Why Fixed Costs Matter for Proof-of-Work Based Cryptocurrencies*

Rodney J. Garratt†
University of California Santa Barbara

Maarten R.C. van Oordt‡
Bank of Canada

First draft: October 2019
This draft: September 2020

Abstract

We assess how the cost structure of cryptocurrency mining affects the response of miners to exchange rate fluctuations and the immutability of cryptocurrency ledgers that rely on proof-of-work. We show that the amount of mining power supplied to currencies that rely on specialized hardware, such as Bitcoin, responds less to adverse exchange rate shocks than other currencies respond to such shocks, a fact that is instrumental to avoiding double-spending attacks. The results may change if mining equipment used for one cryptocurrency can be transferred to another. For smaller currencies with low exchange rate correlation, transferability eliminates the protection that fixed costs provide. Our results weaken doomsday predictions for Bitcoin and other cryptocurrencies with declining block rewards.

Keywords: Cryptocurrency, blockchain, exchange rates, mining revenue.

JEL codes: G10, G29.

---

*We thank Narayan Bulusu, Jonathan Chiu, Pierre-Olivier Goffard, Tyler Moore, Julien Prat, Alex Shkolnik, Harald Uhlig, Peter Zimmerman and participants in the 2019 San Francisco Blockchain Week; the IBEFA Summer Meeting at the 95th Annual Conference of the WEAI; the Ecole Polytechnique CREST Virtual Finance Theory Seminar Series; the UCSB Center for Financial, Mathematical & Actuarial Research Seminar Series; the Crypto Economics Security Conference 2020; the HKBU-NTU-NUC Joint Digital Economy Seminar Series; the Crypto and Blockchain Economics Research Forum; and seminar participants at the Bank of Canada for helpful comments and suggestions. We thank Ramin Shahabadi and Julia Zhu for research assistance. This research was partly conducted while Rodney Garratt was visiting the Bank of Canada. The views expressed in this paper do not necessarily reflect those of the Bank of Canada.

†Corresponding author. Email: garratt@ucsb.edu

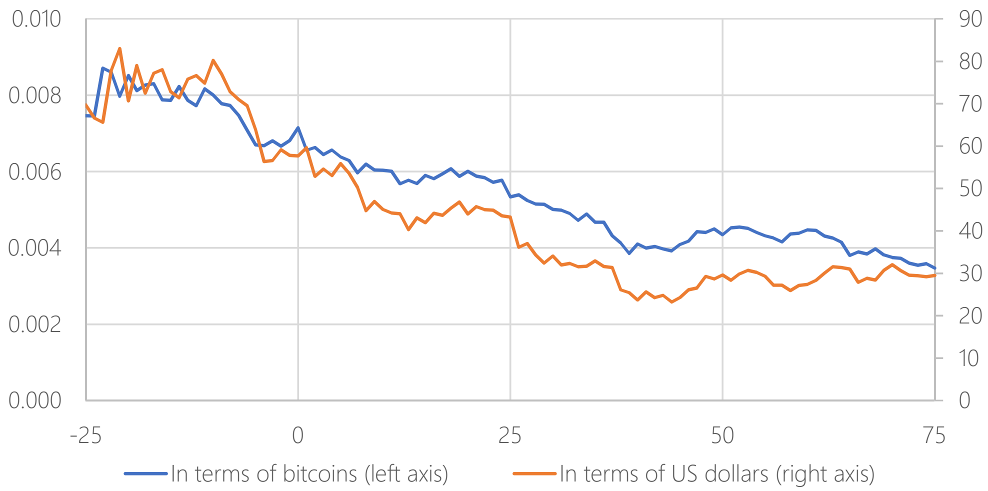
‡Email: mvanoordt@bankofcanada.ca

1 Introduction

The 51% attacks on Bitcoin Gold in May 2018 raise the question of how equipment used for mining operations affects the economics of double-spending attacks on cryptocurrencies. Bitcoin Gold was born as a hard fork of the Bitcoin blockchain in October 2017. Bitcoin Gold differed from Bitcoin in that it relied on a proof-of-work protocol that disabled the use of specialized equipment for mining operations. The goal was to ensure that anyone could participate in mining operations by using widely-available consumer hardware rather than being required to purchase specialized equipment (Bitcoin Gold, 2017). It was envisioned that this move would lead to a higher level of resilience due to a more decentralized mining infrastructure. Unfortunately, this did not happen. Instead, someone successfully double spent Bitcoin Gold using several 51% attacks on the network during 16-19 May, 2018. The attacker was able to rewrite the transaction history and erase earlier transactions where the attacker sent approximately $18 million worth of Bitcoin Gold to various cryptocurrency exchanges (Bloomberg, 2018). Not surprisingly, the announcement of the attack was followed by a considerable decline in the exchange rate of Bitcoin Gold (shown in Figure 1). Currently, the exchange rate in terms of bitcoin is only a sixth of what it was at the time of the attack and the number of transactions has declined to less than a third. Since then, several proof-of-work cryptocurrencies have been subject to successful 51% attacks.

Why was Bitcoin Gold subject to such an attack, while Bitcoin itself has not been? This paper shows that the answer may lie in some very simple economics related to entry and exit in the presence of fixed costs. Surprisingly, the implications we describe here have been missed or ignored (with one partial exception) by the existing economic literature that focuses on flow costs of mining. Papers that formally model Bitcoin mining and double-spending attacks in environments where there is a per-period flow cost of mining, but where there is no fixed cost involved with setting up mining operations, include Kroll et al. (2013), Abadi and Brunnermeier (2018), Pagnotta and Buraschi (2018), Budish (2018), Biais et al. (2019a), Chiu and Koeppl (2019a,b), Cong et al. (forthcoming), Huberman et al. (2019), Gandal and

Figure 1: Exchange Rate of Bitcoin Gold After the 51% Attack in 2018



Note: The solid line shows the exchange rate of Bitcoin Gold during the 25 days before and 75 days after the double-spending attack in May 2018. The start of the double-spending attacks on 15 May, 2018 is indicated by $t = 0$ on the horizontal axis. Source: Binance (cryptocurrency exchange).

Gans (2019) and Auer (2019).[1] The per-period cost of mining is generally interpreted as either the cost of electricity to run mining units or the cost of renting computing power. Easley et al. (2019) consider an environment where miners face a flow cost in the form of depreciation of mining equipment, but they do not further deal with the fixed cost aspect of setting up mining operations. Finally, Prat and Walter (2019) carefully examine the impact of fixed costs on the relationship between the exchange rate of cryptocurrencies and the entry decision of miners, but their main interest is the level of available mining power, rather than the immutability of cryptocurrency ledgers. Their results suggest that, in terms of present value at the time of entry, the fixed costs account for about two-thirds of the total costs of Bitcoin mining (Prat and Walter, 2019, Table 2). The sizable magnitude of these estimates supports the importance of investigating the potential impact of those fixed costs on the security of cryptocurrency transactions.

[1] Budish (2018) gives a verbal discussion on how investment in non-repurposable hardware may prevent double-spending attacks. This is the exception mentioned above. The quantitative results from our formal analysis indeed confirm his intuition that the investment in specialized hardware may be instrumental to avoiding double-spending attacks.

In our model, miners face both a per-period flow cost to mining and a fixed cost to setting up their mining operations. The situation where there is only a per-period flow cost of mining shows up as a special case in our environment. We can therefore conveniently describe how things change with the introduction of fixed costs. We identify four implications of fixed costs.

1. **Downward rigidity in mining**. In the absence of fixed costs, the reduction in mining power that results from a decline in the exchange rate will be proportional to the decline in the exchange rate. This is an immediate implication of free entry and exit without fixed costs. In contrast, fixed costs and a low scrap value introduce downward rigidity in the response of mining power to a decline in the exchange rate. With fixed costs, entry does not occur until the point where the present value of mining revenues exceeds the fixed costs. Hence, for small drops in the exchange rate, entrants prefer to keep mining and recover some of their fixed costs, rather than shut down. This is true up to the point where it is better to sell mining equipment for scrap. Thus, mining power does not respond to small negative shocks in the presence of fixed costs, but mining power may decline in response to large negative shocks in the exchange rate.

2. **Exchange rate drop hits miners**. In the absence of fixed costs, miners face no loss when the exchange rate falls, whereas with fixed costs, miners do face a loss following a drop in the exchange rate, the limit of which is determined by the scrap value of their mining equipment. As discussed above, regardless of whether miners continue mining or sell their equipment for scrap in response to a reduction in the exchange rate, they do not fully recover their fixed cost expenditure and hence the drop in the exchange rate implies a loss.

3. **Protection for double-spending attacks**. A double-spending attack is less likely to be profitable when miners face fixed costs and a low scrap value. In the absence of fixed costs, owners of mining equipment earn no income net of variable costs in

equilibrium, and the cost of an attack to attackers only consists of a loss in the value of mining rewards during the attack. With fixed costs, attackers will also face a loss in the present value of future mining rewards. Calibration results show that the reduction in the value of future mining rewards may increase the estimated cost of an attack to attackers by a factor of 1,000. Hence, ignoring fixed costs can lead to an overly pessimistic view on the likelihood of double-spending attacks and therefore on the immutability of cryptocurrency ledgers that rely on proof-of-work.

4. **Path dependence in mining and security**. When miners face fixed costs and low scrap value, then the mining power and feasibility of profitable double-spending attacks will exhibit path dependence. For any given exchange rate, mining power will be higher if the current exchange rate is the result of a decline from a previous peak. The reason is that the peak induces an expansion of mining operations. If a decline in the exchange rate occurs, then miners are somewhat locked in because the fixed investment in mining equipment is a sunk cost to the extent that the alternative use value is low. The feasibility of profitable double-spending attacks will be higher if the current exchange rate is the result of a decline from a previous peak. The reason is that the locked-in miners have a lower present value of continuing their mining operations, resulting in a lower loss of future mining rewards from participating in a successful attack. In practical terms, higher mining power does not automatically imply that double-spending attacks are less likely.

Our empirical results confirm the importance of fixed costs for mining decisions. The evidence suggests a strong positive relationship between exchange rates and mining power for several proof-of-work cryptocurrencies. We also document path dependence in the level of mining power that is consistent with the presence of fixed costs. In particular, we find that mining power responds less to changes in the exchange rate of a cryptocurrency when the exchange rate fluctuations are below the historical peak. Moreover, there is a greater response to increases in the current exchange rate above the previous peak. Both observations are consistent with the fact that fixed costs cause miners to be locked in when the alternative use value of mining units is low.

We also consider an extension of our model where mining power can seamlessly be transferred between multiple cryptocurrencies that rely on the same mining algorithm. The theoretical predictions are unaffected if exchange rates are perfectly correlated in the sense that exchange rate movements are identical. By contrast, if exchange rates are weakly correlated and cryptocurrencies are small—in terms of the mining rewards they offer measured in fiat money—compared to peers that use the same mining algorithm, then the theory predicts that the mining power of those smaller cryptocurrencies responds to exchange rate movements as if there were no fixed costs. An extension of our empirical results among small cryptocurrencies confirms these theoretical expectations by showing that the path dependence in the mining power of smaller cryptocurrencies becomes weaker in periods when the correlation in exchange rate movements with their larger peer is low.

