Bursting the Bitcoin Bubble: Assessing the Fundamental Value and Social Costs of Bitcoin*

Andrea Podhorsky, York University†

February 2023

Abstract

This paper develops a microeconomic model of bitcoin production to demonstrate that the boom and bust cycles evident in the bitcoin price path are the consequence of a supply-side phenomenon arising from the Bitcoin protocol's system of supply management. After specifying the fundamental value of a bitcoin according to the model, I apply the generalized supremum augmented Dickey-Fuller test to establish that bitcoin is not a bubble. I also show that the difficulty adjustment mechanism results in social welfare losses from March 2014 to January 2019 of 323.8 million USD, which is about 9.3% of the miners' total electricity costs.

Keywords: Bitcoin, Cryptocurrencies, Fintech, GSADF Test, Multiple Bubbles, Valuation

JEL codes: O33, G10, G18

---

*I would like to thank the participants at the conference on Fintech, Social Finance, and Financial Stability sponsored by the Asian Development Bank Institute, the Shenzhen Finance Institute, and the Chinese University of Hong Kong, Shenzhen. I am grateful to Peter Boyd, Ernest Fokoue, Zongbo Huang, Jiasun Li, Adam Majoe, and Gabor Virag for their valuable comments and discussion. I also thank the School of Individualized Study at the Rochester Institute of Technology for hosting me while I conducted the bulk of this research.

†Address: 1058 Vari Hall, York University, 4700 Keele Street, Toronto, Ontario, M3J 1P3 Phone: 585-472-5836 Email: andrea@yorku.ca

"A lot of Bitcoin's value derives from how we envision it within the depths of the internet."

–Bitcoin.com

1 Introduction

In this paper I view bitcoins as tradable commodities whose supply is managed by the Bitcoin protocol.[1] I contend that it makes no sense to value bitcoins as if they were a stock because the Bitcoin network, as an institution, is not owned by anyone. And while it is a digital currency, it cannot assume a value as do fiat currencies, because no government has declared it to be legal tender. Bitcoin is most analogous to a commodity such as coffee, which is produced by 'small' farmers who are uncoordinated in their production decisions. While miners use electricity to produce bitcoins (instead of sunshine), the analogy is not far-fetched, as evidenced by the fact that miners demonstrate a strong preference for joining mining pools,[2] which are similar in structure to coffee cooperatives since they are designed to share the risk among their members.[3] Also, coffee farmers once benefited from the now defunct International Coffee Agreement (ICA), which was a system of quotas that resulted in high and stable prices by organizing the supply of farmers worldwide.[4] Encoded in the Bitcoin protocol is a similar system of supply management that the Bitcoin network sustains by its near-perfect monitoring of the rate of block formation (and thus the quantity of bitcoins supplied) and enforces by regular adjustments in the level of difficulty of mining a bitcoin. Bitcoin, however, has the additional feature of being a medium of exchange and a tradable

[1] I follow the convention of capitalizing the word 'bitcoin' when referring to the protocol or network and writing it in lowercase when referring to the unit of currency.

[2] According to hashrate distribution statistics provided by BTC.com, more than 95% of the Bitcoin network hashrate for 2018 can be attributed to mining pools. See https://btc.com/stats/pool

[3] Mining pools enable miners to decrease the variance of their returns by sharing their processing power over a network and splitting the reward according to the amount of work that each has contributed to the probability of finding a block.

[4] The ICA was a quota system that was in operation between 1962 and 1989. The system was suspended because of failure to agree on the quota distribution and the increasing volume of coffee traded with non-member importing countries at lower prices. See Talbot (2004).

asset with numerous well-developed market exchanges, resulting in a unique class of asset with characteristics that have never before been seen. I show that bitcoin's volatile price path and inefficiency are related, as they both result from the protocol's system of supply management.

Bitcoin, the first cryptocurrency, was invented by an unknown individual who implemented the software as open-source code. Cryptocurrencies such as Bitcoin are electronic payment systems that permit transactions to be made with pseudo-anonymity[5] and without middlemen like banks. Bitcoin was launched on January 3, 2009. Until July 2010, the price of a bitcoin was less than 0.01 USD. By the beginning of 2017, the price had risen astoundingly to a stable 1,000 USD and it reached a peak value of 19,783 USD in December 2017. The price has been generally falling since that time, with the exception of a few resurgences. Bitcoin's price path is notoriously volatile and has evinced a multitude of boom-and-bust cycles over its 10-year lifespan. While there are numerous historical examples of bubbles, starting as far back as the Dutch tulipmania (1634–7),[6] one is hard-pressed to identify an asset price or an episode of market exuberance that exemplifies the ceaseless deflations and re-inflations that are apparent in the price path of Bitcoin and similar cryptocurrencies.[7] It is challenging to identify bubbles in market data because one needs to know an asset's fundamental value in order to identify a divergence between it and the asset's price. Moreover, econometric tests of asset price bubbles do not do a good job of differentiating between misspecified fundamentals and bubbles (Gurkaynak, 2005).

Mining is the process by which bitcoins are created. Bitcoin miners use electricity to solve complex mathematical puzzles in order to verify the transactions added to the blockchain.

[5] Bitcoin addresses are not tied to the identity of their users but since all transactions over the Bitcoin network are completely transparent and traceable, multiple Bitcoin addresses can be clustered together and then associated with a particular user. See Meiklejohn et al. (2013).

[6] See Garber (1989; 1990) and Brunnermeier (2008) for a discussion of the history of price bubbles.

[7] It is theoretically possible, however, for rational bubbles to periodically collapse to a small nonzero value and then to continue to increase. See Evans (1991).

Solving this 'proof of work' (PoW) problem requires tremendous computational power and the first miner to succeed (find a correct hash) is rewarded with new bitcoins.[8] The Bitcoin protocol specifies a target that a correct hash must fall below, which implies a level of difficulty for the computational problem. A lower target corresponds to a greater level of difficulty because it is less likely that a hash will fall within the correct range. Changes in the target and hence the level of difficulty affect the rate of block formation because an increase (decrease) in difficulty decreases (increases) the probability that a miner will find a correct hash. Since the production of a block increases the supply of bitcoins according to the block reward,[9] changes in the level of difficulty also determine the growth rate of the supply of bitcoins over time.

Although the Bitcoin network is managed by peer-to-peer technology without a central authority, it uses the level of difficulty as an instrument to enforce an inflexible system of supply management. The protocol regulates the quantity of bitcoins that are mined by adjusting the level of difficulty every 2016 blocks (approximately every two weeks). There is an interval of time between adjustments in the level of difficulty, so that the network can accurately estimate the waiting time to find a block. If the network detects that the time required to find the last 2016 blocks differs from 20,160 minutes, then the network uses the estimated mining rate to adjust the level of difficulty proportionally in order to target a ten-minute interval between successive blocks mined. Only when the mining rate is equal to its target will the level of difficulty be unchanged.

To ascertain the value of a bitcoin, in Section 2 of the paper, I model the competitive bitcoin mining industry with free entry of miners in response to profits that are created in accordance with the Bitcoin protocol. For simplicity, there is no secondary market for the bitcoin and all input markets are held constant. I define the fundamental value of the bitcoin

[8] The current block reward is 12.5 bitcoins.

[9] The block reward decreases by one-half only every 210,000 blocks, or approximately four years. See https://en.bitcoin.it/wiki/Controlled_supply.

to be the marginal cost of producing a bitcoin when the mining rate is equal to its target. This is a natural definition since the value of a bitcoin is governed by the protocol's system of supply management, and it is the unique price that is consistent with its rules. The model reveals that the fundamental value of a bitcoin is equal to the miners' equipment and electricity costs, relative to their expected revenue (block reward and fees, multiplied by the expected number of blocks mined). Also, the fundamental value of the bitcoin appreciates by an amount that is equal to the rate of increase in the level of difficulty and, assuming a constant-elasticity demand curve for bitcoin, the return on bitcoin is proportional to the rate of increase in the level of difficulty. I establish how adjustments of the level of difficulty in response to demand shocks result in exaggerated price movements that may be mistaken for a bubble. The supply of bitcoins is upward sloping since a higher price of a bitcoin results in a greater number of entrants (miners), which increases the network hashrate and thus the number of blocks mined per day. If a positive demand shock results in a mining rate that exceeds its target, then the Bitcoin protocol will stipulate an increase in the level of difficulty. I show that an increase in difficulty decreases the supply of bitcoins (it rotates the supply curve upward) since it results in greater marginal electricity costs for the miners. This causes an exaggerated upward price movement since the initial price increase caused by the demand shock is amplified by the decrease in supply. Since the protocol aims at maintaining a constant supply of bitcoins per day, prices are largely demand driven and thus variations in demand are transformed by the process of adjusting the level of difficulty into price volatility.

Interestingly, if the increase in demand is due to the optimistic beliefs of investors regarding the future price of bitcoins, the subsequent increase in difficulty will work to validate investor's beliefs, encouraging another round of optimism. While I do not model beliefs in this paper, it is intuitively clear how the protocol can interplay with investor's beliefs, resulting in the momentum of price movements over time: a greater demand for bitcoins causes higher bitcoin prices, which causes more miners to enter the industry, which results in a mining rate that exceeds its target, which leads to intervention by the protocol and a higher level of difficulty, which causes greater than laissez-faire prices, which leads to greater demand for bitcoins by investors... and so on, until an exogenous unanticipated event (such as a hack on a bitcoin exchange) breaks the cycle. The resulting sequence of positive demand shocks amplified by increases in the level of difficulty can result in an explosive price path that may be mistaken for a bubble despite being based on marginal costs. The analysis of a negative demand shock is analogous: a series of negative demand shocks may be mistaken for a bursting bubble since the equilibrium price will fall rapidly as the difficulty decreases. It follows that the economic functioning of the Bitcoin protocol can result in boom-and-bust cycles in the price of the bitcoin. Unlike a bubble, however, the price is equal to marginal cost all the while.

Next, I show that because the protocol intervenes in the market to control the supply of bitcoins, welfare losses must occur as a result. An increase in difficulty works analogously to a government's placing an ad valorem tax on the price of the bitcoin since the supply price increases in proportion to the difficulty adjustment. Instead of accruing tax revenue, however, the increase in difficulty imposes additional electricity costs on the miners. While a higher price for the bitcoin is obtained, the rents that would have arisen from limiting the supply are wasted as they neither benefit a government nor the miners. A decrease in the level of difficulty works analogously to a government that provides an ad valorem subsidy (a negative tax) to the miners, but I show that the welfare effects of an increase in difficulty are not offset by a decrease in difficulty by the same proportion since the absolute change in electricity costs is greater under the increase, and a distortion loss must be experienced under either. Ironically, while the bitcoin is esteemed for its nongovernmental design, it follows that its system of supply management is far less efficient than if a government were to regulate the quantity of bitcoins by imposing a tax on its price.

Bitcoin is a particularly advantageous choice of asset for studying price behavior since the protocol's rules are clearly stated and thus the functioning of the overall system is fully transparent. Also, the entire population of data pertaining to the supply of bitcoins and how the Bitcoin protocol is implemented over time are readily available from its blockchain ledger.[10] I parse the Bitcoin blockchain to obtain time series data for the network level of difficulty, the number of blocks mined per day, the block reward and fees, and describe the data in Section 3 along with data pertaining to bitcoin mining equipment specifications and costs, and the average USD market price of the bitcoin across major bitcoin exchanges. I examine model diagnostics and show that the data is largely consistent with the model developed in Section 2.

Since prices are typically well approximated by a random walk in the absence of bubbles but are characterized by an explosive path during periods of bubbles, recent econometric techniques identify rational speculative bubbles by testing for a mildly explosive departure from a random walk.[11,12] Such tests were originally proposed by Phillips et al. (2011) and further developed by Phillips and Yu (2011), Homm and Breitung (2012), and Phillips et al. (2015a; 2015b). In Section 4, I outline the generalized version of the supremum augmented Dickey–Fuller (GSADF) test based on Phillips et al. (2015a; 2015b), which delivers a consistent date-stamping strategy for the origination and termination of multiple bubbles, and apply it to determine whether the boom-and-bust cycles evident in bitcoin price data can be explained by the fundamentals derived in Section 2. I also apply the model developed in Section 2 to estimate the welfare losses that are due to adjustments in the level of difficulty throughout the sample period. Since estimating welfare losses requires an estimate of the price elasticity of demand for bitcoins, I exploit the timing of adjustments in the difficulty to

[10] The blockchain ledger also records all transactions between users with the exception of 'off-chain' transactions such as those occurring on bitcoin exchanges.

[11] These tests can detect rational bubbles as well as other bubble-generating mechanisms, such as intrinsic bubbles, herd behavior and time-varying discount factor fundamentals.

[12] For a survey of the literature on bubbles see Brunnermeier and Oehmke (2012).

isolate periods that are characterized by large supply shocks in order to identify the demand curve.

I present the results in Section 5. I find that while the raw bitcoin price data demonstrates evidence of bubble formation, the residuals after fitting the price to the fundamental value as defined by the model do not. This provides strong evidence that the model can explain the apparent bubbles since, after accounting for the protocol's difficulty adjustment mechanism, the price path reverts to a random walk. I obtain an estimate for the total welfare losses from 17 March 2014 to 13 January 2019 of 323.82 million USD, which is about 9.3% of the total electricity costs to power the Bitcoin network during this time.

Section 6 presents the conclusions.

There is a small but rapidly growing economics literature on the topic of Bitcoin and cryptocurrencies. The comprehensive empirical analysis conducted in Liu and Tsyvinski (2018) using price data for Bitcoin, Ethereum, and Ripple demonstrates that the mean and standard deviation of returns for cryptocurrencies are an order of magnitude higher than those for traditional asset classes. Also, with the exception of the exposure of Ethereum to gold, cryptocurrencies have no exposure to most common stock market and macroeconomic factors, and their returns can be best predicted by two factors specific to their markets: momentum and investor attention. Bianchi (2018) uses a large panel of prices, traded volumes, and market capitalization on 14 actively quoted cryptocurrencies to empirically investigate their relation with standard asset classes. The main empirical results suggest that, except for a mild correlation with gold and crude oil, there is no significant relation between returns on cryptocurrencies and more traditional asset classes. Dong et al. (2018) find that bitcoin price dynamics are significantly sensitive to investor sentiment. The authors use sentiment data to show that stricter regulations for Bitcoin predict a decrease in future returns and an increase in the probability of a future price collapse, and that market sentiment positively comoves with bitcoin prices.

