Taxing Bitcoin: Incentivizing the Difficulty Adjustment Mechanism to Reduce Electricity Usage

Andrea Podhorsky
Department of Economics, York University, Toronto, Canada M3J 1P3
email: andrea@yorku.ca

February 2022

Abstract

This paper develops a model of the bitcoin market that views the bitcoin as a tradeable commodity whose supply is managed by the Bitcoin protocol. Miners utilize equipment and electricity to solve complex computational problems and the first miner to solve a problem is rewarded with bitcoins. The protocol adjusts the difficulty of the problem to target a constant growth rate in the supply of bitcoins over time. The model demonstrates that an increase (decrease) in the difficulty works in effect like a government's placing an ad valorem tax (subsidy) on the price of a commodity. The rents that would have arisen from limiting supply, however, are wasted as electricity costs. I show that an actual tax on the price of the bitcoin can be used to displace the electricity costs. Using data from March 2014 to January 2019, I estimate that the difficulty adjustment mechanism resulted in net welfare losses to the miners and users of bitcoins of 373.8 million USD. Average initial tax rates of 35% and 347.5% would have fully displaced the electricity costs and maximized their reduction, respectively.

Keywords: Bitcoin, Cryptocurrencies, Fintech, Supply Management, Difficulty Adjustment, Proof of Work, Social Welfare

JEL codes: O33, G18, H20

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."

−Satoshi Nakamoto, P2P Foundation Forum 2009

1 Introduction

This paper studies how a tax on the price of the bitcoin affects the workings of the Bitcoin network's difficulty adjustment mechanism and the implications for its electricity usage.[1] It sheds light on the current debate over taxing the crypto industry, given its energy and environmental impacts, by demonstrating how a hypothetical tax should be chosen to decrease a Proof of Work (PoW) network's electricity costs. This paper demystifies the workings of the Bitcoin protocol by modeling the bitcoin market in a standard supply-and-demand framework. I show that the Bitcoin protocol's rules-based system of supply management imposes losses on the miners and users of bitcoins, since it transfers their rents from limiting the supply of bitcoins to the providers of electricity. In turn, the additional electricity generation imposes an environmental externality due to the associated CO_2 emissions. Ironically, while some hold their wealth in bitcoins to avoid the inflation that can arise with fiat currencies due to the discretion of central banks, whenever the network's difficulty rises, the miners and users of bitcoins are implicitly 'taxed' by the protocol. I show that an actual tax on the price of the bitcoin can be used to displace the electricity costs that the difficulty adjustment mechanism induces, decreasing electricity usage and generating government revenue. A tax can improve social welfare because the difficulty adjustment mechanism causes a second-best world to arise. A miner who decides whether to enter imposes a negative externality on the bitcoin market since he does not take into consideration his effect on the subsequent level of

[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.

difficulty and the consequence for the network's electricity costs. I use data to estimate the welfare losses that are due to adjustments in the difficulty for a nearly 3-year sample period. For each interval between difficulty adjustments, I also estimate the initial tax that would have resulted in no additional electricity costs and, since electricity costs decrease when the protocol lowers the difficulty, the initial tax that would have maximized their reduction.

Cryptocurrencies such as Bitcoin are electronic payment systems that permit transactions to be made with pseudo-anonymity[2] (Meiklejohn et al., 2013; Malinova and Park, 2017) and without middlemen like banks. The Bitcoin blockchain is an evolving distributed ledger of the transactions made by bitcoin users that is maintained and validated by members of the Bitcoin network. Since it is permissionless, anyone can join the network. To establish trust, Bitcoin's PoW consensus mechanism requires miners to use resources (electricity) to solve complex computational problems in order to confirm transactions and add new blocks to the blockchain ledger. Mining is the process by which bitcoins are created since the first miner to solve the current computational problem (find a correct hash) is rewarded with new bitcoins.[3] Miners utilize equipment that rapidly creates hashes, where a hash is one computation or guess at solving a block. Changes in the difficulty of the computational problem alter the rate of block formation because an increase (decrease) in the difficulty decreases (increases) the probability that a miner will find a correct hash. Given the current block reward, the protocol adjusts the level of difficulty at regular intervals of blocks to target a constant rate of growth in the supply of bitcoins over time.

To demonstrate the network security that PoW provides, if a malicious organization wanted to reverse transactions, it would have to use at least as much processing power as the rest of the network combined. In a '51% attack,' the entity would need to successfully

[2]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.

[3]The current block reward is 6.25 bitcoins. The block reward decreases by one-half only every 210,000 blocks, or approximately four years. See https://en.bitcoin.it/wiki/Controlled_supply

mine blocks on a longer copy of the network's chain out of public view, since the longest chain is what individual nodes accept as the valid version of the blockchain. It could then send a transaction to a victim, launch the attack and double spend the same coins back to itself. Ensuring the network's security requires that the equilibrium per-block payment to miners for running the blockchain is large relative to the one-off benefits of attacking it (Budish, 2018). While there have been many attempts to address the limitations of permissionless blockchains with improved technology, mechanisms able to reach consensus and at the same time preserve transaction security have remained costly (Bakos and Halaburda, 2021).

The remarkable increase in the price of the bitcoin since the network's inception has prompted a rapid surge in mining activity and innovations in mining equipment.[4] The ensuing mining 'arms race' has resulted in an exponential growth in the level of difficulty and thus the amount of electricity directed toward the network (Blandin et al., 2020). Today, in terms of electricity usage, Bitcoin's existence is synonymous with adding a small country to the world. Recent estimates place the annual electricity consumption of the Bitcoin network at 123.64 Terawatt-hours (TWh), which is enough to power Pakistan for a year.[5] Since electricity generation is one of the leading sources of greenhouse gas emissions, Bitcoin production could be imposing a large carbon footprint depending on the miners' geographical locations and the corresponding fuel mixes for electricity generation (Krause and Tolaymat, 2018; Mora et al., 2018; Stoll et al. 2018; Dittmar and Praktiknjo, 2019). It is difficult to precisely estimate the CO_2 emissions from mining since the network largely conceals the miners' locations, thwarting meaningful climate action for the industry. There are now more than 400 PoW cryptocurrencies in existence that have a 1.09 trillion USD market sector capitalization.[6] Unlike typical organizational structures, permissionless blockchains have no

[4]For example, as shown in Table 1 of the Appendix, Bitmain's Antminer S11 rig, which was available 5 years after its first mining rig, the Antminer S1, was more than 100 times more powerful in terms of its hashrate and required only 3.5% of the energy per gigahash.

[5]See: https://www.cbeci.org/cbeci/comparisons

[6]See: https://cryptoslate.com/cryptos/proof-of-work

accountable, centralized decision-making authority. Their networks, which must follow the rules defined in their protocols, are fueled and perpetuated by miners that transcend national boundaries in search of profit.

In Section 2 of the paper, I model the competitive bitcoin mining industry with the free entry of miners in response to profits that are created in accordance with the Bitcoin protocol. I hold all input markets constant and assume that there is no secondary market for the bitcoin. While this facilitates a cleaner analysis, it also emphasizes the fact that miners control the supply of bitcoins, as they receive all of the newly issued bitcoins, and are the main driving force of sell pressure on the Bitcoin network.[7] Miners now receive 27,000 bitcoins per month (valued at 1.3 billion USD using current prices) and must sell bitcoins to cover their operating expenses. Also, the trading volume on exchanges mostly creates volatility and is likely to have a greater effect on the price of the bitcoin in the short run.[8]

I measure the private welfare losses that arise from the difficulty adjustment mechanism and fall on the miners and users of the bitcoin. While I do not explicitly consider the external environmental costs of bitcoin production, since CO_2 emissions can be expressed as a proportion of the Bitcoin network's total electricity usage, this paper establishes an initial point from which to address them by way of incentivizing the protocol to decrease the network difficulty. I also abstract from the external benefits that arise from the difficulty adjustment mechanism due to the disciplining of governments' monetary policy (Raskin et al., 2019) and the provision of a relatively stable alternative to financial markets during times of economic distress (Yu and Zhang, 2018). While it is difficult to measure whether the external benefits of the difficulty adjustment mechanism outweigh its external environmental costs, this paper

[7] D'Souza et al. (2020) provide evidence of the fundamental role of miners in the bitcoin market.

[8] An excellent example of this is the precipitous 40% drop in the price of the bitcoin from approximately 8,000 USD on 11 March 2020 to 4,800 USD on 12 March 2020, which was caused by mass liquidations on the BitMEX exchange. The price quickly rebounded to 6,000 USD by the next day, and was close to 7000 USD just one week later. See: https://www.coindesk.com/bitcoins-crash-triggers-over-700m-in-liquidations-on-bitmex

demonstrates that any net benefits must come at a cost to the miners and users of bitcoins, and the use of a tax to decrease the network's electricity costs will tip the balance in favor of the benefits.

In Section 3, I apply the model to show that welfare losses must occur whenever the protocol intervenes in the market to control the supply of bitcoins. An increase in the 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, it imposes additional electricity costs on the miners. While a higher price for the bitcoin is obtained, the rents that would have arisen from limiting supply are transferred to the producers of electricity. A decrease in the level of difficulty works analogously to a government that provides an ad valorem subsidy (a negative tax) to the miners. I show that the welfare effects of an increase in the difficulty, however, are not offset by a decrease in the 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. In Section 4, I analyze the use of an actual tax on the price of the bitcoin to reduce electricity costs. A tax disincentivizes the entry by miners and substitutes for an increase in the difficulty, displacing electricity costs and generating tax revenue instead. It ultimately improves economic efficiency since electricity generation imposes environmental damages. I demonstrate how a tax affects the workings of the difficulty adjustment mechanism and characterize the tax rates that fully displace and minimize the network's electricity costs. In Section 5, I describe the data and show that the model developed in Section 2 is highly consistent with it. I estimate the price elasticity of demand for the bitcoin and apply the model to estimate the welfare losses that are due to adjustments of the difficulty. I also estimate the initial tax that would have resulted in no additional electricity costs and the initial electricity cost-minimizing tax, for each interval between difficulty adjustments.

Section 6 presents the results. I estimate the price elasticity of demand to be .17, in-

dicating that demand for the bitcoin is quite inelastic. This is plausible since there are few substitutes for the bitcoin due to its unparalleled network security.[9] I estimate the net welfare losses that fall on the miners and users of the bitcoin over the nearly 3-year sample period to be 373.8 million USD, which is about 10.3% of the total electricity cost to power the Bitcoin network during this time period. The magnitude of these losses demonstrates that a significant cost falls on the miners and users of the bitcoin to regulate the supply of bitcoins over time. I estimate the average initial tax that would have fully displaced the electricity costs to be 35% and the average initial tax that would have maximized the reduction in electricity costs to be 347.5%. These rates should be interpreted as the requisite initial corrections to achieve these objectives during the sample period. Since the relation between the change in electricity costs and the tax is monotonic and continuous, the rates provide important benchmarks to guide policy makers in understanding how an arbitrary tax will affect electricity costs.

There is a rapidly growing literature that analyzes the economic functioning and significance of Bitcoin and other cryptocurrencies. Athey et al. (2016) parse the Bitcoin blockchain to examine individual transactions and find that only a small fraction of users fall into the category of transacting for more than 10% of their time as active users. Biais et al. (2019) model the proof-of-work blockchain protocol as a stochastic game and show that mining the longest chain is a Markov perfect equilibrium but that there also exist equilibria with forks, leading to orphaned blocks and persistent divergences between chains. Chiu and Koeppl (2019) assess the welfare costs that arise endogenously from supporting bitcoin transactions without the threat from double spending and find they are about 500 times as large as in a monetary economy with 2% inflation. Prat and Walter (2021) propose a model that uses the bitcoin exchange rate to predict the computing power of the Bitcoin network. They provide

[9] Bitcoin's network hashrate is greater than all of the other cryptocurrencies combined. See: https://www.coinwarz.com/charts/network-hashrate-charts

convincing evidence that miners operate in a market where perfect competition is a good approximation of reality.

Most closely related to this paper are Benetton et al. (2021) and Easley et al. (2018). Benetton et al. (2021) study the spillovers from cryptomining on households and small businesses that occur through the interaction of supply and demand in the electricity market. They use a constant elasticity demand curve to empirically estimate the effect on community welfare of an increase in electricity prices due to the entry of miners in the Upstate New York region. While Benetton et al. (2021) measure the spillovers in a specific geographic area that are caused by an increase in the electricity demanded by miners, the present paper estimates the portion of the global Bitcoin network's electricity costs that is incurred to maintain the target quantity of bitcoin production over time. Easley et al. (2018) develops a game theoretic model to explain the strategic behavior of miners and users, demonstrating that equilibrium in the bitcoin blockchain is a complex balancing of user and miner participation. While Easley et al. (2018) study how the Bitcoin protocol affects the interaction between the miners and users, and thus the determination of fees, the present paper treats the fees as exogenous and studies how the protocol affects the interaction between the miners and buyers of bitcoins, who may hold or use them, and thus the determination of the price of the bitcoin in the market. In comparison with other papers in this literature, the present paper does not assume that the target quantity of bitcoin output always holds and gives special attention to the workings of the difficulty adjustment mechanism. The model permits an analysis of how a tax on the price of the bitcoin can be used to incentivize the network's difficulty adjustment mechanism to reduce the electricity costs it induces.

2 The model

I model the bitcoin as a tradable commodity whose supply is managed by the Bitcoin protocol. For ease of exposition, I suppress the daily time index t since the difficulty adjustments occur in regular intervals of blocks rather than time. As I explain further below, a subscript index denotes the order of changes in key variables during a given interval between difficulty adjustments.