The possibility of transferring mining power between different cryptocurrencies may also increase the vulnerability of those cryptocurrencies to double-spending attacks. In particular, if the exchange rates of other cryptocurrencies that can be mined with the same equipment are expected to be relatively unresponsive to an attack on a single cryptocurrency, then, ceteris paribus, the viability of a profitable double-spending attack will be higher than in the single-cryptocurrency case. The size of the attacked cryptocurrency also plays a role because an attack on a tiny currency is unlikely to greatly affect the average return from a mining unit. Hence, fixed costs alone may be insufficient to avoid profitable double-spending attacks on a new cryptocurrency that would, at least initially, offer relatively small mining rewards in terms of fiat money. To benefit from the protection that fixed costs may add to avoiding double-spending attacks, it is also necessary to ensure that the equipment that can be used to mine the cryptocurrency efficiently is unique compared to other large cryptocurrencies.

This paper fits into a growing body of theoretical literature on the exchange rates of cryptocurrencies. Previous theoretical studies discuss the impact of factors such as transactional usage and speculative demand on the exchange rate of cryptocurrencies; see, e.g., Garratt and Wallace (2018), Bolt and Van Oordt (2020), Athey et al. (2016), Schilling and Uhlig (2019), Biais et al. (2019b) and Zimmerman (2020).[2] Differently from those studies, our work abstracts from factors that affect the equilibrium exchange rate of cryptocurrencies except for the occurrence of a successful double-spending attack. A successful double-spending attack on a cryptocurrency is likely to reduce the perceived security of making transactions using that currency. This may put negative pressure on speculative demand due to more pessimistic expectations regarding future usage (Bolt and Van Oordt, 2020) and reduce transactional demand due to a lower number and smaller size of current cryptocurrency transactions (Chiu and Koeppl, 2019b).[3] Both of these aspects would have a negative impact on the cryptocurrency exchange rate.

The remainder of the paper is structured as follows. Section 2 discusses the incentives to operate hardware for mining cryptocurrencies in the presence of fixed costs for a given level of the exchange rate. Section 3 sets out how the optimal amount of mining would change after a hypothetical decline to the exchange rate. These results are used in Section 4 to derive how many units of cryptocurrency one should be able to double spend in order for an attack to be profitable. Appendix A provides the reader with a form to calculate this number based on reader-provided parameters. Section 5 reports the empirical results. Section 6 presents empirical and theoretical results for an extension to an environment with multiple cryptocurrencies and transferable mining power. Section 7 concludes. Appendix B reports our data sources and descriptive statistics. Appendix C shows that our empirical findings are robust to allowing changes in price expectations triggered by an increase in the historical peak in the exchange rate.

[2]See Hałaburda and Haeringer (2019) for a literature survey.

[3]Some cryptocurrency exchanges have responded to successful double-spending attacks by requiring a higher number of block confirmations for deposits in those cryptocurrencies, while others have gone as far as completely delisting vulnerable cryptocurrencies (Coindesk, 2018). Both responses reduce the convenience of transactions with cryptocurrencies that have been subject to attacks.

2 Model

The exchange rate of a cryptocurrency, or the price of cryptocurrency in terms of fiat money, is denoted as S. The proof-of-work protocol rewards miners with an aggregate of b coins of the cryptocurrency per solved block ("block rewards" and transaction fees). One can mine the cryptocurrency using mining units that have a lifetime $\bar{T}$.[4] Those mining units can be purchased and installed at a fixed cost F and require a per-period flow cost of ε to operate (e.g., electricity). The continuously compounded cost of capital is denoted by $r > 0$. The total number of mining units that are currently in operation, the "mining power," is denoted by Q. The number of mining units in operation can be equal to or less than the total number of mining units that have been installed, which is denoted as Q^I.

The proof-of-work protocol is structured such that the arrival of solved blocks follows a Poisson process. The proof-of-work protocol adjusts the difficulty of mining Q^D at regular intervals such that the anticipated arrival rate of blocks solved by all miners equals λ per period. As a consequence, the arrival of blocks solved by a single mining unit follows a Poisson process with an arrival rate that equals λ/Q^D. Without loss of generality, we normalize the length of the period such that $\lambda = 1$.

Given these preparations, we calculate the net present value of operating a mining unit as follows. Let $N(T)$ denote the stochastic number of blocks that are solved by a single mining unit after operating for T periods. Moreover, let the stochastic arrival time of the kth block solved by that mining unit be denoted as T_k. Then the expected present value of operating a mining unit for T periods given difficulty level Q^D equals

$$\underbrace{\mathbb{E}\left[\sum_{k=1}^{N(T)} e^{-rT_k} Sb\right]}_{\text{Mining rewards}} - \underbrace{\int_0^T e^{-rt} \varepsilon dt}_{\text{Operating cost}} = \frac{1 - e^{-rT}}{r} \times \left[\frac{Sb}{Q^D} - \varepsilon\right].$$

[4]Lifetime can be the period until failure or until the mining unit is made obsolete by the introduction of new, more advanced mining units. See Garratt and Hayes (2015) for a discussion of how the introduction of a new generation of application-specific integrated circuits (ASICs) undermines the profitability of existing mining chips.

The proof-of-work protocol adjusts the difficulty level to the current level of mining power ($Q^D \to Q$). Moreover, to reduce complexity, we assume a mining unit has an infinite lifetime ($\bar{T} \to \infty$). All that our analysis actually requires is that mining units last longer than the duration of a double-spending attack. The implications of modeling finite mining unit lives beyond this point are discussed in the concluding remarks. Thus, the net present value of setting up a new mining unit can simply be calculated as

$$\left[\frac{Sb}{Q} - \varepsilon\right]\frac{1}{r} - F. \tag{1}$$

There is a profit motive to install and operate new mining units whenever this quantity is larger than zero. As a consequence of free entry, mining units will be added under profit maximization as long as the expression in (1) is positive.[5] Hence, it will be profitable to install and operate new mining units until the mining power $Q \geq Q^*(F)$ where

$$Q^*(F) = \frac{Sb}{rF + \varepsilon}. \tag{2}$$

When there are $Q = Q^*(F)$ mining units in operation, then the mining rewards for the network equal exactly the aggregated flow costs of operating the network plus the cost of capital for the mining equipment. When we consider the equilibrium mining power of the network, the cost of capital to cover the fixed cost thus enters the calculation in a very similar manner as the flow cost of operating the mining equipment.[6] However, as a consequence of the sunk cost nature of the fixed costs, this will not be the case for the optimal level of

[5]The miners in our framework are not averse to the risk of the stochastic process of solving blocks. Cong et al. (forthcoming) model how miners almost completely diversify this risk by joining revenue-sharing groups, so-called "mining pools." The operator of such a mining pool may charge a small fee. Our framework can account for this by considering parameter b as the number of coins earned net of fees to the mining pool.

[6]The derivation of the equilibrium number of mining units in equation (2) assumes that mining equipment is used for "honest mining" in contrast to the concept of "selfish mining" of Eyal and Sirer (2018). Equation (2) also applies in an environment where mining pools use equipment for selfish mining as long as there is free entry into these mining pools.

mining equipment in response to a negative shock in the exchange rate that occurs after the mining power has reached its equilibrium level.

3 Mining After a Shock to the Exchange Rate

Suppose the mining capacity is Q^I, where $Q^*(F) \leq Q^I \leq Q^*(V)$, and an unanticipated drop in the exchange rate of $l > 0$ percent occurs. What would be the optimal response of miners?

Mining units have an alternative use value $0 \leq V \leq F$. The alternative use value depends on the equipment used for mining a specific cryptocurrency, which may depend on the type of proof-of-work protocol. Throughout the analysis we consider three different cases: no alternative use value $V = 0$ (labelled "ASICs" for application-specific integrated circuits), a partial alternative use value $0 < V < F$ (labelled "GPUs" for graphics processing units) and full alternative use value $V = F$ (labelled "general purpose hardware" for hardware that could be used equally well for other purposes). The situation of full alternative use value is conceptually close to the situation where there are no fixed costs of operating mining units.

A drop in the exchange rate of l percent reduces the mining rewards. It is only profitable to continue operating mining units when the present value of the mining rewards minus the operating cost exceeds the alternative use value of the mining unit. That is, it is only profitable to continue operating mining units as long as the following condition holds true:

$$\left[\frac{S(1-l)b}{Q} - \varepsilon\right]\frac{1}{r} \geq V.$$

We can show that under profit maximization, the mining power in response to the decline in the exchange rate will equal

$$Q^R(V, l, Q^I) = \begin{cases} Q^I & \text{if } l < \theta(V, Q^I) \\ (1-l)Q^*(V) & \text{if } l \geq \theta(V, Q^I), \end{cases} \tag{3}$$

where

$$\theta(V, Q^I) = 1 - Q^I/Q^*(V). \tag{4}$$

If the number of installed mining units has reached its equilibrium value, i.e., if $Q^I = Q^*(F)$, we have that the threshold in equation (4) equals

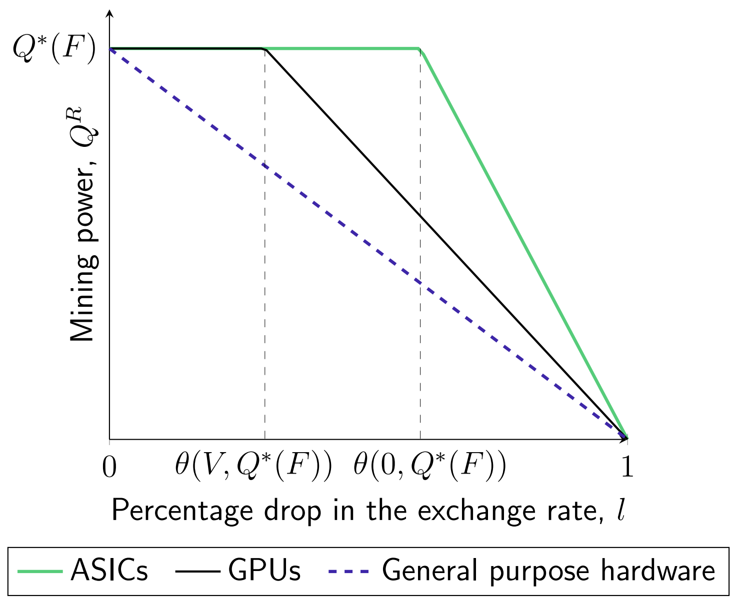
$$\theta(V, Q^*(F)) = \frac{F - V}{F + \varepsilon/r}. \tag{5}$$

This expression shows that whether mining power will change in response to a negative shock in the exchange rate once the number of installed mining units has reached its equilibrium value $Q^*(F)$ depends on the values of F and V.