These empirical studies characterize features of Bitcoin returns that are consistent with the main premise of this paper: the bitcoin is a tradable commodity whose supply is managed by the Bitcoin protocol, which creates an asset that is radically different from those belonging to traditional asset classes. As discussed above, since the protocol uses a difficulty adjustment mechanism to target a constant supply of bitcoins per day, prices are in excess of their laissez-faire counterparts and are demand driven. As such, it is intuitive that bitcoin returns are supernormal and volatile, and that prices are highly sensitive to investor attention and sentiment. Also, since the difficulty adjustment mechanism works to validate investor's beliefs regarding future price movements, it is natural that the bitcoin price path would demonstrate momentum. While Dong et al. (2018) attribute the price responses to bubbles, in this paper I show that it is the fundamental value of Bitcoin that manifests volatile and potentially explosive behavior due to the effect of difficulty adjustments on the miners' costs.

The papers most closely related to the present paper are Pagnotta and Buraschi (2018) and Easley et al. (2017). Pagnotta and Buraschi (2018) study the general equilibrium of a decentralized financial network and derive closed-form solutions linking the bitcoin price to market fundamentals. The authors develop a theoretical model where the Bitcoin network's value is driven by the number of users and miners who provide computing resources that affect the network's trustworthiness. They find that, counterintuitively, the price of the bitcoin decreases whenever the marginal cost of mining increases since it will induce miners to provide a lower hashrate, which reduces network trust and ultimately the equilibrium price. Easley et al. (2017) develop a game theoretic model to explain the strategic behavior of miners and users, and demonstrate that equilibrium in the bitcoin blockchain is a complex balancing of user and miner participation. The authors find that transaction fees play a crucial role in influencing the stability of the blockchain and that higher transaction fees are driven by the queuing problems facing users, rather than by reductions in block rewards.

In contrast with Pagnotta and Buraschi (2018), the present paper considers a relatively unstructured demand side of the bitcoin market, focusing instead on the supply-side effect of the protocol. I treat network quality and security, in addition to investor's beliefs, and specific use cases that are mostly unobservable due to the pseudo-anonymity of bitcoin transactions, as exogenous factors that may drive the demand for bitcoins. I show that because the protocol adjusts the level of difficulty in response to changes in the equilibrium mining rate detected by the network, which depends on the supply and demand for bitcoins, the difficulty is a sufficient statistic for the determinants of demand. The model in this paper predicts a positive relation between the rate of increase in the price of a bitcoin and the rate of increase in the level of difficulty, a key determinant of the marginal cost of mining, and I show that this prediction is strongly supported by the data. While Easley et al. (2017) study how the Bitcoin protocol affects the interaction between miners and users, and thus the determination of fees, the present paper treats fees as exogenous and studies how the protocol affects the interaction between the miners and the purchasers of bitcoins (who may either hold it or use it to make transactions), and thus the determination of the price of the bitcoin in the market. By leveraging an understanding of the microeconomics of bitcoin production, I develop a simple model that is amenable to empirical analysis to demonstrate that the boom and bust cycles evident in the bitcoin price path are the consequence of a supply-side phenomenon arising from the protocol's difficulty adjustment mechanism.

2 The model

A miner must collect new transactions into a block and then hash the block header to form a 256-bit block hash value. If the value is below a target set by the protocol, which corresponds to a given level of difficulty δ, then other miners will confirm the solution and agree that the block can be added to the blockchain. Because the header contains a 32-bit nonce field whose value is adjusted by the miners in an attempt to find an acceptable solution, the expected number of hashes per second needed to find a solution is $\delta 2^{32}$. It follows that the expected waiting time for a miner to find a block (in seconds) is $\frac{\delta 2^{32}}{\phi 10^9}$, where ϕ is the hashrate employed by the miner measured in gigahashes per second.[13] When a miner 'solves a block,' the miner earns the block reward ω (denominated in bitcoins) and may also earn fees f per block (denominated in bitcoins) that senders of bitcoins can include in any transaction to reduce their waiting time.

The protocol regulates the quantity of bitcoins that are mined by adjusting the difficulty every 2016 blocks. It adjusts the difficulty in such a way that the current network hashrate results in a ten-minute block interval.[14] If the network detects that the time required to find the last 2016 blocks differs from 20,160 minutes, which is a daily mining rate that differs from 144 blocks per day, then the level of difficulty will be adjusted as follows:

$$\frac{\delta_2}{\delta_1} = \frac{20,160 \text{ minutes}}{\text{Actual time of last 2016 blocks in minutes}} = \frac{\text{daily mining rate}}{144} \tag{1}$$

where δ_2 is the new level of difficulty and δ_1 is the previous level of difficulty.[15] If, for instance, the actual time of the last 2016 blocks was only 10,080 minutes (7 days), then since the daily mining rate is $\frac{2016}{7} = 288$, the network hashrate is such that twice as many blocks are mined per day relative to the objective of 144 blocks, so that δ_2 will be set twice as high as δ_1. Only when the average number of blocks discovered per day is equal to 144 will the difficulty remain unchanged.

I assume that there are identical potential entrants (miners) to the bitcoin mining industry. Each miner is risk neutral, knows the rules of the Bitcoin protocol that govern the network, and must pay a fixed cost F (thereafter sunk) to purchase mining equipment in

[13] There are 10^9 hashes in a gigahash.

[14] See Antonopoulos (2017).

[15] The second equality follows because $\frac{\text{20,160 minutes}}{\text{Actual time of last 2016 blocks in minutes}} = \frac{\text{2016 blocks}}{\text{Actual time of last 2016 blocks in minutes} * \frac{\text{144 blocks per day}}{\text{24*60 minutes per day}}} = \frac{\text{2016 blocks}}{\text{Actual time of last 2016 blocks in days} * \text{144 blocks per day}} = \frac{\text{daily mining rate (blocks per day)}}{\text{144 blocks per day}}$.

order to enter. Upon entry, a miner's daily expected bitcoin production is

$$x(\tau_i) = \frac{\omega \tau_i 60^2}{\frac{\delta 2^{32}}{\phi 10^9}} \tag{2}$$

where $\tau_i 60^2$ is the number of seconds spent mining per day. Hence if $\phi 10^9 \tau_i 60^2$ hashes are created by a miner in one day, the expected number of blocks mined is $\frac{\phi 10^9 \tau_i 60^2}{\delta 2^{32}}$ per day, at a reward of ω bitcoins per block. A miner's daily electricity cost is

$$\frac{\phi \xi \tau_i}{1000} p_e \tag{3}$$

where ξ is the energy efficiency of the miner's hardware measured in joules per gigahash (and hence $\phi\xi$ is the power usage measured in joules per second, or watts) and p_e is the dollar price of electricity per kilowatt hour (kWh). It follows from (2) and (3) that a miner's operating profit is linear in τ_i and if the dollar price of a bitcoin (the exchange rate) $p_b > \frac{\delta 2^{32} \xi p_e}{(\omega+f)(1000)60^2 10^9} \equiv \underline{p_b}$, then it is optimal the miner to set $\tau_i = 24$ and 0 otherwise.

Since hashing power scales linearly (doubling the number of miners doubles the network hashrate), the total hashpower of the Bitcoin network is ϕM, where M is the total number of miners who enter the industry. It follows that gross of investment costs, miners' aggregate expected daily profits are given by

$$\Pi = \left[\frac{p_b(\omega + f) 60^2 10^9}{\delta 2^{32}} - \frac{\xi p_e}{1000}\right] 24 \phi M \tag{4}$$

where I assume $p_b > \underline{p_b}$. Since $\frac{1}{\delta 2^{32}}$ is the probability that a miner will find a correct hash, it is clear from (4) that mining is akin to a lottery: the payoff from playing is uncertain while the cost of playing is not. Because an increase in the number of miners M increases the network hashrate proportionally, each miner has the same expected profit $\frac{\Pi}{M}$ regardless of the number of entrants. Every 2016 blocks, however, the level of difficulty δ is adjusted so that the average waiting time to find a block on the network is approximately 10 minutes (600 seconds), so that $\frac{\delta 2^{32}}{\phi M 10^9} = 600$ or

$$\delta = \frac{600\phi M 10^9}{2^{32}}. \tag{5}$$

Since the target waiting time to find a block on the network in (5) is encoded in the protocol and known to the potential entrants, it pins down the number of miners M. From (4) and (5) it follows that the expected daily profit for a miner is

$$\begin{aligned} \pi &= \frac{\Pi}{M} - \eta F \\ &= \left[\frac{p_b (\omega + f) 60^2}{600\phi M} - \frac{\xi p_e}{1000} \right] 24\phi - \eta F \end{aligned} \tag{6}$$

where η is the daily depreciation rate of the miner's equipment. Since there is free entry to the bitcoin mining industry, miners have zero expected profits and hence the number of miners per day is given by $\pi = 0$ or

$$M^* = \frac{p_b (\omega + f) \left[\frac{(24)60^2}{600} \right]}{\eta F + \frac{\phi \xi}{1000} (24) p_e}. \tag{7}$$

From (7) it is clear that the number of miners is equal to the total size of the 'pie' shared among the miners each day (the dollar value of the block reward and fees, for each of the 144 possible blocks mined), divided by each miner's daily equipment and electricity costs

$$\eta F + \frac{\phi \xi}{1000} (24) p_e. \tag{8}$$

While the number of entrants adjusts immediately to changes in the price of a bitcoin p_b, the level of difficulty adjusts only approximately every two weeks while the network learns the network hashrate ϕM^* from observing the average number of blocks mined per day (the daily mining rate). The aggregate supply of bitcoins per day X_S is equal to the block reward multiplied by the daily mining rate, which is determined by the network hashrate ϕM^* for a given δ. If $p_b > \underline{p_b}$, it follows that

$$X_S = \frac{\omega\,(24)\,60^2}{\frac{\delta 2^{32}}{\phi M^* 10^9}} \tag{9}$$
$$= \frac{p_b\,(\omega + f)\left[\frac{(24)60^2\phi 10^9}{\delta 2^{32}}\right]}{\eta F + \frac{\xi\phi}{1000}\,(24)\,p_e}\overline{X}$$

where the second line follows from M^* of (7) and

$$\overline{X} = \frac{\omega\,(24)\,60^2}{600}$$
$$= 144\omega$$

is the target supply of bitcoins per day since the protocol adjusts δ so that one block is created approximately every 10 minutes (600 seconds).[16,17] The supply curve relates each price p_b to an optimal quantity of bitcoins supplied since we can alternatively use (2) and (7) to express X_S of (9) as $X_S = M^*x^*$, where $x^* = x(\tau_i^*)$ and $\tau_i^* = 24$. An increase in the price p_b results in a movement up along the aggregate supply curve since, from (7), a greater number of miners M^* will enter the industry, which increases the network hashrate ϕM^* since more equipment and electricity will be used to generate hashes, which results in

[16] To demonstrate that X_S is equal to the block reward multiplied by the daily mining rate, we can express X_S of (9) as $X_S = \omega \frac{2016}{\frac{\delta 2^{32}}{\phi M^* 10^9} * 2016 * \frac{1}{(24)60^2}} = \omega \frac{2016 \text{ blocks}}{\text{Actual time of last 2016 blocks in days}}$.

[17] It follows from (8) and (9) that, for a given price of a bitcoin p_b, an increase in the miners' hashrate ϕ results in an increase in the daily electricity costs $\frac{\xi\phi}{1000}(24)\,p_e$, which works to decrease the supply of bitcoins X_S. Since an increase in ϕ also increases the expected number of blocks solved per day on the network $\frac{(24)60^2\phi 10^9}{\delta 2^{32}}$, however, the net effect of an increase in ϕ is to increase the supply of bitcoins X_S.

a greater number of blocks mined per day and thus a greater quantity of bitcoins supplied per day. From (9) it follows that the supply curve is linear, because hashing power scales linearly. Also, since the quantity supplied increases proportionally to the price, the price elasticity of supply is unity.

Since the network's choice of the level of difficulty depends on the network hashrate ϕM^*, the equilibrium level of difficulty δ^* will depend on M^*. Hence it follows from substituting (7) into (5) that the equilibrium level of difficulty is

$$\delta^* = \frac{p_b\left(\omega + f\right)\left[\frac{(24)60^2\phi 10^9}{2^{32}}\right]}{\eta F + \frac{\phi\xi}{1000}\left(24\right)p_e}. \tag{10}$$

From (10) it is clear that, for a given price of a bitcoin p_b, the difficulty will increase in response to an increase in the hashrate of miners' equipment ϕ, an improvement in the energy efficiency of the miners' equipment (a decrease in ξ), a decrease in the price of electricity p_e, or an increase in the Bitcoin block reward ω or fees f. It follows from (9) and (10) that we can write $X_S = \frac{\delta^*}{\delta}\overline{X}$ and hence $X_S = \overline{X}$ if and only if $\delta = \delta^*$. In other words, in the interim between adjustments of the level of difficulty, the quantity of bitcoins supplied will not equal its target. Once the difficulty is adjusted according to (10), however, the protocol will be in equilibrium.[18]

I assume that the daily demand for bitcoins by individuals who buy bitcoins in the market is given by the constant elasticity demand curve

$$X_D = \alpha p_b^{-\varepsilon} \tag{11}$$

where the elasticity of demand is $\varepsilon > 0$. For simplicity, I assume that all bitcoins that have been previously purchased are either held or transferred to another user. While miners may

[18] As we will see in Section 3, Figure 8 shows that the number of blocks mined per day frequently differs from its target.

also hold or transfer the bitcoins they obtain from mining rather than selling them in the market, the market price establishes their opportunity cost of doing so.

I define a comprehensive equilibrium to be a four-tuple $(X^*, p_b^*, \delta^*, M^*)$, where the first element is the equilibrium quantity of bitcoins supplied per day, the second element is the equilibrium price, the third element is the equilibrium level of difficulty and the fourth element is the equilibrium number of miners per day, which determines the equilibrium hash rate. A comprehensive equilibrium is the unique solution to the system of equations determined by the zero profit condition obtained from setting (4) equal to miners' fixed costs, the Bitcoin protocol's specified waiting time to find a block of (5), the supply curve of (9) and the demand curve of (11).[19] In a comprehensive equilibrium, since $X_S(p_b^*; \delta^*) = X_D(p_b^*) = X^*$ and $X_S = \overline{X}$ if and only if $\delta = \delta^*$, it follows that $X^* = \overline{X}$. We have seen that since the level of difficulty δ is adjusted only at intervals, an equilibrium in the market $(X_S(p_b^*; \delta) = X_D(p_b^*) = X^*)$ may not happen at the same time as an equilibrium in the protocol $(\delta = \delta^*, M = M^*)$.