2.1 Supply

A miner collects new transactions into a block and then hashes the block header to form a 256-bit block hash value.[10] If the value is below a target set by the protocol, which corresponds to a given level of difficulty δ, then the other miners will confirm the solution and agree that the block can be added to the blockchain. Because the minimum level of difficulty (equal to 1) requires the hash of the block header to start with 8 hexadecimal zeros, which represents 32 bits, the expected number of hashes per second needed to find a solution is $\delta 2^{32}$, where the difficulty δ is a unitless scaling parameter that is a multiple of the minimum amount of work that any valid block can contain. 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 and there are 10^9 hashes in a gigahash. When a miner 'solves a block,' the miner earns the block reward ω of newly minted bitcoins (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.[11]

[10] A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (the hash value or hash) and is a one-way function that is practically infeasible to invert. See https://en.wikipedia.org/wiki/Cryptographic_hash_function

[11] As shown by Easley et al. (2018), an increase in transaction fees ultimately leaves the rate at which new blocks are added to the blockchain unchanged and serves to shorten the waiting time of fee-paying users relative to non-fee-paying users. It follows that treating fees as exogenous in the present paper is of no consequence since user waiting times are not considered.

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. 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, δ_1 is the previous level of difficulty and the daily mining rate is the number of blocks mined per day. 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 target 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.[12] Each miner is risk neutral,[13] knows the rules of the Bitcoin protocol that govern the network, and must pay a fixed cost F (thereafter sunk) to purchase mining equipment with the hashrate ϕ in order to enter. Upon entry, a miner's daily expected bitcoin production is

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

where $t_i 60^2$ is the number of seconds spent mining per day. If $\phi 10^9 t_i 60^2$ hashes are created in one day, the expected number of blocks mined is $\frac{\phi 10^9 t_i 60^2}{\delta 2^{32}}$ per day, at a reward of ω bitcoins

[12] Assuming a representative miner is a good approximation of reality because miners with equipment that is not near the technological frontier will find it difficult to generate profits, which will necessitate their eventual exit from the industry.

[13] Easley et al. (2018) also assume that miners are risk neutral.

per block. A miner's daily electricity cost is

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

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 t_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 for the miner to set $t_i = 24$ and 0 otherwise.[14]

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

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

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. Each miner has the same expected profit $\frac{\Pi}{M}$ regardless of the number of entrants since an increase in the number of miners M increases the network hashrate proportionally.

Every 2016 blocks, the level of difficulty δ is adjusted so that the average waiting time

[14] These corner solutions realistically capture the fact that when the price of the bitcoin falls to the point where it is suficiently low (ie. $p_b \leq \underline{p_b}$), the miners simply turn off their machines until the price recovers. See: https://www.cnbc.com/2018/03/15/bad-news-for-bitcoin-miners-as-its-no-longer-profitable-to-create-the-cryptocurrency.html

to find a block on the network is approximately 10 minutes (600 seconds), so that

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

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

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

where η is the daily depreciation rate of the miner's equipment.[15] 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

$$M^* = \frac{p_b\left(\omega + f\right)\left[\frac{(24)60^2}{600}\right]}{\eta F + \frac{\phi\xi}{1000}\left(24\right)p_e}. \tag{6}$$

From (6) it is clear that the number of miners is equal to the total size of the 'pie' shared among the miners each day, which is 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

$$\eta F + \frac{\phi\xi}{1000}\left(24\right)p_e. \tag{7}$$

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

[15] Note that the existence of mining pools would affect the variance of the miners' returns and not their expected return. Any fixed fee charged by a pool could be subsumed in F and is therefore omitted for the sake of brevity.

the equilibrium network hashrate from observing the number of blocks discovered.

The aggregate supply of bitcoins per day X_S is equal to the block reward ω multiplied by the daily mining rate, which is determined by the network hashrate ϕM^* for a given level of difficulty δ. If $p_b > \underline{p_b}$, it follows that

$$\begin{aligned} X_S &= \frac{\omega\,(24)\,60^2}{\frac{\delta 2^{32}}{\phi M^* 10^9}} \\ &= \frac{p_b\,(\omega + f)\left[\frac{(24)60^2\phi 10^9}{\delta 2^{32}}\right]}{\eta F + \frac{\xi\phi}{1000}\,(24)\,p_e}\overline{X} \end{aligned} \tag{8}$$

where the second line follows from M^* of (6) and

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

is the target supply of bitcoins per day.[16] The supply curve relates each price p_b to an optimal quantity of bitcoins supplied since we can alternatively use (2) and (6) to express X_S of (8) as $X_S = M^* x^*$, where $x^* = x\,(t_i^*)$ and $t_i^* = 24$. The supply curve is upward sloping because an increase in p_b increases the network hashrate ϕM^* since, from (6), a greater number of miners will enter the industry. A greater quantity of bitcoins will be supplied per day since more equipment and electricity will be used to generate hashes, which, for a given level of difficulty δ, increases the number of blocks mined per day. From (8) it follows that the supply curve is linear, because hashing power scales linearly, and since the quantity supplied increases proportionally to the price, the price elasticity of supply is unity.

Since the network's choice of the difficulty depends on the network hashrate ϕM^*, the

[16] It follows from (7) and (8) 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 discovered per day $\frac{(24)60^2\phi 10^9}{\delta 2^{32}}$, however, the net effect is to increase the supply of bitcoins X_S.

equilibrium level of difficulty δ^* will depend on M^*. Hence it follows from substituting (6) into (5) that

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

From (9) 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.[17]

It follows from (8) and (9) 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, whenever $\delta \neq \delta^*$, the quantity of bitcoins supplied X_S is not equal to its target $\overline{X}$. Once the difficulty is adjusted according to (9), however, the protocol is in equilibrium since $X_S = \overline{X}$.[18]

2.2 Demand

There are $i = 1...N$ potential users of Bitcoin. Their use case is making a remittance or an anonymous payment. A representative agent i's utility from using bitcoin at a given point in time is

$$U_i = u\left(x_i, r, A, S\right)$$

where u is continuous and quasi-concave, x_i is the quantity of bitcoins held by user i, r is the one period return from holding bitcoin, A represents the anonymity associated with the transfer of bitcoins and S is the security of the Bitcoin network. I assume that r is constant over time, which follows from the assumption that the price of the bitcoin p_b follows a random

[17] As shown in Table 2 of the Appendix and discussed in Section 5, Eq. (9) fits the data exceptionally well, yielding an adjusted R^2 of 97%.

[18] As shown in Figure 9 of the Appendix and discussed in Section 5, data parsed from the Bitcoin blockchain demonstrate that the number of blocks mined per day (the daily mining rate) frequently differs from its target.

walk with drift r.[19] I also assume that A is constant over time since the degree of anonymity of bitcoin transactions is a function of the network's fixed architecture.

Network security S is determined by the daily cost of launching a 51% attack, which is the cost of generating 51% of the current network hashrate. From a miner's daily equipment and electricity costs in (7), it follows that network security is given by

$$\begin{aligned} S &= (.51)\left(\eta F + \frac{\phi\xi}{1000}(24)\, p_e\right) M^* \\ &= (.51)\, p_b\, (\omega + f)\left[\frac{(24)\, 60^2}{600}\right] \end{aligned} \tag{10}$$

if $S \geq \underline{S}$, and $S = -\infty$ otherwise, where $\underline{S}$ is the minimal level of security that does not trigger an attack. The second line of (10) follows from M^* in (6) and hence, due to free entry, network security S is directly proportional to the value of the daily block reward and fees. For the malicious entity, the cost of launching an attack approaches 51% of the miners' daily revenue as the market competition among miners increases.[20]

For the purpose of undertaking an empirical analysis, I specify the aggregate daily demand for the bitcoin as a standard constant elasticity of demand function

$$X_D = \beta_0 W^{\beta_1} p_b^{-\varepsilon} \tag{11}$$

where β_0 and β_1 are constants, ε is the elasticity of demand, and W includes the other determinants of the demand for the bitcoin such as the miners' revenue in S of (10). The return from holding the bitcoin r and the anonymity of bitcoin transactions A are subsumed in the constant β_0. In Section 5, I apply Eq. (11) to approximate the demand for the bitcoin in the region of the data used for the estimation. I undertake empirical analysis with the

[19] See, for instance, the constant expected return model in Fan and Yao (2017).

[20] Budish (2018) underscores the expense of requiring large flow payments to miners relative to the one off stock benefits of attacking the network.

view that (11) is a structural model of demand, which I use to estimate features of the data that are assumed to be invariant to policy changes. Since network security S is increasing in the price of the bitcoin p_b, an increase in p_b can increase the quantity demanded via S. I assume that this channel is not strong enough, however, to result in an upward sloping demand curve and we'll see in Section 6 that this assumption is empirically validated in the data.

2.3 Equilibrium

The supply curve in (8) and the demand curve in (11) simultaneously determine the equilibrium market price of the bitcoin p_b^*. Given p_b^*, the equilibrium network hashrate ϕM^* is determined according to M^* in (6) and the equilibrium quantity of bitcoins supplied X^* can be determined according to X_S in (6) or X_D in (11).

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. A comprehensive equilibrium is the unique solution to the system of equations determined by the zero profit condition obtained from setting (4) equal to the miners' fixed costs, the Bitcoin protocol's specified waiting time to find a block of (5), the supply curve of (8) and the demand curve of (11). It necessitates that an equilibrium in the market ($X_S(p_b^*; \delta) = X_D(p_b^*) = X^*$) occurs at the same time as an equilibrium in the protocol ($\delta = \delta^*$, $M = M^*$). In a comprehensive equilibrium, since $X_S = \overline{X}$ if and only if $\delta = \delta^*$, it follows that $X^* = \overline{X}$. As we have seen, since the level of difficulty δ is adjusted only at intervals, an equilibrium in the market can occur while the protocol is in disequilibrium.

2.4 Difficulty adjustment

Figure 1 depicts the aggregate daily supply of bitcoins and the aggregate daily demand for bitcoins in the bitcoin market. 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, a level of difficulty δ_1, and a level of security S_1, an increase in demand from X_D to X'_D leads to an increase in the price 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 and the level of network security increases to $S_2 = S(p_{b2})$ in the market equilibrium labeled 2a. The new equilibrium will be short-lived, however, since the mining rate exceeds the target mining rate of 144 blocks per day.

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 (8) and δ^* of (9) that the protocol will choose the new level of difficulty δ_2 consistent 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 and target mining rates are $\frac{X_S(p_{b2};\delta_1)}{\omega}$ and $\frac{\overline{X}}{\omega} = 144$, respectively.

From X_S of (8), 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 p_{b2} is unchanged, the difficulty

adjustment preserves the level of security S_2 that occurs in equilibrium 2a. Also, it follows from M^* in (6) that the increase in difficulty does not result in an exit of miners from the industry. Recall that the number of miners adjusts immediately to changes in the price of a bitcoin p_b and the difficulty adjusts in turn to target $\overline{X}$ while maintaining a constant network hashrate. 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}, the security to rise to S_3, and the number of miners to increase to M_3 since the increase in the market price from p_{b2} to p_{b3} incentivizes additional entry. 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 the difficulty and the market price exceeds the laissez-faire price p_{b2}.

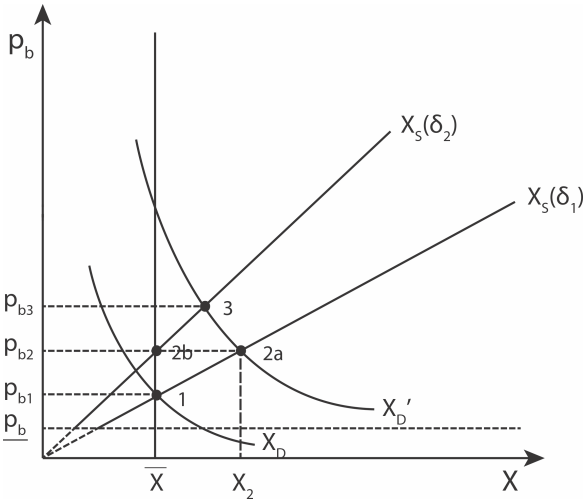

Figure 1. Bitcoin price adjustment.

In summary, we have established that the supply of bitcoins is linear and upward sloping

through the origin. Adjustments of the difficulty result in shocks to the supply curve since the difficulty determines its slope. 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 so that the mining rate is equal to its target at the existing network hashrate. Laissez-faire prices do not exist in the bitcoin market since the protocol regularly intervenes in the market to adjust the difficulty. The bitcoin is an excellent store of value for the electricity used in its production, however, since its price is equal to the marginal cost of its production due to the free entry of miners to the industry. Network security benefits from adjustments of the difficulty only to the extent that they result in a higher price of the bitcoin.

3 Welfare

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 the intervention. Instead of accruing tax revenue, however, the increase in difficulty imposes additional electricity costs on the miners. An analogous scenario obtains whenever the protocol decreases the level of difficulty.

Recall that an increase in the 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 $\delta_2 > \delta_1$, it follows from X_S of (8) that

$$\frac{p_b\left(X;\delta_2\right)}{p_b\left(X;\delta_1\right)} = \frac{\delta_2}{\delta_1} \equiv 1 + \psi \tag{13}$$

where $p_b\left(X;\delta\right)$ is the inverse supply curve derived from (8). It follows from (13) that an increase in the difficulty is equivalent to a government's imposing an ad valorem tax on the price of the bitcoin equal to the percentage increase in the difficulty $\psi > 0$.

