of Bitcoin today may be driven more by ideological principles and price speculation, there is no *a priori* reason why utility derived from secure transaction and data services should be ignored. In a competitive, unrestricted environment, Bitcoin could compete with existing services (and has some natural advantages to other systems, by design). The analysis presented here could be developed more in the direction of a fully-fledged mainstream DSGE model (Christiano et al., 2018), with stochastic shocks, clearing conditions, simulation of linearised equations, and so on. This work can also be taken in different directions, including empirical testing of the rational benchmark assumptions laid out here, policy analysis, and long term thought experiments on how Bitcoin could evolve in the future. For the assumptions laid out here, it has demonstrated that in the medium run, when leaders consider investing in R&D that improves the efficiency of hashing (and/or new equipment that is more energy efficient), aggregate energy use unambiguously falls. In the long run, forward-looking miners are incentivised to optimally pivot towards investing relatively more in transaction processing capital, and relatively less in hash capital. As they do so, aggregate transaction volumes rise, average Bitcoin transaction fees fall, and, as long as the demand for transaction and ledger services is elastic enough, aggregate energy use per transaction falls. Although Bitcoin is complex by design, this remarkable result mostly derives from a very simple idea: dynamic competition. Figure 3 shows the competitive arena where contests determine one single winner every 10 min. It is permission-less in the sense that any enterprise is free to enter and leave any time, but only the strong survive. If a miner's average hash, transaction processing, networking and other relevant costs are too high compared to their competitors, they make a loss, leading to either bankruptcy, or substitution of capital redirected elsewhere.

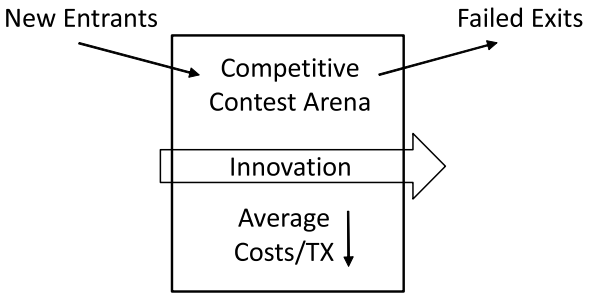


FIGURE 3
Long run competitive forces.

The short contests determine a single winner every 10 min, not by miner benevolence (though that can be a motive as well), but by one miner demonstrating proof of work from conducting hashes that are costly in real economic terms. Forward-looking miners gain more profit by seeking and finding innovations and investing in the latest, most efficient technology. In the long run, although the proof of work process will always form the basis of establishing winners of these contests, miners will only earn reward by harvesting transaction fees into blocks, so their ability to run hashes has to be balanced with their ability to efficiently conduct these other activities. This paper has made a step forward towards understanding how this balance plays out in a long run equilibrium. Interestingly, just as in prior work, there is a hint here at the possibility of more efficiency from multiplier effects: the

most efficient miners tend to provide the largest proportion of hash effort, and the higher are the potential rewards from gathering transaction fees, the more effort there will be. If this effort makes the blockchain more secure, this in turn should increase demand, further increasing potential rewards and so on. This effect (endogenising the connection between overall hash rates, Blockchain security, and transaction service utility) would strengthen the positive conclusions laid out here, as would positive network effects that increase utility for end-users.

Another implication of this work relates to the possibility of selfish mining strategies laid out originally in Eyal and Sirer (2018) (see also Negy et al., 2020, and Hinzen et al., 2022 for an example of concerns over stable consensus achievement). If, however, miners find it profitable to signal their behaviour to each other by their actions as described in this paper, deviations from these equilibria could become unprofitable. Similarly, miners can be ignored by the consensus if they deviate from any agreed interpretation of the rules laid out in the Bitcoin whitepaper, so these concerns may be over-stated.

