The empirical analysis of Bitcoin market in the general equilibrium framework *

Jun Aoyagi †

Takahiro Hattori‡

July 31, 2019

Abstract

This paper firstly pursues the fundamental price of Bitcoin in the general equilibrium framework and its empirical characteristics. Our theoretical model predicts that (i) the Bitcoin price and the total hash rate are determined simultaneously in the long-run and (ii) the hash rate of Bitcoin Granger-causes Bitcoin prices in the short-run. Using a cointegration framework, our empirical analysis provides consistent results with these theoretical predictions. Our empirical results suggest that the Bitcoin market has been under a fundamental value instead of speculative bubbles.

JEL classification: E43, G18, G28, H12.

Keywords: cryptocurrency, asymmetric information, arbitrage, cointegration.

---

*We thank Christine Parlour for the helpful comments. The views expressed in this paper are those of the author and not those of the Ministry of Finance or the Policy Research Institute. All remaining errors are our own. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

†Department of Economics, University of California at Berkeley. jun.aoyagi@berkeley.edu.

‡Ministry of Finance, Japan. hattori0819@gmail.com. 3-1-1 Kasumigaseki Chiyoda-ku Tokyo Japan.

1 Introduction

The explosive increase in price and market cap of Bitcoin and blockchain technology is controversial. As Hu et al. (2018) document, the returns and volatilities of cryptocurrency are high, although the substantial related media coverage makes some people skeptical about the cryptocurrency and even about the functionality of the blockchain system. The frequent ups and downs of the cryptocurrency price are often described as "bubbles," which means that the price is driven by some non-fundamental factors, and no factors can be tied to the cryptocurrency price by the *arbitrage* relationship. Several empirical works, such as Cheah and Fry (2015), Su et al. (2018), and Fry (2018), have analyzed cryptocurrency prices series to show their bubble-like features.

In contrast to the opinions of the general public, as well as some empirical works, several theoretical studies indicate the existence of a fundamental value in the cryptocurrency price (Aoyagi and Adachi, 2018; Cong et al., 2018; Chiu and Koeppl, 2019). This could be a strictly positive value because it works as a means of transaction in blockchain-based platforms, and people seek to use them because the platforms provide some specific service that users can enjoy.

This paper contributes to the literature both theoretically and empirically. We introduce a dynamic general equilibrium (GE) model to determine the fundamental price of Bitcoin, and show that the total hash rate should be a factor to Bitcoin prices. Figure 1 describes the long-run relationship between Bitcoin price and the total hash rate, indicating that there has been a clear and tight relationship among them. In light of this, our GE framework shows that these two variables must be determined simultaneously and strongly tied to each other in the *long-run*. Moreover, in a higher-frequency time frame, the total hash rate has Granger-causality on Bitcoin prices. To test this relationship, we empirically show the existence of a sufficient arbitrage between these variables by using the cointegration framework. In addition, we find the total hash rate of Bitcoin Granger-causes Bitcoin prices.

In our theoretical part, a specific function of the blockchain-based transaction is attributed to its ability to mitigate asymmetric information between traders (Aoyagi and

Adachi, 2018; Cong and He, 2019) . One of the most widely known examples of the asymmetric information in digital currency network is a ”double spending” problem, i.e., one can forge her past payment information so that she can use her digital currency twice or more (Chiu and Koeppl, 2019). This problem implies that, even if a trader pays dollars to get Bitcoin, she cannot receive it in exchange because her trading counterpart has fraudulent information on his ledger.

Bitcoin and blockchain tackle with this problem through the distributed ledger system (DLS) and the competition between blockchain miners (record keepers). This is a salient difference from the existing digital currency, in which a centralized authority (e.g., a bank) keeps track of transaction information.

Blockchain miners competitively keep track of the record of transactions by supplying computing power—i.e., “hash rate”—to generate a consensus regarding every traders’ state information. This consensus works as a signal for traders who suffer from information asymmetry, which provides an incentive to use blockchain as a trading method.

The miners are incentivized to leverage their hash rate by a monetary reward paid in cryptocurrency. Thus, a fluctuation in the cryptocurrency price influences the miners’ incentive to act as miners and changes the configuration of miners’ competition, which leads to a different quality of consensus information. Our model formulates this relationship: i.e., at the equilibrium, the aggregate hash rate is a function of cryptocurrency price. This equilibrium illustrates the miners’ incentive structure, which we call the *miner-side partial equilibrium*.

However, traders have an incentive to exploit the signal generated by the blockchain to resolve the double-spending risk. Naturally, the higher the quality (precision) of the blockchain consensus, the more traders are willing to use it. This derives a larger demand for the cryptocurrency and has a positive pressure on the cryptocurrency price. That is, the *trader-side partial equilibrium* generates another relationship between the cryptocurrency price and the quality of the blockchain consensus (or, equivalently, the total hash rate).

GE framework yields two equations that relate the total hash rate to the cryptocurrency price via the interaction of the miner-side and trader-side partial equilibria. The GE boils down to a fixed point problem that determines the aforementioned variables *simultaneously*. One of the most obvious implications of this equilibrium characterization is the existence of long-run cointegration relationship between the Bitcoin price and the total hash rate, i.e., the total hash rate can be a candidate for a long-run arbitrage factor to the Bitcoin price.

Empirically, a large body of literature pursues the econometric tests for asset price bubbles and arbitrage relationships.[1] For example, by exploiting the cointegration framework, Diba and Grossman (1988) and Bhargava (1986) find dividends and stock prices are cointegrated in level, concluding that there are no bubbles.[2] Instead of rational bubbles, intrinsic bubbles are driven exclusively by the fundamentals in non-linear way, which is firstly proposed by Froot and Obstfeld (1991). An intrinsic bubble insists on nonlinear relationship between stock prices and dividends, which is tested by Ma and Kanas (2004) by using nonlinear cointegration. Chen et al. (2009) empirically evaluate whether the asset price is under a bubble by cointegration and Granger causality test.

We follow these works empirically and analyze the validity of our model's prediction in the cointegration framework, i.e., a long run arbitrage relationship between the total hash rate and the Bitcoin price. Our empirical results show the existence of cointegration between these variables and indicate that they have some common stationary linkage in the long-run. In practice, this result implies that investing in Bitcoin using the total hash rate as a factor is reasonable, as suggested by some real-world investment strategies. Moreover, the cointegration requires the high-frequency vector auto regression (VAR) to correct deviations from this long-run relationship. We incorporate this result and show that the total hash rate at t Granger-causes the Bitcoin price at $t+1$ in the short run.