Figure 2a extends Figure 1 to assess the effect on social welfare of an increase in difficulty by employing a partial equilibrium framework. As shown in Figure 2a, after the increase in the difficulty, the price of a bitcoin rises to p_{b3} and the equilibrium quantity of bitcoins falls to X_3. Under the higher level of difficulty, there is a wedge between the price buyers pay p_{b3} and the lower price that miners receive p'_{b3}, where $p_{b3} = (1+\psi)\, p'_{b3}$. A total of $\psi p'_{b3}$ for each of the X_3 bitcoins that are produced per day is dissipated as additional electricity costs ΔE, which is depicted by the large diamond-gridded rectangular area. It follows from Eqs. (12) and (13) that $\psi = \frac{\delta_2}{\delta_1} - 1 = \frac{X_2}{X} - 1$. Since $X_2 - X_3$ bitcoins are no longer traded in the market, the surplus that occurs in market equilibrium 2 is also reduced by the distortion depicted by the dotted triangular area. Hence an increase in the difficulty results in losses to both the miners and users of the bitcoin due to the transfer of their rents to the providers of electricity and the distortion. While an equivalent tax on the price of the bitcoin would have resulted in the same distortion loss, it would have provided tax revenue while the rents that go toward electricity generation result in external environmental damages.

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. Figure 2b 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} and a decrease in the quantity of bitcoins

produced per day to X_2. In the subsequent equilibrium labeled 2, since the mining rate is less than 144 blocks per day, the protocol will decrease the level of difficulty from δ_1 to $\delta_2 < \delta_1$ and the supply curve will rotate downward until the mining rate is equal to the target $\overline{X}$ given the network hashrate associated with p_{b2}. It follows that the price falls to p_{b3} and the equilibrium quantity increases to X_3 in the equilibrium labeled 3. A decrease in the difficulty is equivalent to a government's providing an ad valorem subsidy to miners equal to the percentage decrease in the level of difficulty φ, where $\varphi = \left|\frac{\delta_2}{\delta_1} - 1\right| = \left|\frac{X_2}{\overline{X}} - 1\right|$. There is a wedge between the price consumers pay p_{b3} and the higher 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 $\Delta\widetilde{E}$. As shown in Figure 2b, the resulting level of output X_3 is too large for market participants to capture the full benefit since the reduction in electricity costs is reduced by a distortion loss. A decrease in the difficulty is far more efficient than the equivalent ad valorem subsidy to the miners, however, since it would result in the same distortion loss but there is no cost to the government due to providing the subsidy.

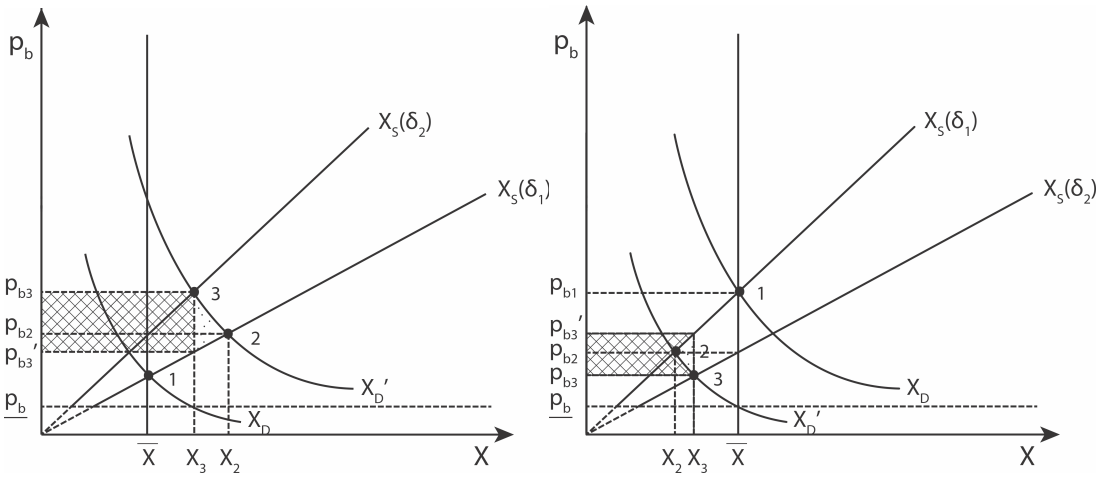

Figure 2. a) (left) An increase in the difficulty. b) (right) A decrease in the difficulty.

The following proposition quantifies the welfare loss (gain) due to an increase (decrease) in the difficulty.

Proposition 1 *(i) The average daily welfare loss due to a percentage increase in the level of difficulty given by* $\psi = \frac{\delta_2}{\delta_1} - 1$ *is approximately*

$$\Gamma(\psi) = \psi p_b(X_3; \delta_1) X_3 + \frac{1}{2} \frac{\varepsilon}{1+\varepsilon} p_b(X_2; \delta_1) X_2 \psi^2 \tag{14}$$

where $X_3 \approx \frac{1+\varepsilon(1-\psi)}{1+\varepsilon} X_2$ *is the equilibrium quantity after the increase in the difficulty and* X_2 *is the equilibrium quantity before the change in difficulty from* δ_1 *to* $\delta_2 > \delta_1$*. (ii) The average daily welfare gain due to a percentage decrease in the level of difficulty given by* $\varphi = \left|\frac{\delta_2}{\delta_1} - 1\right|$ *is approximately*

$$\Omega(\varphi) = \varphi p_b(X_3; \delta_1) X_3 - \frac{1}{2} \frac{\varepsilon}{1+\varepsilon} p_b(X_2; \delta_1) X_2 \varphi^2 \tag{15}$$

where $X_3 \approx \frac{1+\varepsilon(1+\phi)}{1+\varepsilon} X_2$ *is the equilibrium quantity after the decrease in the difficulty and* X_2 *is the equilibrium quantity before the change in difficulty from* δ_1 *to* $\delta_2 < \delta_1$*.*

Proof. See the Appendix. ■

The following proposition compares the size of the loss Γ that is due to an increase in the difficulty with the size of the gain Ω that is due to an equivalent percentage decrease in the difficulty. It demonstrates that the loss must exceed the gain because increases in the difficulty occur over a larger range of output $X > \overline{X}$.

Proposition 2 *For any given* $\varepsilon > 0$*, the welfare loss* $\Gamma(\psi)$ *due to an increase in the difficulty is greater than the welfare gain* $\Omega(\varphi)$ *due to a decrease in the difficulty whenever* $\psi = \varphi$*.*

Proof. See the Appendix. ■

The proof of Proposition 2 is illustrated in Figure 3 for the case where the initial level of the difficulty is the same. The figure depicts an increase in the difficulty from δ_1 to δ_2 and

a decrease in the difficulty from δ_1 to $\widetilde{\delta}_2$ by an equal percentage, so that $\frac{\delta_2}{\delta_1} - 1 = \left|\frac{\widetilde{\delta}_2}{\delta_1} - 1\right|$. Although the proportional change in the difficulty is equivalent, since an increase (decrease) in the difficulty occurs whenever the equilibrium quantity X_2 is greater (less) than the target quantity of bitcoins $\overline{X}$, the proportion is applied to a higher price under the increase since the supply curve is upward sloping. Moreover, the distortion loss that occurs each time the level of difficulty is adjusted by the protocol further increases the welfare losses and reduces the welfare gains.

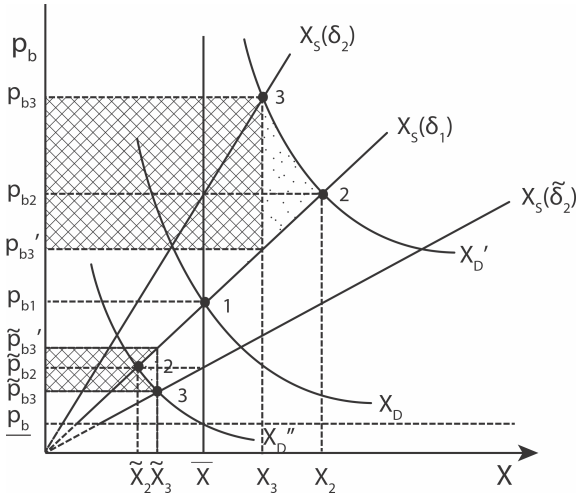

Figure 3. An equivalent proportional increase and decrease in difficulty.

Thus far we have seen how the Bitcoin protocol's difficulty adjustment mechanism imposes costs and benefits on the participants in the bitcoin market. Proposition 1 quantifies the welfare losses and gains that are incurred by the miners and users of bitcoins. Proposition 2 demonstrates that the welfare loss that arises due to an increase in the difficulty is not offset by an equivalent proportional decrease in the difficulty, and hence even a relatively stable difficulty that fluctuates about a constant level will impose net losses on market participants that amass over time.

4 Taxation to reduce electricity costs

In this section we analyze how a tax incentivizes the difficulty adjustment mechanism to decrease the electricity costs that it induces. Each miner imposes a negative externality on the market since the protocol responds automatically to entry by increasing the difficulty by more whenever the quantity of bitcoins produced per day exceeds $\overline{X}$ or by decreasing the difficulty by less whenever the quantity of bitcoins produced per day falls short of $\overline{X}$. The protocol's difficulty adjustment mechanism functions external to the market and, as we have seen, alters laissez-faire prices and decreases the size of the social pie. Since a miner who decides whether to enter the market does not take into consideration his effect on the subsequent level of the difficulty, it follows that social welfare can be improved by the imposition of a tax on the price of the bitcoin. A tax disincentivizes the entry by miners, thereby lowering the network hashrate and the magnitude of the impeding difficulty adjustment.

I analyze a given interval between difficulty adjustments and assume that the timing is as follows. First, an initial level of difficulty δ_1 is chosen by the Bitcoin protocol. Second, any demand shocks take place, resulting in an equilibrium level of output X_2. The government then applies an ad valorem tax τ on the price of the bitcoin, which decreases the equilibrium level of output under the tax to X_2^τ. Analogous to Proposition 1, we have that $X_2^\tau = \frac{1+\varepsilon(1-\tau)}{1+\varepsilon}X_2$. Once 2016 blocks have been mined, the protocol adjusts the difficulty to δ_2^τ, where $\frac{\delta_2^\tau}{\delta_1} = \frac{X_2^\tau}{\overline{X}}$. After the difficulty adjustment, the equilibrium level of output under the tax is X_3^τ, where, analogous to Proposition 1, $X_3^\tau = \frac{1+\varepsilon(1-\psi^\tau)}{1+\varepsilon}X_2^\tau$ if the difficulty increased or $X_3^\tau = \frac{1+\varepsilon(1+\phi^\tau)}{1+\varepsilon}X_2^\tau$ if the difficulty decreased and ψ^τ (ϕ^τ) is the percentage increase (decrease) in the difficulty under the tax.

A tax on the price of the bitcoin is similar to a tax that corrects a negative environmental externality, such as pollution that is a by-product of production, since it deters entry and

decreases the network hashrate. In contrast, however, the tax does not result in a long run tradeoff between the output of bitcoins and the reduction in electricity costs, since the difficulty adjustment mechanism compensates for the tax's effect on output. Since the protocol maintains a constant level of output, and output is determined by the network hashrate relative to the difficulty, the tax is ultimately expressed in a lower level of the difficulty.[21]

The following proposition establishes that a tax causes the difficulty adjustment mechanism to decrease the difficulty over a wider range of output in order to target $\overline{X}$.

Proposition 3 *The difficulty adjustment under an ad valorem tax τ on the price of the bitcoin is given by $\frac{\delta_2^\tau}{\delta_1} = \left(1 - \frac{\varepsilon}{1+\varepsilon}\tau\right)\frac{X_2}{\overline{X}}$, where $\tau \in \left(0, \overline{\overline{\tau}}\right)$ and $\overline{\overline{\tau}} = \frac{1+\varepsilon}{\varepsilon}$ is the tax that solves $X_2^\tau = 0$.*

Proof. See the Appendix.

Corollary 4 *The steady state level of output under the tax τ is $\overline{X}^\tau = \frac{1+\varepsilon}{1+\varepsilon(1-\tau)}\overline{X}$.*

■

Figure 4 illustrates Proposition 3 by contrasting the relationship between the new level of difficulty under the tax relative to the previous level $\frac{\delta_2^\tau}{\delta_1}$ and the level of output prior to the imposition of the tax X_2, with that which would have prevailed in the absence of a tax. As shown in the figure, the tax decreases $\frac{\delta_2^\tau}{\delta_1}$ proportionally by a factor of $1 - \frac{\varepsilon}{1+\varepsilon}\tau$ for all X_2. It follows that, after the tax, changes in the difficulty are less sensitive to deviations of output X_2 from the target level $\overline{X}$. Also, the difficulty will be decreased by the protocol over a wider range of output under the tax since, as shown by Corollary 4, the steady state level of output for which the difficulty will not change $\overline{X}^\tau > \overline{X}$. An increase in the tax

[21] Recall from (8) that the expected number of blocks mined per day is $\frac{\phi M^* 10^9 (24) 60^2}{\delta 2^{32}}$ and hence a constant level of output in the bitcoin market is consistent with a lower network hashrate ϕM^* and a lower difficulty δ.

results in a greater downward rotation of $\frac{\delta_2^\tau}{\delta_1}$, and thus a greater steady state level of output $\overline{X}^\tau$, but it has no effect on the protocol's target $\overline{X}$.[22] This is because the protocol lowers the difficulty under the tax precisely to offset the effect of the tax on output. For instance, if $X_2 \in \left[\overline{X}, \overline{X}^\tau\right)$, then the protocol responds by decreasing the difficulty to target $\overline{X}$ since output under the tax X_2^τ falls below $\overline{X}$.[23] Although the tax has a negligible effect on output following the difficulty adjustment, the electricity costs are smaller because the new level of difficulty is lower than in the absence of the tax.