In the scenario where there is a fixed cost but no alternative use value ($F > 0$ and $V = 0$), miners will not respond to small adverse shocks to the exchange rate where $l < \theta(V, Q^*(F))$. Since there is no alternative use value, the cost of acquiring mining units is entirely a sunk cost from the perspective of the miners. For the decision to continue mining it is only relevant whether the mining rewards cover the operating cost ε. Miners continue to mine whenever the drop in the exchange rate is less than the fixed cost as a ratio of the total cost to operate a mining unit over its lifetime. The mining power will be unchanged at $Q^*(F)$ unless the decline in the exchange rate exceeds the threshold. If the drop exceeds the threshold, then miners reduce their mining activity proportionally to the decline in excess of the threshold as illustrated by the solid green line in Figure 2.

In the scenario where there is no fixed cost ($F = V = 0$) or where the fixed cost equals the alternative use value ($F = V$), the threshold drop in equation (4) equals zero. Miners optimally respond by reducing the mining power in proportion to the shock in the exchange rate. This is illustrated by the dashed line in Figure 2. Since the alternative use value equals the fixed costs, miners can flexibly exit the market without incurring a loss. Profit-maximizing miners will continue exiting the market until the sum of the operating cost and the cost of capital equals the value of the mining rewards at the lower exchange rate.

Figure 2: Mining Power after an Unanticipated Drop in the Exchange Rate

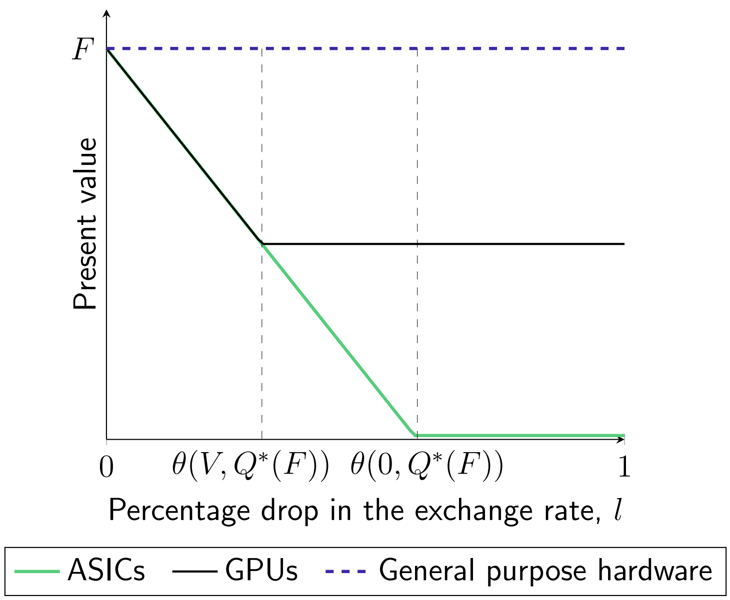


The situation of a partial alternative use value of mining units ($0 < V < F$) is in between the two extremes because the mining rewards need to cover both the operating cost and the cost of capital for the alternative use of the mining unit (the black solid line in Figure 2).

Altogether, equation (3) suggests that the level of mining power is expected to be path dependent in environments where fixed costs and low alternative use values play a role in the mining decision: Mining power is expected to be higher if the current level of the exchange rate is the result of a decline from a previous peak rather than the result of an increase in the exchange rate. In contrast, an environment without fixed costs suggests that mining power is independent of the path towards the current exchange rate.

The flip side of the unresponsiveness of mining power to an unanticipated decline in the exchange rate is that the drop translates into a decrease in the value of mining equipment as measured by the present value of the mining rewards. The present value of the mining rewards prior to the unanticipated decline in the exchange rate equals the fixed cost in

Figure 3: Value of a Mining Unit after a Drop in the Exchange Rate



equilibrium. The equilibrium present value of a mining unit after a given drop in the exchange rate l is given by

$$PV(V, l) = \max \left[\frac{1}{r} \times \left(\frac{S(1-l)b}{Q^*(F)} - \varepsilon \right), V \right]. \tag{6}$$

The present value of a mining unit cannot fall below its alternative use value V. If the alternative use value equals the fixed cost, then the value of a mining unit is independent of the drop in the exchange rate, as indicated by the dashed line in Figure 3. If the alternative use value is less than the fixed cost, then a drop in the exchange rate leads to a loss in the value of the mining equipment owned by the miners, as indicated by the solid lines in Figure 3. As a consequence, investors in mining equipment will be more concerned with potential declines in the exchange rate when the fixed cost is high and the alternative use value is low.

4 Double-Spending Attacks

We consider the situation where a coalition of miners considers the possibility of engaging in a double-spending attack. The purpose of this section is to calculate the impact of the fixed cost and the alternative use value on the profitability of a double-spending attack. We do so by calculating the minimum number of coins that the attackers must be able to double spend as part of an attack in order for the attack to be profitable.

We first consider the costs of double-spending attacks. Successful double-spending attacks are costly because they have a negative impact on the exchange rate of a cryptocurrency. This leads to two potential sources of reduced revenue. First, any mining rewards gained during the time of the attack must be liquidated at a lower exchange rate after the attack, while the mining rewards in the absence of an attack could be liquidated at a higher exchange rate.[7] Second, there is a reduction in revenues that will be earned by the mining equipment after the attack. The magnitude of this loss in revenue is shown in equation (6). The loss is linear in the decline in the exchange rate, unless the present value of mining the cryptocurrency drops below the alternative use value of the mining units. Adding these two costs gives a per mining unit cost of a double-spending attack that is successful after t periods for a given decline in the exchange rate l that equals

$$L(V,t) = \underbrace{\frac{1-e^{-rt}}{r} \times \frac{lSb}{Q^*(F)}}_{\substack{\text{Lower value mining rewards} \\ \text{during the attack}}} + \underbrace{e^{-rt} \min\left(\frac{1}{r} \times \frac{lSb}{Q^*(F)}, F - V\right)}_{\substack{\text{Lower present value of operating a} \\ \text{mining unit after the attack}}}. \tag{7}$$

Suppose that a coalition of miners controlling a fraction α of mining units, where $1/2 < \alpha < 1$, can perform a double-spending attack that ultimately succeeds if the attack continues sufficiently long. Let $\phi(\alpha, t)$ denote the density of the probability function that a double-

[7] As long as the difficulty Q^D is fixed during the attack, the expected number of blocks that the attacking coalition solves within the duration of a successful attack will be exactly equal to the expected number of blocks that could be solved by the members of the attacking coalition with honest mining. Hence, participating in a successful attack does not affect the mining rewards through the expected number of blocks that can be solved during the attack.

spending attack was successful after time period t.[8] Then the per mining unit cost incurred by the attacking coalition equals

$$\int_0^\infty \phi(\alpha, t) L(V, t) dt.$$

The attacking coalition benefits from a successful attack because it allows them to sell, i.e., "double spend," d coins of the cryptocurrency. They can do so by rewriting the transaction history and replacing their previous transactions in the cryptocurrency ledger. Assuming that the attack will be discovered when the attackers attempt to double spend the coins, the attackers can only sell them at the lower exchange rate of $(1 - l)S$. If we weigh the benefits and the cost of the attack, a profitable double-spending attack by a coalition of miners is feasible whenever

$$d(1 - l)S > \alpha Q^*(F) \times \int_0^\infty \phi(\alpha, t) L(V, t) dt. \tag{8}$$

One of the complications of the cost-benefit analysis in equation (8) is that the cost of the attack will depend on the duration of a successful attack, which is stochastic. Because of the functional form of $L(V, t)$, we can exactly analyze the cost-benefit analysis in equation (8) based on a number that can be interpreted as the representative duration of a successful double-spending attack $t = t^*$, where

$$t^* =: -\log \left(\int_0^\infty \phi(\alpha, t) e^{-rt} dt \right) / r.$$

[8]There is no simple general function for $\phi(\alpha, t)$. Suppose a successful double-spending attack requires the attacking coalition to release a chain that is m blocks longer in order to convince the other miners to adopt the attacker's chain as the valid chain, while the initial transactions that will be double spent need to be included in a block that is followed by at least k blocks on the chain maintained by the honest miners (k is the required number of "block confirmations" for payments to be accepted). Then the density function is the result of a race between two Poisson processes, one with an arrival rate of $\alpha Q^*(F)/Q^*(F) = \alpha$ (the attacking coalition), denoted by $A(t)$, and one with an arrival rate of $1 - \alpha$ (the honest nodes), denoted by $H(t)$. The race between $A(t)$ and $H(t)$ starts as soon as the transactions that will be double spent are transmitted to the network. The double-spending attack is successful at the random time $\tau_{m,k} = \inf\{t > 0 : A(t) \geq H(t) + m, H(t) \geq k\}$. The density function is then given by $\phi_{m,k}(\alpha, t) = \partial_t \Pr(\tau_{m,k} \leq t)$. Goffard (2019, Theorem 1) provides a solution for the special case $\phi_{m,0}(\alpha, t)$ (i.e., where $k = 0$). The double-spending attack will be successful with probability 1 as $t \to \infty$ if $1/2 < \alpha < 1$.

For reasonable choices for the discount rate, the level of t^* will be close to, but not exactly the same as, the average duration of a successful double-spending attack. More precisely, since the function e^{-rt} is convex in t, the level of t^* will be slightly below the average duration.

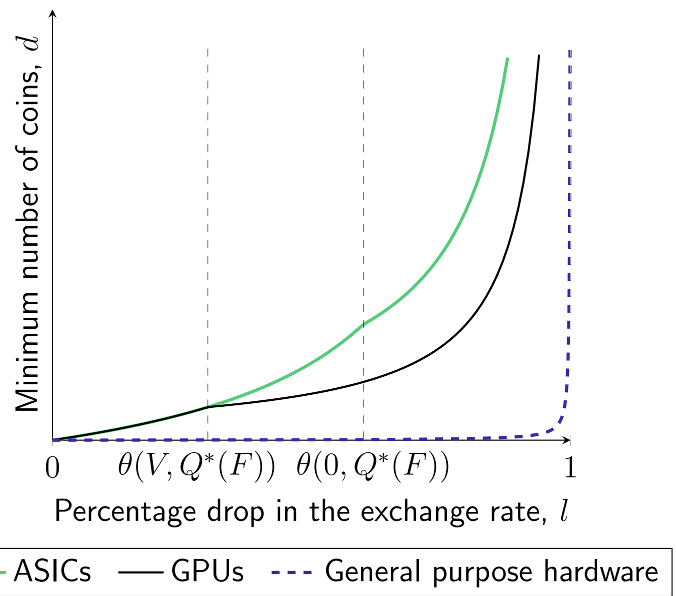
By using t^* in equation (7) we can avoid the integration used in equation (8) and solve for the minimum number of coins the attacking coalition must be able to double spend, as a multiple of the per-block mining rewards, in order for a profitable attack to be feasible as

$$\frac{d}{b} = \alpha \times \frac{1}{1-l} \times \left[\frac{1-e^{-rt^*}}{r} \times l + \frac{e^{-rt^*}}{r} \times \min\left(l, \frac{F-V}{F+\varepsilon/r} \right) \right]. \tag{9}$$

The multiple increases in the fraction of mining units who incur the cost of participating in the attacking coalition α, and it increases in the ratio $1/(1-l)$ because coins must be double spent against a lower exchange rate. The first term between the square brackets corresponds to the percentage drop in the exchange rate multiplied by the discounted number of solved blocks during the attack. The second term corresponds to the discounted number of blocks that could be solved after the attack multiplied by the percentage loss in the present value of owning a mining unit.