Our contribution to the literature can be divided into two parts. First, this paper explicitly provides a theoretical model that generates empirical predictions, which is still quite rare in academic works on Bitcoin. An explosive number of papers about Bitcoin have emerged in the recent literature, although most of them only focus on either theoretical work or empirical analysis. Our paper fills this gap between theoretical and empirical

[1]See the survey paper Gürkaynak (2008) for details.

[2]Evans (1991) criticize these tests.

works, which is necessary in this field. Second, our paper follows the empirical methods proposed by the previous literature on asset pricing and bubbles. We extend these methods to the cryptocurrency market and provide evidence that Bitcoin is under the fundamental price, which is a surprising fact about the Bitcoin market.

Theoretically, our paper also contributes to the literature that investigates the general equilibrium implications of the blockchain economics, such as Abadi and Brunnermeier (2018), Chiu and Koeppl (2018), Pagnotta and Buraschi (2018), Aoyagi and Adachi (2018) and Easley et al. (2019). Our model differs from most of the literature because the effect of miners' behavior on the traders' incentive is decomposed into the endogenous positive network and negative congestion effects. In addition, we introduce an endogenous reconfiguration of settlement risk (Kurlat, 2013) by the platform choice of traders. These ingredients contribute to the non-monotonic fundamental equations of the cryptocurrency price, which provides rich implications.[3]

The remainder of this paper is organized as follows. Section 2 explains the overview of Bitcoin and Blockchain Technology. Section 3 specifies empirical hypotheses with the economics models. Section 4 demonstrates the empirical result using cointegration. Section 5 concludes.

2 Overview of Bitcoin and Blockchain Technology

The viability of digital currencies has been exposed to the risk of counterfeiting. Digital records are easily forged and manipulated, encouraging users to copy and re-use the digital currencies—what is called a "double spending" problem.

Traditional paper-based cash or coins can easily deal with this problem because a piece of paper cannot physically be in Alice's wallet if it is in Bob's pocket. Also, technological development, such as esoteric inks and holographic strips, makes it hard to forge physical currencies.

In contrasts, digital currencies before the advent of Bitcoin deals with the risk of double

[3] An exception is Aoyagi and Adachi (2018), on which we construct our theoretical part.

spending by relying on a trusted and centralized record-keeping authority (e.g., a bank). However, as the record is stored by a centralized agency, it is easily attacked and hacked by potential antagonists. Thus, the robustness of the settlement and the credibility of a centralized authority have been a primary concern of their users.

The blockchain's approach to the double spending problem differentiates itself from the existing digital currencies; The key innovation is the distributed ledger system (DLS) and its algorithm that translates the competition between decentralized record keepers to the consensus record, called the Proof-of-Work (PoW).

Distributed Ledger System and Blockchain

Instead of a centralized record keeper, the blockchain's DLS publicly distributes transaction information to a number of nodes in the blockchain network. Each node is operated by a record keeper called "miner" who tries to validate each transaction information. The validation process involves a solution of a cryptographic problem, and solving a problem requires miners to leverage computing power, called the "hash power".

Every single information about transactions on the blockchain is stored in a pool of unvalidated transaction records (called the "transaction pool"). In each round of PoW, the miners pick one of the unvalidated transaction information from the pool and competitively leverage their hash rate to be the first miner to get the solution of cryptgraphic problem. If a miner gets to be the first miner, she publishes the transaction toward the network and other nodes agree on it, thereby making it the consensus transaction record. This information is then recorded in a digital wallet (ledger) of traders.

The incentive of miners is sustained by a monetary reward, i.e., if a miner becomes the first validator, she obtains a reward. Importantly, this reward is paid in cryptocurrency (e.g., Bitcoin). Because of this structure, the cryptocurrency price directly affects the incentive of miners, from which we can derive the miner-side relationship between the cryptocurrency price and total hash supply.

As the wallet's information is managed by the multiple nodes in DLS, failure in a part of computers, potentially by hackers, does not cause a problem. Also, the competitive algorithm makes it almost impossible for a single malicious miner to forge the wallet, as it requires her to outperform all the other computers in the network.

Once a set of transaction information is validated, it is stored in a *block*. A block includes encrypted information of past blocks, thereby dynamically connecting the series of blocks—a *blockchain*. Due to this dynamic nature, rewriting a piece of information in block-t causes changes in all the subsequent blocks ($t+1, t+2, \cdots$). Once again, overturning the consensus takes a huge computational cost, meaning that the record on the blockchain is almost immutable.

Bridging a lift to the theoretical part

In general, having a sufficiently positive amount of currency in a wallet (or digital ledger) is a necessarily condition for traders to make a transaction. For example, even if Alice tries to use her debit card for grocery shopping, the card will be declined (or transaction will be rejected) if her bank account does not have a sufficient balance. In other words, if a card is accepted and transaction is executed, these facts should convey a signal that Alice has a sufficient balance, and the payment will be transferred to the grocery store's bank account. However, the double spending problem risks the grocery store, as the information about Alice's account can be manipulated—she rewrites insufficient balance as if it has a sufficient amount—and the payment will not be transferred after the delivery of goods.

We use $s \in \{0,1\}$ to indicate the true state of a payer (Alice) which is her *private information*: $s = 1$ indicates a payer actually has a sufficient amount of balance. She obviously tries to write $s = 1$ in her digital ledger because it may allow her to obtain goods even if she has no balance ($s = 0$).

A transaction system (e.g., Bitcoin's blockchain, debit card agencies, and so on) is operated by record keeper(s) who tries to validate users' private s. In the blockchain system, this is operated by miners, while, in the traditional system, it is played by a centralized record keeper (e.g., banks). They provide balance information $\hat{s} \in \{0,1\}$ after the validation of true s.

Conditional on a payer has a sufficient amount of value on her digital ledger, $\hat{s} = 1$, transaction is consummated. As such, the fact that a transaction is executed implies to a receiver (a grocery store) that her counterpart (Alice) has $\hat{s} = 1$. The problem is that this signal is not 100% accurate due to the incentive problem of the record keeper(s). In the following model, we show that (i) the miners' hash supply determines the credibility of the blockchain's information, $\hat{s}$, and how it is affected by the cryptocurrency price. As well, (ii) traders' transaction demand via the blockchain system critically depends on this credibility, thereby generating the interaction between the traders' and miners' behavior.

3 The Model

This section provides a theoretical framework and derives hypothesis on the relationship between the cryptocurrency price and total hash rate in blockchain.

Consider an infinite horizon economy with two sets of agents: the blockchain miners and the traders. Both types of agents live two periods and constitute overlapping generations (young and old). The traders are uniformely distributed in $[0, 1]$, while the miners are in set $\mathcal{M}$ with a finite measure. All agents are risk neutral.