Figure 1 depicts the aggregate daily supply of bitcoins by miners and the aggregate daily demand for bitcoins by individuals. Starting from an initial comprehensive equilibrium labeled 1 with price p_{b1}, a level of output $X_1 = \overline{X}$, a mass of entrants M_1, and a level of difficulty δ_1, an increase in demand from X_D to X_D' leads to an increase in the price of a bitcoin to p_{b2} and a movement along the supply curve consistent with an increase in the number of entrants to M_2. Because the probability of successfully mining a block is determined by δ_1 and more hashpower ϕM_2 is directed at the network, the quantity of bitcoins supplied increases to $X_2 = X_S(p_{b2}; \delta_1)$ per day in the market equilibrium labeled 2a. The new equilibrium will be short-lived, however, since the mining rate exceeds the Bitcoin protocol's target mining rate of 144 blocks per day.

[19]See the preliminaries of the Appendix for a proof of the existence and uniqueness of a comprehensive equilibrium.

I assume that equilibrium 2a is representative of the daily mining rate during a 2016-block period. As such, the Bitcoin protocol will choose the new level of difficulty $\delta_2 = \delta^* (p_{b2})$. It follows from X_S of (9) and δ^* of (10) that the protocol will choose the new level of difficulty δ_2 in accordance with (1) since

$$\delta_2 = \frac{p_{b2} (\omega + f) \left[\frac{(24)60^2 \phi 10^9}{2^{32}} \right]}{\eta F + \frac{\phi \xi}{1000} (24) \, p_e} = \delta_1 \frac{X_S (p_{b2}; \delta_1)}{\overline{X}} \tag{12}$$

and the daily mining and target mining rates are given by $\frac{X_S(p_{b2};\delta_1)}{\omega}$ and $\frac{\overline{X}}{\omega} = 144$, respectively.

It follows from X_S of (9) that the increase in the level of difficulty from δ_1 to δ_2 results in an upward rotation of the supply curve. Referring to Figure 1, the supply curve rotates upward until $X_S = \overline{X}$ at the price p_{b2}, since p_{b2} gives rise to the network hashrate ϕM_2. The marginal cost of mining has increased because the greater difficulty causes miners to expend more resources on electricity to mine a given number of blocks. Since the price p_{b2} is unchanged, it follows from (7) that an increase in difficulty does not result in an exit of miners from the industry.[20] At the point labeled 2b, the protocol is in equilibrium since the mining rate is equal to its target given the network hashrate ϕM_2, and the network has no further incentive to change the level of difficulty. Since the protocol has no knowledge of the demand curve, however, 2b is not, in general, a market equilibrium. At 2b there is excess demand, which causes the price of a bitcoin to rise to p_{b3} and the number of miners to increase to M_3. At the market equilibrium labeled 3 with price p_{b3}, the demand X'_D is equal to the supply of bitcoins given the new level of difficulty δ_2. While the protocol is no longer in equilibrium, the mining rate is closer to its target than before the increase in difficulty.

More pertinently, however, since p_{b3} exceeds p_{b2}, it is clear from Figure 1 that the decrease in supply due to the greater difficulty results in an exaggerated price response relative to the

[20] Recall that the number of miners adjusts immediately to changes in the price of a bitcoin p_b, and then the difficulty adjusts in turn.

price that would have prevailed had the difficulty not been adjusted. The resulting price, however, *is fully supported* by marginal costs since the price is equal to the marginal cost in the new equilibrium labeled 3.

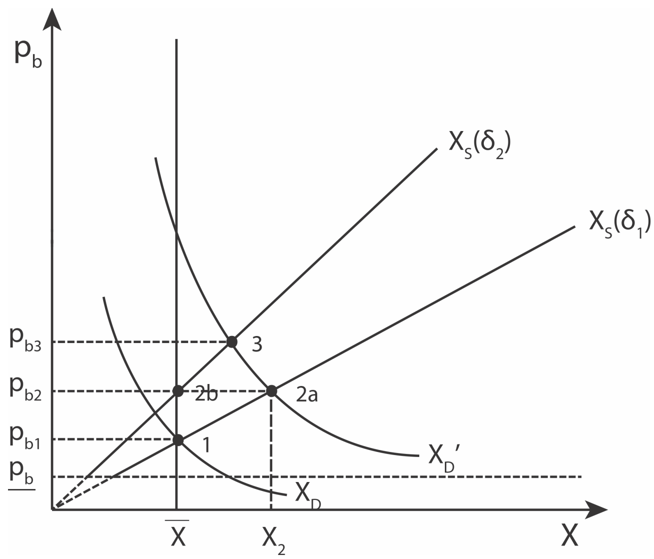

Figure 1. Bitcoin price adjustment.

Figure 2 depicts successive positive demand shocks and demonstrates that they result in a rapidly increasing price path that may be mistaken for a bubble despite being based on marginal costs. While the increase in demand may be due to the optimistic beliefs of investors regarding the future price of bitcoins, the protocol will work to increase the level of difficulty correspondingly, validating investors' beliefs, and encouraging another round of optimism! The analysis of a negative demand shock is analogous and a series of negative demand shocks may be mistaken for a bursting bubble since the equilibrium price will fall rapidly as the level of difficulty decreases. It follows that the interaction of the Bitcoin protocol with investors' beliefs can manifest as momentum and boom-and-bust cycles in the price of bitcoins. Unlike a bubble, however, price is equal to marginal cost all the while.

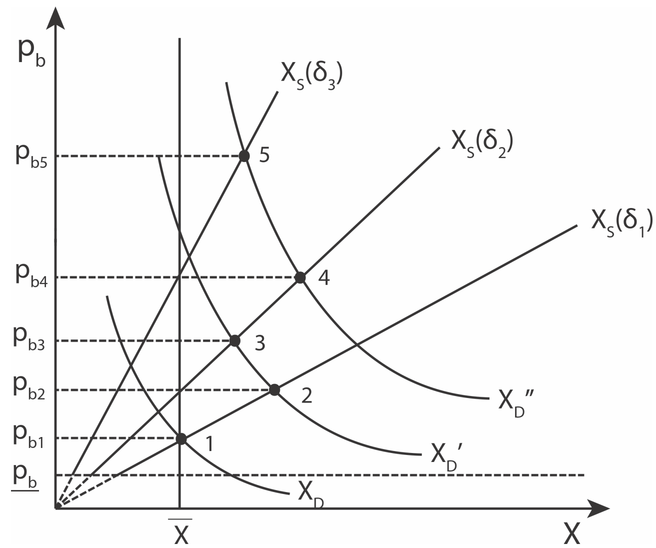

Figure 2. Successive positive demand shocks.

I define the fundamental value of a bitcoin p_b^f to be that price such that the protocol is in equilibrium. For a given level of difficulty δ, the fundamental value is given by the inverse supply curve $p_b(X;\delta)$ evaluated at $X = \overline{X}$. While the fundamental value is not necessarily equal to the market price of a bitcoin, it provides an appropriate theoretical benchmark since it is the protocol that governs its value. As shown in Figure 3, if a demand shock is permanent, the market price will approach the fundamental value consistent with a comprehensive equilibrium since successive adjustments of the difficulty will occur until the mining rate is equal to its target in the limiting comprehensive equilibrium. Given that the market is competitive, the protocol is constantly maneuvering the market price toward a price consistent with equilibrium in the protocol, a process that is only temporarily disrupted by shocks to demand. Referring to Figure 1, it is clear from the equilibrium labeled 1 that because three curves intersect at the same point in a comprehensive equilibrium: the supply X_S, the demand X_D, and the target $X = \overline{X}$, the fundamental value can be identified by using the information contained in only the supply curve X_S and the target $X = \overline{X}$. The level of difficulty can be viewed as a sufficient statistic for the demand parameters α and ε since the difficulty is adjusted by the protocol according to the equilibrium mining rate detected by the network, which depends on both the supply and demand for bitcoins. The fundamental value of a bitcoin p_b^f need not depend directly on the determinants of demand since the same information is contained in the level of difficulty.[21] Also, since the fundamental value depends on the level of difficulty, it follows that the difference between the market price and the fundamental value at a given point in time can be represented by a shift in demand that originated from a comprehensive equilibrium, along a *constant* supply curve. For instance, referring to Figure 1, the difference between the market price p_{b2} and the fundamental value p_{b1} while $\delta = \delta_1$, is due to the demand shock while holding the supply curve $X_S(\delta_1)$ constant.

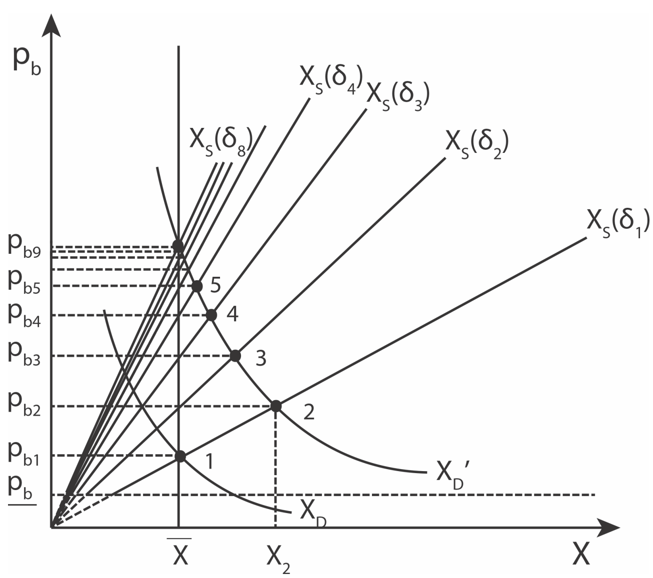

Figure 3. Limiting bitcoin price adjustment.

The following proposition characterizes the bitcoin's fundamental value and uses it as a

[21] As we'll see in Section 3, the fundamental value depicted in Figure 14 closely follows the market price of a bitcoin without using any direct information about demand.

benchmark to relate the return on bitcoins to the rate of increase in the level of difficulty.

Proposition 1 *(i) The fundamental value of a bitcoin p_b^f is equal to the miners' costs relative to their expected block reward and fees, and appreciates by an amount which is equal to the rate of increase in the level of difficulty δ. (ii) The market price of a bitcoin p_b appreciates by an amount which is equal to $\frac{1}{1+\varepsilon}$ times the rate of increase in the level of difficulty δ.*

Proof. See the Appendix. ■

From the supply curve X_S of (9), it follows that the marginal cost of producing $\overline{X}$ bitcoins at a given level of difficulty δ is

$$p_b^f \equiv p_b\left(\overline{X};\delta\right) = \frac{\left[\eta F + \frac{\xi\phi}{1000}\left(24\right)p_e\right]M^*}{\left(\omega + f\right)\left[\frac{(24)60^2\phi M^* 10^9}{\delta 2^{32}}\right]}. \tag{13}$$

Proposition 1 demonstrates that since the fundamental value is found at the intersection of the supply curve X_S of (9) with the vertical line $X = \overline{X}$, an increase in difficulty causes the fundamental value to appreciate at a rate that is equal to the rate of increase in the level of difficulty. Referring to Figure 1, an increase in difficulty from δ_1 to δ_2 results in an increase in the fundamental value of a bitcoin from $p_{b1} = p_b\left(\overline{X};\delta_1\right)$ to $p_{b2} = p_b\left(\overline{X};\delta_2\right)$, where $\frac{p_b\left(\overline{X};\delta_2\right)}{p_b\left(\overline{X};\delta_1\right)} = \frac{\delta_2}{\delta_1}$. An increase in difficulty causes the market price of bitcoins to appreciate at a rate that is *less* than the rate of increase in the level of difficulty, however, because the market price is found at the intersection of the supply curve X_S of (9) with the demand curve X_D of (11), and hence an upward rotation of the supply curve results in an increase in the market price that is less than the proportional increase in difficulty.[22] This divergence is even greater for higher elasticities of demand. Referring again to Figure 1, an increase in the level of difficulty from δ_1 to δ_2 results in an increase in the market price from p_{b2} to p_{b3},

[22] As we will see in Section 3, Figure 13 depicts the relation between the market price of bitcoins and the level of difficulty as predicted by Proposition 1(ii).

which corresponds to a movement along the demand curve from point 2a to point 3. Since $\frac{p_b(X_2;\delta_2)}{p_b(X_2;\delta_1)} = \frac{\delta_2}{\delta_1}$, it is clear from Figure 1 that $\frac{p_{b3}}{p_{b2}} < \frac{\delta_2}{\delta_1}$.

In summary, we have established that the supply of bitcoins is linear and upward sloping through the origin. An increase (decrease) in the level of difficulty results in an upward (downward) rotation of the supply curve. After 2016 blocks have been mined, if the Bitcoin network detects that the mining rate differs from the target of 144 blocks per day, the protocol will adjust the difficulty in such a way that the existing network hashrate will result in a 10-minute interval between successive blocks mined. The protocol's enforcement of a fixed quantity of bitcoins supplied over time results in exaggerated price responses and successive positive demand shocks result in a rapidly increasing price path that may be mistaken for a bubble despite being based on marginal costs. Proposition 1 characterizes the fundamental value of a bitcoin and establishes that the return on bitcoins is proportional to the rate of increase in the level of difficulty.

2.1 Efficiency

We have seen that the Bitcoin protocol uses the level of difficulty as an instrument to maintain a mining rate of 144 blocks per day. In this section we will see that an increase in difficulty works in effect like a government's placing an ad valorem tax on the price of a commodity. Hence, whenever the protocol increases the difficulty, a distortion loss results because too few bitcoins are produced relative to the equilibrium quantity that would exist in the absence of an intervention. Instead of accruing tax revenue, however, the increase in difficulty imposes additional electricity costs on miners. Although a higher price for the bitcoin is obtained, the rents that would have arisen from limiting the supply are wasted as they neither benefit a government nor the miners. An analogous scenario obtains whenever the protocol decreases the level of difficulty.