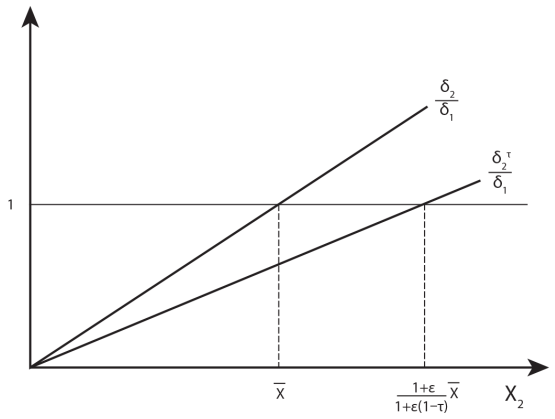

Figure 4. The effect of a tax on the difficulty adjustment mechanism.

To illustrate the effect of a tax on the bitcoin market, Figure 5a extends Figure 2a for the case where $X_2^\tau > \overline{X}$, for the purpose of comparison with the baseline case outlined in Figure 2a. The supply curve inclusive of the ad valorem tax τ, X_S^τ, for an initial level of difficulty δ_1, is given by[24] $X_S^\tau\left(p_b;\delta_1\right) = \frac{X_S(p_b;\delta_1)}{1+\tau}$. From M^* of (6), an ad valorem tax on the price of the bitcoin decreases entry to $M^{*\tau} = \frac{M^*}{1+\tau}$ and hence the network hashrate falls to

[22] In the limit, as $\tau \to \overline{\overline{\tau}}$, $\overline{X}^\tau \to \infty$ and the protocol will respond with a level of difficulty under the tax $\delta_2^\tau \to 0$.

[23] More generally, we have that $X_2 < \overline{X}^\tau$ if and only if $X_2^\tau < \overline{X}$.

[24] And the inverse supply curve inclusive of the tax is $p_b^\tau\left(X;\delta\right) = \left(1+\tau\right)p_b\left(X;\delta\right)$.

$\frac{\phi M^*}{1+\tau}$. As shown in Figure 5a, the tax decreases miners' incentives to enter the market since it lowers the price they receive net of the tax to $p_{b2}^{\tau\prime} = p_b^{\tau}\left(X_2^{\tau};\delta_1\right)$ and the output of bitcoins per day falls to $X_2^{\tau} < X_2$. The tax yields revenue equal to $\Delta TR = \tau p_{b2}^{\tau\prime} X_2^{\tau}$, which is depicted as the grey shaded area in Figure 5a. Since the quantity of bitcoins mined per day is lower than in the absence of the tax, it follows from (12) that the protocol subsequently increases the difficulty to δ_2^{τ}, where the percentage increase in the difficulty is only $\psi^{\tau} = \frac{X_2^{\tau}}{\overline{X}} - 1$. Recall from Figure 2a that in the absence of a tax the percentage increase in the difficulty is $\psi = \frac{X_2}{\overline{X}} - 1 > \psi^{\tau}$. The tax squeezes the electricity costs to $\Delta E^{\tau} = \psi^{\tau} p_{b3}^{\tau\prime} X_3^{\tau}$, which is depicted as the hatched area in Figure 5a, where $p_{b3}^{\tau\prime} = p_b^{\tau}\left(X_3^{\tau};\delta_1\right)$ and the resulting level of output after the difficulty adjustment is X_3^{τ}.[25]

Figure 5b extends Figure 2b to assess the impact of a tax on the electricity costs that are gifted by the protocol for the case where $X_2 < \overline{X}^{\tau}$. As in Figure 5a, the tax lowers the price miners receive net of the tax to $p_{b2}^{\tau\prime}$ and the output of bitcoins per day falls from X_2 to X_2^{τ}, yielding tax revenue equal to $\Delta TR = \tau p_{b2}^{\tau\prime} X_2^{\tau}$, which is depicted as the grey shaded area in Figure 5b. Since the number of bitcoins mined per day X_2^{τ} is smaller than in the absence of the tax X_2, it follows from (12) that the protocol subsequently decreases the difficulty to δ_2^{τ}, where the percentage decrease in difficulty is as large as $\varphi^{\tau} = \left|\frac{X_2^{\tau}}{\overline{X}} - 1\right|$. Recall from Figure 2b that in the absence of the tax the percentage decrease in the difficulty is $\varphi = \left|\frac{X_2}{\overline{X}} - 1\right| < \varphi^{\tau}$. The tax increases the savings in electricity costs to $\Delta\widetilde{E}^{\tau} = \varphi^{\tau} p_{b3}^{\tau\prime} X_3^{\tau}$, which is depicted as the hatched area in Figure 5b, where $p_{b3}^{\tau\prime} = p_b^{\tau}\left(X_3^{\tau};\delta_1\right)$ and the resulting level of output after the difficulty adjustment is X_3^{τ}.

In summary, Figure 5 illustrates that, for any given tax $\tau \in \left(0, \overline{\overline{\tau}}\right)$, the electricity costs

[25] Note that the tax that would fully displace any difficulty adjustment, which solves $X_2^{\tau} = \overline{X}$, is greater than the percentage change in the difficulty in the absence of the tax ψ. This is because the protocol has no knowledge of the demand curve and output can only iteratively approach $\overline{X}$ over time under successive difficulty adjustments. This is clear from the example drawn in Figure 5a since the tax τ is greater than the increase in the difficulty ψ but not large enough to fully displace the difficulty adjustment since the protocol increases the difficulty further under the tax since $\psi^{\tau} > 0$.

are reduced by the tax since, if $X_2^\tau > \overline{X}$, then $0 < \Delta E^\tau < \Delta E$, and if $X_2^\tau < \overline{X}$, then $\Delta E^\tau < \Delta E < 0$ since $\Delta \widetilde{E}^\tau = -\Delta E^\tau$ and $\Delta \widetilde{E} = -\Delta E$.

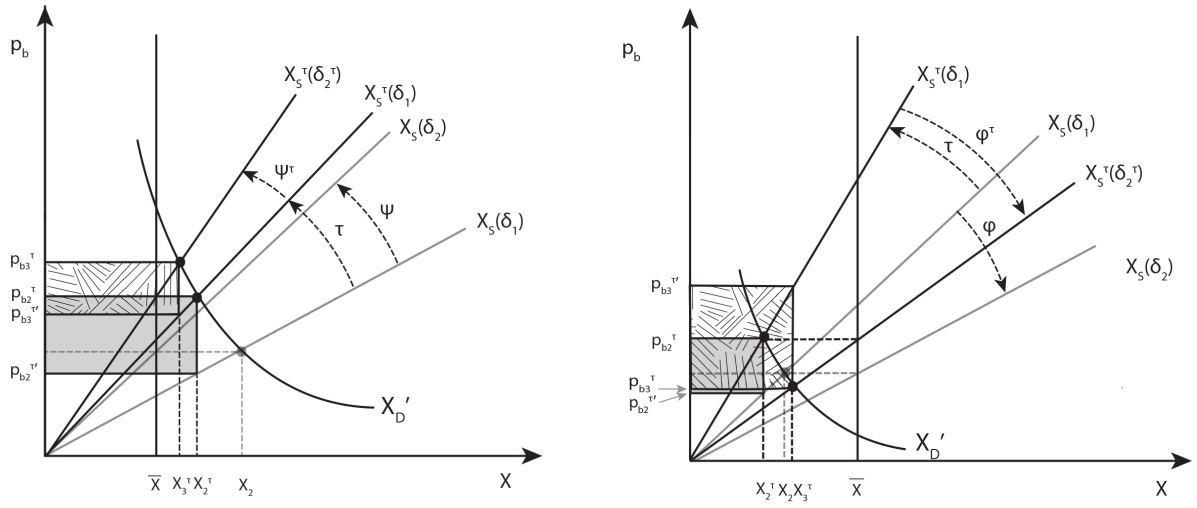

Figure 5. a) (left) Case $X_2^\tau > \overline{X}$. b) (right) Case $X_2^\tau < \overline{X}$.

Since the tax is a substitute for an impending increase in the difficulty whenever $X_2^\tau > \overline{X}$, there is a tax rate $\overline{\tau}$ that fully crowds out any increase in the difficulty, resulting in no additional electricity costs, or $\Delta E^\tau = 0$. Also, since the tax is a complement to an impending decrease in the difficulty whenever $X_2^\tau < \overline{X}$, there is a tax rate τ^* that maximizes the reduction in the electricity costs $\Delta \widetilde{E}^\tau$, or, equivalently, minimizes the electricity costs ΔE^τ. The following proposition establishes the existence of and characterizes these tax rates, for any given level of output X_2. It also demonstrates that there is a tradeoff between minimizing the electricity costs ΔE^τ and maximizing the tax revenue ΔTR.

Proposition 5 *(i) There exists a unique tax rate* $\overline{\tau} = \left(1 - \frac{\overline{X}}{X_2}\right) \frac{1+\varepsilon}{\varepsilon}$ *such that* $\Delta E^\tau|_{\tau=\overline{\tau}} = 0$. *(ii) There exists a unique tax rate* $\tau^* = \arg\min\left(\Delta E^\tau\right)$, *where* $\tau^* \in \left(\overline{\tau}, \overline{\overline{\tau}}\right)$. *(iii) There exists*

a unique $X_2' > 0$ *such that* $\tau^* < \tau^{TR}$ *if and only if* $X_2 < X_2'$, *where* $\tau^{TR} = \arg\max(\Delta TR) = \frac{1+\varepsilon}{3\varepsilon}$.

Proof. See the Appendix. ■

Corollary 6 *The cost-minimizing tax* τ^* *results in an impending decrease in the level of difficulty.*

Part (i) of the proposition establishes that the electricity cost-displacing tax $\overline{\tau} = \left(1 - \frac{\overline{X}}{X_2}\right)\frac{1+\varepsilon}{\varepsilon}$. Hence $\overline{\tau} > 0$ whenever $X_2 > \overline{X}$ and $\overline{\tau} < 0$ (a subsidy is required) whenever $X_2 < \overline{X}$. If $\overline{\tau}$ is applied in each period between difficulty adjustments as a function of the resulting level of output following any additional demand shocks, the difficulty will remain unchanged over time since $X_2 = \overline{X}^{\tau}$. Alternatively, setting the tax equal to $\overline{\tau}$ whenever $X_2 > \overline{X}$ and 0 otherwise can dominate setting $\tau = \overline{\tau}$ for all X_2 since it permits the protocol to gift electricity whenever $X_2 < \overline{X}$, and hence $\Delta E^{\tau} \leq 0$, while the tax revenue ΔTR will be (weakly) greater since the bitcoin is never subsidized.

Part (ii) of the proposition characterizes the electricity cost-minimizing tax and the corresponding proof in the Appendix demonstrates how to implicitly solve for τ^*. As shown in the Appendix, τ^* is a function of the equilibrium level of output prior to the imposition of the tax X_2 relative to the target level of output $\overline{X}$, and the price elasticity of demand ε. This is because $\frac{X_2^{\tau}}{\overline{X}}$ determines the percentage change in the difficulty under the tax, which τ^* minimizes in balance with its effect on the equilibrium level of output after the adjustment in the difficulty X_3^{τ}. Analogous to Proposition 1, X_2^{τ} and X_3^{τ} are functions of the elasticity ε and X_2.

To facilitate an understanding of the relationship between the electricity cost-minimizing tax τ^* and the revenue-maximizing tax τ^{TR}, Figure 6 depicts how the additional electricity costs ΔE^{τ} and tax revenue ΔTR depend on the tax rate τ. As shown in the figure, if X_2^{τ} is

greater than $\overline{X}$ when $\tau = 0$, the impending change in the electricity costs ΔE^{τ} is positive since the protocol will increase the difficulty over this range of output. As τ is first increased from 0, ΔE^{τ} is decreasing in τ. The percentage increase in the difficulty $\psi^{\tau} = \frac{X_2^{\tau}}{\overline{X}} - 1$ is decreasing in τ because the level of output under the tax X_2^{τ} is decreasing in τ. When $\tau = \overline{\tau}$, since $X_2^{\tau} = \overline{X}$, ΔE^{τ} is equal to 0 since the protocol will not change the level of difficulty. Once $\tau > \overline{\tau}$, since $X_2^{\tau} < \overline{X}$, ΔE^{τ} is negative since the protocol will decrease the difficulty over this range of output. As τ continues to increase, ΔE^{τ} continues to decrease in τ since the decrease in the difficulty $\varphi^{\tau} = \left| \frac{X_2^{\tau}}{\overline{X}} - 1 \right|$ is increasing in τ. Since X_2^{τ} approaches 0 as τ approaches $\overline{\overline{\tau}}$, however, ΔE^{τ} must eventually reach a minimum over $\left(\overline{\tau}, \overline{\overline{\tau}}\right)$ and then increase toward 0 in the limit. It follows that ΔE^{τ} is quasi-convex in τ and that there is a unique tax $\tau^* \in \left(\overline{\tau}, \overline{\overline{\tau}}\right)$ that minimizes ΔE^{τ}. Since the protocol can be induced to gift electricity whenever $X_2^{\tau} < \overline{X}$, choosing the tax to eliminate any difficulty adjustments ($\tau = \overline{\tau}$) or to eliminate all bitcoin production ($\tau = \overline{\overline{\tau}}$) does not yield the smallest possible electricity costs since they can be negative.