The expression in equation (9) shows the importance of taking into account fixed costs and alternative use value when calculating the minimum number of coins that must be successfully double-spent in a profitable attack. In the absence of fixed costs, or if there is a full alternative use value ($V = F$), then the attacker only needs to cover the reduction in the mining rewards that occurs during the attack, and hence the second multiplicative term inside the square brackets in equation (9) is equal to 0. If $V < F$, so that fixed costs matter, then both terms inside the square brackets in equation (9) are positive, and hence the loss that needs to be covered includes reductions in revenue that occur after the attack, and is potentially much larger. Three scenarios for the value of V are illustrated in Figure 4. The dashed line indicates the minimum value of d/b that would be necessary to facilitate a profitable double-spending attack with full alternative use value ($V = F$). The

Figure 4: Minimum Gain for Profitable Double-Spending Attack



solid dark and solid light lines show the minimum multiple d/b for partial ($0 < V < F$) and no alternative use values ($V = 0$), respectively. The dashed line is very close to zero when compared with the solid lines, except in the case where the drop in the exchange rate is close to 100%. If the value of the cryptocurrency drops to zero, then no number of coins that can be double spent would be sufficient to make up for the loss suffered by the attackers.

Table 1 shows the specific number of coins that an attacker would need to double spend in order for an attack to be profitable under several scenarios. The parameter values used are meant to illustrate the importance of fixed costs and a low alternative use value in order to prevent attacks from occurring. The first line of each panel reports the number of coins that an attacker should be able to double spend in an environment with full alternative use value. The low numbers are in line with the low cost of double-spending attacks in the absence of fixed costs as estimated by Budish (2018, Table 1) or the long confirmation times necessary to secure transactions as estimated by Auer (2019, Figure 9). The table shows that moving from a full alternative use value to a zero alternative use value can increase the number of coins that one should be able to double spend by a factor of 1,000. So the feasibility of profitable double-spending attacks decreases substantially when taking fixed costs into

Table 1: Minimum Size of Double-spend for Profitable Attack

Panel (a): Current mining rewards (b=6.67 per block)

Drop in the exchange rate:		15%	30%	60%
	100%	60	146	510
Alternative use value:	50%	124,794	151,608	265,569
	0%	157,759	303,070	530,628

Panel (b): Only transaction fees (b=0.42 per block)

Drop in the exchange rate:		15%	30%	60%
	100%	4	9	32
Alternative use value:	50%	7,858	9,547	16,722
	0%	9,934	19,084	33,413

Note: The table reports the minimum number of coins that attackers would need to double spend in order for an attack to be profitable. Parameter choices are: $t^* = 100$, $r = 0.20$ (annualized), $\alpha = 0.51$, $\varepsilon = 1,350$ (annualized), $F = 2,100$. The calibration of the fixed cost is motivated by the rounded list price of the "Antminer S17+ 70TH/s" (including taxes) on Bitmain.com (April 2020), which can be used to mine Bitcoin. The calibration of the annualized per-period cost is motivated by its electricity consumption of 2.8 kWh and an electricity cost of 0.055 USD/kWh (this exceeds the average price of electricity to ultimate customers in the industrial sector in the six cheapest states; see U.S. Department of Energy, 2020, Table 5.6.b). Theoretically, the fixed costs should also include other costs (e.g., installation costs), and the per-period cost should also include other operational costs (e.g., maintenance). The transaction fees of 0.42 per block are based on the average transaction fees for Bitcoin over the period 2019Q1-Q3.

account. The parameter values clearly do not cover all conceivable scenarios. Appendix A includes a form where one can easily make adjustments in order to automatically calculate the double spend threshold for alternative parameter values.

5 Empirical Results

This section provides empirical evidence of the theoretical model and the relevance of fixed costs for mining power. In order to do so, we collect a panel data set with monthly data on the exchange rate in USD of proof-of-work cryptocurrencies and their mining power as measured by the total "hash power" of the miners. Appendix B reports our data collection procedure as well as descriptive statistics and unit root tests. Panel unit root tests suggest that the levels of cryptocurrency exchange rates and their mining power are integrated with order one, but there is strong evidence that the first differences are stationary. We therefore estimate the relationship between mining power and cryptocurrency exchange rates in first differences.

Economic incentives induce investors to increase the amount of mining power when cryptocurrency exchange rates are higher. However, once the amount of mining equipment deployed has reached the equilibrium for that higher level of the exchange rate, then a decrease in the exchange rate should have a smaller impact on mining power if fixed costs are relevant (as shown in Figure 2). Accordingly, to test for the empirical relevance of fixed costs, we estimate a stylized model that includes not only the current exchange rate, but also the historical peak in the exchange rate. Let q_{it} and s_{it} denote respectively the log levels of the mining power and the exchange rate of cryptocurrency i at time t. Moreover, let $s_{it}^{MAX} = \max\{s_{i1}, ..., s_{it}\}$ denote the historical peak in the exchange rate. Finally, let D_{it} denote a dummy variable for major changes in block rewards. It takes a value one if there is a major drop in the block rewards due to the mining protocol (e.g., so-called "halving" events in the case of Bitcoin), and a value zero, otherwise. Then, we estimate the model

$$\Delta q_{it} = \beta_0 + \beta_1 \Delta s_{it} + \beta_2 \Delta s_{it}^{MAX} + \mu_i D_{it} + u_{it}. \tag{10}$$

The coefficients, β_1 and β_2, measure the impact of changes in the exchange rate on mining power. A significantly positive $\hat{\beta}_1$ and insignificant $\hat{\beta}_2$ indicate that mining power responds proportionally and in a symmetrical way to positive and negative changes in the exchange rate. In contrast, a significantly positive $\hat{\beta}_2$ and insignificant $\hat{\beta}_1$ indicate that mining power increases in response to an increase in the exchange rate only when the exchange rate rises above its recent high, and does not respond to decreases in the exchange rate. If fixed costs play no role, then our theory predicts that only coefficient $\hat{\beta}_1$ will be significant and positive (consistent with the dashed line in Figure 2), while coefficient $\hat{\beta}_2$ must be insignificant. In

Table 2: Empirical Mining Power and Exchange Rates

VARIABLES	(1) Bitcoin	(2) Ethereum	(3) Litecoin	(4) Monero	(5) Dash	(6) Panel
Change in log exchange rate (Δs_{it})	0.085	0.226*	0.074	0.050	0.575***	0.169
	(0.139)	(0.116)	(0.092)	(0.089)	(0.130)	(0.096)
Change in log peak level (Δs_{it}^{MAX})	0.670***	0.269*	0.591***	0.676***	0.285	0.537***
	(0.145)	(0.159)	(0.125)	(0.166)	(0.173)	(0.078)
Change in Bitcoin block rewards	-0.293***					-0.324***
	(0.095)					(0.016)
Change in Ethereum block rewards		-0.251**				-0.609***
		(0.105)				(0.034)
Change in Litecoin block rewards			-0.440***			-0.177***
			(0.115)			(0.024)
Change in Dash block rewards					-0.754***	-0.399***
					(0.191)	(0.039)
Constant	0.384***	0.230***	0.331***	-0.030	0.542***	0.297***
	(0.055)	(0.056)	(0.055)	(0.055)	(0.116)	(0.013)
Observations	106	48	85	61	66	366
R-squared	0.483	0.641	0.577	0.421	0.468	0.478

Note: The dependent variable is the quarterly log change in log mining power (Δq_{it}). Exchange rates are measured in terms of US dollars. Variables are measured at the end of each month. The variable for the change in block rewards takes a value one if the mining protocol prescribes a major decline in the block rewards during the quarter, and a value zero otherwise. This variable does not exist for Monero, because it uses a smooth function for changes in the mining rewards. All models are estimated with least squares. Robust standard errors are reported in parentheses. The panel model is estimated with fixed effects to allow for cryptocurrency-specific time trends. Statistical significance at the 1%, 5% and 10% significance levels are indicated by ***, ** and *, respectively.

contrast, if fixed costs play a role, then our theory predicts that $\hat{\beta}_2$ will be significant and positive (consistent with the solid lines in Figure 2).

We estimate the model in equation (10) for a variety of proof-of-work cryptocurrencies that utilize five different proof-of-work protocols. The selection criteria are outlined in Appendix B. The model estimates suggest that fixed costs play an important role in the relationship between mining power and cryptocurrency exchange rates. Table 2 reports the estimates for individual cryptocurrencies as well as for the entire panel. Every column in Table 2 reports significantly positive estimates for coefficients β_1 or/and β_2. This suggests that mining power indeed responds positively to increases in the exchange rate as one may generally expect. Importantly, for most cryptocurrencies, it is the coefficient for β_2 that is largest in terms of magnitude and significance. This confirms that, empirically, the mining power tends to respond to exchange rate shocks in an asymmetrical manner. This holds particularly true for Bitcoin, and to a lesser extent for the other cryptocurrencies. For example, the mining power for Bitcoin tends to respond with an elasticity of $0.085 + 0.670 = 0.755$ to increases in Bitcoin's exchange rate when the exchange rate is at an all-time high, but only with an elasticity of 0.085 when the exchange rate is below its historical peak. The results for Bitcoin are particularly supportive of the theory since Bitcoin mining involves ASIC chips with a near zero alternative use value. In contrast, Dash, which can be successfully mined using CPUs, with a high alternative use value, has an elasticity that is largely unaffected by the historical peak.

The constant in the model allows for a time trend, which can capture features such as technological progress in mining equipment. The estimated constant in the model is in general also significantly positive. The coefficient for major declines in block rewards also has the expected negative sign.

6 Extension to Cryptocurrency Groups with Transferable Mining Power

In this section, we address the fact that sometimes multiple cryptocurrencies are based on the same underlying protocol and hence can be mined effectively using the same equipment. Whether or not this affects the earlier comparative static results depends on the relative sizes of cryptocurrencies within a common mining group and on the co-movement of their exchange rates. If exchange rates are perfectly correlated in the sense that exchange rate movements are identical, then the analysis for the single cryptocurrency case remains valid. This is also true, to a reasonable approximation, if one cryptocurrency is very large relative to others in its group. In contrast, if one cryptocurrency is very small in size and there is weak exchange rate correlation with the larger cryptocurrency, then it is as if fixed costs do not matter for the smaller one. The intermediate cases, where both cryptocurrencies are large in size and there is weak correlation, permit a muted impact due to fixed costs.

