From Hotelling to Nakamoto: The Economics of Bitcoin Mining

Min DAI, Wei JIANG, Steven KOU and Cong QIN

31 January 2021

From Hotelling to Nakamoto: The Economics of Bitcoin Mining *

Min Dai[†]   Wei Jiang[‡]   Steven Kou [§]   Cong Qin [¶]

Jan 31, 2021

Abstract

We propose a unified dynamic framework to study the economics of the supply side of bitcoin mining, such as endogenous transaction fees, the miners' liquidation policies, and endogenous inventory holdings, in the face of declining system block rewards and stochastic demand. The model yields two economic insights: First, high jump risk and transaction fees income can be major forces driving miners to significantly reduce their inventory even when bitcoin prices are relatively low. Second, the model explains the observed co-movements of average transaction fees, average block sizes, and Bitcoin prices.

[†]National University of Singapore. E-mail: mindai@nus.edu.sg

[‡]The Hong Kong University of Science and Technology. E-mail: weijiang@ust.hk

[§]Boston University. E-mail: kou@bu.edu

[¶]Soochow University. E-mail: congqin@suda.edu.cn

The computer science meaning of Bitcoin[1] mining is to prevent double-spending in a probabilistic way in terms of proof-of-work. Indeed, how to prevent double-spending becomes a severe problem in a distributed network without a central authority. This is a particular case of reaching consensus in a distributed network, which has shown to be impossible under traditional deterministic consensus framework; see, e.g., Lamport et al. (1982) and Fischer et al. (1985). A revolution pioneered by Nakamoto (2009) was that the double-spending problem might be solved in a probabilistic way by using blockchains and "mining" (a form of proof-of-work). More computer science background of Bitcoin mining is given in Appendix A.

However, so far, the economic meaning of Bitcoin mining has not been exploited in detail. To do this, one needs to study the economics of the supply side of Bitcoin mining, such as endogenous transaction fees, the miners' liquidation policies, the miners' endogenous inventory holdings, in the face of declining system block rewards and stochastic demand.

In particular, we consider two research questions. First, how miners endogenously liquidate their bitcoins. More precisely, when is the miners' optimal time to sell, and what is their optimal selling rate? Because block rewards are the only way that new bitcoins are supplied, any bitcoins must be first held by miners before entering into circulation. As Athey et al. (2016) observed, the miners' share kept declining from 2013 to 2015, regardless of bitcoin price's drastic fluctuation; see Fig. 1. In particular, conscious of the scarcity of bitcoin, miners still kept selling their bitcoins even when the bitcoin price was relatively low. A natural question arises: Why did miners sell so early and so fast?

The second research question is related to the co-movements of average transaction fee rate, average block sizes,[2] and Bitcoin prices. The miners get two income sources, block rewards predetermined by the system and the voluntary transaction fees attached by users to the block. The transaction fees will be the miners' sole income source after the systematic termination of block rewards around the year 2140. As shown by Fig. 2, the average transaction fee rate was relatively

---

[1]Since Bitcoin is both a currency and a protocol, we use Bitcoin (an upper case letter B) to label the protocol, software, and community, and bitcoin (a lower case b) to label the currency.

[2]The block size refers to the size of transaction data written in a block.

1
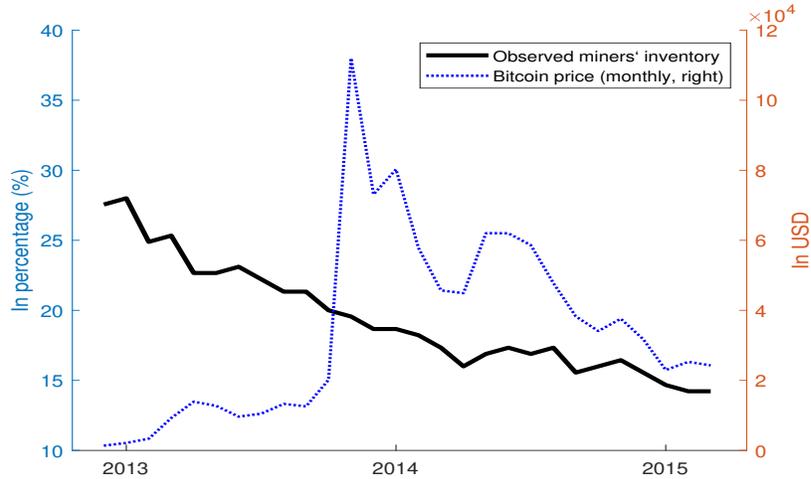
Figure 1: **Miner's inventory proportional to the supply from 2013 to 2015** (Athey et al., 2016). Propotional inventory $= \frac{\text{Miners' aggregate inventory at time t}}{\text{Cumulative Bitcoin supply at time t}}$.