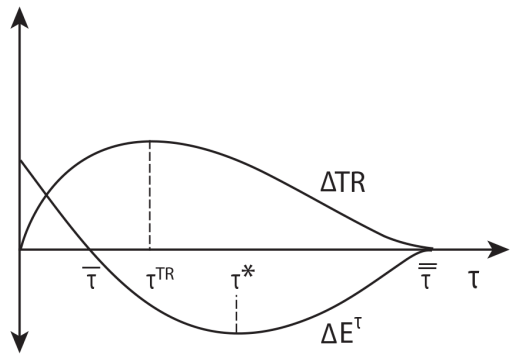

Figure 6. ΔE^{τ} and ΔTR as functions of τ. Case: $X_2 > \overline{X}$.

Figure 6 can be used to guide policy makers in understanding how an arbitrary tax on

the price of the bitcoin will affect electricity costs. Since the relation between the change in the electricity costs ΔE^{τ} and the tax τ is monotonic and continuous over $[0, \tau^*]$, a tax $\tau < \overline{\tau}$ will work to increase the electricity costs while $\tau > \overline{\tau}$ will work to decrease the electricity costs, where the maximal reduction occurs at $\tau = \tau^*$.

In contrast with the electricity costs, the tax revenue is unaffected by the impending difficulty adjustment since the imposition of the tax precedes it. Figure 6 depicts how the change in tax revenue ΔTR depends on the tax rate τ. For any given X_2, as τ is first increased from 0, the tax revenue ΔTR first increases from 0 because of the higher tax rate. Since X_2^{τ} approaches 0 as τ approaches $\overline{\overline{\tau}}$, however, ΔTR must reach a maximum over $\left(0, \overline{\overline{\tau}}\right)$ and then decrease toward 0 in the limit. It follows that the tax revenue ΔTR is quasi-concave in τ and that there is a unique tax rate $\tau^{TR} \in \left(0, \overline{\overline{\tau}}\right)$ that maximizes ΔTR. As shown in the Appendix, $\tau^{TR} = \frac{1+\varepsilon}{3\varepsilon}$, which is independent of the level of output prior to the imposition of the tax X_2.

Whenever X_2 decreases relative to $\overline{X}$, the relation between ΔE^{τ} and τ shifts to the left while the relation between ΔTR and τ is unchanged. A smaller tax is required to achieve a given level of the electricity costs ΔE^{τ} because the impending difficulty adjustment will be smaller. It follows that the cost-minimizing tax τ^* decreases and part (iii) of the proposition follows because τ^* will be less than the revenue-maximizing tax τ^{TR} whenever X_2 is sufficiently small. For example, as shown in the proof of Proposition 5(iii) in the Appendix, if $\varepsilon = .17$,[26] then the threshold level of output is given by $X_2' = 0.51\overline{X}$.

Corollary 6 highlights the fact that since τ^* exceeds $\overline{\tau}$, the level of output under the cost-minimizing tax $X_2^{\tau^*} < \overline{X}$ and the impending difficulty adjustment must be downward. If the cost-minimizing tax is applied in each period between difficulty adjustments as a function of the resulting level of output following any additional demand shocks, the difficulty must

[26] As we'll see in Section 6, I derive this estimate of the price elasticity of demand for the bitcoin from the data.

follow a downward path over time. The decrease in the difficulty will not result in a more rapid discovery of blocks since the network hashrate also falls after each successive tax and the equilibrium quantity of bitcoins produced per day after the difficulty adjustment X_3^τ will be approximately equal to the target $\overline{X}$. It follows that since, in actuality, the Bitcoin network's hashrate and difficulty have been generally increasing over time, successive cost-minimizing taxes would rewind them back to the levels that existed closer to the inception of the network despite that the current hashrate of mining equipment ϕ would not be any lower.

It also follows from Corollary 6 that to determine the best tax over time, it is necessary to consider a lower bound on the network hashrate to preserve the network's security. A 51% attack becomes more likely whenever the cost of launching it decreases, since the expected benefit of an attack is limited only by the quantity of bitcoins that an attacker could double-spend. Hence an attack becomes feasible whenever the costs become low enough for a malicious entity to be able to cover them. A tax can trigger an attack because it creates a wedge between the market price of the bitcoin p_b^τ, which determines the value of the double-spending and thus the expected benefit of launching an attack, and the lower price that the miners receive under the tax $p_b^{\tau\prime}$, which determines the network hashrate $\phi M^{*\tau}$ and thus the cost of launching an attack. From S of (10) and since $M^{*\tau} = \frac{M^*}{1+\tau}$, it follows that network security under the tax $S^\tau = \frac{S}{1+\tau}$ and hence there is a threshold tax τ' such that $S^\tau < \underline{S}$ if and only if $\tau > \tau'$. While estimating a value for $\underline{S}$ is an open question beyond the scope of this paper, if the current level of network security S is sufficiently large relative to the lowest level that safeguards the network $\underline{S}$, there will be sufficient leeway to apply the cost-minimizing tax to reduce electricity costs while maintaining adequate network security. As $S^\tau \to \underline{S}$, the authority could apply the tax $\tau = \overline{\tau}$ to stabilize the entry of miners $M^{*\tau}$ and thus the level of security S^τ.

In practice, for tax purposes bitcoin mining revenue is typically treated as ordinary

income using the fair market value of the bitcoins at the end of the year or at the time the bitcoins were mined. Capital gains taxes are typically applied in situations where the bitcoins are purchased or received from a transaction and are levied only on gains that are realized from a sale.[27] While the purpose of these taxes is not to reduce electricity usage, as we have seen in Figure 6, any given tax on the price of the bitcoin will reduce electricity costs. To properly correct miners' incentives, however, we have seen that the tax should be based on the current market information conveyed by the level of output in the bitcoin market relative to the target $\frac{X_2}{\overline{X}}$ and the price elasticity of demand ε. While from M^* in (6) it follows that the prices of miners' equipment and electricity in (7) could also be taxed to reduce the network hashrate, again, the tax rate should be based on current bitcoin market conditions to effectively reduce or minimize electricity costs. We have also seen that the tax rate should be adjusted in each period between difficulty adjustments. While this may be administratively burdensome, if the demand for the bitcoin is relatively stable over time, then the tax rate will stabilize to a relatively constant rate after an initial correction. Moreover, an effectual tax must be applied uniformly throughout the world to prevent leakage due the migration of miners to countries with low or non-existent taxes.[28]

In summary, this section establishes how a tax incentivizes the Bitcoin protocol to decrease the network's electricity costs and how it can be used to rewind the difficulty and the network hashrate back to the levels that existed closer to the inception of the Bitcoin network. Proposition 3 demonstrates how a tax affects the protocol's difficulty adjustment mechanism and Corollary 4 shows that the protocol decreases the difficulty over a wider range of bitcoin output under a tax. Proposition 5 establishes the existence of and characterizes the tax that fully displaces the electricity costs, the tax that minimizes the electricity costs and the tax

[27] See OECD (2020) for a comprehensive analysis of cryptocurrency tax treatments for more than 50 jurisdictions.

[28] The same argument applies to a carbon tax (or some form of carbon pricing), which is nevertheless applied by most of the world's developed countries.

that maximizes the tax revenue, and compares their magnitudes. It demonstrates that there is a tradeoff between minimizing the electricity costs and maximizing the tax revenue, and hence minimizing the electricity costs does not entail squeezing as much money as possible from the bitcoin market. Corollary 6 deduces that the cost-minimizing tax results in an impending decrease in the difficulty since it is consistent with a level of output under the tax that is less than the target. To ensure that the tax does not trigger a 51% attack, the tax should not be set above a threshold that compromises the network's security.

5 Empirical analysis

In this section, I describe the data and present the econometric method I use to estimate the price elasticity of demand. I also outline how I apply Propositions 1 and 5 to estimate the cumulative net welfare losses over the sample period, as well as the initial tax that fully displaces the electricity costs and the initial electricity cost-minimizing tax for each interval between difficulty adjustments.

5.1 Data description

The data were acquired from several sources. The daily average USD price of the bitcoin across major bitcoin exchanges, the daily difficulty level, the daily block rewards and fees, and the number of blocks mined per day were acquired by using Blocksci, an open-source software platform for blockchain analysis.[29,30] The daily USD price data for new Antminer mining rigs produced by Bitmain (models S1, S2, S3, S4, S5, S7, S9 and S11) sold on Amazon Marketplace by third party sellers was acquired by using an API for the Amazon price tracker

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

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

Keepa.com.[31] The reported price is the lowest of the prices available from the sellers and does not include shipping costs; missing data correspond to periods of time when all sellers are out of stock.[32] To include all intervals between difficulty adjustments, the gaps in the Antminer price data were filled by replacing each missing value with the most recent present value prior to it. 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, weighting each price equally. 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 a 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 its price information was tracked by Keepa.com. While there are numerous brands of bitcoin mining rigs available on the market, the Antminer rigs are on the technological frontier in terms of their power and energy efficiency and Bitmain's market share is about $70\% - 80\%$.[33] I conservatively estimate the average price of electricity used in mining to be 0.05 USD per kWh since Bitmain, which owns one of the world's largest bitcoin mines, was known to be paying just 4 cents per kWh of electricity in Inner Mongolia (de Vries, 2018). Also, I estimate the expected lifespan of a

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

[32] These periods are: 12 October 2017 to 17 October 2017, 19 October 2017 to 26 October 2017, 13 November 2017 to 17 November 2017, 24 November 2017 to 5 December 2017, 9 December 2017 to 10 December 2017, and 3 January 2018 to 4 January 2018.

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

mining rig to be two years, so that the daily depreciation rate is $\frac{1}{730}$, since large companies like Bitmain are constantly working on releasing faster and more efficient models that render their predecessors obsolete.

5.2 Preliminary analysis and model diagnostics

Figure 7 plots the daily level of the difficulty over the sample period. It is clear that the level of difficulty has been increasing exponentially until 17 October 2018 and 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. To verify that the difficulty adjustment mechanism is consistent with Eq. (12), Figure 8 plots the ratio of the new difficulty relative to the previous level, against the daily mining rate divided by the target mining rate of 144. The two variables have a correlation of .99 and it's clear from the figure that the data line up along the 45 degree line. Figure 9 presents a standard plot and a boxplot of the number of blocks mined per day, where a horizontal line is drawn at the target of 144 blocks. It is clear from the figure that the daily 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, confirming that market equilibria frequently occur while the protocol is in disequilibrium. Also, since the mean and median blocks mined per day are 151.6 and 151, respectively, the daily mining rate typically exceeded the target during the sample period, which is consistent with the exponential growth in the difficulty that is evident in Figure 7.

To verify that the difficulty increases in response to the entry of miners that is incentivized, in part, by a higher price of the bitcoin, I use ordinary least squares (OLS) to test Eq. (9) by regressing the (log) subsequent level of difficulty δ_2 on the (log) price of the bitcoin

p_b, the (log) fees f, the (log) block reward ω, and the (log) cost F, the (log) gigahashes per second ϕ and the (log) joules per gigahash ξ averaged over all Antminer models available for sale, where, prior to taking the logarithm, all of the regressors are averaged over the 2016 block period that precedes the difficulty adjustment δ_2. The regressors are reasonably exogenous since they occur prior to the difficulty adjustment δ_2. Table 2 reports the results. It's clear that the model fits the data exceptionally well since the adjusted R^2 is .97. Moreover, all of the coefficients have the correct sign, consistent with Eq. (9). All but the coefficient on the (log) joules per gigahash ξ are significant, and the coefficients on the (log) price of the bitcoin p_b, the (log) gigahashes per second ϕ and the (log) cost F of available Antminers are highly significant with p-values $< .001$. Since the estimated coefficient on the (log) price of the bitcoin p_b is .61, holding all other variables constant, it follows that the percentage change in the difficulty is equal to 61% of the average return on the bitcoin in the 2016 block period prior to the adjustment.

Figure 10 further plots the (log) subsequent difficulty δ_2 against the (log) price of the bitcoin, where the price was averaged over the 2016 block period preceding δ_2. It's clear that there is a strong positive linear relationship between the two variables, where the largest deviations from the line of best fit occurred in mid 2014 and late 2017. During these time periods, impediments to entry prevented the network hashrate from increasing in line with prices, resulting in difficulty levels that were too low relative to the prevailing prices. In 2014, specialized mining equipment with application-specific integrated circuits (ASICs) had become main stream, and mining bitcoin with the central processing units (CPUs) or graphics processing units (GPUs) of commonly used computers was no longer profitable.[34] Entry to the industry at that time was temporarily impeded by the necessity of investing in new equipment and learning how to mine with ASICs. Also, during the high prices that occurred during the "bubble" period of late 2017, mining equipment was in short supply, resulting in

[34]See Franco (2015), Figure 9.3.

its extraordinarily high price or lack of availability.[35] If we subset the data to include only the observations starting from 1 January 2015, and to also remove the period from 1 September 2017 to 1 February 2018, the correlation between the (log) difficulty δ_2 and the (log) price of the bitcoin p_b averaged over the interim prior to the difficulty adjustment increases from 88.1% to 97.5%.

In summary, the data strongly support the model outlined in Section 2. Since the daily mining rate frequently differs from its target, market equilibria frequently occur while the protocol is in disequilibrium. I estimate the percentage change in the difficulty to be 61% of the average return on the bitcoin in the 2016 block period prior to the adjustment. Also, the correlation between the (log) difficulty and the (log) price of the bitcoin p_b averaged over the interim prior to the difficulty adjustment is 88.1% for the entire sample of data, and significantly higher during time periods when there is no impediment to the free entry of miners.