6.1 Mining Flexibility

Suppose the mining units can be used to mine either of a pair of cryptocurrencies.[9] For the purpose of this subsection, we introduce subscripts A and B to distinguish between the two cryptocurrencies, whenever it becomes necessary. So, the exchange rates are denoted as S_A and S_B, the mining benefits by b_A and b_B, the mining power by Q_A and Q_B, etc. Variables related to the characteristics of the mining equipment that the two cryptocurrencies have in common, such as V and F do not require subscripts. Finally, Q^I will refer to the total number of mining units that can be used to mine either cryptocurrency.

The possibility of switching between cryptocurrencies that use similar mining equipment introduces an additional equilibrium condition. In equilibrium, it cannot be possible to increase the revenue of a mining unit by switching from mining one cryptocurrency to mining another. This holds true only if the benefits from using a mining unit to mine either of the two cryptocurrencies are the same, i.e., if

$$\frac{S_A b_A}{Q_A} = \frac{S_B b_B}{Q_B}. \tag{11}$$

[9]The results extend easily to more than two cryptocurrencies. In particular, one may simply redefine the shares in (12) and the weighted-average drop in the exchange rates in (13) for more than two cryptocurrencies. The equilibrium condition in (11) will then hold true for any currency pair and the result in (14) will hold true for any of the cryptocurrencies.

Whenever this equilibrium condition does not hold true, then profit maximization will induce miners to switch cryptocurrencies, which leads to adjustments in Q_A and Q_B, until the condition in (11) holds true.

The equilibrium condition in (11) can be written in an economically meaningful way. Let the share of total mining revenues for cryptocurrency i, where $i \in \{A, B\}$, be denoted as

$$w_i := \frac{S_i b_i}{S_A b_A + S_B b_B}. \tag{12}$$

Then one can rewrite equation (11) as

$$\frac{Q_i}{Q_A + Q_B} = w_i.$$

Hence, the share of the total mining power used to mine a particular cryptocurrency equals in equilibrium the proportion of mining revenues that is offered as remuneration for mining that cryptocurrency.

Profit maximization will induce miners to install and operate new mining units to mine cryptocurrencies A and B until the moment where, respectively, $Q_A = Q_A^*(F)$ and $Q_B = Q_B^*(F)$, where $Q_i^*(F) =: (S_i b_i)/(rF + \varepsilon)$. So, once the mining rewards plateau on an all-time high, then the total number of mining units that will be operated in equilibrium equals the sum of the numbers of mining units that we would obtain if we were to consider each of the cryptocurrencies individually, i.e., in equilibrium, $Q^I = Q_A^*(F) + Q_B^*(F) = (S_A b_A + S_B b_B)/(rF + \varepsilon)$.

As before, we now consider the impact of adverse shocks to the exchange rates l_A and l_B on the mining power of each cryptocurrency. For this purpose, let the weighted drop in total mining rewards be denoted as

$$\bar{l}(l_A, l_B) = l_A w_A + l_B w_B. \tag{13}$$

The response to the mining power of a cryptocurrency will depend on how the drop in its exchange rate compares to the weighted average drop for all cryptocurrencies $\bar{l}(l_A, l_B)$.

Given these preparations, we can derive the response of the mining power to the adverse shocks to the exchange rate (l_A, l_B) as

$$Q_i^R(V, l_A, l_B, Q^I) = \begin{cases} w_i Q^I \times \dfrac{1 - l_i}{1 - \bar{l}(l_A, l_B)} & \text{if } \bar{l}(l_A, l_B) < \theta(V, w_i Q^I) \\ (1 - l_i) Q^*(V) & \text{if } \bar{l}(l_A, l_B) \geq \theta(V, w_i Q^I). \end{cases} \tag{14}$$

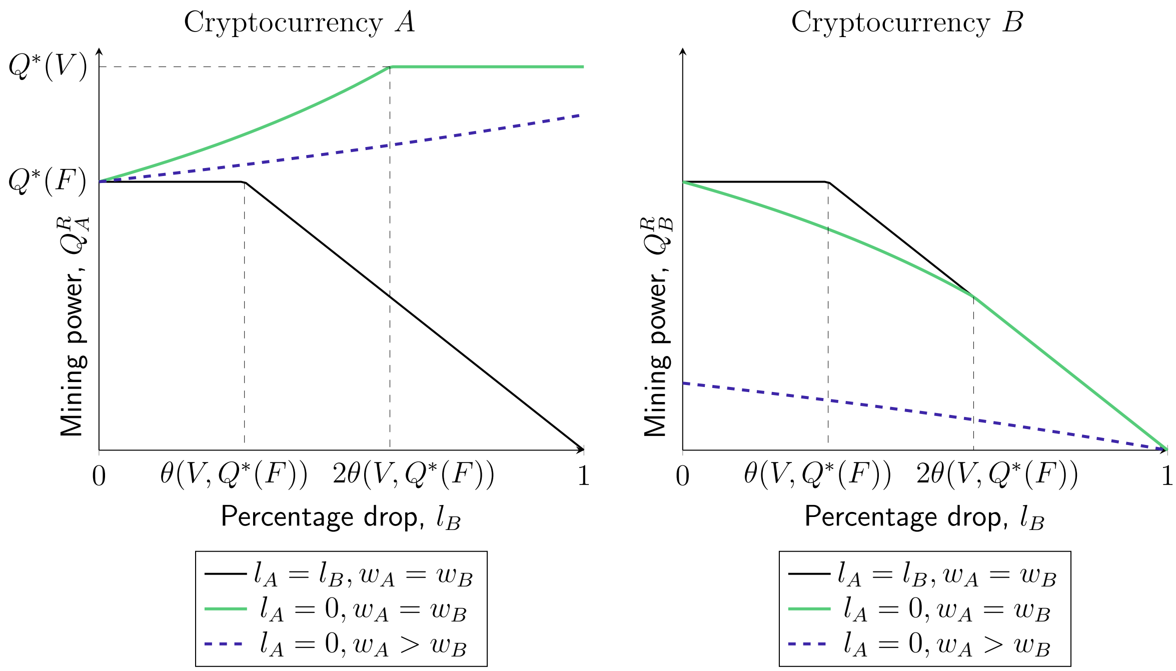
Note that the threshold $\theta(V, w_i Q^I)$ now applies to the weighted average drop in the exchange rate of all cryptocurrencies that can be mined with the equipment rather than to the drop in the exchange rate of a single cryptocurrency. In every other respect, the threshold is identical to the one used in the situation where mining equipment can be used for only a single currency.[10]

We now evaluate the response in mining power to adverse exchange rate shocks in different environments based on the result in equation (14). First, we consider an environment where the adverse shocks to both exchange rates are perfectly correlated in the sense that $l_A = l_B$. In this situation, the response in mining power to an adverse shock is identical to that in the situation where there is only a single cryptocurrency that can be mined with the equipment. The level in the mining power in equation (14) is the same as that in equation (3) whenever $l_i = \bar{l}(l_A, l_B)$.[11] This is illustrated for the situation where mining equipment has a partial alternative use value $(0 < V < F)$ by the black solid line in Figure 5, which shows the same pattern as the black solid line in the single-currency setting in Figure 2. There is no response in the mining power when the adverse shock to the exchange rates is small because the mining revenues still exceed the per-period cost of mining. However, the mining power will drop once the shock to the exchange rates exceeds the threshold, because the

[10]Note that $\theta(V, w_A Q^I) = \theta(V, w_B Q^I)$.

[11]The initial mining power used to mine a single currency in the multi-currency setting is expressed as $w_i Q^I$, while it is expressed as Q^I in the single-currency setting (the weight w_i is essentially one in the single-currency setting).

Figure 5: Mining Power After Drop in Cryptocurrency B's Exchange Rate



Note: The figure shows how an unanticipated drop in cryptocurrency B's exchange rate affects the mining power of cryptocurrencies A and B when mining units can be used to mine both cryptocurrencies. The parameters for the mining equipment correspond to those for a partial alternative use value ($0 < V < F$). The scenario $l_A = l_B$ corresponds to the situation where both cryptocurrencies suffer the same decline in the exchange rate. The scenario $l_A = 0, w_A = w_B$ corresponds to the situation where the shock is only to cryptocurrency B's exchange rate when both cryptocurrencies offer the same mining rewards in terms of fiat money. The scenario $l_A = 0, w_A > w_B$ corresponds to the situation where the shock is only to cryptocurrency B's exchange rate when cryptocurrency B offers substantially smaller mining rewards in terms of fiat money than cryptocurrency A.

mining revenues no longer exceed the per-period cost of mining plus the cost of capital of the alternative use value at this point.

Second, we consider an environment where the adverse shock only occurs to the exchange rate of one of the two currencies ($l_B > 0$, $l_A = 0$) and where both currencies are similarly sized in the sense that they pay the same level of mining benefits in terms of fiat money ($w_A = w_B$). This environment is represented by the solid green line in Figure 5. In this environment, even a small decline in the exchange rate will lead to a decline in mining power of cryptocurrency B as $l_B > \bar{l}(0, l_B)$. The reason is not because it is no longer profitable to continue operating those mining units, but because a larger share of the mining power is allocated towards mining cryptocurrency A, which now offers a larger share of the total mining revenue as $l_A < \bar{l}(0, l_B)$. Mining units will be taken out of operation only if the drop in the exchange rate, l_B, is sufficiently high. However, whether the loss is sufficiently high depends on the weighted average decline in both exchange rates rather than the decline in a single exchange rate. In the scenario we consider, where each currency has the same initial weight while there is no loss to the exchange rate of cryptocurrency A, the threshold in terms of l_B will be exactly twice as high as in the single-currency case. Once the drop in the exchange rate of cryptocurrency B exceeds the higher threshold, then there are no longer incentives to redistribute mining power to cryptocurrency A. Any further decline in the exchange rate of cryptocurrency B beyond the threshold will reduce the number of operating mining units. All remaining mining units that mine either cryptocurrency A or B earn exactly the per-period mining cost plus the cost of capital of the alternative use value.

Third, we consider an environment where the adverse shock occurs to the exchange rate of a cryptocurrency ($l_B > 0$, $l_A = 0$) that is substantially smaller in terms of the mining benefits as measured in fiat money ($w_A > w_B$). This environment is represented by the dashed line in Figure 5. The decline in the exchange rate of cryptocurrency B will lead to a reallocation of mining power to cryptocurrency A, as was the case in the previous environment. However, if the total benefits of mining cryptocurrency B are substantially smaller than those of cryptocurrency A, then any drop in the exchange rate of cryptocurrency B will be insufficient for the average decline to hit the threshold. The mining power of the smaller cryptocurrency B will respond in a close to linear fashion to declines in the exchange rate. In particular, in the limit where cryptocurrency B is infinitely small compared to cryptocurrency A, the remaining share of mining power that will be used to mine cryptocurrency B after a shock to its exchange rate equals

$$\lim_{w_B \to 0} \frac{Q_B^R(V, l_A, l_B, Q^I)}{w_B Q^I} = \lim_{w_B \to 0} \frac{1 - l_B}{1 - w_B l_B} = 1 - l_B.$$

This is simply a linear response, which is the same response in mining power as in the situation where there are no fixed costs, or where the alternative use value equals the fixed costs (see the dashed line in Figure 2). Hence, when exchange rates are uncorrelated, the mining power of a small cryptocurrency that uses the same mining equipment as a much larger cryptocurrency may respond to an exchange rate shock as if there were no fixed costs.