low and remained fairly flat for an extended period (e.g., 2014-2016), but increased dramatically in 2017, and dropped down quickly afterward. In the meantime, the block size first raised gradually to the system recommended capacity 1MB till 2017, and then remained stable afterward, while the bitcoin prices fluctuated dramatically. Obviously, the average transaction fee rate is endogenously linked to both the bitcoin price and block size. A question that we attempt to investigate is why the average transaction fee rate and block size endogenously exhibited such an observed pattern in the face of the bitcoin price movement.

It is challenging to build a comprehensive model to have bitcoin prices, inventory, average transaction fee rates all endogenously determined. For example, the determination of equilibrium bitcoin prices alone is a difficult problem due to the highly speculative nature. Instead, in this paper, we take the bitcoin prices as given and determine the others endogenously.

To answer the two research questions. We build a continuous-time dynamic model inspired by the classical Hotelling model for exhaustible resources (Hotelling, 1931). Note that both Fig. 1 and Fig. 2 are related to time series and cannot be addressed by a static model. Unlike the Hotelling model, in which the production rate is the only control variable, the production rate is predetermined by the Bitcoin system in the form of block rewards and cannot be controlled by

2
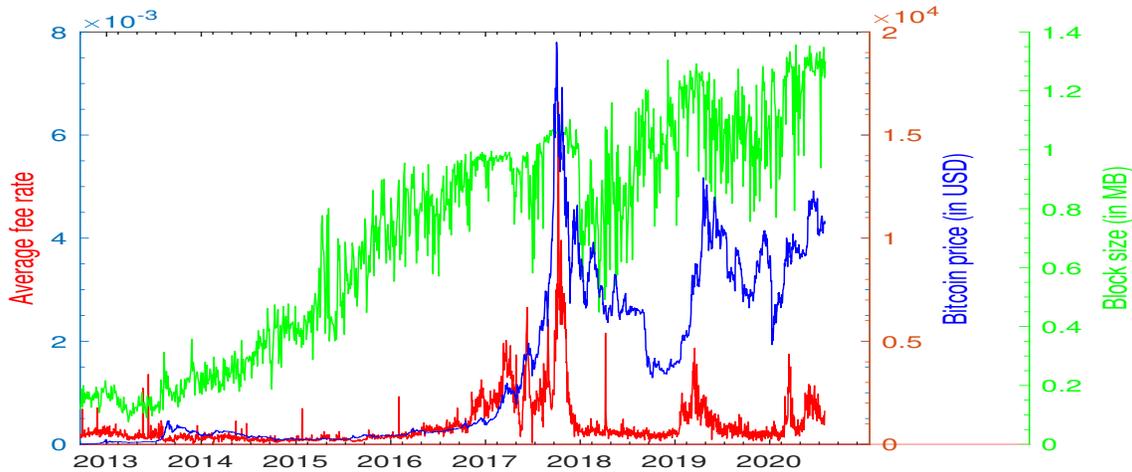
Figure 2: **The dynamics of average transaction fee rate and bitcoin price from Jan 2013 to Sept 2020**. The bitcoin price only shows the part below 10000 USD. Average transaction fee rate = $\frac{\text{Transaction fees (in bitcoin)}}{\text{Validated transaction volume (in bitcoin)}}$.

miners. Instead, here the miners' objective is to maximize the profit by controlling the selling rate of bitcoins. Furthermore, our model has to incorporate particular constraints and systematic state variables especially relevant to Bitcoin networks, such as transaction fees voluntarily attached by users, physical block capacity constraint, declining block rewards, and random demand shocks. In particular, our model incorporates the interaction between miners and users that is missing in traditional resource models: Bitcoin miners, to whom the system first distributes bitcoins as rewards, sell their holdings to users, while in turn, users pay miners a certain amount of bitcoins (i.e., voluntary transaction fees) upon transactions.

In terms of the first research question, our model with calibrated parameters suggests that it is optimal for miners to keep reducing their inventory in 2013-2015, as displayed in Fig. 1, regardless of the drastic fluctuation of bitcoin prices. Our model reveals three possible causes of this pattern. First, miners sell their bitcoins to make profits and sustain their mining service. Second, high jump risk is one of the major forces driving miners to sell their bitcoins at an early stage, even when bitcoin prices are relatively low. We also point out a reasonably high volatility cannot explain why miners kept selling their inventory in 2014-2015. Third, the transaction fee mechanism is another driving force for miners to liquidate their bitcoins: The less the miners' inventory is, the more the

3

bitcoins held by users, and thus the higher the transaction fees.