Recall that an increase in the level of difficulty rotates the supply curve upward so that, for a given quantity of bitcoins supplied, the supply price under the new level of difficulty is proportional to the supply price under the previous level of difficulty. When the protocol increases the difficulty from δ_1 to δ_2, it follows from X_S of (9) that

$$\frac{p_b\left(X;\delta_2\right)}{p_b\left(X;\delta_1\right)} = \frac{\delta_2}{\delta_1} \equiv 1 + \psi \tag{14}$$

and hence an increase in difficulty is equivalent to a government's imposing an ad valorem tax on the price of bitcoins equal to the percentage increase in the level of difficulty $\psi > 0$.

Figure 4a extends Figure 1 to assess, employing a partial equilibrium framework, the effect on social welfare of an increase in difficulty. As shown in Figure 4a, after the increase in difficulty, the price of a bitcoin rises to p_{b3} and the quantity of bitcoins produced per day falls to X_3. There is a wedge between the price consumers pay p_{b3} under the higher difficulty level and the price miners receive p'_{b3}, where $p_{b3} = (1+\psi)\,p'_{b3}$, since a total of $\psi p'_{b3}$ for each of the X_3 bitcoins that are produced per day is dissipated as additional electricity costs. Since $X_2 - X_3$ bitcoins are no longer traded in the market, the consumer and producer surplus that occurs in market equilibrium 2 is reduced by the distortion or 'deadweight' loss depicted by the dotted triangular area. The consumer and producer surplus that occurred in equilibrium 2 is also reduced by the additional electricity costs depicted by the large hatched rectangular area.

It follows that *both* consumers and miners that participate in equilibrium 2 are adversely affected by the increase in difficulty,[23] and that an increase in difficulty is far less efficient than if a government were to impose an equivalent ad valorem tax on miners that would yield the same equilibrium price p_{b3} and quantity X_3. While the tax would result in the same distortion loss as the difficulty adjustment, it would provide government revenue while

[23] The relative proportion of losses depends on the relative elasticities of supply and demand.

the rents that go toward the additional electricity costs under the difficulty adjustment are simply wasted.

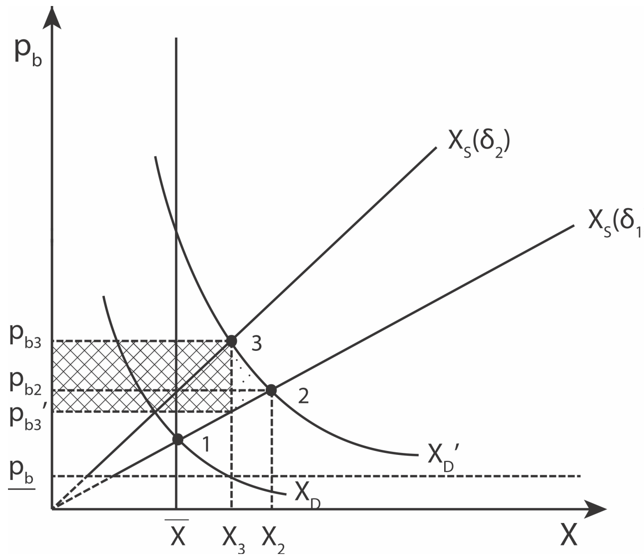

Figure 4a. An increase in the level of difficulty.

The following proposition quantifies the total welfare losses that result from an increase in the Bitcoin level of difficulty as the sum of the additional electricity costs and the distortion loss.

Proposition 2 *(i) The welfare loss due to a percentage increase in the level of difficulty given by* $\psi = \frac{\delta_2 - \delta_1}{\delta_1} > 0$ *is approximately*

$$\Gamma(\psi) = \psi p_b (X_3; \delta_1) X_3 + \frac{1}{2} \frac{\varepsilon}{1+\varepsilon} p_{b2} X_2 \psi^2 \tag{15}$$

where ε *is the elasticity of demand,* p_{b2} *and* X_2 *are the equilibrium price and quantity before the increase in difficulty from* δ_1 *to* δ_2*, and* X_3 *is the equilibrium quantity after the increase in difficulty. (ii) The equilibrium quantity* X_3 *after the increase in difficulty is approximately* $\frac{1+\varepsilon-\varepsilon\psi}{1+\varepsilon} X_2$.

Proof. See the Appendix. ■

If instead there is a negative demand shock that leads to a mining rate that is less than 144 blocks per day, the operation of the Bitcoin protocol is symmetric in the sense that the level of difficulty will decrease. Analogously to Proposition 2, we can express the welfare gain due to a percentage decrease in difficulty given by $\varphi = \frac{\delta_2 - \delta_1}{\delta_1} < 0$ as approximately

$$\Omega(\varphi) = -\varphi p_b(X_3; \delta_1) X_3 - \frac{1}{2}\frac{\varepsilon}{1+\varepsilon} p_{b2} X_2 \varphi^2 \tag{16}$$

where ε is the elasticity of demand, p_{b2} and X_2 are the equilibrium price and quantity before the decrease in difficulty from δ_1 to δ_2, and X_3 is the equilibrium quantity after the decrease in difficulty. Figure 4b depicts an initial comprehensive equilibrium labeled 1, with price p_{b1}, quantity $\overline{X}$ and level of difficulty δ_1, and a negative demand shock that leads to a decrease in the market price to p_{b2}. Because some miners will exit the industry in response to the lower price of bitcoins, in the subsequent equilibrium labeled 2, the mining rate is less than 144 blocks per day. Consequently, the protocol will decrease the level of difficulty from δ_1 to δ_2. The supply curve rotates downward until the mining rate is equal to the target $\overline{X}$ given the network hashrate associated with p_{b2}. Consequently, the price falls to p_{b3} and the mining rate increases to X_3 in the equilibrium labeled 3. It follows from (14) that a decrease in difficulty is equivalent to a government's providing an ad valorem subsidy to miners equal to the percentage decrease in the level of difficulty (i.e., when $\varphi < 0$). There is a wedge between the price consumers pay p_{b3} under the lower level of difficulty δ_2 and the price that miners receive p'_{b3}, where $p_{b3} = (1+\varphi) p'_{b3}$, since a total of $-\varphi p'_{b3}$ for each of the X_3 bitcoins that are produced per day is gifted by the protocol as lower electricity costs. As shown in Figure 4b, the reduction in costs results in a level of output X_3 that is too large for consumers and producers to capture the full benefit, since the hatched rectangular area is reduced by a distortion loss depicted by the dotted triangular area. A decrease in difficulty, however, is far more efficient than the equivalent ad valorem subsidy to the miners since it would result in the same distortion loss but there is no cost to the government due to providing the subsidy.

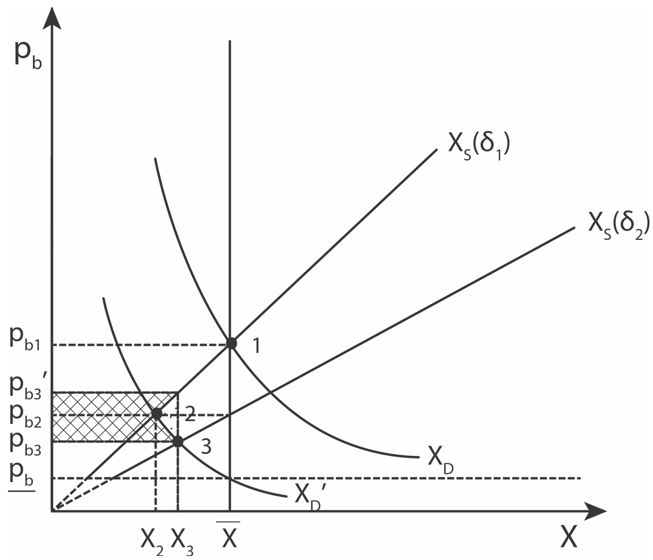

Figure 4b. A decrease in the level of difficulty.

The following proposition compares the loss due to an increase in the level of difficulty with the gain that is due to an equivalent percentage decrease in the difficulty. It demonstrates that the welfare cost of an increase in difficulty is larger than the welfare benefit of an equivalent proportional decrease in the difficulty.

Proposition 3 *The welfare loss due to a percentage* ψ *increase in difficulty is greater in absolute value than the gain in welfare due to a percentage decrease in the difficulty by the same percentage.*

Proof. See the Appendix. ■

Figure 4c depicts a decrease in difficulty and an increase in difficulty by the same proportion. Since an increase in the difficulty occurs whenever the equilibrium quantity prior to the change in difficulty is greater than the target supply of bitcoins $\overline{X}$, whereas a decrease in the difficulty occurs whenever the equilibrium quantity is lower than $\overline{X}$, the wedge between the price consumers pay under the new level of difficulty and the price that miners receive is larger under the difficulty increase. While the *proportional* change is the same, it is, under the increase in difficulty, applied to a higher price, and over a greater quantity. Hence, as shown in Figure 4c, because the supply curve is upward sloping, increases in difficulty are not offset by commensurate proportional decreases in difficulty since their welfare effects do not have the same size. Moreover, the distortion losses that amass each time the level of difficulty is changed reduce the welfare benefits and further increase the welfare costs.

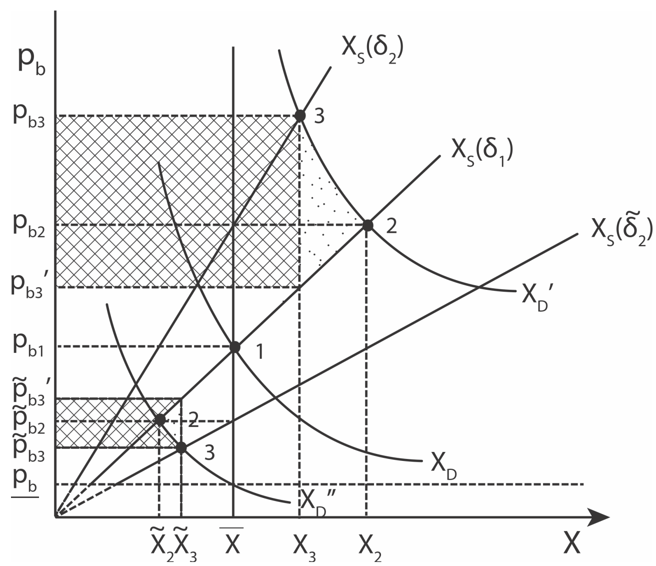

Figure 4c. An equivalent proportional increase and decrease in difficulty.

In this section we have established that while Bitcoin is a decentralized peer-to-peer payment network with no central authority, its protocol regularly intervenes in the market by using the level of difficulty as an instrument to maintain a constant supply of bitcoins over time. Consequently, demand shocks give rise to volatile prices and the price path may exhibit momentum and boom-and-bust cycles. Proposition 1 establishes that the fundamental value of the bitcoin is characterized by miners' equipment and electricity costs relative to their expected block reward and fees. Using it as a benchmark, it follows that the market price of bitcoins appreciates in proportion to the rate of increase in the level of difficulty. While the market is allocatively efficient, since price is equal to marginal cost (and hence the bitcoin is an efficient store of value for the electricity costs used in its production), Proposition 2 establishes that losses are incurred by contemporaneous consumers and producers (miners) of bitcoins whenever the level of difficulty rises. Moreover, Proposition 3 demonstrates that the welfare costs that arise because of increases in the level of difficulty are not offset by equivalent proportional decreases in the level of difficulty, and hence the protocol imposes welfare losses on society that accumulate over time. While the bitcoin is esteemed for its nongovernmental design, its system of supply management is far less efficient than if a government were to regulate the number of bitcoins by imposing a tax on its price.

3 Data description

In this section I describe the data and perform model diagnostics to assess how well the theoretical model set out in Section 2 fits the data.

The data was acquired from several sources. The daily average USD price of the bitcoin across major bitcoin exchanges, daily data on the Bitcoin difficulty level, the Bitcoin block reward and fee, and the number of blocks mined per day, were acquired by using Blocksci, an open-source software platform for blockchain analysis.[24,25] Daily USD price data for new (unused) Antminer mining rigs (models S1, S2, S3, S4, S5, S7, S9 and S11) sold on Amazon Marketplace by third party sellers, which is accessible from Amazon.com, was acquired by using an API for the Amazon price tracker Keepa.com.[26] The reported price is the lowest of the prices available from the sellers and does not include shipping costs; missing data

[24] See Kalodner et al. (2017) and https://github.com/citp/BlockSci.

[25] Note that Blocksci utilizes an API for coindesk.com to provide the end of day price of a bitcoin.

[26] The Amazon standard identification numbers (ASIN) that identify the models are: B00I0F4IMI, B00KH9339O, B00NZDBWKG, B00NWHT18A, B00RCTIY4G, B014OGCP6W, B01MCZVPFE, and B07KPF2DJJ.

correspond to periods of time when all sellers are out of stock. The mining rig specifications regarding the hash rate and energy efficiency were obtained directly from Amazon.com and are provided in Table 1. Since several Antminer models may be sold in the Amazon Marketplace at a given point in time, I constructed the daily average USD price by averaging over the prices of all Antminer models that were available for sale on a given day. Similarly, to obtain the daily average hashrate and the daily average energy efficiency of the Antminer rigs, I averaged over the gigahashes per second (GHash/s) and the joules per gigahash (Joules/GHash) of all Antminer models that were available for sale on the given day, respectively.

The sample period is 17 March 2014 to 13 January 2019. Although the first Antminer rig (model S1) was available to the public from Amazon Marketplace on 30 December 2013, as shown in Table 1, 17 March 2014 was the first day that price information on the Antminer S1 rig was tracked by Keepa.com. While there are numerous brands of bitcoin mining rigs available on the market (and it is possible for miners to build their own rig), Antminer rigs, which are produced by the Chinese company Bitmain, are on the technological frontier in terms of their power and energy efficiency. Bitmain sells its hardware to the general public and its market share is estimated to be 70%–80%.[27]

Mining typically takes place in countries where there is cheap electricity, such as the People's Republic of China, the Czech Republic, Iceland, Japan, the Republic of Georgia, Russian Federation, Sweden, and the United States. However, by far the most mining takes place in the People's Republic of China.[28] Bitmain, which owns one of the world's largest bitcoin mines, in Inner Mongolia, was known to be paying just 4 cents per kWh of electricity (DeVries, 2018). Consequently, I conservatively estimate the average price of electricity used

[27] See https://coincentral.com/how-antminer-became-the-best-bitcoin-mining-hardware-in-less-than-two-years/.

[28] It is estimated that Chinese mining pools control more than 70% of the Bitcoin network's collective hashrate. See https://www.buybitcoinworldwide.com/mining/china/.

in mining to be 0.05 USD per kWh. Also, I estimate the expected lifespan of a mining rig to be two years, so that the daily depreciation rate is 1/730.