5.3 Estimating the price elasticity of demand

This section describes the econometric strategy for estimating the price elasticity of demand ε for bitcoins. As we have seen from Propositions 1 and 5, an estimate of the elasticity is necessary to approximate the net private welfare losses that are due to adjustments of the difficulty, the tax that fully displaces the electricity costs, and the electricity cost-minimizing tax. To this end, I estimate the parameters of the demand curve in (11), where I use the method of instrumental variables (IV) since the price of the bitcoin p_b is not exogenous because it is determined only in part by market demand. I use the bitcoin difficulty as an instrument for the price since, as we've seen in Section 2, the difficulty adjustments result in shocks to the supply curve, which permit identification of the demand curve.

[35] Recall from Footnote 32 that the periods of time when all sellers in the Amazon Marketplace were out of stock took place during late 2017 and early 2018.

Applying this logic, I estimate the first stage equation

$$\log(p_{bt}) = \alpha_1 \log(\delta_t) + \alpha_2 \log(\omega_t + f_t) + d_t + u_t \tag{16}$$

which regresses the (log) price of the bitcoin on the (log) difficulty and the other exogenous variables: the (log) miners' revenue $\omega_t + f_t$ and annual time fixed effects d_t, where t indexes days and the error term is u_t. The mining revenue term comprises the exogenous component of network security S in (10) and year fixed effects control for other exogenous factors that might shift demand. The second stage regression model is determined by log-linearizing the daily demand for the bitcoin in (11) and is given by

$$\log(X_{Dt}) = \beta_1 \log(\omega_t + f_t) - \varepsilon \widehat{\log(p_{bt})} + d_t + \upsilon_t \tag{17}$$

where the price of the bitcoin p_{bt} is instrumented in the first stage regression (16) and the error term is υ_t. Since Eqs. (16) and (17) are log linear, the estimates can be interpreted as elasticities. The price elasticity of demand ε is our key parameter of interest and the coefficient β_1 reveals the sensitivity of demand to a change in network security S.[36]

5.4 Estimating the net welfare losses

To estimate the total net welfare losses incurred by the miners and users of bitcoins over the sample period, I apply the formulas provided in Proposition 1 for the average loss Γ in (14) or the average gain Ω in (15) for each interval between difficulty adjustments, depending on whether the difficulty has increased or decreased. I proceed by first determining the average daily equilibrium quantity of bitcoins X_2 for each interval between difficulty adjustments by

[36] If we express demand in (11) as $\log(X_{Dt}) = \gamma_1 \log(S_t) + \gamma_2 \log(p_{bt}) + d_t + \upsilon_t$, then from S in (10) we have that $\log(X_{Dt}) = \gamma_1 \log(\omega_t + f_t) + (\gamma_1 + \gamma_2) \log(p_{bt}) + d_t + \upsilon_t$. Hence from (17) it follows that $\gamma_1 = \beta_1$ (and $\gamma_2 = -\varepsilon - \beta_1$).

multiplying the daily mining rate and the block reward. I estimate the corresponding price $p_b(X_2;\delta_1)$ from the inverse supply curve derived from Eq. (8), holding the initial level of difficulty δ_1 constant. To obtain the percentage change in the difficulty, I subtract 1 from the ratio of the difficulty at the end of the interval δ_2 to the difficulty at the beginning of the interval δ_1. Using this information and the estimate for the elasticity $\widehat{\varepsilon}$, I estimate the average daily quantity of bitcoins supplied after the difficulty adjustment X_3 by applying the formulas provided in Proposition 1, depending on whether the difficulty has increased or decreased. Given X_3, I estimate the price $p_b(X_3;\delta_1)$ from the inverse supply curve derived from Eq. (8), holding the initial level of difficulty δ_1 constant. Finally, I estimate the total net welfare losses due to adjustments of the difficulty by multiplying each average loss or gain by the length of the interval (the number of days between the respective difficulty adjustments) and aggregating the total losses net of the total gains throughout the sample period. I also decompose the net welfare losses into electricity costs and distortion losses. To determine the relative magnitude of the electricity costs that are due to adjustments of the difficulty, I express them as a proportion of the total electricity cost of running the bitcoin network for each year in the sample. I estimate the terawatt hours used by the network as $\phi M^* \xi \frac{24}{10^{12}}$ per day, where M^* is given in (6), and determine the electricity costs by applying a 0.05 USD per kWh price of electricity.

5.5 Estimating the tax rates

To estimate the tax that fully displaces the electricity costs $\overline{\tau}$, I apply the formula provided in Proposition 5(i), which requires an estimate of the average daily equilibrium quantity of bitcoins X_2 and the elasticity $\widehat{\varepsilon}$, which are determined as explained in Sections 5.3 and 5.4 above. I calculate the target level of output $\overline{X}$ by multiplying the block reward by 144. To estimate the cost-minimizing tax τ^* for each period between difficulty adjustments, I

solve for the largest root of the cubic polynomial equation F_3 provided in Eq. (A8) of the Appendix, which implicitly defines τ^*. Estimating the coefficients of F_3 requires estimates of X_2, $\overline{X}$ and $\widehat{\varepsilon}$, as determined above.

For either tax, since counterfactual data on the difficulty adjustment under the tax δ_2^τ is not available, I treat the intervals between difficulty adjustments as independent. Hence each estimate of the tax that fully displaces the electricity costs $\overline{\tau}$ should be interpreted as the *initial* tax necessary to align output under the tax X_2^τ with the target level $\overline{X}$, and each estimate of the cost-minimizing tax τ^* should be interpreted as the *initial* tax necessary to align output under the tax X_2^τ with its cost-minimizing level $X_2^{\tau^*}$. I find the average initial tax by averaging over the tax rates that are estimated for each interval.

Finally, I estimate the tax that eliminates all bitcoin production $\overline{\overline{\tau}}$ and the revenue-maximizing tax τ^{TR} by applying the formulas provided in Propositions 3 and 5(iii), using the estimate of the elasticity $\widehat{\varepsilon}$.

6 Results

The results for the first stage and instrumental variables (IV) regressions in (16) and (17) are presented in Table 3 along with, for the sake of comparison, the results from the OLS regression of (17), which ignores the endogeneity of p_{bt}. The results reaffirm that the model set out in Section 2 fits the data exceptionally well since the adjusted R^2 values exceed .99. The estimates from the first stage regression reveal that the sensitivity of the price of the bitcoin to changes in the level of difficulty $\widehat{\alpha_1} = .38$ (p-value $< .001$). In other words, a 10% increase in the contemporaneous difficulty is associated with a 3.8% increase in the price of the bitcoin. The estimates from the IV regression reveal that the sensitivity of demand to changes in network security $\widehat{\beta}_1 = .94$ (p-value $< .001$) and the price elasticity of demand $\widehat{\varepsilon} = .17$ (p-value $< .001$). In other words, a 10% increase in the level of security is associated

with a 9.4% increase in the quantity of bitcoins demanded and a 10% increase in the price of the bitcoin is associated with a 1.7% decrease in the quantity of bitcoins demanded. The estimates are highly significant and their signs are consistent with the model from Section 2. Diagnostic tests for the IV regression demonstrate that the difficulty is a strong instrument, since the null hypothesis that the instrument is weak is strongly rejected (p-value $< .001$), and confirm the necessity of using instrumental variables, since Wu-Hausman test for endogeneity is strongly rejected (p-value $< .001$). Also, from the third column of Table 3, it's clear that without correcting for endogeneity, the OLS estimate for the price elasticity of demand is upward biased since $-.02 > -.17$.

I calculate the total net welfare losses incurred by the miners and users of the bitcoin from 17 March 2014 to 13 January 2019 to be 373.83 million USD. (I estimate the total welfare losses to be 440.26 million USD and the total welfare gains to be 66.43 million USD.) The net welfare losses can be further broken down into total electricity costs of 369.76 million USD and total distortion losses of 4.07 million USD. The large magnitude of the losses relative to the gains is in accordance with Proposition 2 and because only 15.9% of the difficulty adjustments during the sample period were downward. Table 4 breaks down, for each year in the sample period,[37] the electricity costs due to adjustments of the difficulty as a proportion of the total electricity costs to run the bitcoin network. Since the difficulty is increasing exponentially during the sample period, the electricity costs due to adjustments of the difficulty are also increasing exponentially over time. As a proportion of the total electricity costs, however, they are fairly stable and are, on average, equal to 10.27% of the total electricity costs.

Figure 11 plots the tax that fully displaces the electricity costs $\overline{\tau}$, the cost-minimizing tax τ^*, the revenue-maximizing tax τ^{TR} and the tax that fully displaces all bitcoin production $\overline{\overline{\tau}}$ for each interval between difficulty adjustments over the sample period. As shown, $\overline{\tau}$

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

ranges from -122% to 137% during the sample period, with a mean of 35.0%. The cost-minimizing tax τ^* ranges from 301.9% to 384.9% during the sample period, with a mean of 347.5%. While these tax rates are large, on average, recall from Section 4 that they should be interpreted as initial corrections. The magnitude of the estimated cost-minimizing tax is consistent with the fact that, as shown in Figure 9, the daily mining rate typically exceeded the target during the sample period, resulting in large increases in electricity costs, while τ^* induces the protocol to gift the maximal amount of electricity. As shown in Figure 11, the estimate of the revenue-maximizing tax is 229.4%, which is less than all estimates of the electricity cost-minimizing tax. This is consistent with Proposition 5(iii) since $X_2' = 0.51\overline{X}$ and the daily mining rate exceeded $0.51\overline{X}$ throughout the entire sample period. Finally, as shown in Figure 11, the estimate of the tax that fully displaces all bitcoin production $\overline{\overline{\tau}}$ is 688.2%.

It's also evident from Figure 11 that the variance of $\overline{\tau}$ exceeds that of τ^*. Since $\overline{\tau}$ fully displaces the impending difficulty adjustment, it must exceed, in absolute value, the percentage change in the difficulty.[38] In contrast, τ^* minimizes the percentage change in the difficulty under the tax in balance with its effect on the equilibrium level of output. Hence the variance of $\overline{\tau}$ (.175) is more than 8-fold greater than the variance of τ^* (.020). If the tax $\overline{\tau}$ is implemented only when it is positive, so that the bitcoin is never subsidized, then its variance falls to 0.121, which is about 6-fold greater than the variance of τ^*.

In summary, this section quantifies the results of Propositions 1 and 5 using data for the nearly five-year sample period: 17 March 2014 to 13 January 2019. I first estimate the price elasticity of demand for the bitcoin by using the difficulty as an instrument for the price, yielding an estimate of $\widehat{\varepsilon} = .17$. Applying Proposition 1, I determine that the net cost incurred by the miners and users of bitcoins due to the protocol's use of the difficulty to target a constant rate of growth in the quantity of bitcoins during this time is 373.83

[38] Recall Footnote 25.

million USD. Applying Proposition 5, I estimate the average initial tax that fully displaces the electricity costs $\overline{\tau}$ to be 35% and the average initial cost-minimizing tax τ^* to be 347.5%. Applying Figure 6, it follows that, on average, initial tax rates that would have resulted in an increase in electricity costs are between 0 and $\overline{\tau} = 35\%$ while tax rates that would have resulted in a decrease in electricity costs are greater than $\overline{\tau} = 35\%$, where the greatest reduction would have occurred at $\tau^* = 347.5\%$.

7 Conclusion

This paper develops a microeconomic model to analyze the functioning of the Bitcoin protocol's difficulty adjustment mechanism. Although Bitcoin is a decentralized peer-to-peer network with no central authority, its process for adjusting the level of difficulty amounts to an inflexible system of supply management. Laissez-faire prices do not exist in the bitcoin market since the Bitcoin protocol regularly intervenes to adjust the difficulty. These adjustments result in welfare losses that fall on the miners and users of the bitcoin. Ironically, while many of these market participants hold their wealth in the form of bitcoins to guard against inflation, the protocol implicitly taxes them whenever the difficulty rises. An actual tax on the price of the bitcoin administered by a government can be used to incentivize the difficulty adjustment mechanism to decrease the electricity costs it induces. To accurately correct the miners' incentives, the tax must be based on the current information conveyed by the level of output in the bitcoin market and the price elasticity of demand for the bitcoin. If the electricity cost-minimizing tax is applied in each period between difficulty adjustments, the network hashrate and the difficulty will follow downward paths over time. Hence it is possible to use a tax to rewind the network hashrate and the difficulty back to the levels that existed closer to the inception of the network. To preserve network security, however, it is necessary to determine an upper bound on the tax to ensure that the cost of launching

a 51% attack does not fall below a minimal level that safeguards the network. The issue of taxing bitcoin makes it pertinent to specify this level, which remains an open research question. Simulations could be used to build on the empirical results of this paper, to reveal the electricity cost-displacing and cost-minimizing paths of tax rates over time, and their sensitivity to demand shocks and less regular adjustments of the tax rate. I leave these important questions for future research.

References

[1] Athey, S., Parashkevov, I., Sarukkai, V. and Xia J. (2016): "Bitcoin Pricing, Adoption, and Usage: Theory and evidence." Working Paper.

[2] Bakos, Y. and Halaburda, H. (2021): "Tradeoffs in Permissioned vs Permissionless Blockchains: Trust and Performance." Working Paper.

[3] Benetton, M., Compiani, G., and Morse, A. (2021): "When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy." Working Paper.

[4] Biais, B., Bisiere, C., Bouvard, M., Casamatta, C. (2019): "The Blockchain Folk Theorem." *The Review of Financial Studies*, 32(5): 1662-1715.

[5] Blandin, A., Pieters, G., Wu, Y., Eisermann, T., Dek, A., Taylor, S., and Njoki, D. (2020): "3rd Global Cryptoasset Benchmarking Study." Cambridge Centre for Alternative Finance Report. Available from: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study

[6] Budish, E. (2018): "The Economic Limits of Bitcoin and the Blockchain." NBER Working Paper 24717.