6.2 Empirical Results

We assess whether these theoretical predictions for groups of cryptocurrencies with transferable mining power are supported by empirical patterns in the data. We do so by estimating the model in (10) based on a sample of smaller cryptocurrencies that have large peers that use the same mining algorithm, while allowing for modifying effects based on the characteristics of those cryptocurrencies. Table 3 reports the results.

The first model in Table 3 tests whether the mining power of a small cryptocurrency with a large peer exhibits less downward rigidity when the exchange rate drops in comparison to the large peers. It does so by extending the estimation sample with the smaller cryptocurrencies, while using the interaction between a dummy and the price change to allow the impact of price changes to be different if there exists a large peer cryptocurrency that uses the same mining algorithm (in terms of market capitalization). Less downward rigidity means a lower coefficient $\hat{\beta}_2$, and a higher coefficient $\hat{\beta}_1$ for smaller cryptocurrencies. The signs of the estimated coefficients for the interactions are consistent with this theoretical prediction. The estimated coefficient $\hat{\beta}_2$ for the smaller cryptocurrencies with large peers is $0.537 - 0.225 \approx 0.312$, which is statistically significantly lower than the coefficient for the large peers at a 5 percent significance level. The coefficient $\hat{\beta}_1$ is about the same amount higher for the smaller cryptocurrencies, although the difference with larger coins is statistically insignificant.

The second and third models in Table 3 assess whether the downward rigidity in the mining power of small cryptocurrencies depends on the return correlation with their large peers

Table 3: Comparing Larger and Smaller Cryptocurrencies

VARIABLES	(1) Large versus small	(2) Static correlation	(3) Dynamic correlation
Change in log exchange rate (Δs_{it})	0.169*	0.778	0.756**
	(0.090)	(0.630)	(0.209)
Indicator for small coins × change in log exchange rate	0.147		
	(0.172)		
Static return correlation × change in log exchange rate		-0.831	
		(0.955)	
Dynamic return correlation × change in log exchange rate			-0.816**
			(0.251)
Change in log peak level (Δs_{it}^{MAX})	0.537***	0.373*	-0.039
	(0.074)	(0.147)	(0.148)
Indicator small coin × change in log peak level	-0.225**		
	(0.089)		
Static return correlation × change in log peak level		0.014	
		(0.252)	
Dynamic return correlation × change in log peak level			0.636
			(0.358)
Dynamic return correlation			0.706**
			(0.252)
Constant	0.225***	0.267***	-0.096
	(0.041)	(0.014)	(0.099)
Observations (cryptocurrencies)	678 (10)	312 (5)	312 (5)
R-squared	0.375	0.272	0.374

Note: The dependent variable is the quarterly log change in log mining power (Δq_{it}). Exchange rates are measured in terms of US dollars. Variables are measured at the end of each month. The indicator for small coins is a dummy that has value one for the small cryptocurrencies and value zero otherwise (see Appendix B for the classification). The static return correlation is calculated as the Pearson correlation coefficient over the entire sample between the monthly log returns of the small cryptocurrency and the returns of the largest cryptocurrency that uses the same mining algorithm. The dynamic return correlation is calculated as the Pearson correlation coefficient between the monthly log returns of the small cryptocurrency with those of the largest cryptocurrency that uses the same mining algorithm using a rolling window that uses the two quarters before and the two quarters after the observation. The estimated coefficients for the dummy variables for the change in block rewards for each cryptocurrency have been suppressed in the output. All models are estimated with least squares. Robust standard errors are reported in parentheses. Each model is estimated with fixed effects to allow for cryptocurrency-specific time trends. Statistical significance at the 1%, 5% and 10% significance levels are indicated by ***, ** and *, respectively.

that use the same algorithm. In order to do so, we estimate for each small cryptocurrency the correlation between the changes in its exchange rate and those in the rate of its larger peer. We estimate a static correlation over the entire horizon, as well as a correlation based on a rolling window of six months before and six months after each observation. We interact the price changes with the correlation to assess whether the correlation modifies the impact of price changes on mining power. Everything else equal, we expect the mining power of small cryptocurrencies to exhibit more downward rigidity (i.e., high $\hat{\beta}_2$, low $\hat{\beta}_1$) when the return correlation with their larger peers is high, while the mining power should exhibit less downward rigidity when the correlation is low (i.e., low $\hat{\beta}_2$, high $\hat{\beta}_1$).

The results are broadly in line with the theoretical prediction. The results for the static correlation have the correct sign, but are statistically insignificant. This could be the consequence of the correlations changing over time (see, e.g., the findings of Gandal and Hałaburda, 2016). The estimated model with the dynamic correlation suggests that the mining power of a small cryptocurrency, when price changes are uncorrelated, responds strongly towards positive and negative price changes ($\hat{\beta}_1 \approx 0.756 - 0 \times 0.816 = 0.756$) and exhibits no downward rigidity ($\hat{\beta}_2 \approx -0.039 + 0 \times 0.636 = -0.039$). By contrast, in the extreme case where the correlation is perfect, the model suggests strong price rigidity: The mining power is completely unresponsive to negative price changes ($\hat{\beta}_1 \approx 0.756 - 1 \times 0.816 = -0.060$), but may respond to price changes beyond the previous peak level ($\hat{\beta}_2 \approx -0.039 + 1 \times 0.636 = 0.597$).

6.3 Implications for Double-Spending Attacks

Our conclusions regarding the viability of double-spending attacks may also be affected by the existence of other cryptocurrencies with transferable mining power. The key issue is how the exchange rates of other cryptocurrencies that rely on the same mining equipment are expected to respond to a double-spending attack on a single cryptocurrency. If the exchange rates of all cryptocurrencies that rely on the same mining equipment suffer the same declines in response to an attack on a single currency, then the viability of double-spending attacks is the same as in the single-currency case. If the exchange rates of the other cryptocurrencies that can be mined with the same equipment are expected to be unresponsive or less responsive to an attack on a single cryptocurrency, then, ceteris paribus, the viability of a profitable double-spending attack will be higher than in the single-cryptocurrency case. The reason is that the option to mine the other cryptocurrencies whose exchange rates have not dropped (as much) provides miners with a smaller downside risk.

The extent to which the reallocation of mining equipment provides a good outside option will depend on the relative size of each cryptocurrency in terms of the share of mining benefits it offers in terms of fiat money. If the attacked cryptocurrency is sizable relative to other currencies, as in the second environment we consider, then mining benefits from mining an alternative cryptocurrency will drop considerably once miners start to switch. In this situation, there remains an important role of fixed cost in terms of avoiding a profitable double-spending attack. However, if the size of the attacked cryptocurrency is tiny comparable to other cryptocurrencies, as in the third environment we consider, then the reallocation of miners to the larger currency is unlikely to affect the mining rewards much. In this situation, fixed costs do not help much in terms of reducing the viability of profitable double-spending attacks. Hence, in the hypothetical situation where one were to set up a new cryptocurrency that would initially offer relatively small mining rewards in terms of fiat money, the fixed costs alone may be insufficient to avoid profitable double-spending attacks, and it may also be necessary to ensure that the mining equipment that can be used to mine the cryptocurrency efficiently is unique compared to other large cryptocurrencies.

Finally, the analysis reveals that previous declines in the exchange rate of another cryptocurrency may affect the viability of profitable double-spending attacks if mining power is transferable between different cryptocurrencies. In the second environment we consider, a sufficiently large decline in the exchange rate of cryptocurrency B, a decline that exceeds the threshold $2\theta(V, w_B Q^I)$, would reduce the mining rewards for mining either currency towards a level where it equals the per-period cost plus the cost of capital of the alternative use value.

In this situation, the miners of either cryptocurrency are indifferent between continuing mining or liquidating the mining equipment against its alternative use value. Hence, after such a drop in the exchange rate of cryptocurrency B, the vulnerability of cryptocurrency A to double-spending attacks would be comparable as in the counterfactual scenario where there would be no fixed costs of mining cryptocurrency A.

7 Concluding Remarks

The properties of mining hardware have important implications in terms of setting the "number of block confirmations" required for cryptocurrency payments (i.e., the number of blocks a recipient requires to be finalized since the payment before funds are considered to be received). A well-known strategy for those who accept payments in a particular cryptocurrency is to reduce their vulnerability to double-spending attacks by requiring a relatively high number of block confirmations. This increases the expected duration of a successful attack—a higher t^* in equation (9)—because it increases the number of blocks that the honest miners need to solve before transactions of potential attackers can be double spent. Equation (9) shows that such a strategy is particularly useful when the mining hardware is characterized by only a small difference between fixed costs and the alternative use value. Increasing the loss in mining revenue during the attack by increasing t^* can be an effective strategy when miners face few consequences from a reduction in future mining revenue. By contrast, there is less need of setting a high required number of block confirmations for payments with cryptocurrencies where owners of mining equipment care about future mining revenue because the equipment is characterized by a low alternative use value compared to the fixed costs. Some cryptocurrency exchanges have slowly started to take differences in characteristics of mining hardware into account when setting the required number of block confirmations for payments in different cryptocurrencies (Coinbase, 2019).

Our baseline analysis evaluates the cost of a double-spending attack under the assumption that mining hardware lasts forever. Suppose instead that mining units last for a finite number of periods, $\bar{T}$, and that this duration exceeds the number of periods required for a successful double-spending attack.[12] There are two implications. The first implication is that the number of blocks that can be mined with the equipment after a potential attack is smaller than before. This seems to suggest that miners have less to lose as a consequence of the double-spending attack. However, there is also an equilibrium effect, which is that the break-even level of mining power decreases. Miners now need to earn back their fixed costs in a smaller amount of time. The expression in equation (2) becomes $Sb/\left(rF/(1-e^{-r\bar{T}})+\varepsilon\right) < Q^*(F)$. Because mining equipment lasts less time, the equilibrium level of mining power corresponding to any level of fixed costs F must drop to make mining per period more profitable. This means miners have more income per period to lose. Fixed costs gain weight in the miner's decision, because they have to be earned back quickly, while the present value of the future per-period cost ε becomes smaller. This second implication suggests that a limited lifetime increases the potential loss to miners from double-spending attacks. In terms of equation (9), the combined implication is that the ε in the final term in square brackets, which captures the present value of the future per-period cost ε after the attack, is discounted by $(1-e^{r\bar{T}})/r$ instead of $1/r$. Shortening the unit life decreases the weight on ε and thus potentially raises the minimum number of coins the attacking coalition must be able to double spend as part of a profitable attack. In short, the equilibrium effect dominates the mechanical implication, meaning that moving to finite-lived mining equipment magnifies the importance of fixed costs as a deterrent to double-spending.