Figure 5 depicts the bitcoin price path over the sample period in both levels and logs. While the price has an exponential growth, since the logarithm of the price is approximately linear, numerous boom-and-bust cycles are also evident, with the largest boom occurring in late 2017. On 16 December 2017, bitcoin reached its maximum price of 19,343.04 USD,[29] and the price has predominantly decreased since that time up to the end of the sample period. Figure 6 depicts the daily level of difficulty over the sample period in both levels and logs. It is clear that the level of difficulty has been increasing exponentially until 17 October 2018, which is about 10 months beyond the point at which the price of a bitcoin began to fall. After 17 October 2018, the difficulty has predominantly decreased (4 of the 6 remaining difficulty adjustments were decreases). Over the sample period, the level of difficulty was adjusted downward only 21 times, which is 15.9% of all difficulty adjustments. Figure 7 depicts the sum of the Bitcoin block reward and fees over the sample period. It is clear that the block reward was halved from 25 bitcoins to 12.5 bitcoins on 9 July 2016 and that fees were much more prevalent throughout 2017, probably due to congestion in the Bitcoin blockchain. Figure 8 presents a standard plot and a boxplot of the number of blocks mined per day (the daily mining rate), where a horizontal line is drawn at the target mining rate of 144 blocks. It is clear that the mining rate frequently differs from its target, reaching a minimum of 80 blocks per day (on 11 and 12 November 2017) and a maximum of 216 blocks per day (on 10 December 2015) during the sample period. The mean and median blocks mined per day are 151.6 and 151, respectively, indicating that the daily mining rate typically exceeds the target during the sample period.

Figure 9 depicts the Antminer rig specifications over the sample period. We can see

[29] Recall that the price data is an average over the major bitcoin exchanges. As stated in the Introduction, the highest price reached by Bitcoin on a single exchange was 19,783.21 USD.

that, on average, Antminer rigs have become more powerful over time, since their hashrate is increasing. While the energy efficiency of the rigs is improving, as the rate of joules per gigahash is decreasing over time, their greater power is large enough to result in greater energy use since the number of watts used (joules per second) is increasing over time. Note that the gaps in the Antminer rig specification data from 12 October 2017 to 17 October 2017, from 19 October 2017 to 26 October 2017, from 13 November 2017 to 17 November 2017, from 24 November 2017 to 5 December 2017, from 9 December 2017 to 10 December 2017, and from 3 January 2018 to 4 January 2018 correspond to periods of time when none of the sellers in the Amazon Marketplace had any of the Antminer rigs listed in Table 1 in stock. This demonstrates that there was probably excess demand for mining equipment during this time period, which was when the price of the bitcoin was quite high (approximately 5,500 USD) and rising rapidly. Figure 10 depicts the average price of Antminer rigs over the sample period and their average price per gigahash per second. We can see that mining equipment costs have generally increased in tandem with the market price of the bitcoin (the correlation between the bitcoin's price and the average price of Antminer rigs is .59). The average price of Antminer rigs relative to their average gigahash per second, however, has been steadily decreasing over time and reached a low of 0.03 USD by the end of the sample period. Figure 11 depicts the miners' daily average equipment and electricity costs as defined in (8) and the proportion of electricity in their daily costs over time.[30] With the exception of late 2017, when mining equipment was extraordinarily costly due to the plausible excess demand, electricity costs were growing as a share of the miners' daily costs. Electricity costs approached 80.2% of daily costs by the end of the sample period due to the increasing energy usage of the mining equipment evident in Figure 9 and the falling price of mining rigs evident in Figure 10.

[30]Which, from (8), is $\frac{\frac{\phi\xi}{1000}(24)p_e}{\eta F+\frac{\phi\xi}{1000}(24)p_e}$.

3.1 Model diagnostics

Figure 12 assesses whether the Bitcoin network adjusts the difficulty according to Eq. (12). The diagram plots the ratio of the new level of difficulty relative to the previous one against the mining rate divided by the target mining rate of 144, where the mining rate is the average number of blocks mined per day during the interval between difficulty adjustments. It is clear that the data are consistent with (12) since the points line up on the 45 degree line and the two variables have a correlation of .99.

To check Proposition 1, which states that the bitcoin's market price p_b appreciates at a rate of $\frac{1}{1+\varepsilon}$ times the rate of increase of the level of difficulty δ, Figure 13 plots the log of the bitcoin's market price against the log of the level of difficulty, where the price data have been aggregated by taking the mean over the interval between adjustments of the level of difficulty. We can see that the relation between the price and difficulty is remarkably strong and, as predicted by the model, log-linear. Using least squares provides an estimate of the slope equal to 0.58, where the regression line is drawn in Figure 13 along with the 45 degree line. (The regression results are provided in Table 2.) In accordance with Proposition 1, the rate of increase in the market price is estimated to be less than the rate of increase in the level of difficulty. Also, it follows from Proposition 1 that we can then estimate the elasticity of demand ε to be equal to .72,[31] which is close to the estimate of ε I obtain directly through identification of the demand curve in Section 5.2 below.[32]

Next, I use the data to simulate the fundamental value of the bitcoin defined in (13) and compare it with the market price of the bitcoin. As we have seen in Section 2, the fundamental value is not necessarily equal to the market price. While the fundamental value is independent of the demand parameters α and ε, the level of difficulty δ is a sufficient statistic for them, since, as described in Section 2, adjustments in difficulty depend on the

[31] We have that $\frac{1}{1+\varepsilon} = .58$ or, equivalently, $\varepsilon = .72$.
[32] We will see in Section 5.2 that I obtain an estimate of the price elasticity of demand equal to .73.

equilibrium mining rate detected by the network, which depends on both the supply and demand for bitcoins. Figure 14 depicts the simulated fundamental value and the actual price of the bitcoin in both levels and logs. The fundamental value tracks variations in the market price quite well since the correlation between them is .79. We can see that the fundamental value rose sharply in July 2016 when the block reward was halved, since a decrease in the block reward decreases the miners' expected block reward. It also fell sharply in July 2017 because of the introduction of the powerful Antminer S9,[33] since an increase in the hashpower of the miners' equipment increases the miners' expected block reward. It is plausible that the market price of a bitcoin does not exhibit such sharp adjustments because both of these events could have been anticipated by participants in the bitcoin market. From Figure 14 it is clear that the fundamental value follows the general shape of the bitcoin price path since it exhibits an exponential upward trend and a large boom and bust phase that started in late 2017, albeit with a lag. As such, Figure 14 presents evidence that adjustments in the level of difficulty by the protocol are in response to the level of market prices *prior* to the new level of difficulty, during the interim between difficulty adjustments, as they incentivize the network hashrate in accordance with the model set out in Section 2.[34] Figure 15 plots the difference between the actual bitcoin price and the simulated fundamental value, in both levels and logs. We can see that the market price was in line with the fundamental value well up to late 2017, after which the actual price exceeded the fundamental value by 100% to 185% until early 2018. After 17 August 2018, the price exceeded the fundamental value by less than 35% in absolute value and was again in line with the fundamental value.

To better understand the discrepancy between the market price and the fundamental value between 1 July 2017 and 31 December 2017, it is informative to compare the network

[33] We can see from Figure 9 that the Antminer S9 became the dominant Antminer rig in the market in July 2017 since the average hashpower of the Antminer rigs approaches 14,000 GHash/s.

[34] From Figure 1 it is clear that after the difficulty adjustment to δ_2, the fundamental value is equal to p_{b2}, which is the price that incentivized the network hashrate during the interim between the difficulty adjustments δ_1 and δ_2.

hashrate ϕM^* inferred from (7) as a function of the market price p_b and the network hashrate determined by solving for the target waiting time to find a block of (5) for ϕM as a function of the level of difficulty δ. The former network hashrate presumes the instantaneous free entry of miners in response to expected profits driven by the market price of bitcoin. Given the network's choice of difficulty, the latter network hashrate yields a ten-minute interval between successive blocks mined. If the free entry of miners is an accurate assumption, then both approaches must yield the same network hashrate when the level of difficulty is adjusted since whenever $M = M^*$, from (5) it follows that $\delta = \delta^*$. As shown in Figure 16, however, the network hashrate predicted by (7) was significantly larger in late 2017 than the network hashrate that yields a ten-minute block time of (5), indicating that there were probably barriers to entry during this time period. Despite the soaring price of the bitcoin, it is clear from Figure 8 that the average number of blocks mined per day (the mining rate) reached its lowest values in the sample period during late 2017 and it is clear from Figure 6 that the network decreased the level of difficulty four times between 1 July 2017 and 31 December 2017,[35] which are consistent with insufficient mining. It is plausible that entry was unable to keep step with rapidly increasing prices due to a shortage of mining equipment, exacerbated by the obsolescence of the mining equipment that was already in operation. As noted above, during this six-month period, there were occasions when none of the sellers in the Amazon Marketplace had an Antminer rig in their inventory, indicating that state-of-the-art rigs were generally difficult to acquire.[36] Also, the introduction of the Antminer S9, whose hash power is nearly three times that of the S7 and more than seven times that of the S5, could have forced the exit of miners whose equipment was no longer profitable. Moreover, significant time lags between higher bitcoin prices and the adoption of new equipment could have been

[35] This represents 19% of the total number of decreases in difficulty that were granted by the network in a six-month period, during the almost five-year sample period.

[36] Massive demand for mining equipment is not unprecedented. For instance, the rise of bitcoin mining was responsible for creating a global shortage of graphics cards, which were initially a profitable way to mine for bitcoins prior to the invention of application specific integrated circuits (ASICs).

caused by requisite learning costs for miners. It follows that the anomalous 10 month period between December 2017 and October 2018, during which the difficulty was increasing while the price of a bitcoin was decreasing, could have occurred because the rate of mining was catching up to the rate that was consistent with the incentives provided by market prices, given the hashpower of the latest equipment.[37]

In summary, we have seen that the data is largely consistent with the model formulated in Section 2. While there was a large discrepancy between the market price of the bitcoin and its fundamental value in late 2017, this probably resulted from barriers to entry that are not wholly captured by the model. It remains to test whether fluctuations in the price path that are not explained by the model can be attributed to price bubbles caused by investor behavior.

4 Econometric model

4.1 Testing for multiple bubbles

In this section I apply the bubble detection method developed in Phillips et al. (2015a; 2015b) to determine whether deviations of the market price of the bitcoin from its fundamental value as defined in Section 2 demonstrate evidence of explosive behavior.[38] Phillips et al. (2015a; 2015b) extend Phillips et al. (2011), which develops a supremum augmented Dickey–Fuller (SADF) test for the presence of a bubble based on a sequence of forward recursive right-tailed ADF unit root tests, and a dating strategy that identifies points of origin and termination of a bubble based on a backward regression technique. The generalized supremum ADF (GSADF) method developed in Phillips et al. (2015a; 2015b) also relies on recursive right-

[37]For a discussion of this anomalous time period, see the article in The Economist, available at https://www.economist.com/graphic-detail/2019/02/07/will-bitcoins-price-crash-cut-into-its-energy-use.

[38]Note that in order to carry out the tests, gaps in the Antminer rig specification and price data during late 2017 were filled by replacing each missing value with the most recent present value prior to it.

tailed ADF tests but uses flexible window widths in its implementation. Instead of fixing the starting point of the recursion at the first observation, the GSADF test extends the sample coverage by changing both the starting point and the endpoint of the recursion over a feasible range of flexible windows. This enhanced approach is designed to outperform previous bubble detection methods in detecting explosive behavior whenever multiple bubble episodes occur in the data, since it covers more subsamples of the data and has greater window flexibility. It also delivers a consistent dating mechanism whenever multiple bubbles occur.

Specifically, for a times series y_t that has size T, the ADF test for a unit root against the alternative of an explosive root (right-tailed) is undertaken by using least squares to estimate the following autoregressive specification

$$\Delta y_t = \alpha_{r_1,r_2} + \beta_{r_1,r_2} y_{t-1} + \sum_{i=1}^{k} \psi^i_{r_1,r_2} \Delta y_{t-i} + \upsilon_t,\ \ \upsilon_t \sim NID\left(0, \sigma^2_{r_1,r_2}\right) \tag{17}$$

for a given lag order k, where NID denotes independent and normally distributed. Eq. (17) is estimated repeatedly using subsets of the sample data. If we renormalize the indices of the time series to lie within the interval $[0, 1]$, then the total sample can be indexed by values of r that range from 0 to 1. If r_1 and r_2 are the starting and ending points of a regression sample, the ADF statistic calculated from the sample is the t-ratio for the estimate of β_{r_1,r_2} and is denoted by $ADF^{r_2}_{r_1}$. The SADF statistic is defined as the supremum of the ADF statistics over the range of r_2

$$SADF\left(r_0\right) = \sup_{r_2 \epsilon [r_0,1]} ADF^{r_2}_{0}$$

where r_0 is the minimum window size. In contrast with the SADF test, the GSADF test varies the endpoint r_2 from the minimum window size r_0 to 1, and the starting point r_1 also varies from 0 to $r_2 -\ r_0$. The GSADF statistic is defined as the supremum of the ADF statistics in a double recursion over all feasible ranges of r_1 and r_2

$$GSADF\left(r_0\right) = \sup_{\substack{r_2 \epsilon [r_0, 1] \\ r_1 \epsilon [0, r_2 - r_0]}} ADF_{r_1}^{r_2}.$$

Date stamping bubble episodes under the new approach of Phillips et al. (2015a; 2015b) involves constructing a supremum ADF test on a backward expanding sample sequence where the endpoint of each sample is fixed at r_2 and the start point r_1 varies from 0 to $r_2 - r_0$. (The backward ADF test in Phillips et al. (2011) is a special case of the backward supremum ADF test with $r_1 = 0$.) The estimated origination date of a bubble is defined as the first observation whose backward supremum ADF statistic exceeds its corresponding critical value, which is based on $r_2 T$ observations. The estimated termination date of a bubble is the subsequent observation (that exceeds a specified period of time) whose backward supremum ADF statistic falls below its corresponding critical value. The date-stamping strategy may be used as an ex ante real-time dating procedure, whereas the GSADF test is an ex post statistic used for analyzing a given data set for bubble behavior.