3.1 The Traders' Behavior

Each young trader is endowed with cash (dollars) and invests in the cryptocurrency (Bitcoin) at price p_t. When she is old, she sells her Bitcoin holding at price p_{t+1}, consumes the return, and exits from the market. We also assume that each young trader derives stochastic private utility β from the Bitcoin holding, where β follows $U[0, 1]$. Following the literature on market microstructure (Glosten and Milgrom, 1985), assume that the traders can hold at most one unit of Bitcoin and cannot shortsell. Also, for the sake of simplicity, suppose that there is no saving facility other than the Bitcoin.

3.1.1 Young Traders' Behavior and Demand for Bitcoin

By letting $x_t \in [0,1]$ be the investment in the Bitcoin, a young trader at t with β maximizes the following:

$$V_t(\beta) = \max_{x_t \in [0,1]} (p_{t+1} + \beta)\mathbb{E}[\tilde{x}_{t+1}] - p_t x_t.$$

First, there is no uncertainty in the price dynamics. However, the holding of Bitcoin in the next period, $\tilde{x}_{t+1}$, is stochastic for the current young traders. This is because of the "double spending" problem: even though a young trader invests x_t by paying the price p_t, the Bitcoin may not be delivered to her because her trading partner (an old trader as a seller) can manipulate his wallet information to double spend.

Suppose that π_t^θ denotes endogenous probability that an old seller is an authentic seller, i.e., not a double spender. Then, we have

$$\tilde{x}_{t+1} = \begin{cases} x_t & \text{with } \pi_t^\theta \\ 0 & \text{otherwise.} \end{cases}$$

Namely, even if a young trader buys x_t of Bitcoin at p_t, it is not delivered, and she cannot sell and consume it in the next period.

Then, the optimization problem of young traders generates a threshold private value that differentiates the set of young traders into buyers and inactive young traders. In the following, we focus on an interior solution for the threshold:

Proposition 1. *There exists a threshold β_t, and the optimal investment is given by*

$$x_t(\beta) = \begin{cases} 1 & \text{if } \beta > \beta_t \\ 0 & \text{if } \beta \leq \beta_t, \end{cases} \tag{1}$$

where

$$\beta_t = \frac{q_t}{\pi_t^\theta} - q_{t+1}.$$

From this behavior of young agents, we can derive the aggregate demand function for the Bitcoin as follows:

$$D_t = \int_0^1 x_t(\beta)d\beta = 1 - \beta_t.$$

Note that, within this $1-\beta_t$ of young traders, only π_t^θ fraction of them finally obtain the Bitcoin due to the double spending. This implies that the measure of the old traders who hold the Bitcoin at the begening of date $t+1$ is given by

$$\pi_t^\theta(1-\beta_t). \tag{2}$$

3.1.2 Old Traders' Behavior and Bitcoin Supply

When the traders get old, they sell their Bitcoin holding to get cash return p_{t+1}. Importantly, an old trader can claim that she has Bitcoin so that she obtains payment p_{t+1} from young traders without actually deliverying the Bitcoin, i.e., by double spending. However, because of the record keeping by the blockchain miners, this attempt is fullfilled only with probability $1-\theta_t$. Put differently, an old trader who attempts to double-spend is declined with probability θ_t. This θ_t is derived as an endogenous variable in the later section.

As the cost of double spending is zero in our model, all of the old traders with no Bitcoin holding attempt to double-spend. As a result of (1) and (2), the measure of authentic sellers at date t—those who actually hold the Bitcoin—is given by $\pi_{t-1}^\theta(1-\beta_{t-1})$. The rest of the old suppliers with measure $1-\pi_{t-1}^\theta(1-\beta_{t-1})$ are double spenders.

Similarly, the aggregate supply attempts of the Bitcoin from the old traders at date t is given by

$$S_t = \pi_{t-1}^\theta(1-\beta_{t-1}) + (1-\theta_t)[1-\pi_{t-1}^\theta(1-\beta_{t-1})] \tag{3}$$

where, as mentioned eariler, θ_t is the detection of double spending by the blockchain miners. It must be underlined that S_t only represents the supply from the old traders: a miner who obtains a Bitcoin reward also tries to sell it. We denote this supply at date t from a miner as B_{t-1} which is defined later.

By using this formula, we can derive the endogenous probability of authentic sellers π_t^θ as follows:

Proposition 2. *At date t, the share of authentic sellers after the screening by the Bitcoin blockahin (θ_t) is given by*

$$\pi_t^\theta = \frac{\pi_{t-1}^\theta(1-\beta_{t-1}) + B_{t-1}}{1-\theta_t+\theta_t\pi_{t-1}^\theta\beta_{t-1}+B_{t-1}} \tag{4}$$

where B is the Bitcoin supply from the miners.

We call this probability of the authentic sellers the "quality" of the Bitcoin market. This dynamic equation implies that the quality at date t is positively affected by the previous quality at date $t-1$ with other variables fixed. This is because a larger share of the authentic sellers in the previous period makes the inter-generations flow of the Bitcoin larger, thereby mitigating the risk of double-spending.

3.2 The Miners' Behavior

Next, we analyze the miners' behavior that competitively determines θ as a function of the cryptocurrency price p. In this subsection, we give each old trader an index β for the notational convenience, and we call them "suppliers."

At date t, each supplier's state before she makes a transaction is either holding the Bitcoin or not. This state is given by the realization of $\tilde{x}$:

$$s_t \equiv \tilde{x}_t = \begin{cases} 1 & \text{with } \pi_{t-1}^\theta \text{ and } x_{t-1}=1 \\ 0 & \text{o/w.} \end{cases}.$$

That is, state $s_t = 1$ for an old trader at t implies that she purchased the Bitcoin when she was young, and she gets to avoid the double spenders, i.e., she gets to become an authentic supplier.

There is a transaction pool, $\mathcal{P}$, that stores the state information of traders who intend to trade via the blockchain. Since the state of suppliers is the only source of asymmetric information, the blockchain (miners) tries to track s of every supplier. Therefore, we define $\mathcal{P}_t \equiv \{s_t(\beta)|\beta \in [0,1]\}$.

Every $s_t(\beta) \in \mathcal{P}_t$ is validated by the young miners via the consensus algorithm hardwired in the DLS (defined later), and the consensus is issued as the wallet information $\hat{s}_t(\beta)$. Contingent on the consensus, transaction-β is executed if, and only if, the wallet information states $\hat{s}_t(\beta) = 1$. Otherwise, it is declined.