[7] Chiu, J. and Koeppl, T. (2019): "The Economics of Cryptocurrencies–Bitcoin and Beyond." Bank of Canada Staff Working Paper 2019-40.

[8] Dittmar, L. and Praktiknjo, A. (2019): "Could Bitcoin Emissions Push Global Warming Above 2 Degrees Celsius?" *Nature Climate Change,* 9: 656–657.

[9] D'Souza, M., Chwarzynski, S., Jappa, M., and Adams, G. (2020): "Understanding Bitcoin Market Participants – Vulnerabilities in the Price of Bitcoin Driven by Miners." Blockware Solutions Research Report. Available from https://www.blockwaresolutions.com/research-and-publications/2020-halving-analysis

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

[11] Fan, J. and Yao, Q. (2017): *The Elements of Financial Econometrics*. Cambridge University Press.

[12] Franco, P. (2015): *Understanding Bitcoin: Cryptography, Engineering and Economics*. Wiley.

[13] Easley, D., O'Hara, M., and Basu, S. (2018): "From Mining to Markets: The Evolution of Bitcoin Transaction Fees." *Journal of Financial Economics*, 134(1): 91-109.

[14] 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

[15] Krause, M., and Tolaymat, T. (2018): "Quantification of Energy and Carbon Costs for Mining Cryptocurrencies." *Nature Sustainability*, 1(7): 11–8.

[16] Malinova, K. and Park, A. (2017): "Market Design with Blockchain Technology." Working Paper, University of Toronto.

[17] 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): 127–40.

[18] Mora, C., Rollins, R., Talada, K., Kantar, M., Chock, M., Shimada, M. and Franklin, E. (2018): "Bitcoin Emissions Alone Could Push Global Warming Above 2 Degrees Celsius." *Nature Climate Change,* 8: 924–36.

[19] OECD (2020): Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues, OECD, Paris. Available from www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging- tax-policy issues.htm

[20] Prat, J. and Walter, B. (2021): "An Equilibrium Model of the Market for Bitcoin Mining." *Journal of Political Economy,* 129(8):2415–2452.

[21] Stoll, C., Klaassen, L. and Gallersdorfer, U. (2018): "The Carbon Footprint of Bitcoin." *Joule* 3(7): 1647–61.

[22] Raskin, M., Saleh, F. and Yermack, D. (2019): "How Do Private Digital Currencies Affect Government Policy?" NYU Law and Economics Research Paper No. 20-05.

[23] Yu, G. and Zhang, J. (2018): "Flight to Bitcoin." Working Paper.

Appendix

Proof of Proposition 1:

(i) From Figure 2a 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, so that $\Delta E = \psi p'_{b3} X_3$ where $p'_{b3} = p_b(X_3; \delta_1)$. It remains to derive the deadweight (distortion) loss DWL, or the second term of (14).

In equilibrium, we have

$$X_S(p_b) = X_D(q_b) \tag{A1}$$

where the price paid by consumers is $q_b = p_b(\psi)(1+\psi)$ and the price received by miners is $p_b(\psi)$. Differentiating (A1) 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

$$\frac{dp_b}{d\psi} = \frac{\frac{\partial X_D}{\partial q}p_b}{\frac{\partial X_S}{\partial p_b} - \frac{\partial X_D}{\partial q}(1+\psi)\frac{\frac{p_b}{X}}{\frac{p_b}{X}}} \approx -\frac{\varepsilon}{1+\varepsilon}p_b \tag{A2}$$

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,

$$\frac{dq_b}{d\psi} = \frac{dp_b}{d\psi}(1+\psi) + p_b \approx \frac{1}{1+\varepsilon}p_b$$

applying (A2) 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 difficulty adjustment on equilibrium output is given by

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

applying (A2) and the fact $\frac{\partial X_S}{\partial p_b}\frac{p_b}{X} = 1$. It follows that $\Delta X \approx \frac{dx}{d\psi}\psi = -\frac{\varepsilon\psi}{1+\varepsilon}X$ and

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

where p_{b2} and X_2 are the equilibrium price and quantity of bitcoins prior to the difficulty adjustment. It follows that we can approximate X_3, the equilibrium quantity of bitcoins after the difficulty adjustment with

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

Hence the welfare loss due to a percentage increase in the difficulty ψ is $\Gamma(\psi) = \psi p_b(X_3;\delta_1) X_3 + \frac{1}{2}\frac{\varepsilon}{1+\varepsilon} p_{b2} X_2 \psi^2$, where $X_3 \approx \left(\frac{1+\varepsilon-\varepsilon\psi}{1+\varepsilon}\right) X_2$.

Since a decrease in difficulty is just the negative of an increase in difficulty, it's clear from the arguments above that under a percentage decrease in difficulty φ, $\Delta p_b \approx \frac{\varepsilon}{1+\varepsilon} p_b \varphi$ and $\Delta q_b \approx -\frac{1}{1+\varepsilon} p_b \varphi$, and hence $|\Delta p_b| + |\Delta q_b| \approx p_b \varphi$. It follows that $DWL \approx \frac{1}{2}\frac{\varepsilon}{1+\varepsilon} p_{b2} X_2 \varphi^2$ and $X_3 \approx \left(1 + \frac{\varepsilon\varphi}{1+\varepsilon}\right) X_2$. Hence the welfare gain due to a percentage decrease in the difficulty φ is approximately $\Omega(\varphi) = \varphi p_b(X_3;\delta_1) X_3 - \frac{1}{2}\frac{\varepsilon}{1+\varepsilon} p_{b2} X_2 \varphi^2$, where $X_3 \approx \left(\frac{1+\varepsilon+\varepsilon\varphi}{1+\varepsilon}\right) X_2$.

Proof of Proposition 2:

Let $\psi = -\varphi$, $X_2 > \overline{X}$, and $\widetilde{X_2} < \overline{X}$. From (14) and (15) we have that

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

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

Proof of Proposition 3 and Corollary 4:

It follows from Proposition 1(i) that, after applying an ad valorem tax τ on the price of the bitcoin, the equilibrium quantity is given by $X_2^\tau = \left(1 - \frac{\varepsilon}{1+\varepsilon}\tau\right) X_2$. Hence, from (12), the protocol will adjust the difficulty such that

$$\frac{\delta_2^\tau}{\delta_1} = \frac{X_2^\tau}{\overline{X}} = \left(1 - \frac{\varepsilon}{1+\varepsilon}\tau\right)\frac{X_2}{\overline{X}}.$$

Consequently, the steady state level of output under the tax, which occurs when $\delta_2^\tau = \delta_1$, is $\overline{X}^\tau = \frac{1+\varepsilon}{1+\varepsilon(1-\tau)}\overline{X}$.

Proof of Proposition 5:

(i) and (ii): From Proposition 1 it follows that the equilibrium quantity produced under the tax is given by

$$X_2^\tau = \left(\frac{1+\varepsilon-\varepsilon\tau}{1+\varepsilon}\right) X_2 \tag{A3}$$

and, from (12), the protocol will adjust the difficulty by the percentage ψ^τ where

$$1 + \psi^\tau = \frac{\delta_2^\tau}{\delta_1} = \frac{X_2^\tau}{\overline{X}} = \left(\frac{1+\varepsilon-\varepsilon\tau}{1+\varepsilon}\right)\frac{X_2}{\overline{X}}. \tag{A4}$$

Also, we have that $\overline{\tau}$, which is defined by $X_2^\tau = \overline{X}$, is

$$\overline{\tau} = \frac{1+\varepsilon}{\varepsilon}\left(1 - \frac{\overline{X}}{X_2}\right)$$

and $\overline{\overline{\tau}}$, which is defined by $X_2^\tau = 0$, is

$$\overline{\overline{\tau}} = \frac{1+\varepsilon}{\varepsilon}.$$

The tax revenue is given by

$$\begin{aligned} \Delta TR &= \tau p_b\left(X_2^\tau;\delta_1\right) X_2^\tau \\ &= \tau\gamma\left(\delta_1\right)\left(\frac{1+\varepsilon-\varepsilon\tau}{1+\varepsilon}\right)^2 X_2^2 \end{aligned} \tag{A5}$$

where, from (8), the inverse supply curve can be expressed as $p_b = \gamma(\delta) X$, where $\gamma(\delta) = \frac{\eta F + \frac{\xi\phi}{1000}(24)p_e}{(\omega+f)\left[\frac{(24)60^2\phi 10^9}{\delta 2^{32}}\right]\overline{X}}$, and the third line follows from (A3). After the protocol increases the difficulty, it follows from Proposition 1(i) that equilibrium output is given by

$$\begin{aligned} X_3^\tau &= \left(\frac{1+\varepsilon-\varepsilon\psi^\tau}{1+\varepsilon}\right) X_2^\tau \\ &= \left(\frac{1+\varepsilon-\varepsilon\psi^\tau}{1+\varepsilon}\right)\left(\frac{1+\varepsilon-\varepsilon\tau}{1+\varepsilon}\right) X_2 \end{aligned} \tag{A6}$$

where the second line follows from (A3).

It follows from (A3), (A4) and (A6) that electricity costs under the tax are

$$\begin{aligned} \Delta E^\tau &= \psi^\tau p_b^\tau\left(X_3^\tau;\delta_1\right) X_3^\tau \\ &= \left(\frac{1+\varepsilon-\varepsilon\tau}{1+\varepsilon}\frac{X_2}{\overline{\overline{X}}} - 1\right)(1+\tau)\,\gamma\left(\delta_1\right)\left(\frac{1+\varepsilon-\varepsilon\left(\frac{1+\varepsilon-\varepsilon\tau}{1+\varepsilon}\frac{X_2}{\overline{\overline{X}}}-1\right)}{1+\varepsilon}\right)^2\left(\frac{1+\varepsilon-\varepsilon\tau}{1+\varepsilon}\right)^2 X_2^2 \end{aligned} \tag{A7}$$

since $p_b^\tau\left(X_3^\tau;\delta_1\right) = (1+\tau)\, p_b\left(X_3^\tau;\delta_1\right)$. We can express (A7) as

$$\Delta E^\tau = \left((1-\upsilon\tau)V - 1\right)(1+\tau)\left(1-\upsilon\left((1-\upsilon\tau)V-1\right)\right)^2(1-\upsilon\tau)^2\,\gamma\left(\delta_1\right) X_2^2$$

where $V = \frac{X_2}{\overline{\overline{X}}}$ and $\upsilon = \frac{\varepsilon}{1+\varepsilon}$. It follows that $-\frac{\partial \Delta E^\tau}{\partial \tau} = F_1 F_2 F_3$, where $F_1 = (\upsilon\tau - 1)\,\gamma\left(\delta_1\right) X_2^2$, $F_2 = \upsilon - V\upsilon + V\upsilon^2\tau + 1$ and

$$F_3 = a\tau^3 + b\tau^2 + c\tau + d \tag{A8}$$

where

$$
\begin{aligned}
a &= 6V^2\upsilon^4 \\
b &= 5V^2\upsilon^4 - 13V^2\upsilon^3 + 9V\upsilon^3 + 4V\upsilon^2 \\
c &= 8V^2\upsilon^2 - 10V^2\upsilon^3 + 7V\upsilon^3 - 8V\upsilon^2 - 5V\upsilon + 3\upsilon^2 + 3\upsilon \\
d &= 5V^2\upsilon^2 - V^2\upsilon - 7V\upsilon^2 - V\upsilon + V + 2\upsilon^2 + \upsilon - 1.
\end{aligned}
$$

It follows that $F_1 < 0$, if $\tau < \overline{\overline{\tau}}$. Also, $F_2 > 0$ if and only if $\tau > \overline{\tau} - \frac{1}{V\upsilon^2}$. The discriminant of $\frac{\partial F_3}{\partial \tau} = 3a\tau^2 + 2b\tau + c$ is the following quadratic in V

$$
b^2 - 3ac = V^2\upsilon^4\left[\left(25\upsilon^4 + 50\upsilon^3 + 25\upsilon^2\right)V^2 - \left(36\upsilon^3 + 50\upsilon^2 + 14\upsilon\right)V + 27\upsilon^2 + 18\upsilon + 16\right] > 0
$$

which is positive since the coefficient of the V^2 term is positive and its discriminant

$$
\begin{aligned}
&\left(36\upsilon^3 + 50\upsilon^2 + 14\upsilon\right)^2 - 4\left(25\upsilon^4 + 50\upsilon^3 + 25\upsilon^2\right)\left(27\upsilon^2 + 18\upsilon + 16\right) \\
&= -36\upsilon^2\left(\upsilon + 1\right)^2\left(39\upsilon^2 + 22\upsilon + 39\right) < 0
\end{aligned}
$$

is negative, and $V > 0$. It follows that F_3 has two distinct real extrema given by

$$
\begin{aligned}
\tau_1 &= \frac{-b - \sqrt{b^2 - 3ac}}{3a} \\
\tau_2 &= \frac{-b + \sqrt{b^2 - 3ac}}{3a}
\end{aligned}
\tag{A9}
$$

where τ_1 corresponds to the interior maximum of F_3 and τ_2 corresponds to the interior minimum of F_3, and three real roots given by $\tau = r_1$, r_2 and r_3,[39] labelled such that $r_1 < t_1 < r_2 < t_2 < r_3$. As we'll see below, $r_3 \in \left(\overline{\tau}, \overline{\overline{\tau}}\right)$ and hence r_3 corresponds to the maximum of $-\Delta E^\tau$ and $\tau^* = r_3$. We have that $-\frac{\partial \Delta E^\tau}{\partial \tau}\Big|_{\tau = r_3} = 0$ since $F_3|_{\tau = r_3} = 0$ and, for any small $\delta > 0$, $\frac{\partial \Delta E^\tau}{\partial \tau}\Big|_{\tau = r_3 - \delta} > 0$ and $\frac{\partial \Delta E^\tau}{\partial \tau}\Big|_{\tau = r_3 + \delta} < 0$ since $F_3|_{\tau = r_3 - \delta} < 0$ and $F_3|_{\tau = r_3 + \delta} > 0$, because F_3 is increasing in the neighborhood of r_3, and $F_1|_{\tau = r_3} < 0$ and $F_2|_{\tau = r_3} > 0$, from the definitions of F_1 and F_2 above since $r_3 \in \left(\overline{\tau}, \overline{\overline{\tau}}\right)$.