As shown in the Appendix,[39] from X_S of (9) and X_D of (11) it follows that the relation between the market price of a bitcoin p_b and its fundamental value p_b^f is log-linear:

$$\log\left(p_b\right) = \frac{1}{1+\varepsilon}\log\left(\alpha\right) - \frac{1}{1+\varepsilon}\log\left(\overline{X}\right) + \frac{1}{1+\varepsilon}\log\left(p_b^f\right). \tag{18}$$

Treating demand shocks α as random, I use ordinary least squares (OLS) to estimate the relation between the price of a bitcoin and its fundamental value

$$\log p_{bt} = \alpha_0 + \alpha_1 \log p_{bt}^f + \upsilon_t \tag{19}$$

[39] See the proof of Proposition 1.

for daily observations indexed by t.

The estimates obtained for α_0 and α_1 are reliable because serial correlation in the errors will not affect the unbiasedness or consistency of OLS estimators.[40] Any departures of the price of bitcoin from the marginal cost of mining must be evident in the residuals from the regression $\widehat{\upsilon_t} = \log p_{bt} - \widehat{\alpha_0} - \widehat{\alpha_1} \log p_{bt}^f$. For this reason, I apply the SADF and GSADF tests to the residuals to determine if there is any empirical evidence of explosive behavior to infer the existence of bubbles.[41] While this approach is consistent with the model of Section 2, as a robustness check, I also test whether there is evidence of explosive behavior in the difference $\log p_{bt} - \log p_{bt}^f$, which does not rely on performing least squares. Measuring the price of the bitcoin relative to its fundamental value amounts to holding the supply curve constant for a given level of difficulty, which isolates changes in the price of a bitcoin that are due to shifts in the demand curve during the interim between adjustments of the difficulty, and removes the effects of the difficulty adjustment mechanism on the price.

4.2 Estimating efficiency losses

In order to estimate the efficiency losses net of gains established in (15) and (16), I first estimate the elasticity of demand ε for bitcoins. The model set out in Section 2 indicates that short intervals of time surrounding adjustments in the Bitcoin difficulty level will be characterized by large supply shocks that are likely to swamp any shocks to demand, permitting identification of the demand curve.

After log linearizing X_S of (9) and X_D of (11), it follows that the structural supply and demand equations are given by

$$X_D = \varepsilon p_b + \upsilon_d \tag{20}$$

[40] Serial correlation in the errors will affect the efficiency of the estimates, however, and with positive serial correlation, the OLS estimates of the standard errors will be smaller than the true standard errors. See Pindyck and Rubinfeld (1997).

[41] I undertake both tests for the sake of completeness and to provide the reader with as much evidence as possible.

$$X_S = \gamma_1 p_b + \gamma_2 z + \upsilon_s$$

where ε is the parameter of interest and the exogenous supply shifters included in z (the level of difficulty, block reward and fees, mining hashrate, energy efficiency, and equipment costs), enter only the supply equation and not the demand equation. The asymptotic bias in the least squares estimate of ε depends on the correlation of p_b with the demand shocks υ_d since

$$\text{plim } \widehat{\varepsilon}_{OLS} = \varepsilon + \frac{cov\left(\upsilon_d, p_b\right)}{var\left(p_b\right)}.$$

It follows that if least squares is used to estimate ε during a period in which supply shocks are large relative to demand shocks, there will be large supply-induced changes in p_b with only small changes in υ_d. Least squares will not be very biased since the numerator of the bias term will be small while the denominator will be large.

To distinguish periods of time in which difficulty adjustments have large effects on the supply, I choose intervals of sizes 7, 9, 11 and 13 days centered at the time of the difficulty adjustment. This procedure uses about 50% to 93% of the data, since there are approximately 14 days between difficulty adjustments. The size of the interval trades off the need to have enough data to estimate the demand curve accurately with the need to hone in on a period of time in which there is relatively more variation in supply than demand. After fixing the length of the time interval, I use least squares to estimate Eq. (20) for each interval that occurs during the sample period, and keep only those estimates of ε that are significant at a 5% (or better) level. For each length of time interval (7, 9, 11 and 13 days), I obtain an estimate of ε by averaging over the retained estimates for that time interval, yielding an estimate that has a lower variance than any estimate obtained from an interval around a single difficulty adjustment. Since this procedure provides an estimate of ε for each interval length, the robustness of the method is indicated by the stability of the estimate over the four window sizes. Finally, I derive a single estimate for ε by averaging over these estimates, providing a further reduction in variance.

Next, I estimate Γ of (15) and Ω of (16) for each interval between difficulty adjustments, to find the total efficiency losses over the sample period.[42] For each interval between difficulty adjustments, I find the average number of blocks mined per day (the daily mining rate) to determine the average quantity of bitcoins supplied per day X_2 and then, holding the initial level of difficulty δ_1 constant, use the inverse supply curve derived from (9) to estimate the corresponding price p_{b2}. I use the approximation for X_3 provided in Proposition 2 to find the average quantity of bitcoins supplied after the difficulty adjustment and then obtain the corresponding price $p_b\left(X_3;\delta_1\right)$ from the inverse supply curve derived from (9). The percentage change in the level of difficulty ψ is obtained by subtracting 1 from the ratio of the level of difficulty at the end of the interval δ_2 to the level of difficulty at the beginning of the interval δ_1 according to Eq. (14). I use the estimate of the elasticity of demand ε obtained from the procedure described above. Finally, if the percentage change in the level of difficulty is positive, I calculate the average loss according to Γ of (15) and if it is negative, I calculate the average benefit according to Ω of (16). I estimate the total net efficiency loss due to adjustments in the Bitcoin difficulty level by multiplying each average loss or benefit by the length of the interval (the number of days between the respective difficulty adjustments) and then aggregate the total losses net of the total benefits throughout the sample period.

[42] Note that in order to include all intervals, gaps in the Antminer rig specification and price data during late 2017 were filled by replacing each missing value with the most recent present value prior to it.

5 Results

5.1 Testing for multiple bubbles

I first estimate Eq. (19) to obtain the regression residuals. The regression results are reported in Table 3 and Figure 17 depicts the scatter plot of the log price of bitcoin versus the log of its fundamental value, and plots the regression line in addition to the 45 degree line. It is clear from Figure 17 that there is a strong, positive log-linear relation between the market price of the bitcoin and its fundamental value. Also, the slope of the regression line is less than 1, which, as shown in (18), is in accordance with the model.

I apply the summary SADF and GSADF tests to the log bitcoin price data, the OLS residuals from the regression of the log bitcoin price on the log fundamental value, and difference between the log bitcoin price and the log fundamental value. Table 4 presents the test statistics and the finite sample critical values of the two tests obtained from Monte Carlo simulations with 2,000 replications of 1764 observations. In performing the ADF regressions and calculating the critical values, the smallest window contains 93 observations of the sample, based on the rule $r_0 = .01 + 1.8/\sqrt{1764}$.

In regard to the log price data series, from Table 4, the SADF and GSADF statistics are 3.7 and 3.9, which both exceed their 1% right-tailed critical values ($3.7 > 2.2$ and $3.9 > 2.9$), providing strong evidence of explosive subperiods in the raw bitcoin price data. Figure 18 depicts the backward ADF sequence (based on the SADF test) and the corresponding 95% and 99% ADF critical values obtained from Monte Carlo simulations with 2,000 replications for each observation of interest, for the log price data series (and, for the sake of completeness, each time series in question). Figure 19 depicts the analogous information for the backward SADF sequence (based on the GSADF test). From Figure 18 it is clear that there is one identified period of explosive behavior for the log price time series, when the recursive ADF statistic exceeds the 95% critical value sequence, that is at least one week long. This is

2017-05-01 to 2018-11-15. The recursive ADF statistic continues to exceed the 99% critical value sequence for two subsets of this time period. These are 2017-05-20 to 2018-03-30; and 2018-04-08 to 2018-05-25. From Figure 19, there are seven identified periods of explosive behavior for the log price time series, when the recursive SADF statistic exceeds the 95% critical value sequence, that are at least one week long. These are 2014-09-28 to 2014-10-08; 2015-01-13 to 2015-01-20; 2015-11-02 to 2015-11-09; 2016-05-28 to 2016-06-21; 2016-12-22 to 2017-01-05; 2017-03-01 to 2018-05-22; and 2018-11-19 to 2018-12-16. The recursive SADF statistic continues to exceed the 99% critical value sequence for four subsets of these time periods. These are 2016-06-03 to 2016-06-20; 2016-12-23 to 2017-01-04; 2017-05-19 to 2018-03-06; and 2018-11-20 to 2018-12-08. It is clear from comparing Figures 18 and 19 that the strategy based on the recursive SADF test statistic is more sensitive since, at the 5% level of significance, it identifies periods of explosive behavior that are not detected by the strategy based on the recursive ADF test statistic.

Once we take into account the fundamental value of the bitcoin, however, it is clear from Table 4 that the SADF and GSADF statistics for the OLS residuals and the difference between the log price and the log fundamental value are well below their 10% right-tailed critical values. There is no overwhelming evidence of bubbles in the price of the bitcoin since we cannot reject the null hypothesis of no bubbles at even the 10% significance level. It follows that once we take into account the Bitcoin protocol's difficulty adjustment mechanism, the explosive behavior that is apparent in the bitcoin price path is explained.

5.2 Estimating efficiency losses

For each length of the intervals (7, 9, 11 and 13 days), centered at the time of the difficulty adjustment, the estimates of the elasticity of demand ε are 0.112, 1.16, 0.847, and 0.818, respectively. The average estimate, then, is .73, which demonstrates that there is a fairly inelastic demand for the bitcoin. Using this estimate for the elasticity of demand, I estimate the total net efficiency losses from 17 March 2014 to 13 January 2019 to be 323.82 million USD.[43] Table 5 shows the breakdown of the net losses for each year in the sample period and Figure 20 presents a plot of the net efficiency losses for each year along with the unique levels of difficulty over time.[44] While the total net losses imply an average annual net loss of approximately 66.39 million USD, as shown in Figure 20, the average is misleading as a measure of the annual costs since the net efficiency losses were increasing exponentially throughout the majority of the sample period. Since, from Γ of (15), the losses are an increasing function of the change in the level of difficulty δ, this is due to the fact that the level of difficulty was increasing exponentially during that time. To put these losses into perspective, I estimate the total electricity used by the Bitcoin network in terawatt hours (TWh), which is provided in the third column of Table 5.[45] Assuming an electricity cost of 0.05 USD per kWh, the net efficiency losses due to adjustments in the level of difficulty as a percentage of the total cost of electricity used to power the Bitcoin network are shown in the fourth column of Table 5. Since the electricity used by the Bitcoin network also has been increasing exponentially due to the fact that the level of difficulty was increasing exponentially over the majority of the sample period, the efficiency losses as a percentage of total electricity costs have been fairly stable and are, on average, 9.3% of the total electricity costs.

In this section we have seen that while both the SADF and GSADF tests provide evidence of explosiveness in the bitcoin price path, applying the same tests after specifying

[43] I estimate the total efficiency losses to be 390.73 million USD and the total efficiency benefits to be 66.91 million USD. The large magnitude of losses relative to gains is in accordance with Proposition 3 and because only 15.9% of the difficulty adjustments during the sample period were downward.

[44] Note that the first year is only approximately 10 months long due to the length of the sample period.

[45] Since the network hashrate is ϕM^* gigahashes per second, the terawatt hours used by the network can be estimated as $\phi M^* \xi \frac{24}{10^{12}}$ per day, where M^* is given in (7). While using M^* to estimate the hashrate presumes the free entry of miners, it is consistent with the estimate of efficiency losses Γ of (15) and benefits Ω of (16), which also presume free entry.

fundamentals in accordance with the model does not. While there was a significant difference between the fundamental value of the bitcoin and its price during late 2017 (as shown in Figure 15), the discrepancy does not provide evidence for explosive behavior and hence, even during this time period, there is no evidence of bubble formation. As discussed in Section 3.1, this discrepancy is probably due to entry barriers not taken into account by the model. It follows that the model is sufficient to explain any explosive behavior in bitcoin prices. This result provides strong evidence that the boom and bust cycles apparent in the bitcoin price data are not bubbles caused by investor behavior but rather are a consequence of the economic functioning of the Bitcoin protocol. We have also seen that in order to maintain a constant supply of bitcoins in the market, the protocol imposes efficiency losses (benefits) on contemporaneous consumers and miners of bitcoin whenever the level of difficulty rises (falls). On average, net costs were about 9.3% of the total electricity costs to run the Bitcoin network during the sample period.

6 Conclusion

This paper has developed a microeconomic model to analyze the economic functioning of the Bitcoin protocol. The model established that the fundamental value of a bitcoin is equal to the miners' equipment and electricity costs relative to their expected block reward and fees. While Bitcoin is a decentralized peer-to-peer network with no central authority, the mechanism for adjusting the level of difficulty encoded in its protocol amounts to an inflexible system of supply management. Hence, demand shocks have an exaggerated effect on the price of the bitcoin and each adjustment in the level of difficulty of mining a bitcoin results in social welfare losses. We have seen that once we specify the fundamentals, which include the miners' costs and their expected block reward and fees, there is no evidence of the formation of bubbles in the price of the bitcoin. Also, we have seen that the social welfare losses imposed by the protocol's intervention in the market add up to over 320 million USD from March 2014 to January 2019. While these costs were incurred by the contemporaneous consumers and miners, it is the eventual holders of bitcoins who benefit over time since the price of the bitcoin appreciates by an amount proportional to the rate of increase in the Bitcoin difficulty level. To the extent that bitcoin mining is not powered by renewable resources, we should further take into consideration the external costs of bitcoin production, since electricity generation is one of the leading sources of greenhouse gas emissions. I leave a thorough analysis of this important issue for future research.

References

[1] Antonopoulos, A. (2017): *Mastering Bitcoin: Programming the Open Blockchain.* Sebastopol, CA: O'Reilly.

[2] Bianchi, D. (2018): "Cryptocurrencies as an Asset Class? An Empirical Assessment," Working paper.

[3] Brunnermeier M. (2008): "Bubbles," in Palgrave Macmillan, eds., *The New Palgrave Dictionary of Economics*. Palgrave Macmillan, London.

[4] Brunnermeier, M., and Oehmke, M. (2012): "Bubbles, Financial Crises, and Systemic Risk," in George M. Constantinides, Milton Harris, and Rene M. Stulz, eds., *Handbook of the Economics of Finance*, Volume 2, 1221-88. Amsterdam: North-Holland.

[5] de Vries, A. (2018): "Bitcoin's Growing Energy Problem," *Joule,* 2, 801–9.

[6] Dong, F., Xu, Z., and Zhang, Y. (unpublished): "Bubbly Bitcoin," Working paper.