Our analysis suggests that the historical path of the exchange rate may be an important factor for setting the required number of block confirmations. The feasibility of profitable double-spending attacks will exhibit path dependence when miners face fixed costs and low scrap value. A previous high level of the exchange rate may have induced operators of mining

[12] This is not a strong assumption given that double-spending attacks in the vicinity of 100 periods or more would still take place over hours or days.

equipment to expand their operations. A decline in the exchange rate leads to a loss in the present value of continuing mining operations, which reduces the potential loss from the decline in the exchange rate following a subsequent double-spending attack. This reduces the deterrence of double-spending attacks. Our findings indicate that exchanges should consider requiring a higher number of block confirmations after cryptocurrencies have been subject to a steep decline in their exchange rate to offset the increased vulnerability to double-spending attacks.

An expectation-based channel has been raised as an alternative explanation for the significant positive coefficient for the historical peak level in the exchange rate in Table 2. That is, the expectation of miners regarding the future appreciation of the exchange rate, which is important for their investment decision, could increase with the level of the historical peak of the exchange rate. We address this issue in Appendix C. The results in this appendix suggest that the historical peak in the exchange rate remains significant when controlling for an expectation-based channel.

The popular narrative is that the development of ASICs for cryptocurrency mining has had a negative impact on the cryptocurrency landscape. Some have, for example, expressed concerns about vulnerabilities arising from dependability of the entire production of mining hardware on a single or small number of firms. Others have expressed concerns regarding the risks arising from centralization, where a small number of agents controlling a significant share of the mining hardware could potentially use their position to introduce censorship in cryptocurrency payments. The possibility of anybody with a computer being able to profit from mining is also often expressed as a desirable distributional feature of cryptocurrencies. Our analysis focuses on a widely ignored aspect, which is the impact of the type of mining hardware on the feasibility of profitable double-spending attacks. Our results suggest that the development of ASICs for cryptocurrency mining is instrumental in avoiding double-spending attacks, and therefore allows for a flourishing landscape of proof-of-work cryptocurrencies such as Bitcoin.

References

J. Abadi and M. Brunnermeier. Blockchain Economics. *NBER Working Paper*, 25407, 2018.

S. Athey, I. Parashkevov, V. Sarukkai, and J. Xia. Bitcoin Pricing, Adoption, and Usage: Theory and Evidence. *Working Paper*, 2016.

R. Auer. Beyond the Doomsday Economics of "Proof-of-Work" in Cryptocurrencies. *BIS Working Paper*, 765, 2019.

B. Biais, C. Bisière, M. Bouvard, and C. Casamatta. The Blockchain Folk Theorem. *Review of Financial Studies*, 32(5):1662–1715, 2019a.

B. Biais, C. Bisière, M. Bouvard, C. Casamatta, and A. Menkveld. Equilibrium Bitcoin Pricing. *Working Paper*, 2019b.

Bitcoin Gold. Bitcoin Gold Road Map. *White Paper*, 2017.

Bloomberg. Cryptocurrency Attacks Are Rising as Rogue Miners Exploit Flaw. News Report (29 May), 2018. URL https://www.bloomberg.com/news/articles/2018-05-29/cryptocurrency-attacks-are-rising-as-rouge-miners-exploit-flaw.

W. Bolt and M.R.C. Van Oordt. On the Value of Virtual Currencies. *Journal of Money, Credit and Banking*, 52(2):835–862, 2020.

E. Budish. The Economic Limits of Bitcoin and the Blockchain. *NBER Working Paper*, 24717, 2018.

J. Chiu and T.V. Koeppl. Blockchain-based Settlement for Asset Trading. *Review of Financial Studies*, 32(5):1716–1753, 2019a.

J. Chiu and T.V. Koeppl. The Economics of Cryptocurrencies: Bitcoin and Beyond. *Bank of Canada Staff Working Paper*, 2019-40, 2019b.

I. Choi. Unit Root Tests for Panel Data. *Journal of International Money and Finance*, 20 (2):249–272, 2001.

Coinbase. How Coinbase Views Proof of Work Security. Blog Post (8 November), 2019. URL https://blog.coinbase.com/how-coinbase-views-proof-of-work-security-f4ba1a139da0.

Coindesk. Bittrex to Delist Bitcoin Gold by Mid-September Following $18 Million Hack of BTG in May. News Report (4 September), 2018. URL https://cointelegraph.com/news/bittrex-to-delist-bitcoin-gold-by-mid-september-following-18-million-hack-of-btg-in-may.

L.W. Cong, Z. He, and N. Wang. Decentralized Mining in Centralized Pools. *Review of Financial Studies*, forthcoming.

D. Easley, M. O'Hara, and S. Basu. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics*, 134(1):91–109, 2019.

I. Eyal and E.G. Sirer. Majority is not Enough: Bitcoin Mining is Vulnerable. *Communications of the ACM*, 61(7):95–102, 2018.

N. Gandal and J.S. Gans. More (or Less) Economic Limits of the Blockchain. *NBER Working Paper*, 26534, 2019.

N. Gandal and H. Hałaburda. Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market. *Games*, 7(3):16, 2016.

R. Garratt and R. Hayes. Entry and Exit Leads to Zero Profit for Bitcoin Miners. *Liberty Street Economics*, August 2015. URL https://libertystreeteconomics.newyorkfed.org/2015/08/entry-and-exit-leads-to-zero-profit-for-bitcoin-miners.html.

R. Garratt and N. Wallace. Bitcoin 1, Bitcoin 2, ... : An Experiment on Privately Issued Outside Monies. *Economic Inquiry*, 56(3):1887–1897, 2018.

P.-O. Goffard. Fraud Risk Assessment within Blockchain Transactions. *Advances in Applied Probability*, 51(2):443–467, 2019.

H. Hałaburda and G. Haeringer. Bitcoin and Blockchain: What We Know and What Questions are Still Open. *Working Paper*, 2019.

G. Huberman, J. Leshno, and C.C. Moallemi. An Economic Analysis of the Bitcoin Payment System. *Columbia Business School Research Paper*, 17-92, 2019.

K.S. Im, M.H. Pesaran, and Y. Shin. Testing for Unit Roots in Heterogeneous Panels. *Journal of Econometrics*, 115(1):53–74, 2003.

F. Kroll, I. Davey, and E. Felten. The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries. *Princeton University Working Paper*, 2013.

I. Makarov and A. Schoar. Trading and Arbitrage in Cryptocurrency Markets. *Journal of Financial Economics*, 135(2):293–319, 2019.

E. Pagnotta and A. Buraschi. An Equilibrium Valuation of Bitcoin and Decentralized Network Assets. *Working Paper*, 2018.

J. Prat and B. Walter. An Equilibrium Model of the Market for Bitcoin Mining. *Working Paper*, 2019.

B. Rossi. Exchange Rate Predictability. *Journal of Economic Literature*, 51(4):1063–1119, 2013.

L. Schilling and H. Uhlig. Some Simple Bitcoin Economics. *Journal of Monetary Economics*, 106:16–26, 2019.

U.S. Department of Energy. Electric Power Monthly with Data for December 2019. *Statistical Report*, 2020.

P. Zimmerman. Blockchain Structure and Cryptocurrency Prices. *Bank of England Staff Working Paper*, 855, 2020.

Appendix A: Form to Calculate Profitability of Attack

This form calculates the minimum number of coins that attackers should be able to double spend in order for an attack to be profitable. The form is based on equation (9).

Cryptocurrency blockchain

Typical mining rewards per block, b (coins) 6.67

Normal block time (minutes) 10

Attack

Average duration of successful attack, t^* (block time) 100

Fraction of mining units participating, α 0.51

Projected drop in exchange rate, l (coins) 0.30

Mining equipment

Fixed cost of equipment, F (dollars) 2100

Alternative use value of equipment, V (dollars) 0

Annualized flow cost, ε (dollars) 1350

Annualized cost of capital, r 0.20

Profitable attack?

Only when attackers can double spend more coins than: 303070.05

Appendix B: Data

We collect data on the exchange rates, mining power and major changes in block rewards as prescribed by the mining protocol for all minable cryptocurrencies listed on coinmarketcap.com that satisfy the following criteria: (a) the cryptocurrency relies on proof-of-work to update the ledger, (b) data for the mining power and the exchange rate are available over a period of at least three years, (c) the algorithm to mine the cryptocurrency did not undergo any major changes and (d) the market capitalization exceeded 5 million USD on 2 January 2020. Table 4 reports the cryptocurrencies that we found satisfy these criteria.

Table 4: Data Sources

Cryptocurrency (Algorithm)	Observations	Source mining power	Source exchange rate
Larger cryptocurrencies:			
Bitcoin (SHA256)	2011M1-2019M10	charts.bitcoin.com/btc	charts.bitcoin.com/btc
Ethereum (Ethash)	2015M11-2019M10	bitinfocharts.com	bitinfocharts.com
Litecoin (Scrypt)	2012M10-2019M10	bitinfocharts.com	bitinfocharts.com
Monero (Cryptonight)	2014M9-2019M9	bitinfocharts.com	bitinfocharts.com
Dash (X11)	2014M5-2019M10	bitinfocharts.com	bitinfocharts.com
Smaller cryptocurrencies:			
Namecoin (SHA256)	2013M1-2019M10	bitinfocharts.com	bitinfocharts.com
Ethereum Classic (Ethash)	2016M11-2019M10	coinwarz.com	coingecko.com
Dogecoin (Scrypt)	2014M3-2019M10	bitinfocharts.com	bitinfocharts.com
Einsteinium (Scrypt)	2014M7-2019M10	coinwarz.com	coingecko.com
Bytecoin (Cryptonight)	2014M9-2019M10	bytecoins.world	coingecko.com

In total, our dataset contains ten proof-of-work cryptocurrencies, which rely on five different mining algorithms. The cryptocurrencies are split into two groups. The group with "larger cryptocurrencies" concerns the largest cryptocurrencies for each mining algorithm in terms of market capitalization. The "smaller cryptocurrencies" contains all the other cryptocurrencies. Table 5 reports the descriptive statistics of the observations used in the regressions for each of these two groups.

Panel unit root tests suggest that the levels of cryptocurrency exchange rates and the mining power are integrated with order one, while the first differences are stationary. Table 6 reports panel unit root tests. None of the panel unit root tests rejects the null hypothesis of a unit root in the levels in all panels versus the alternative of stationarity of the levels in one or some panels. The null hypothesis of a unit root in the first differences is strongly rejected by all tests. The application of the panel unit root tests based on Choi (2001) fits our dataset well, because we have a finite number of panels and a relatively long time dimension. The panel unit root test of Im et al. (2003) is reported because of its popularity, but its use is less appropriate in our context because it requires the number of panels to tend to infinity.