3.2.1 Miners' Decision Making

The young miners' problem at date t consists of three steps: (i) participation decision, (ii) hash rate decision, and (iii) subsequent reporting decision. At step (i), each miner, indexed by i, decides whether to act as a miner by paying a fixed cost C. This corresponds to a set-up cost of a specific computer or the cost of purchasing a computer chip, such as ASIC.[4] Once a miner sets up her computer, she decides how intensively leverage her computing power at step (ii), i.e., she determines her hash rate, $\lambda_{t,i}$. It takes a convex variable cost $\frac{\tau}{2}\lambda^2$, and we interpret this as an electricity cost. At step (iii), we suppose that each miner can observe true $s_t(\beta)$ in $\mathcal{P}$. Then, she submits her report on her observation, denoted by $\hat{s}_{t,i}(\beta) \in \{0, 1\}$, to obtain a reward. This behavior at step (iii) amounts to the mining behavior in PoW.

3.2.2 The Wallet Information and Reward

Hereafter, we focus on transaction-β and discuss how the consensus on $s_t(\beta)$ is generated. So, we omit the index, β, from $s_t(\beta)$, unless otherwise noted.

Upon reviewing the miners' behavior at step (iii), the blockchain algorithm randomly picks one of the reports from the set $\{\hat{s}_{t,i}\}_{i\in\mathcal{A}}$, where $\mathcal{A} \subset \mathcal{M}$ represents a set of *active* miners determined at step (i). The selected report $\hat{s}_{t,i}$ is declared as the *blockchain consensus* $\hat{s}_t$, i.e., $\hat{s}_t = \hat{s}_{t,i}$, and published as the wallet information of supplier-β.

In the consensus generating process, miner i's report ($\hat{s}_{t,i}$) is selected as the consensus with probability proportional to her hash rate:

$$\Pr(\hat{s}_t = \hat{s}_{t,i}) = \frac{\lambda_{t,i}}{\Lambda_t} \equiv w_{t,i}, \tag{5}$$

[4] The assumption that the participation cost is sunk is reasonable because, as of May 2019, the fastest computing chip is ASIC, which is not a general purpose device and cannot be reused for other activity than mining. See Budish (2018) and Hashimoto and Noda (2019) for more details.

where $\Lambda \equiv \sum_{j\in\mathcal{A}} \lambda_j$ is the total hash rate. Also, since $\hat{s}_{t,i}$ takes only zero or one, we have the following unconditional probability:

$$\Pr(\hat{s}_t = 1) = \mathbb{E}[\hat{s}_t] = \sum_{i\in\mathcal{A}_t} w_{t,i}\hat{s}_{t,i}. \tag{6}$$

If $\hat{s}_{t,i}$ is selected as a consensus, miner i obtains the *reward*, B_t, where B_t denotes the quantity of cryptocurrency per reward at date t. This constitutes the economy-wide supply of the Bitcoin. We suppose that B_t evolves as follows:

$$B_{t+1} = \frac{B_t}{1+g} \tag{7}$$

where $g \in (0,1)$ denotes the rate of shrinkage of Bitcoin supply.[5]

3.2.3 Step (iii): Reporting Decision

We consider the problem of miners by taking steps backward. At step (iii), given that a miner is active, she has an incentive to misreport (Cong and He, 2018). One of the reasons is the overlapping communities of traders and miners: since the liquidity takers will purchase the cryptocurrency from supplier-β if and only if $\hat{s}_t = 1$, the supplier-β has an incentive to make the consensus $\hat{s}_t = 1$ even if the true state is $s_t = 0$. This is "double spending" in the Bitcoin network. To accomplish this, a part of suppliers with $s_t = 0$ may participate as miners and misreport that $\hat{s}_{i,t} = 1$.

Following Cong and He (2018), we incorporate this incentive by giving the miners a positive private utility $\sigma > 0$ of executing transactions, while misreporting takes some random reputational costs c_i. Then, miners at step (iii) obtain the following utility:

$$U(\hat{s}_{t,i}; \hat{s}_t, s_t) = \sigma \mathbb{I}_{\{\hat{s}_t=1\}} - c_i|\hat{s}_{t,i} - s_t|.$$

[5]As of May 2019, Bitcoin blockchain has a deterministic supply at $B_s = 25$BTC. However, due to the structure of Bitcoin supply is deflationary, meaning that the supply amount does down over time. Even though its time path is a step function, we approximate it by assume that it depreciates every period by rate g.

We assume that the reputational cost c_i follows the uniform distribution $U[0,1]$ and realizes after the participation and hash decisions are made.

Then, miner i decides her report by $\hat{s}_{t,i} = \arg\max_{\tilde{s}\in\{0,1\}} \mathbb{E}[U(\tilde{s};\hat{s}_t, s_t)|s_t, \tilde{s}, c_i]$. By using (6), the optimal reporting behavior is summarized as follows:

$$\hat{s}_{t,i} = \begin{cases} 1 & \text{if } s_t = 1 \text{ or } "s_t = 0 \text{ and } c_i < \sigma w_i" \\ 0 & \text{otherwise .} \end{cases} \tag{8}$$

This shows that a miner who observes $s_t = 0$ provides a fraudulent information ($\hat{s}_{t,i} = 1$) if the return from this behavior is higher than the cost of it, $c_i < \sigma w_i$.

From (8), we can derive $\theta_t \equiv 1 - \Pr(\hat{s}_t = 1|s_t = 0)$:

$$1 - \theta_t = \sum_{i\in\mathcal{A}} w_i \Pr(c_i < \sigma w_i) = \sum_{i\in\mathcal{A}} \sigma w_i^2. \tag{9}$$

3.2.4 Steps (i) and (ii): Hash Rate and Participation Decision

In addition to the private utility in step (iii), a miner gets rewarded if she becomes *the* miner who generates the consensus. Importantly, the reward is paid in cryptocurrency with dollar price p, but the miner gets to exchange it to cash with a certain time lag, i.e., k-blocks rule (Biais et al., 2018). For the sake of tractability, we assume that the miner can use her reward with one-period time lag: the rewarded young miner at t can use it at date $t+1$ when she is old. This gives her dollar return $p_{t+1}B_t$. After consuming it, old miners exit.

Thus, given U in step (iii), the *ex-ante* expected utility is given by the following, where we make the index β explicit:

$$W_{t,i} = \max_{\lambda_{t,i}} \int_\beta \mathbb{E}\left[p_{t+1}B\mathbb{I}_{t\{\hat{s}_t(\beta)=s_{t,i}(\beta)\}} + \mathbb{E}[U(\hat{s}_{t,i}(\beta);\hat{s}_t(\beta), s_t(\beta))|s_t(\beta), \hat{s}_{t,i}(\beta)]\right] dG_t(\beta, s(\beta)) - L(\lambda_{t,i}) \tag{10}$$

where the first integral is over transaction β that has cumulative joint measure G (defined later), the expectation is on $\hat{s}_t(\beta)$ and $s_t(\beta)$, and $L(\lambda) = C + \frac{\tau}{2}\lambda^2$ represents the total cost of operation. We denote the p.d.f. of G as g.