[7] Easley, D., O'Hara, M., and Basu, S. (2018): "From Mining to Markets: The Evolution of Bitcoin Transaction Fees," *Journal of Financial Economics*, Forthcoming.

[8] Evans, G. (1991): "Pitfalls in Testing for Explosive Bubbles in Asset Prices," *American Economic Review*, 81(4), 922–30.

[9] Garber, P. (1989): "Tulipmania," *Journal of Political Economy* 97(3): 535–60.

[10] Garber, P. (1990): "Famous First Bubbles," *Journal of Economic Perspectives* 4(2): 35–54.

[11] Gurkaynak, R. (2005): "Econometric Tests of Asset Price Bubbles: Taking Stock," Finance and Economics Discussion Series 2005-04, Board of Governors of the Federal Reserve System (US).

[12] Homm, U., and Breitung, J. (2012): "Testing for Speculative Bubbles in Stock Markets: A Comparison of Alternative Methods," *Journal of Financial Econometrics*, 10(1), 198–231.

[13] Kalodner, H., Goldfeder, S., Chator, A., Möser, M., and Narayanan, A. (2017): "BlockSci: Design and applications of a blockchain analysis platform." Available from https://arxiv.org/pdf/1709.02489.pdf

[14] Liu, Y., and Tsyvinski, A. (2018): "Risks and Returns of Cryptocurrency," National Bureau of Economic Research Working Paper 24877.

[15] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013): “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names,” in Proceedings of the 2013 Internet Measurement Conference (IMC), pp. 127–40.

[16] Pagnotta, E. and Buraschi, A. (2018): "An Equilibrium Valuation of Bitcoin and Decentralized Network Assets," Working paper.

[17] Phillips, P., Shi, S.-P., and Yu, J. (2015a): “Testing for Multiple Bubbles: Historical Episodes of Exuberance and Collapse in the S&P 500”, *International Economic Review*, 56, 1043–78.

[18] Phillips, P., Shi, S.-P., and Yu, J. (2015b): Testing for Multiple Bubbles: Limit Theory for Real Time Detectors. *International Economic Review*, 56(4), 1079–1134.

[19] Phillips, P., Wu, Y., and Yu, J. (2011): “Explosive Behavior in the 1990s Nasdaq: When Did Exuberance Escalate Asset Values?” *International Economic Review*, 52, 201–26.

[20] Phillips, P., and Yu, J. (2011): “Dating the Timeline of Financial Bubbles During the Subprime Crisis,” *Quantitative Economics*, 2, 455–91.

[21] Pindyck, R., and Rubinfeld, D. (1997): *Econometric Models and Economic Forecasts*. New York, NY: McGraw-Hill/Irwin.

[22] Talbot, J. (2004): *Grounds for Agreement: The Political Economy of the Coffee Commodity Chain*. Lanham, MD: Rowman & Littlefield.

Appendix

Preliminaries:

The existence and uniqueness of a comprehensive equilibrium follows from the fact that there exists a unique equilibrium in the protocol for any given $p_b \geq 0$ and a unique equilibrium in the market for any given $\delta \geq 0$. (i) Since Eq. (4) set equal to miners' daily fixed costs ηMF and Eq. (5) are both linear in δ and M, and Eq. (5) goes through the origin while the free entry condition obtained from Eq. (4) results in a constant level of δ for all M, there is a unique solution (δ^*, M^*) for any given $p_b \geq 0$ and set of parameters. (ii) Since Eq. (9) is linear through the origin and Eq. (11) is convex to the origin, there is a unique solution (X^*, p_b^*) for any given $\delta \geq 0$ and set of parameters. (iii) It follows that there exists a unique comprehensive equilibrium $(X^*, p_b^*, \delta^*, M^*)$ whenever $\delta = \delta^*$ and $p_b = p_b^*$.

Proof of Proposition 1:

From the supply curve X_S of (9), it follows that the marginal cost of producing $\overline{X}$ bitcoins at a given level of difficulty δ is

$$p_b^f \equiv p_b\left(\overline{X};\delta\right) = \frac{\left[\eta F + \frac{\xi\phi}{1000}(24)\, p_e\right] M^*}{(\omega + f)\left[\frac{(24)60^2\phi M^* 10^9}{\delta 2^{32}}\right]} \tag{A1}$$

where $p_b(X;\delta)$ is the inverse supply curve. From (A1) it follows that $\frac{d\log\left(p_b^f\right)}{d\log(\delta)} = 1$ and hence the fundamental value of a bitcoin p_b^* appreciates at a rate equal to the rate of increase in the level of difficulty δ.

Also, from X_S of (9) and X_D of (11) it follows that

$$\begin{aligned} p_b &= \left[\frac{\alpha\left[\eta F + \frac{\xi\phi}{1000}(24)\, p_e\right]}{(\omega+f)\left[\frac{(24)60^2\phi 10^9}{\delta 2^{32}}\right]\overline{X}}\right]^{\frac{1}{1+\varepsilon}} \\ &= \left[\frac{\alpha}{\overline{X}}\right]^{\frac{1}{1+\varepsilon}} p_b^f(\delta)^{\frac{1}{1+\varepsilon}}. \end{aligned}$$

Taking logs and then differentiating with respect to δ while holding the demand curve constant yields

$$\log(p_b) = \frac{1}{1+\varepsilon}\log(\alpha) - \frac{1}{1+\varepsilon}\log\left(\overline{X}\right) + \frac{1}{1+\varepsilon}\log\left(p_b^f(\delta)\right)$$

and hence

$$\begin{aligned} d\log(p_b) &= \frac{1}{1+\varepsilon} d\log\left(p_b^f(\delta)\right) \\ &= \frac{1}{1+\varepsilon} d\log(\delta). \end{aligned}$$

Proof of Proposition 2:

From Figure 4a it is clear that a total of $p_{b3} - p'_{b3} = \psi p'_{b3}$ for each of the X_3 bitcoins that are produced per day is dissipated due to the additional electricity costs, given by $\psi p_b (X_3; \delta_1) X_3$, where $p'_{b3} = p_b (X_3; \delta_1)$. It remains to derive the deadweight (distortion) loss DWL, or the second term of (15).

In equilibrium, we have

$$X_S (p_b) = X_D (q_b) \tag{A2}$$

where the price paid by consumers is $q_b = p_b (\psi) (1 + \psi)$ and the price received by producers is $p_b (\psi)$. Starting in an initial equilibrium such as equilibrium 2 depicted in Figure 4a, prior to an increase in the level of difficulty, we have that $\psi = 0$ and $q_b = p_b$.

Differentiating (A2) with respect to ψ yields $\frac{\partial X_S}{\partial p_b} \frac{dp_b}{d\psi} = \frac{\partial X_D}{\partial q} \left[\frac{dp_b}{d\psi} (1 + \psi) + p_b \right]$ and it follows that

$$\begin{aligned} \frac{dp_b}{d\psi} &= \frac{\frac{\partial X_D}{\partial q} p_b}{\frac{\partial X_S}{\partial p_b} - \frac{\partial X_D}{\partial q} (1 + \psi)} \frac{\frac{p_b}{X}}{\frac{p_b}{X}} \\ &= \frac{\frac{\partial X_D}{\partial q} \frac{p_b}{X} p_b}{\frac{\partial X_S}{\partial p_b} \frac{p_b}{X} - \frac{\partial X_D}{\partial q} \frac{p_b}{X} (1 + \psi)} \\ &\approx -\frac{\varepsilon}{1 + \varepsilon} p_b \end{aligned} \tag{A3}$$

since ψ is small, where the elasticity of demand $\varepsilon = -\frac{\partial X_D}{\partial q} \frac{p_b}{X} > 0$, and the elasticity of supply $\frac{\partial X_S}{\partial p_b} \frac{p_b}{X} = 1$ since the supply curve is linear through the origin. Hence $\Delta p_b \approx \frac{dp_b}{d\psi} \psi = -\frac{\varepsilon}{1+\varepsilon} p_b \psi$. Also,

$$\begin{aligned} \frac{dq_b}{d\psi} &= \frac{dp_b}{d\psi} (1 + \psi) + p_b \\ &\approx -\frac{\varepsilon}{1 + \varepsilon} p_b + p_b \\ &= \frac{1}{1 + \varepsilon} p_b \end{aligned}$$

where the second line follows from (A3) and the fact that ψ is small. Hence $\Delta q_b \approx \frac{dq_b}{d\psi} \psi = \frac{1}{1+\varepsilon} p_b \psi$ and we have $|\Delta p_b| + |\Delta q_b| = p_b \psi$.

The effect of the adjustment on the equilibrium output is given by

$$\begin{aligned}\frac{dX}{d\psi} &= \frac{\partial X_S}{\partial p_b}\frac{dp_b}{d\psi} \\ &\approx -\frac{\partial X_S}{\partial p_b}\frac{\varepsilon}{1+\varepsilon}p_b \\ &= -\frac{\varepsilon}{1+\varepsilon}X\end{aligned}$$

where the second line follows from (A3) and the third line follows because $\frac{\partial X_S}{\partial p_b}\frac{p_b}{X} = 1$. It follows that $\Delta X \approx \frac{dx}{d\psi}\psi = -\frac{\varepsilon\psi}{1+\varepsilon}X$ and hence

$$\begin{aligned}DWL &= \frac{1}{2}\left(|\Delta p_b| + |\Delta q_b|\right)|\Delta X| \\ &= \frac{1}{2}\frac{\varepsilon}{1+\varepsilon}p_{b2}X_2\psi^2\end{aligned}$$

where p_{b2} and X_2 are the equilibrium price and quantity supplied of bitcoins prior to the difficulty adjustment.

Moreover, we can approximate X_3, the equilibrium quantity of bitcoins after the difficulty adjustment, by

$$\begin{aligned}X_3 &\approx X_2 - |\Delta X| \\ &= \left[1 - \frac{\varepsilon\psi}{1+\varepsilon}\right]X_2.\end{aligned}$$

Proof of Proposition 3:

Let $\psi = -\varphi$, $X_2 > \overline{X}$, and $\widetilde{X_2} < \overline{X}$. From (15) and (16) we have that

$$\begin{aligned}\Gamma(\psi) - \Omega(\varphi) &= \psi p_b(X_3;\delta_1)X_3 + \frac{1}{2}\frac{\varepsilon}{1+\varepsilon}p_{b2}X_2\psi^2 - \left[-\varphi p_b\left(\widetilde{X_3};\delta_1\right)\widetilde{X_3} - \frac{1}{2}\frac{\varepsilon}{1+\varepsilon}\widetilde{p_{b2}}\widetilde{X_2}\varphi^2\right] \\ &= \psi\left[p_b(X_3;\delta_1)X_3 - p_b\left(\widetilde{X_3};\delta_1\right)\widetilde{X_3}\right] + \frac{1}{2}\frac{\varepsilon}{1+\varepsilon}p_{b2}X_2\psi^2 + \frac{1}{2}\frac{\varepsilon}{1+\varepsilon}\widetilde{p_{b2}}\widetilde{X_2}\psi^2 > 0\end{aligned}$$

where the second line is positive because $X_3 \geq \overline{X} \geq \widetilde{X_3}$ and, since the supply curve is upward sloping, $p_b(X_3;\delta_1) \geq p_b\left(\widetilde{X_3};\delta_1\right)$.