Finally, it remains to show that $r_3 \in \left(\overline{\tau}, \overline{\overline{\tau}}\right)$. From the definition of F_3 in (A8) it follows that

$$
\begin{aligned}
F_3|_{\tau = \overline{\overline{\tau}}} &= 2\left(\upsilon + 1\right)^2 > 0 \\
\left.\frac{\partial F_3}{\partial \tau}\right|_{\tau = \overline{\overline{\tau}}} &= \upsilon\left(\upsilon + 1\right)\left(3V + 7V\upsilon + 3\right) > 0 \\
\left.\frac{\partial^2 F_3}{\partial \tau^2}\right|_{\tau = \overline{\overline{\tau}}} &= 2V\upsilon^2\left(9\upsilon + 5V\upsilon + 5V\upsilon^2 + 4\right) > 0
\end{aligned}
$$

[39] It can be shown that the discriminant of F_3 $18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2 > 0$ for all $V > 0$ and $0 < \upsilon < 1$.

which are positive for all $V > 0$ and $0 < \upsilon < 1$. Hence $\overline{\overline{\tau}} > r_3$ since, at $\tau = \overline{\overline{\tau}}$, F_3 is strictly positive, increasing and convex in τ. Also, let's assume by contradiction that $\overline{\tau} \geq r_3$. It follows that $F_3|_{\tau=\overline{\tau}} \geq 0$ and $\frac{\partial F_3}{\partial \tau}\big|_{\tau=\overline{\tau}} > 0$ so that

$$F_3|_{\tau=\overline{\tau}} = -\frac{1}{V}\left(V + V\upsilon - 1\right) \geq 0$$

$$\left.\frac{\partial F_3}{\partial \tau}\right|_{\tau=\overline{\tau}} = \upsilon\left(-3V\upsilon^2 + 3\upsilon + 3V - 5\right) > 0.$$

Since $\frac{1}{1+\upsilon} < \frac{5-3\upsilon}{3(1-\upsilon^2)}$, however, we have a contradiction and it follows that $\overline{\tau} < r_3$.

(iii) We can express the tax revenue ΔTR in (A5) as

$$\Delta TR = \tau\left(1 - \upsilon\tau\right)^2 \gamma\left(\delta_1\right) X_2^2$$

which is maximal at

$$\tau^{TR} = \frac{1}{3\upsilon}. \tag{A10}$$

We first identify the sets $S_1 = \left\{V : F_3|_{\tau=\tau^{TR}} > 0\right\}$ and $S_2 = \left\{V : \tau^{TR} > \tau_2\right\}$ in order to determine $S_1 \cap S_2 = \left\{V : \tau^{TR} > \tau^*\right\}$ and $\left(S_1 \cap S_2\right)^C = \left\{V : \tau^{TR} \leq \tau^*\right\}$. Evaluating F_3 at $\tau = \tau^{TR}$ yields

$$F_3|_{\tau=\tau^{TR}} = \left(\frac{20}{9}\upsilon^2 + \frac{4}{9}\upsilon\right)V^2 - \left(\frac{14}{3}\upsilon^2 + \frac{8}{3}\upsilon + \frac{2}{9}\right)V + 2\upsilon^2 + 2\upsilon$$

and hence $S_1 = \left\{(0, V_1) \cup (V_2, \infty)\right\}$, where

$$V_1 = \frac{1}{4\upsilon + 20\upsilon^2}\left(12\upsilon + 21\upsilon^2 - \sqrt{24\upsilon + 114\upsilon^2 + 72\upsilon^3 + 81\upsilon^4 + 1} + 1\right)$$

$$V_2 = \frac{1}{4\upsilon + 20\upsilon^2}\left(12\upsilon + 21\upsilon^2 + \sqrt{24\upsilon + 114\upsilon^2 + 72\upsilon^3 + 81\upsilon^4 + 1} + 1\right).$$

Also, from (A9) and (A10) we have that $\tau^{TR} > \tau_2$ if and only if $\frac{1}{3\upsilon} > \frac{-b+\sqrt{b^2-3ac}}{3a}$ and hence $S_2 = \left\{ \begin{array}{c} (0, V_3) \text{ if } \upsilon \neq \frac{1}{5} \\ \left(0, \frac{135}{92}\right) \text{ if } \upsilon = \frac{1}{5} \end{array} \right\}$, where

$$V_3 = \frac{1}{8\upsilon - 40\upsilon^2}\left(6\upsilon - 21\upsilon^2 - \sqrt{-60\upsilon + 318\upsilon^2 + 468\upsilon^3 + 441\upsilon^4 + 49} + 7\right).$$

It follows that $S_1 \cap S_2 = \left\{(0, V_1)\right\}$ since $V_1 < V_3 < V_2$ and $|V_1{}_{\upsilon=\frac{1}{5}} < \frac{135}{92} < |V_2{}_{\upsilon=\frac{1}{5}}$. It follows that there exists a $V' > 0$ such that $\tau^{TR} > \tau^*$ if and only if $V < V'$, where $V' = V_1$. If, for example, $\varepsilon = .17$, we have that $V' = 0.51$.

Table 1. Antminer equipment specifications.

	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	18-01-20	16-01-18	14,000	.098	1,372
Antminer S11	18-11-21	18-11-19	19,500	.07	1,365

Table 2. Regression results for Eq. 9.

	OLS
Intercept	17.489 *** (1.108)
(log) Price	.610 *** (.058)
(log) Block Reward	.529 * (.205)
(log) Fees	.078 . (.047)
(log) Antminer hashrate (GHash/s)	1.24 *** (.069)
(log) Antminer price	-.967 *** (.064)
(log) Antminer energy efficiency (Joules/GHash)	.040 (.103)
Adj. R^2	.974
F Stat	802

Note: Column 1 presents the OLS estimates from the regression of Eq. 9. All regressors were averaged for each level of the difficulty prior to taking the logarithm. The dependent variable is the subsequent level of the (log) Bitcoin difficulty. Standard errors are indicated in parentheses, " " indicates p>.1, "." indicates .05<p<.1, "*" indicates .01<p<.05 and "***" indicates p<.001. The number of observations is equal to 133.

Table 3. Regression results for Eqns. 16 and 17.

	First Stage	IV	OLS
(log) Price		-.167 *** (.021)	-.022 *** (.006)
(log) Difficulty	.376 *** (.024)		
(log) Revenue	.066	.939 ***	.959***

	(.064)	(.021)	(.018)
Year Fixed effects	Y	Y	Y
Adj. R^2	.997	.9997	.9998
F Stat	6.495×10^4		9.538×10^5

Note: The dependent variable is the (log) daily quantity of bitcoins supplied. Column 1 presents the OLS estimates of the first stage regression of Eq. 16. Column 2 presents the IV estimates from Eq. 17, using IV Regression. Column 3 presents the OLS estimates of the second stage regression. Standard errors are indicated in parentheses, "***" indicates p<.001 and " " indicates p>.1. The number of observations is equal to 1764.

Table 4. Annual net welfare losses due to difficulty adjustments.

Year	TWh	Electricity Costs (USD)	Percent of Total Cost
2014-03-17 to 2015-01-13	2.08	18,745,122	18.01
2015-01-14 to 2016-01-13	3.91	16,072,899	8.22
2016-01-14 to 2017-01-13	13.20	38,597,303	5.85
2017-01-14 to 2018-01-13	18.77	139,348,818	14.85
2018-01-14 to 2019-01-13	55.13	156,992,441	5.70

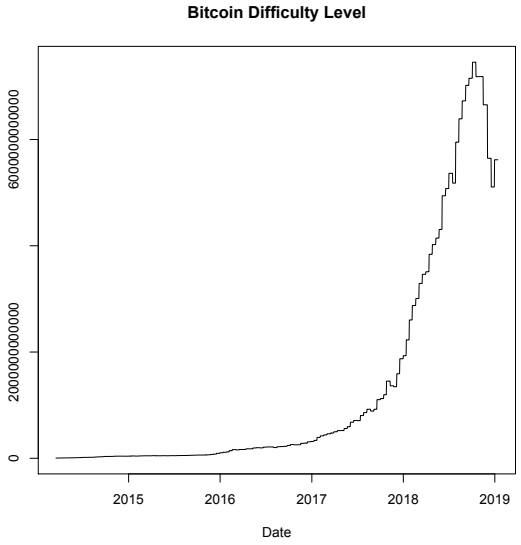

Figure 7. The difficulty level.

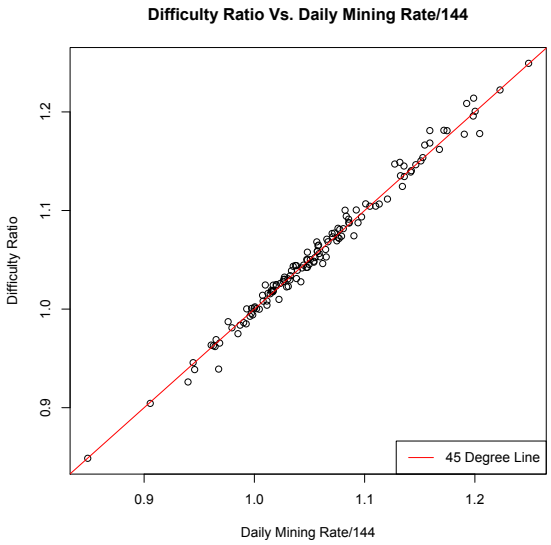

Figure 8. The difficulty adjustment mechanism.

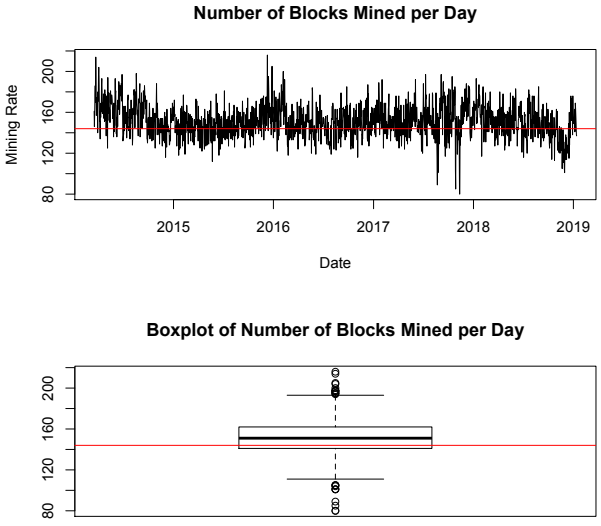

Figure 9. The daily mining rate.

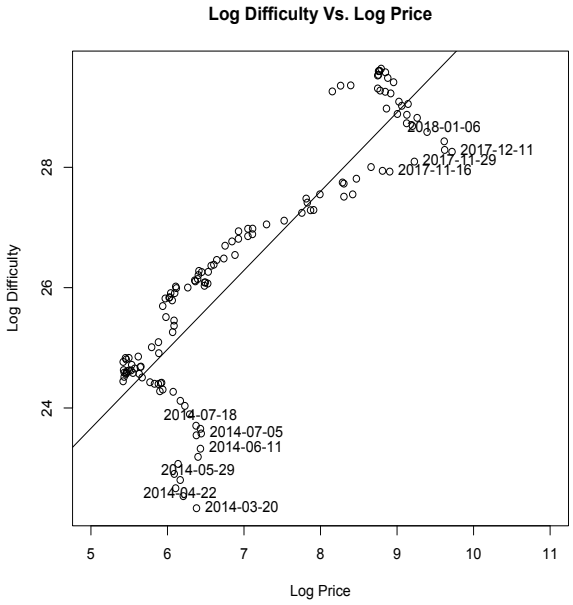

Figure 10. Log difficulty vs. log price.

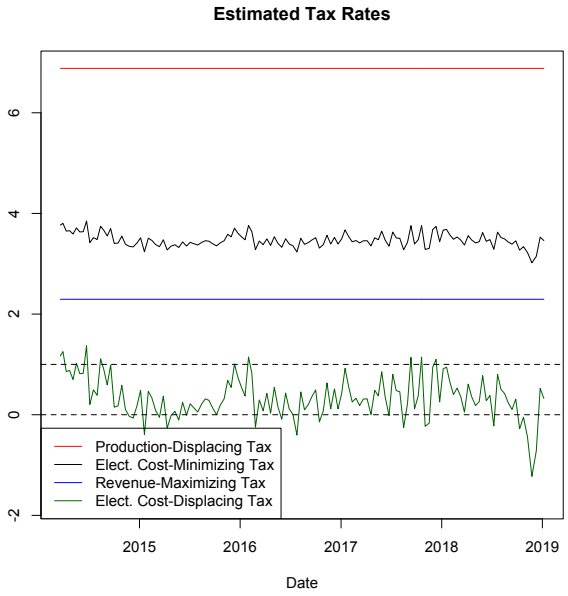

Figure 11. The estimated tax rates.