Table 5: Descriptive Statistics

VARIABLES	Mean	Sd	p10	p90	Obs
Larger cryptocurrencies					
Change in log mining power	0.465	0.729	-0.205	1.289	366
Change in log exchange rate	0.251	0.837	-0.646	1.242	366
Dummy change in block reward	0.090	0.287	0	0	366
Smaller cryptocurrencies					
Change in log mining power	0.377	0.869	-0.435	1.318	312
Change in log exchange rate	0.111	0.894	-0.837	1.305	312
Dummy change in block reward	0.147	0.355	0	1	312
Correlation between smaller and larger peers					
Dynamic correlation	0.501	0.310	0.060	0.860	312

Note: Changes in mining power and exchange rates are measured as quarterly log changes. Variables are measured at the end of each month. Exchange rates are measured in terms of US dollars. The dynamic return correlation is calculated as the Pearson correlation coefficient between the monthly log returns of small cryptocurrencies and the largest cryptocurrency that uses the same mining algorithm using a rolling window of five quarters.

Appendix C: Expectation-Based Mining Decisions

The results in this appendix show that the results reported in Table 2 are robust to the formation of expectations regarding the future exchange rate that are driven by the observation of historical peaks. To consider the expectation-based channel, assume that the mining power today is indeed driven by today's prediction of the future exchange rate rather than the current exchange rate. Let $\mathbb{E}_t(s_{it+1})$ denote the one-quarter-ahead expectation of the exchange rate at time t. Then the change in mining power would depend on the change in the expectations regarding the future exchange rate as

$$\Delta q_{it} = \beta_0 + \beta_1 \left[\mathbb{E}_t(s_{it+1}) - \mathbb{E}_{t-1}(s_{it})\right] + \beta_2 \Delta s_{it}^{MAX} + \mu_i D_{it} + u_{it}. \tag{15}$$

This expectation-based model differs from the original model in (10) in that it includes the change in the predicted exchange rate rather than the actual change in the exchange rate.

Table 6: Panel Unit Root Tests

Panel unit root test	Statistic	In levels: Value	p-value	In first differences: Value	p-value
Exchange rate (s_{it})					
Choi (PP; 3 lags)	P	19.457	0.492	381.58	0.000
Choi (PP; 3 lags)	Z	0.166	0.566	-17.850	0.000
Choi (ADF; 3 lags)	P	19.025	0.520	122.475	0.000
Choi (ADF; 3 lags)	Z	0.069	0.528	-8.734	0.000
IPS (AIC)	$W_{\bar{t}}$	-0.212	0.416	-20.120	0.000
IPS (BIC)	$W_{\bar{t}}$	0.194	0.577	-20.120	0.000
Mining Power (q_{it})					
Choi (PP; 3 lags)	P	9.163	0.981	329.321	0.000
Choi (PP; 3 lags)	Z	1.740	0.959	-16.139	0.000
Choi (ADF; 3 lags)	P	16.809	0.665	78.198	0.000
Choi (ADF; 3 lags)	Z	0.777	0.781	-6.172	0.000
IPS (AIC)	$W_{\bar{t}}$	1.327	0.908	-14.282	0.000
IPS (BIC)	$W_{\bar{t}}$	1.332	0.909	-16.815	0.000

Note: The Choi panel unit root test refers to Choi (2001) using either the Phillips-Perron test (PP) or the augmented Dickey-Fuller (ADF) test. The IPS panel unit root test refers to Im et al. (2003) using either the Akaike Information Criterion (AIC) or the Bayesian Information Criterion (BIC) for lag selection. All panel unit root tests allow for deterministic trends. The panel unit root tests test the null hypothesis of a unit root in all panels against the alternative of stationarity in one panel (Choi) or some panels (IPS).

If the exchange rate is believed to follow a random walk, then the expectation-based model in (15) is identical to the original model in (10) since a random walk implies $\mathbb{E}_t(s_{it+1}) - \mathbb{E}_{t-1}(s_{it}) = s_{it} - s_{it-1} = \Delta s_{it}$. Random walks are generally believed to provide a reasonable approximation of the behaviour of exchange rates (Rossi, 2013). Makarov and Schoar (2019) document the auto-correlations of cryptocurrency exchange rate returns to be small, even at high frequencies, which suggests that there is indeed little predictability in the market.

In contrast, if the exchange rate is not believed to follow a random walk, then rewriting (15) shows that the original model differs from the expectation-based model in that it omits the change in the expected appreciation, since $\mathbb{E}_t(s_{it+1}) - \mathbb{E}_{t-1}(s_{it}) = \Delta s_{it} + \mathbb{E}_t(\Delta s_{it+1}) - \mathbb{E}_{t-1}(\Delta s_{it})$. If miners were to believe that changes in the expected appreciation of the exchange rate, $\mathbb{E}_t(\Delta s_{it+1}) - \mathbb{E}_{t-1}(\Delta s_{it})$, are positively correlated to the changes in the historical peak in the exchange rate, Δs_{it}^{MAX}, then the omission of the change in the expected appreciation could result in observing a positive estimate for the coefficient for the peak level, i.e., β_2, when estimating the model in (10).

We use two different methods to rule out the possibility that the positive coefficient for the peak level in the exchange rate is driven by a positive correlation between the future exchange rate and the historical peak.

The first method uses an explicit model to predict the appreciation in the exchange rate based on the historical price peak. Suppose that miners use predictions based on the following model

$$\Delta s_{it+1} = \delta_0 + \delta_1 (s_{it}^{MAX}/s_{it}) + \varepsilon_{it}. \tag{16}$$

This model allows for more upward potential for the future exchange rate when its current level is further below its historical maximum when $\delta_1 > 0$. We estimate this prediction model in a first-stage regression. We use the estimated coefficients to do in-sample predictions for changes in the future exchange rate as $\Delta \hat{s}_{it+1} = d_0 + d_1 (s_{it}^{MAX}/s_{it})$. These model-based predictions are then used to construct the expected exchange rate appreciation as $\mathbb{E}_t(s_{it+1}) - \mathbb{E}_{t-1}(s_{it}) \approx \Delta s_{it} + \Delta \hat{s}_{it+1} - \Delta \hat{s}_{it}$. This series is then used in a second-stage regression to estimate the expectation-based model in equation (15).

The results from the first method indicate that the expectation-based channel does not explain our results. Table 7, panel (a) presents the results from the first-stage regression for the prediction model for the exchange rate in equation (16). The results suggest that a higher historical peak in the exchange rate is either uncorrelated with the future exchange rate or associated with a significantly lower future exchange rate (Ethereum). Table 7, panel (b) reports the results when we use the change in the prediction based on the first-stage regression as a regressor in Model (15). The coefficients and standard errors are in general very comparable to those in Table 2, which shows that the historical peak level continues to matter. The main difference in the table is observed for Ethereum for which the model estimates show that the historical peak in the exchange rate becomes more important in explaining mining power after accounting for its impact on the predicted exchange rate.

The second method controls for the expectations of miners regarding the future exchange rate by simply including the future change in the exchange rate as an additional regressor in the original model. Table 7, panel (c) shows the results when estimating this version of the expectation-based model. Controlling for the predictions of miners regarding the future exchange rate in this manner has very little impact on our results. The coefficients for the historical peak in the exchange rates have very comparable coefficients and standard errors as before, suggesting that our results are not driven by expectations regarding the future exchange rate.

Table 7: Empirical Mining Power and Predicted Exchange Rate

Panel (a): First-stage regression to predict the future exchange rate (Δs_{it+1})

VARIABLES	Bitcoin	Ethereum	Litecoin	Monero	Dash	Panel
Distance from historical	-0.290	-0.454***	0.019	-0.029	0.049	-0.036
peak (s_{it}^{MAX}/s_{it})	(0.309)	(0.040)	(0.058)	(0.045)	(0.083)	(0.026)
Constant	0.602	0.763***	0.204	0.228**	0.025	0.279***
	(0.396)	(0.108)	(0.201)	(0.088)	(0.205)	(0.032)
Observations	106	45	82	58	63	354
R-squared	0.013	0.223	0.001	0.019	0.003	0.005

Panel (b): Second-stage regression to explain mining power (Δq_{it})

VARIABLES	Bitcoin	Ethereum	Litecoin	Monero	Dash	Panel
Change in exchange rate	0.090	0.236***	0.051	0.046	0.554***	0.155
prediction ($\Delta s_{it} + \Delta\hat{s}_{it+1} - \Delta\hat{s}_{it}$)	(0.119)	(0.081)	(0.097)	(0.098)	(0.134)	(0.093)
Change in log	0.630***	0.325***	0.617***	0.691***	0.478	0.544***
peak level (Δs_{it}^{MAX})	(0.132)	(0.105)	(0.129)	(0.166)	(0.331)	(0.073)
Change in block	-0.287***	-0.265**	-0.419***		-0.784***	–
rewards (D_{it})	(0.094)	(0.102)	(0.117)		(0.214)	
Constant	0.376***	0.225***	0.303***	-0.039	0.527***	0.285***
	(0.055)	(0.056)	(0.054)	(0.055)	(0.110)	(0.011)
Observations	103	45	82	58	63	351
R-squared	0.460	0.685	0.600	0.437	0.377	0.449

Panel (c): Mining power (Δq_{it})

VARIABLES	Bitcoin	Ethereum	Litecoin	Monero	Dash	Panel
Future change in log	0.080	0.038	-0.091	-0.005	-0.018	-0.010
exchange rate (Δs_{it+1})	(0.099)	(0.037)	(0.065)	(0.071)	(0.149)	(0.039)
Change in log	0.072	0.204*	0.078	0.048	0.580***	0.164
exchange rate (Δs_{it})	(0.139)	(0.117)	(0.099)	(0.092)	(0.144)	(0.094)
Change in log	0.689***	0.287*	0.568***	0.685***	0.276	0.540***
peak level (Δs_{it}^{MAX})	(0.142)	(0.156)	(0.133)	(0.170)	(0.204)	(0.080)
Change in block	-0.346**	-0.259**	-0.283***		-0.760***	–
rewards (D_{it})	(0.139)	(0.106)	(0.105)		(0.195)	
Constant	0.363***	0.223***	0.360***	-0.035	0.550***	0.304***
	(0.047)	(0.059)	(0.056)	(0.063)	(0.123)	(0.020)
Observations	106	45	82	58	63	354
R-squared	0.489	0.638	0.577	0.421	0.463	0.472

Note: All changes are quarterly log changes. Exchange rates are measured in terms of US dollars. Variables are measured at the end of each month. The output for the panel regressions in panels (b) and (c) suppress the estimated coefficients for the dummy variables for the change in block rewards for each of the different cryptocurrencies. All models are estimated with least squares. Robust standard errors are reported in parentheses. The panel models are estimated with fixed effects to allow for cryptocurrency-specific time trends. Statistical significance at the 1%, 5% and 10% significance levels are indicated by ***, ** and *, respectively.