The *ex-ante* value of being a miner is an aggregation over each transaction-β for $\beta \in [0,1]$, as (10) shows. As we consider a continuum of traders, this can be calculated by using the LLN: specifically, $g_t(\beta, 1)$ denotes the probability measure of the authentic suppliers at date t and $g_t(\beta, 0)$ is those for the flaudulant suppliers at t. From the behavior of the suppliers, we have

$$g_t(\beta, s) = \begin{cases} \pi^{\theta}_{t-1}(1-\beta_{t-1}) + B_{t-1} & \text{if } s = 1 \\ 1 - \pi^{\theta}_{t-1}(1-\beta_{t-1}) & \text{if } s = 0. \end{cases} \tag{11}$$

Let $g_t \equiv g_t(\beta, 1)$ and $\bar{g}_t \equiv 1 + B_{t-1} - g_t$. Then, (10) reduces to

$$W_{t,i} = \max_{\lambda_{t,i}} \left[p_{t+1} B_t \frac{\lambda_{t,i}}{\Lambda_t} + g_t \sigma + \bar{g}_t \sigma^2 \frac{\sum \lambda_i^2 - \frac{1}{2}\lambda_i^2}{\Lambda^2} - L(\lambda_{t,i}) \right].$$

A young miner decides her hash power $\lambda_{t,i} = \lambda_t^*$ to maximize $W_{t,i}$. By letting n_t be the equilibrium measure of active miners at date t, the FOC at the symmetric equilibrium ($\lambda_{t,i} = \lambda_{t,j} = \lambda_t^*$) gives the optimal hash rate in step (ii) as follows:

$$\lambda_t^* = \sqrt{\frac{p_{t+1} B_t \frac{1}{n_t} + \bar{g}_t \sigma^2 \frac{1}{n_t^2}}{\tau}}. \tag{12}$$

As well, the total hash rate is

$$\Lambda_t^* = \sqrt{\frac{p_{t+1} B_t n_t + \bar{g}_t \sigma^2}{\tau}}. \tag{13}$$

Finally, to solve the participation decision, we exploit a free-entry assumption which captures the mining sector in the real world. As in Glosten and Milgrom (1985), Budish (2018), and Easley et al. (2019), the free-entry condition makes all the miners indifferent between participating and not *ex-ante*, i.e., $W_{t,i} = 0$. This determines the set of active miners, $\mathcal{A}_t$.

Without loss of generality, we assume that the first n_t miners are active, i.e., $\mathcal{A} = \{1, 2, \cdots, n\}$.

This makes $w = n^{-1}$, and the *ex-ante* expected utility, after incorporating λ^*, is reduced to

$$W_{t,i} = g_t\sigma + \bar{g}_t\sigma^2\frac{n_t - 1}{n_t} - C + \frac{1}{2}p_{t+1}B_t\frac{1}{n_t}.$$

With the break-even condition, we can derive the price of cryptocurrency as a function of n:

$$p_{t+1}B_t = 2[(C - g_t\sigma + \bar{g}_t\sigma^2)n_t - \bar{g}_t\sigma^2]. \tag{14}$$

3.2.5 The Precision of the Wallet Information

The above argument allows us to determine the ex-post quality of the blockchain transactions, π_t^θ, as a function of Λ and p. Since every transaction with $\hat{s} = 0$ is declined, the ex-post probability that the cryptocurrency is delivered is calculated. Specifically, (9) and $w = n^{-1}$ yield

$$\theta_t = 1 - \frac{\sigma}{n_t}. \tag{15}$$

Hence, we have

$$\begin{aligned} \pi_t &\equiv \frac{\Pr(\hat{s}_t(\beta) = 1|s_t(\beta) = 1)}{\Pr(\hat{s}_t(\beta) = 1|s_t(\beta) = 1) + \Pr(\hat{s}_t(\beta) = 1|s_t(\beta) = 0)} \\ &= \frac{g_t(\beta, 1)}{g_t(\beta, 1) + g_t(\beta, 0)\frac{\sigma}{n}}. \end{aligned} \tag{16}$$

Note that plugging g in the above equation gives (4). Thus, this discussion serves as a micro-foundation of the ”rejection” and quality in the previous subsection.

4 The Blockchain General Equilibrium

Now, we define the blockchain general equilibrium (BGE) to specify the blockchain-related variables at the general equilibrium.

Definition 1. *Given the initial condition, the blockchain general equilibrium is defined by the sequences of Bitcoin price, $\{p_t\}_{t\geq0}$, the total hash rate, $\{\Lambda_t\}_{t\geq0}$, the measure of young buyers, $\{\beta_t\}_{t\geq0}$, the probability of rejection, $\{\theta_t\}_{t\geq0}$, the quality of the market, $\{\pi_t^\theta\}_{t\geq0}$, and the sequence* *of Bitcoin supply, $\{B_t\}_{t\geq 0}$, such that they satisfy (i) the optimization problems of traders and the miners, defined by (1), (13), and (14), respectively, and (ii) clear the market, i.e., $D_t = S_t + B_{t-1}$ for all t.*

4.1 The Equilibrium Dynamics of the Bitcoin Market

First, the market clearing condition is given by

$$\beta_t = \theta_t \pi^\theta_{t-1}\beta_{t-1} + \theta_t(1 - \pi^\theta_{t-1}) - B_{t-1}. \tag{17}$$

Given the quality of the market, π^θ, and the precision of the wallet information, θ_t, this equations describes the dynamics of the active young traders, $1 - \beta_t$. As long as B is small, which is true for a sufficiently large t, the dynamics of β_t has a unique steady state (SS).

Interestingly, the direct impact of θ on the measure of active young buyers, $1 - \beta$, is negative, i.e., the more precise the wallet information becomes, the less traders participate as Bitcoin buyers. This counter-intuitive result is because of the negative impact of θ on the supply amount. As θ increases, the rejection of double-spenders increases, thereby reducing the total supply of the Bitcoin. Because the market has to clear, this reduces the number of active young buyers.

Moreover, by using the definition of π^θ_t and β_t, we obtain a set of dynamic equations that specify the trader-side partial equilibria (TPE) as follows:

$$p_{t+1} = \frac{p_t}{\pi^\theta_t} - \beta_t, \tag{18}$$

$$\pi^\theta_t = \frac{\pi^\theta_{t-1}(1 - \beta_{t-1}) + B_{t-1}}{1 - \theta_t + \theta_t \pi^\theta_{t-1}\beta_{t-1} + B_{t-1}}. \tag{19}$$

These two equations derive the dynamics of the equilibrium price of Bitcoin, p_t, and the quality of the Bitcoin market, π^θ.