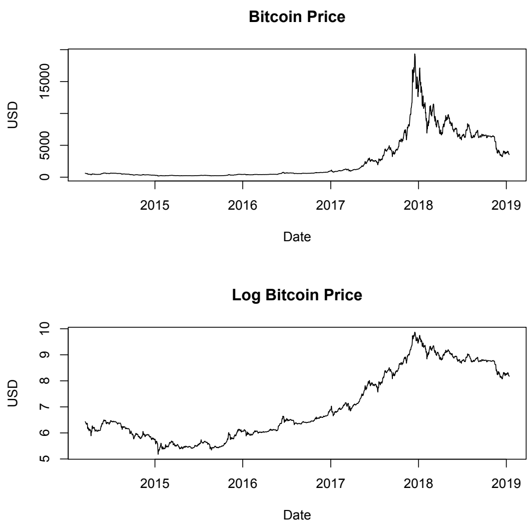

Figure 5

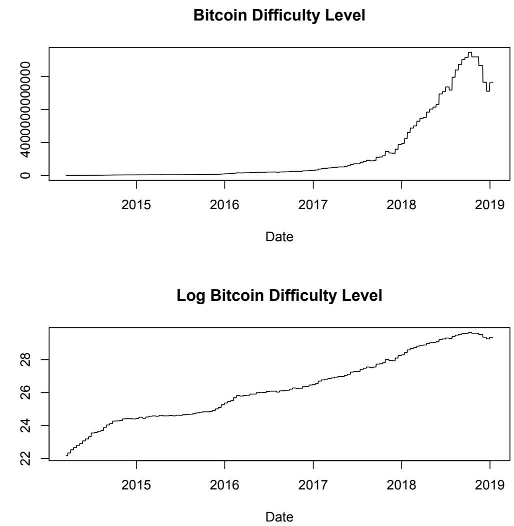

Figure 6

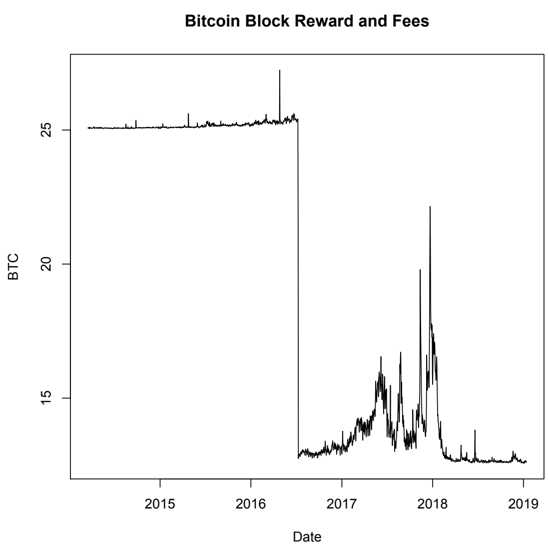

Figure 7

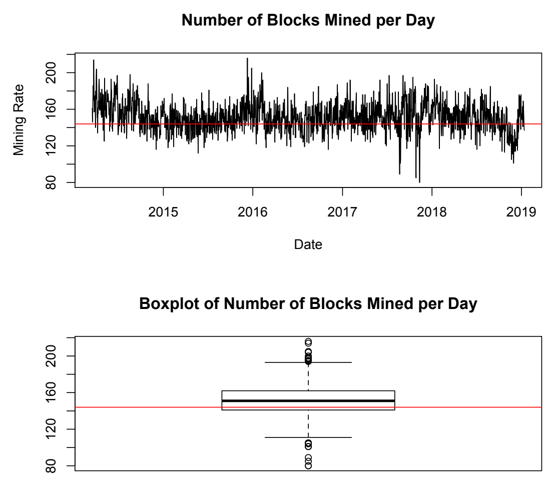

Figure 8

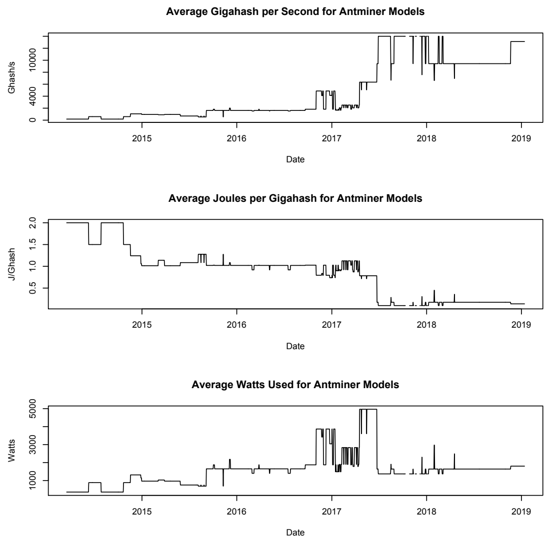

Figure 9

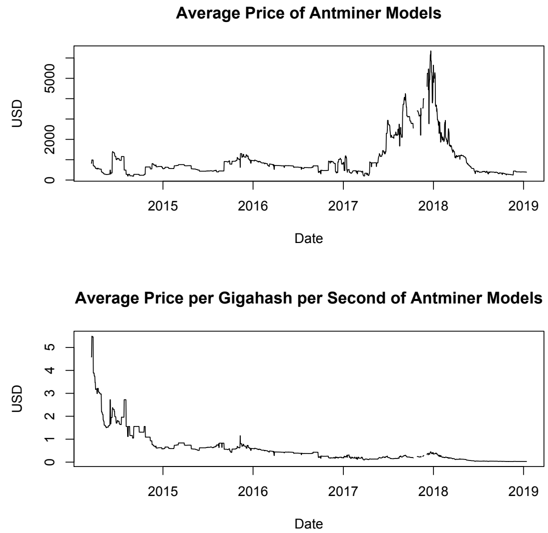

Figure 10

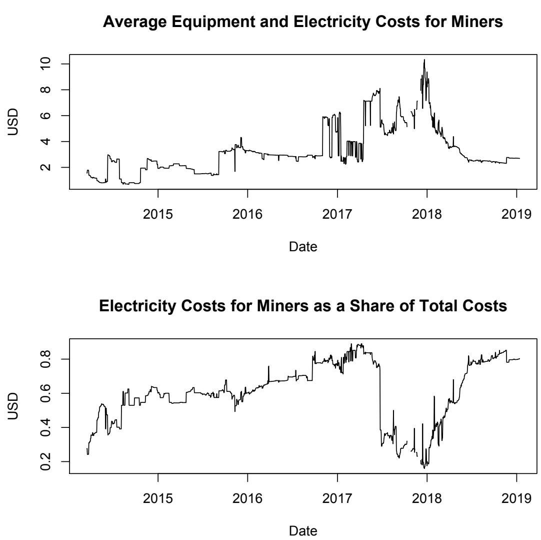

Figure 11

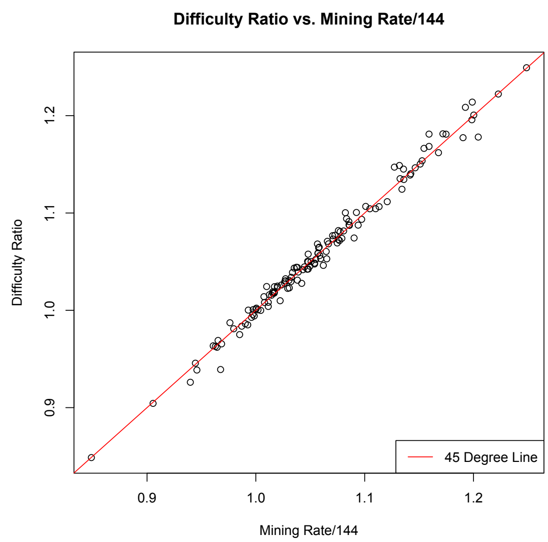

Figure 12

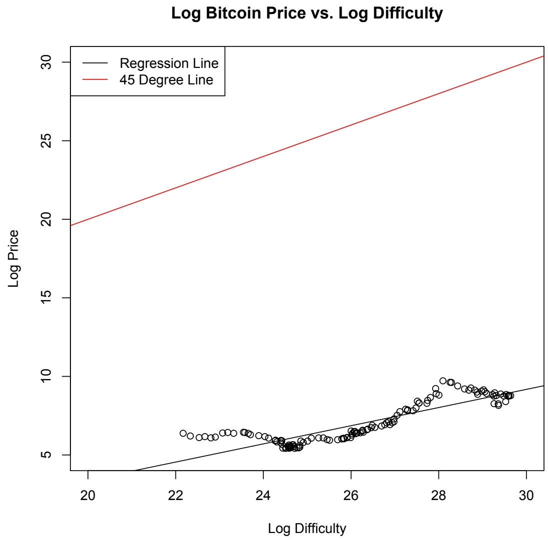

Figure 13

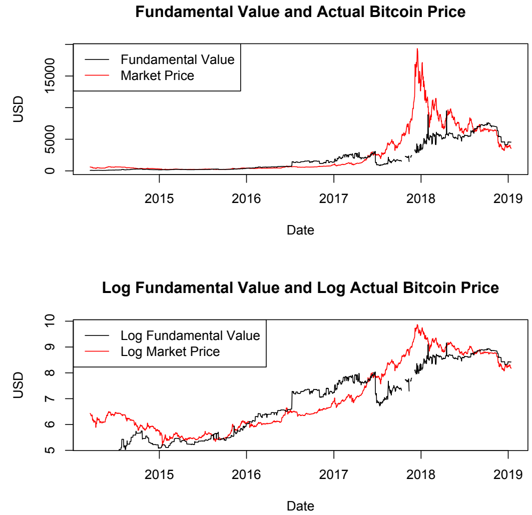

Figure 14

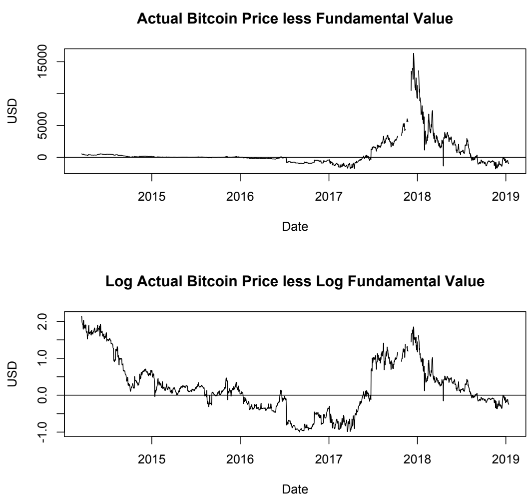

Figure 15

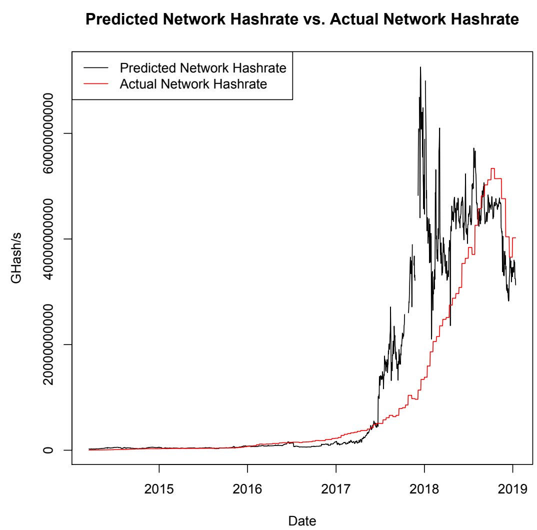

Figure 16

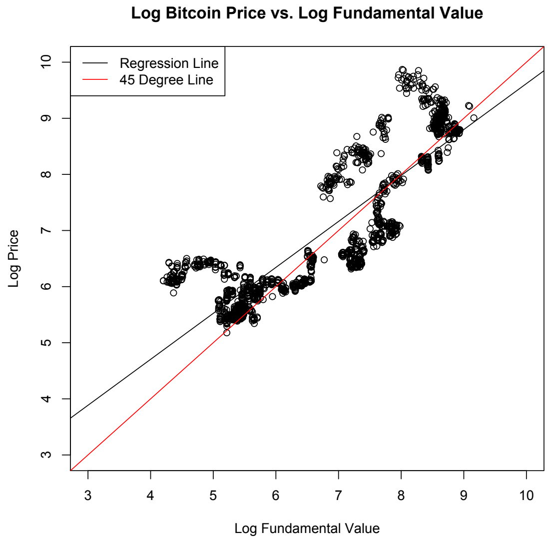

Figure 17

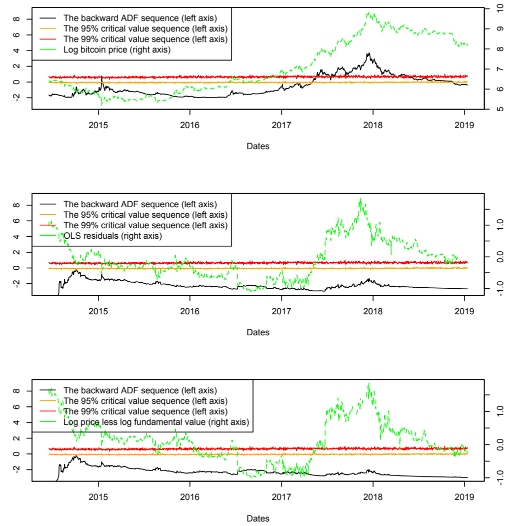

Figure 18

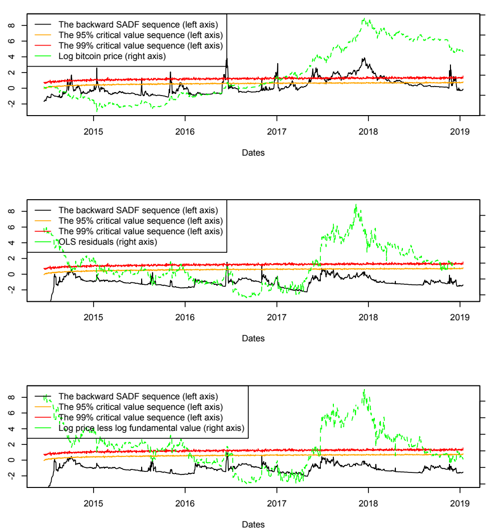

Figure 19

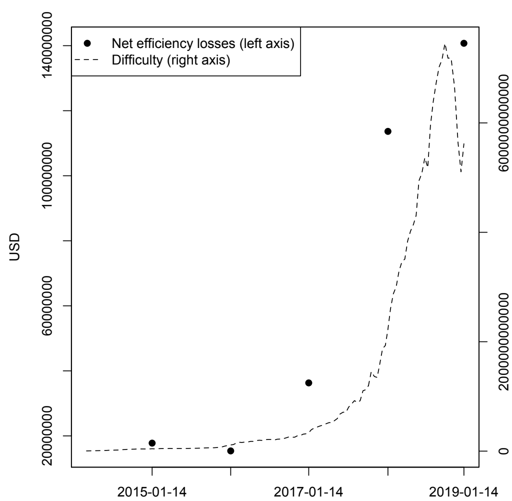

Figure 20

	Tracking Since	First Available	GHash/s	Joules/GHash	Energy Use (Watts)
Antminer S1	14-03-17	13-12-30	180	2	360
Antminer S2	14-06-10	14-05-21	1,000	1	1,000
Antminer S3	14-12-31	14-09-27	441	.83	366
Antminer S4	14-11-18	14-09-25	2,000	.725	1,450
Antminer S5	14-12-28	14-12-22	1,155	.51	590
Antminer S7	15-09-06	15-08-30	4,860	.25	1,210
Antminer S9	16-11-02	18-01-16	14,000	.098	1,372
Antminer S11	18-11-21	18-11-19	20,500	.064	1,312

Table 1. Antminer model specifications.

Constant	–8.179***
	(.74)
Log(Difficulty)	.578***
	(.03)
R-squared	.763
Adjusted R-squared	.7612
No. observations	133

Standard errors are reported in parentheses.
*, **, *** indicates significance at the 95%, 99%, and 100% level, respectively.

Table 2. Regression of the log of the bitcoin's price (averaged over the period for which the difficulty is constant) on the log of the difficulty.

Constant	1.428***
	(.08)
Log(FV)	.819***
	(.01)
R-squared	.7467
Adjusted R-squared	.7465
No. observations	1729

Standard errors are reported in parentheses.
*, **, *** indicates significance at the 95%, 99%, and 100% level, respectively.

Table 3. Regression of the log of the bitcoin's price on the log of the bitcoin's fundamental value.

		Test Statistic	Critical Values		
			90%	95%	99%
Log Price	SADF	3.725	1.3064	1.5806	2.1779
	GSADF	3.8879	2.2066	2.3842	2.8776
Residuals	SADF	–.077541	1.3064	1.5806	2.1779
	GSADF	1.5273	2.2066	2.3842	2.8776
Log Price – Log FV	SADF	–.15092	1.3064	1.5806	2.1779
	GSADF	.96727	2.2066	2.3842	2.8776

Table 4. The SADF and GSADF test statistics and their respective critical values.

Year	Net Efficiency Losses (USD)	TWh	Percent of Total Electricity Costs
2014-03-17 to 2015-01-13	17,770,948	2.1	17.1
2015-01-14 to 2016-01-13	15,378,228	3.9	7.9
2016-01-14 to 2017-01-13	36,294,891	13.2	5.5
2017-01-14 to 2018-01-13	113,643,714	18.8	12.1
2018-01-14 to 2019-01-13	140,735,693	55.1	5.1

Table 5. Net efficiency losses due to difficulty adjustments.