The focus here was on competitive and strategic (game theoretic) interactions between a limited number of miner participants. Easley et al. (2019) and many others assume free entry results in a zero profit condition. Although this is common, some of the economic literature argues that this is not necessary (Ferreira and Dufourt, 2007). Entry/exit and industry structure however, could be further developed by, for example, including a fixed cost term $F$ in the profit function. In the medium run analysis, a zero profit condition like the following that derives directly from the medium run section could be solved to pin down the number of miners $n$. More complex modelling could relax the linear cost function assumptions, and more theoretical work could attempt to generalise these results. In the example below, from the 2 period model with hash capital, the ratio $\frac{F}{2\Omega}$ will define how many miners can enter before profits drop below zero:

$$\left(\frac{2\Omega}{n} - V\right)k_A^\star - F = 0$$

It is conjectured here that this addition will not change key conclusions. Similarly, forces that move the industry towards an asymmetric structure could be modelled. Miners that gain competitive advantages over others end up with higher profits and hash rates, but whether these are reinvested, and what forces push and pull miners up and down the relative size distribution need to be explored. It is highly likely that, just as with many other similar economic phenomena (Gabaix, 2016), Bitcoin miners' size and capabilities naturally end up arranged as a power law structure. Indeed, this is casually what is observed today - empirical work determining their exact structure offering another avenue for further research. Power law structures are even more likely in Bitcoin, partly because actual outcomes at the block competition level are stochastic (specifically following a sum of exponential distributions also known as 'Erlang'), and partly because just as with City size, network effects manifest themselves in various ways. At the level of transactions it is obvious that miners with better capabilities in gathering them gain advantages. But miners also gain from investing in better connections to others in order to gain time advantages by receiving blocks faster (starting the race earlier) and distributing to others faster (ending the race earlier). It is more advantageous to be better connected to the better miners. So modelling how they consolidate into structures like Mandala networks offers an interesting area for further research.

Another area for further work could endogenise risk sharing within mining pools (Cong et al., 2020; Lewenberg et al., 2015), although this is unlikely to change the inter-enterprise interactions laid out here. Two mining pools that compete with each other do so in some ways, similarly to two mining enterprises that are not distributing hash work across multiple parties and sharing the proceeds to smooth revenue streams.

The benefits of providing cheaper transaction services have often been overlooked in the literature, which has instead taken anonymity and small-size, high-frequency miner distributions as goals in their own right (Leshno and Strack (2020) even refer to these outcomes as 'axioms'). However, explicitly modelling how Bitcoin's underlying UTXO model is more efficient than account-based updating systems provides another avenue for further work (including intra-difficulty period "saw tooth" hashing behavior). Similarly, Bitcoin Script, the underlying language transactions are written in, allows highly complex conditionality, and hence token and smart contract systems to be built. What should happen if, for example, miners are able to charge different fees for different sized transactions? Including heterogeneity of transaction types offers an interesting area for extending the demand model laid out here.

Long term governance issues should also be explored further. Today, Bitcoin and many similar distributed public ledger technologies enjoy a certain degree of immunity from regulation by virtue of being 'decentralised', even though critical design changes are frequently made by highly centralised decision-making groups (Walch, 2019). One of the great benefits of Bitcoin is that everything takes place in full, auditable public view, albeit behind private/public signature aliases. This is why attempts to place and distribute AI processes on top of Bitcoin have already begun (Sgantzos and Grigg, 2019), facilitating much needed AI process transparency. By naturally integrating with IPv6, Bitcoin also brings competitive advantage in the form of 'diverse peer-to-peer payment mechanisms and advanced identity-management using cryptographically generated addresses' (Davies and Pagani, 2022). This paper has added to others by highlighting the importance of miner market structure. It assumed transaction fees are set in a free market with no block size cap, but in this case, how can anti-competitive practices be prevented by regulators? To what extent are the benefits that stem from removing a single point of failure maintained even when equilibrium results in just a few very large miners? These, and many other questions are left for exploration in future work.

## Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

## Author contributions

The author confirms being the sole contributor of this work and has approved it for publication.

## Acknowledgments

I am very grateful to Dr. Craig Wright for his patience throughout our conversations related to this topic, and the many insights he has contributed towards this research. This work has also benefited from discussions and feedback from Jerry Chan, Brendan Lee, Xiaohui Liu and Neil Smith. I would also like to thank the Editors and Reviewers who have provided extremely helpful guidance to further develop the paper. Any errors are my own.

## Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Publisher's note



## References

Alsabah, H., and Capponi, A. (2020). Pitfalls of bitcoin's proof-of-work: R\&D arms race and mining centralization. Available at: https://ssrn.com/abstract=3273982.