If θ_t and B_t are fixed, the dynamics of the economy is fully described by these threee equations with three control variables (p, β, π^θ). Specifically, by letting $\theta_t = \theta$ and $B_t = 0$

for all t,[6] (17) and (19) jointly determines (β_t, π_t^θ), and it feeds into (18) to pin down p_t. Clearly, linearlizing the system generates VAR representations.

However, to determine the full equilibrium, we need the miner-side equation that pins down the value of θ_t: from (14) and (15), we have

$$\begin{aligned} p_{t+1}B_t =& 2\left\{C - \sigma\left[\pi_{t-1}^\theta(1-\beta_{t-1}) + B_{t-1}\right] + \left[1 - \pi_{t-1}^\theta(1-\beta_{t-1})\right]\sigma^2\right\}\frac{\sigma}{1-\theta_t} \\ & - 2[1-\pi_{t-1}^\theta(1-\beta_{t-1})]\sigma^2. \end{aligned} \tag{20}$$

Note that, together with the dynamic equation for the Bitcoin supply in (7), we have five dynamic equations with regard to five equilibrium variables, $\{p_t, \beta_t, \pi_t^\theta, \theta_t, B_t\}$. Therefore, we can solve for the equilibrium.

4.2 Steady State Analyses

This subsection derives the long-run steady state (SS) of the dynamic system. Specifically, we consider $t \to \infty$, and a variable X_t at the SS is denoted without time index, X. Notably, from (7), the supply amount of the Bitcoin (i.e., the amount of the reward) shrinks over time and converges to 0. Thus, we impose $B = \lim_{t\to 0} B_t = 0$.

Proposition 3. *(i) There exists at least one steady state if, and only if, $\underline{C} < C < \bar{C}$. (ii) At the steady state $\beta = \frac{1}{2}$ and $\theta \in (\frac{1}{2}, 1)$. (iii) The price and precision are determined as a solution of the following two equations:*

$$p^T = \frac{1}{2}\frac{2\theta - 1}{1-\theta}, \tag{21}$$

$$p^M = \frac{1 - \frac{\sigma - C}{\sigma(\sigma+\theta)}}{2\frac{\sigma - C}{\sigma(\sigma+\theta)} - 1}. \tag{22}$$

Firstly, equation (21) represents the price of the Bitcoin derived from the *trader-side partial equilibrium*, and we can think of it as the price of the Bitcoin that the traders are willing to pay given the precision of the wallet information, θ.

[6] B converges to 0 in the long run due to the supply structure of the Bitcoin specified by (7).

There are two channels through which θ positively impacts p^T. The first effect is straightforward: as the precision of the wallet information increases, the probability of double spending diminishes, i.e., asymmetric information is mitigated. Then, the young buyers face a higher expected return from the Bitcoin holding, thereby increasing its evaluation. This effect stems from the demand-side behavior.

The second chennel is associated with the supply-side behavior. As θ increases, the number of authentic buyers increases, while the total supply declines because the fraudulent sellers are rejected more frequently. We can confirm this effect by equation (3), as it is decreasing in θ_t. Due to a smaller amount of supply, the market equilibrium achieves a higher price p^T.

Secondly, (22) represents positive relationship between the Bitcoin price, p^M, and the precision of the wallet information, θ, derived from the *miner-side partial equilibrium*. Given that the miners' reward is positively affected by the Bitcoin price, the free-entry condition renders this relationship clear. To achieve a higher θ, the blockchain needs a larger set of active miners (see [15]). In turn, to attract a larger set of miners, the price of reward must be higher. In light of this, we can think of p^M as a required price of reward for the miners to achieve a certain level of θ.

Although this set of equations generate some implications, the precision of the wallet signal θ is hard to measure. Thus, we introduce the total hash rate to render it measurable and testable by using available data.

4.2.1 The Total Hash Rate

So far, the equilibrium is characterized by the key variable, θ, that connects the trader-side and miner-side partial equilibria. In this subsection, we replace it by using the total hash rate to make our empirical implications more salient.

From the miner-side partial equilibrium, we obtain the following:

$$H_t \equiv \tau\left(\Lambda^*\right)^2 = p_{t+1} B_t \frac{\sigma}{1-\theta_t} + [1 - \pi^{\theta}_{t-1}(1-\beta_{t-1})]\sigma^2. \tag{23}$$

Proposition 4. *At the steady state, the total hash is represented by a function of θ:*

$$H = \frac{\sigma^2}{2\theta} \in \left[\frac{\sigma^2}{2}, \sigma^2\right].$$

This result is surprising because it indicates that the steady-state total hash is inversely related to the precision of the wallet information. Put differently, the more hash power is devoted to the blockchain, the less precise the wallet information becomes.

This result hinges on the fact that $B = 0$ at the long-run steady state. Without the reward from leveraging the hash power, all of the miners' incentive must be derived from the private utility from excecution of transaction, σ. As mentioned earlier, a higher θ reduces the total amount of supply from the old traders by rejecting double-spending, and the trading via the blockchain becomes less active. This means that the miners face a low frequency of transactions consummation, thus reducing the chance to get σ.

Note that this argument is relevant only at the steady state: the negative impact is dominated by the positive impact of θ when $B > 0$ is sufficiently large, as the first term in (23) suggests. This implies that θ can have non-monotonic impact on H in the transition path. As long as B is large, the first positive term in (23) is dominant, while, as time goes, B dips below some threshold, thereby making H decreasing function of θ.

Finally, by using the total hash rate, the steady state in Proposition 3 is expressed as follows:

Corollary 1. *The steady state is given by the solution of the following two equations:*

$$p^T = \frac{\sigma^2 - H}{2H - \sigma^2},$$
$$p^M = \frac{\sigma^3 + 2H(\sigma^2 - \sigma + C)}{2H[2(\sigma - C) - \sigma^2] - \sigma^3}.$$

Under a parameter restriction, $C \in [\underline{C}, \bar{C}]$, these two equations have at least one solution, (p, H).[7]

The implication of this general equilibrium characterization is that the total hash rate,

[7] This is straightforward because $\lim_{H\to\sigma^2} p^T > \lim_{H\to\sigma^2} p^M = 0$ and $\lim_{H\to 0.5\sigma^2} p^T < \lim_{H\to 0.5\sigma^2} p^M = \infty$.

H, and the equilibrium Bitcoin price, p, must be determined *simultanously* in the long run. That is, these two variables must have common stationary relationship, i.e., an arbitrage relationship. We test this hypothesis in the following empirical section.

5 The empirical analysis

In this section, we empirically show the existence of the arbitrage among the bitcoin price and hash rate. For indicating the sufficient arbitrage, we implement cointegration estimation. Our results show the cointegrating relationship between Bitcoin price and hash rate, suggesting the Bitcoin market is under the fundamental price. We also find the hash rate of Bitcoin Granger-causes Bitcoin prices. Theses empirical facts are consistent with the theoretical prediction we already show in the previous section.

5.1 data

We obtain the data for Bitcoin price from yahoo finance, while the hash rate of Bitcoin is obtained from blockchain.com. Because Blockchain.com provides the hash rate every three days, our dataset is not daily basis but the middle of the daily and weekly bases. We use the data from July 2010 to June 2019.

Figure 1 shows the time series of Bitcoin price and the total hash rate of Bitcoin. Log is taken for these variable. This figure shows the existence of a tight relationship between these variables, and the correlation is 0.96. Table 1 shows the descriptive statistics of Bitcoin price and the hash rate.

For cointegration estimation, we must check whether the variables follow a unit root process. Table 2 shows the result of Augmented Dickey-Fuller (ADF) and Phillips-Perron (PP) unit-root tests for Bitcoin price and the hash rate. This table includes the unit-root tests with and without trend. The constant term is included in these test. The results of these unit root tests indicate the null hypothesis cannot be rejected, therefore these series contain unit root processes.

5.2 Cointegration test

To explore the effects of possible cointegration, we conduct cointegration tests using the methodology proposed by Johansen (1988) and Johansen (1991). The optimal lag lengths are selected using the Schwarz criterion based on a VAR. The variables used are Bitcoin price and the total hash rate, which follow a unit root process.

As Table 3 reports, the Johansen test provides evidence of cointegration among Bitcoin price and the hash rate. Both the trace and maximum eigenvalue tests reject the null hypothesis of no cointegration among the variables at the 5% level, and the hypothesis of one cointegrating vector is accepted. Therefore, there has been the long-run relationship among Bitcoin price and the hash rate, suggesting the Bitcoin price is based on the fundamental price in the long-run.

5.3 Estimation

If cointegration exists among the variables, we have to include an error correction term for Granger causality test. For this purpose, we use Vector Error Correction Model (VECM) as follows:

$$\Delta p_t = c_p + \alpha_p EC_{t-1} + \Sigma_{i=1}^{l} a_{1i} \Delta p_{t-i} + \Sigma_{i=1}^{l} a_{2i} \Delta h_{t-i} + \epsilon_{1t}, \tag{24}$$

$$\Delta h_t = c_h + \alpha_h EC_{t-1} + \Sigma_{i=1}^{l} b_{1i} \Delta p_{t-i} + \Sigma_{i=1}^{l} b_{2i} \Delta h_{t-i} + \epsilon_{1t}. \tag{25}$$

α_p and α_h show the speeds of adjustment, l is the length of lag, and EC_t shows the deviation of the price and hash from their long-run relationship, where the cointegrating relation is $EC_{t-1} = p_{t-1} + \beta h_{t-1}$. The optimal lengths of lag are selected using the Schwarz criterion based on a VAR as Section 4.3.

As we already show, there is a cointegration relatioship between Bitcoin price and the hash rate, therefore VECM is the appropriate specification for the Granger causality test. Table 4 shows the result of the Granger causality test under the specification of VECM. The upper panel of this table shows p-value under the null of no causality from the hash rate to the Bitcoin price, therefore the hash rate Granger-causes the Bitcoin price. On the other hand, the lower panel of the table indicates the Bitcoin price does not lead the hash rate.

6 Conclusion

This paper contributes to the literature both theoretically and empirically. We introduce a dynamic general equilibrium model to determine the fundamental price of Bitcoin, and show that the total hash rate should be a factor to Bitcoin price. Currently, most of the papers on cyptocurrency focus only on either theoretical work or empirical analysis, whereas our paper fills this gap.

Because our general equilibrium framework provides a tight linkage between Bitcoin price and the hash rate, the arbitrage relationship between these two variables are empirically analyzed. We employ the cointegration framework and show the existence of long-run cointegration between the Bitcoin price and total hash rate. We also find the hash rate of Bitcoin Granger-causes Bitcoin prices in the short-run. These results can be seen as the evidence that Bitcoin is under the fundamental price, which is surprising given the existing empirical literature, as well as the public opinion, that claims that the Bitcoin price is speculative and resembles asset price bubbles.

References

Abadi, J. and Brunnermeier, M. (2018). Blockchain economics. Technical report, mimeo Princeton University.

Aoyagi, J. and Adachi, D. (2018). Economic implications of blockchain platforms. *Available at SSRN 3132235*.

Bhargava, A. (1986). On the theory of testing for unit roots in observed time series. *The Review of Economic Studies*, 53(3):369–384.

Biais, B., Bisiere, C., Bouvard, M., and Casamatta, C. (2018). The blockchain folk theorem.

Budish, E. (2018). The economic limits of bitcoin and the blockchain. Technical report, National Bureau of Economic Research.

Cheah, E.-T. and Fry, J. (2015). Speculative bubbles in bitcoin markets? an empirical investigation into the fundamental value of bitcoin. *Economics Letters*, 130:32–36.

Chen, A.-S., Cheng, L.-Y., and Cheng, K.-F. (2009). Intrinsic bubbles and granger causality in the s&p 500: Evidence from long-term data. *Journal of Banking Finance*, 33(12):2275–2281.

Chiu, J. and Koeppl, T. V. (2018). Blockchain-based settlement for asset trading.

Chiu, J. and Koeppl, T. V. (2019). Blockchain-based settlement for asset trading. *The Review of Financial Studies*, 32(5):1716–1753.

Cong, L. W. and He, Z. (2018). Blockchain disruption and smart contracts.

Cong, L. W. and He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, 32(5):1754–1797.

Cong, L. W., Li, Y., and Wang, N. (2018). Tokenomics: Dynamic adoption and valuation.

Diba, B. T. and Grossman, H. I. (1988). Explosive rational bubbles in stock prices? *The American Economic Review*, 78(3):520–530.

Easley, D., O'Hara, M., and Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*.

Evans, G. W. (1991). Pitfalls in testing for explosive bubbles in asset prices. *The American Economic Review*, 81(4):922–930.

Froot, K. A. and Obstfeld, M. (1991). Intrinsic bubbles: The case of stock prices. *The American Economic Review*, pages 1189–1214.

Fry, J. (2018). Booms, busts and heavy-tails: The story of bitcoin and cryptocurrency markets? *Economics Letters*, 171:225–229.

Glosten, L. R. and Milgrom, P. R. (1985). Bid, ask and transaction prices in a specialist market with heterogeneously informed traders. *Journal of Financial Economics*, 14(1):71–100.

Gürkaynak, R. S. (2008). Econometric tests of asset price bubbles: taking stock. *Journal of Economic surveys*, 22(1):166–186.

Hashimoto, Y. and Noda, S. (2019). Pricing of mining asic and its implication to the high volatility of cryptocurrency prices. *Available at SSRN*.