Christiano, L. J., Eichenbaum, M. S., and Trabandt, M. (2018). On dsge models. *J. Econ. Perspect.* 32 (3), 113–140. doi:10.1257/jep.32.3.113

Cong, L. W., He, Z., and Li, J. (2020). Decentralized mining in centralized pools. *Rev. Financial Stud.* 34 (3), 1191–1235. doi:10.1093/rfs/hhaa040

Davies, J., and Pagani, A. (2022). "Ipv4 and ipv6 for blockchain networks: a comparative analysis," in 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain and Beyond (iGETblockchain), Irvine, 7-11 November 2022, 1–5.

Dimitri, N. (2017). Bitcoin mining as a contest. *Ledger* 2, 31–37. doi:10.5195/ledger.2017.96

Easley, D., O'Hara, M., and Basu, S. (2019). From mining to markets: the evolution of bitcoin transaction fees. *J. Financial Econ.* 134 (1), 91–109. doi:10.1016/j.jfineco.2019.03.004

Eyal, I., and Sirer, E. G. (2018). Majority is not enough: bitcoin mining is vulnerable. *Commun. ACM* 61 (7), 95–102. doi:10.1145/3212998

Ferreira, R. D. S., and Dufourt, F. (2007). Free entry equilibria with positive profits: A unified approach to quantity and price competition games. *Int. J. Econ. Theory* 3 (2), 75–94. doi:10.1111/j.1742-7363.2007.00048.x

Fiat, A., Karlin, A., Koutsoupias, E., and Papadimitriou, C. (2019). "Energy equilibria in proof-of-work mining," in *Proceedings of the 2019 ACM conference on economics and computation* (ACM), 489–502.

Fonseca, M. A. (2009). An experimental investigation of asymmetric contests. *Int. J. Industrial Organ.* 27 (5), 582–591. doi:10.1016/j.ijindorg.2009.01.004

Gabaix, X. (2016). Power laws in economics: an introduction. *J. Econ. Perspect.* 30 (1), 185–206. doi:10.1257/jep.30.1.185

Garratt, R., and van Oordt M. R. C. (2020). Why fixed costs matter for proof-of-work based cryptocurrencies. Available at: https://ssrn.com/abstract=3572400.

Hinzen, F. J., John, K., and Saleh, F. (2022). Bitcoin's limited adoption problem. *J. Financial Econ.* 144 (2), 347–369. doi:10.1016/j.jfineco.2022.01.003

Houy, N. (2014). The economics of Bitcoin transaction fees, GATE WP. Avaliable At: https://ssrn.com/abstract=2400519.

Huberman, G., Leshno, J. D., and Moallemi, C. (2021). Monopoly without a monopolist: an economic analysis of the bitcoin payment system. *Rev. Econ. Stud.* 88 (6), 3011–3040. doi:10.1093/restud/rdab014

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

Leshno, J. D., and Strack, P. (2020). Bitcoin: an axiomatic approach and an impossibility theorem. *Am. Econ. Rev. Insights* 2 (3), 269–286. doi:10.1257/aeri.20190494

Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., and Rosenschein, J. S. (2015). "Bitcoin mining pools: A cooperative game theoretic analysis," in Proceedings of the 2015 international conference on autonomous agents and multiagent systems, Istanbul, Turkey, May 4-8, 2015, 919–927.

Ma, J., Gans, J. S., and Tourky, R. (2018). *Market structure in bitcoin mining*. National Bureau of Economic Research.

Nakamoto, S. (2008). *Bitcoin whitepaper*.

Negy, K. A., Rizun, P. R., and Emin, G. (2020). "Selfish mining re-examined," in *International conference on financial cryptography and data security* (Springer), 61–78.

Schilling, L., and Uhlig, H. (2019). Some simple bitcoin economics. *J. Monetary Econ.* 106, 16–26. doi:10.1016/j.jmoneco.2019.07.002

Sgantzos, K., and Grigg, I. (2019). Artificial intelligence implementations on the blockchain. use cases and future applications. *Future Internet* 11 (8), 170. doi:10.3390/fi11080170

Tullock, G., Buchanan, J. M., and Tollison, R. D. (1980). Toward a theory of the rent-seeking society. *Effic. Rent. Seek.* 97, 112.

Walch, A. (2019). *'Deconstructing'decentralization': Exploring the core claim of crypto systems'*. Oxford, United Kingdom: Oxford University Press.