Hu, A., Parlour, C. A., and Rajan, U. (2018). Cryptocurrencies: Stylized facts on a new investible instrument. *Available at SSRN 3182113*.

Johansen, S. (1988). Statistical analysis of cointegration vectors. *Journal of Economic Dynamics and Control*, 12(2-3):231–254.

Johansen, S. (1991). Estimation and hypothesis testing of cointegration vectors in gaussian vector autoregressive models. *Econometrica: Journal of the Econometric Society*, pages 1551–1580.

Kurlat, P. (2013). Lemons markets and the transmission of aggregate shocks. *American Economic Review*, 103(4):1463–89.

Ma, Y. and Kanas, A. (2004). Intrinsic bubbles revisited: Evidence from nonlinear cointegration and forecasting. *Journal of Forecasting*, 23(4):237–250.

Pagnotta, E. and Buraschi, A. (2018). An equilibrium valuation of bitcoin and decentralized network assets.

Su, C.-W., Li, Z.-Z., Tao, R., and Si, D.-K. (2018). Testing for multiple bubbles in bitcoin markets: A generalized sup adf test. *Japan and the World Economy*, 46:56–63.

	Mean	Median	Max	Min	Std. Dev.	Num of Obs
Bitcoin Price	1771	375	19065.7	0.0505	3087	1089
Hash rate	7647050	299461	6.5E+07	0.00167	15499957	1089

This table shows the descriptive statistics of Bitcoin price and the hash rate. The data is from July 2010 to June 2019. The source is yahoo finance and blockchain.com.

Table I: Descriptive Statistics

	Bitcoin price		hash rate	
	ADF	PP	ADF	PP
no trend	-0.62701 (0.8620)	-0.75531 (0.8305)	2.41943 (1.0000)	1.11496 (0.9977)
trend	-2.01457 (0.5922)	-2.13395 (0.5256)	0.54167 (0.9994)	-0.79368 (0.9647)

This table provides the result of the Augmented Dickey-FUller (ADF) and Phillips-Perron (PP) unit-root tests. P-values are shown in parentheses.The data is from July 2010 to June 2019. The source is yahoo finance and blockchain.com.

Table II: Unit-root tests

H0: no cointegration	Eigen value	Trace statistic/ Max-Eigen Statistic	P-value
Trace test			
r=0	0.0228	27.5476	0.0005
r1	0.0024	2.5646	0.1093
Maximum eigen value test			
r=0	0.0228	24.9830	0.0007
r1	0.0024	2.5646	0.1093

This table reports the Johansen test for cointegration vectors for Bitcoin price and the hash rate. $r = 0$ tests the null hypothesis that the number of cointegrating vector is zero while $r \leq 1$ tests the null hypothesis that the number of cointegrating vector is at most equal to one. The optimal lag lengths are selected using the Schwarz criterion based on a VAR. The data is from July 2010 to June 2019. The source is yahoo finance and blockchain.com.

Table III: Johansen test

Dependent variable	Source of causation (independent variable)	
	Bitcoin price	Hash rate
Bitcoin price		0
Hash rate	0.2307	

This table reports the Granger causaulity test based on Vector Error Correction Model. This table shows p-value. In the upper panel of the table, the null of no causality from Hash rate to Bitcoin price is shown while in the lower panel, the null of no causality from Bitcoin price to Hash rate is shown.

Table IV: Granger causality test

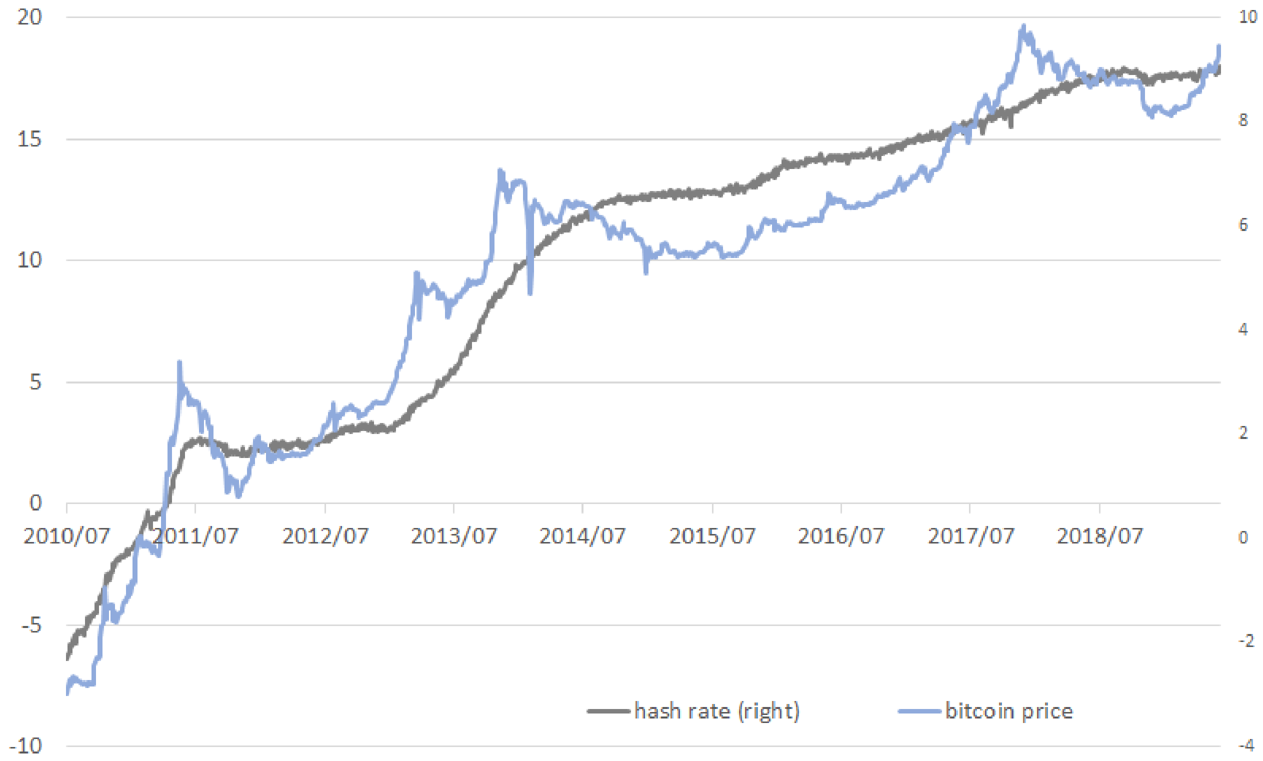

Figure I: Time series of Bitcoin price and hash rate

This figure depicts the times series of Bitcoin price and the hash rate.Log is taken for the data. The sample period is from July 2010 to June 2019.