In terms of the second research question, our calibrated model can explain the observed pattern of the co-movements of the average transaction fee rate, block size, and bitcoin price documented in Fig. 2. The insight gained from the model is as follows. When Bitcoin demand is too low in the early stage to make the block capacity full, miners will process all transactions even for those without attaching any fees, mainly to get block rewards. As a result, the average fee rate tends to be low. When bitcoin price and Bitcoin demand are high, such that the volume of unconfirmed transactions reaches or exceeds the recommended block capacity, miners will process those transactions with higher fees to maximize their profit, which leads the average fee rate to increase drastically. This explains why the average transaction fee rate remained fairly flat in 2014-2016, during which the block size was strictly below the capacity limit but increased significantly in 2017 when the block capacity was almost full, and Bitcoin demand seemed intensive.

Our model has two other economic implications. First, we demonstrate the different roles of transaction fees and block rewards at different time stages. In the early stage, block rewards dominate the miners' value that decreases dramatically with declining block rewards. However, transaction fees will eventually prevail over block rewards and dominate the miners' value as time goes by, even well before the termination of block rewards. Second, the miners' optimal time to sale is characterized by a threshold policy, below which one never sells bitcoins. Because the threshold decreases with the inventory level and all bitcoins are first distributed to miners, miners with a higher inventory level tend to sell more bitcoins to users so as to receive more transaction fees in the future.

Our model is flexible enough to incorporate more practical features. For example, it is possible to extend our model to study an individual miner's optimal exit choice in the Bitcoin mining business; see Appendix D.

<div align="center">4</div>

1 Related Literature

There are several strands of literature relevant to our model. The first is about resource models, dated back to the celebrated paper by Hotelling (1931) and later extended along with many different directions; see, e.g., Stewart (1980), Levhari and Pindyck (1981), and Malueg and Solow (1990). Our work complements this literature by treating Bitcoin mining analogous to the extraction activity in natural resources. However, as mentioned earlier, our Bitcoin model differs from classic resource models primarily in two ways: (1) Instead of the production rate, the liquidation rate of the inventory is the control variable in our model, and the production rate is fixed by the system design. In contrast classic resource models do not involve inventory. (2) We have to incorporate Bitcoin networks' particular features, such as transaction fees, block capacity constraint, and block rewards, posing challenges to the modeling.

The second strand of literature is on transaction fees in Bitcoin payment. Easley, O'Hara, and Basu (2019) developed a Nash equilibrium model to investigate transaction fees' role and explain miners' and users' strategic behaviors. Huberman et al. (2017) used a congestion queuing game to examine how transaction fees and infrastructure levels are determined. They raised concerns about the sustainability of Bitcoin after the termination of block rewards. Our paper complements Easley, O'Hara, and Basu (2019) and Huberman et al. (2017) by modeling transaction fees from the miners' perspective. Both Easley, O'Hara, and Basu (2019) and Huberman et al. (2017) studied transaction fees with static models from the users' perspective, ignoring block rewards or assuming constant block rewards. Our model about transaction fees is dynamic. More importantly, we attempt to address two research questions related to dynamic observations in Figures 1 and 2. Our model works even if the block rewards are terminated, as then the transaction fees would become the only source of income for miners.

The third strand of literature related to our work studies the mining market. Prat and Walter (2018) used the real option theory to examine the Bitcoin miners' optimal entry policy. Cong, He, and Li (2018) studied the role of mining pools in Bitcoin and found that mining pools do not necessarily undermine the decentralization of Bitcoin's network. Alsabah and Capponi (2019)

studied the arms race among miners with respect to endogenous R&D investment and showed that higher investments in research translate into a more aggressive mining game. We complement this strand of literature by focusing on the supply side of Bitcoin mining, which was not addressed there.

Our paper is also loosely related to the literature on studying bitcoin as a currency. Athey et al. (2016) analyzed bitcoin's usage and its value as a currency. Bolt and Oordt (2016) treated Bitcoin as a medium of exchange and used the equation of quantity to analyze the virtual currency exchange rate. Recently, Schilling and Uhlig (2019) provided a model of an endowment economy for Bitcoin as a medium of exchange and found that its fundamental price is a martingale. Benigno, Schilling, and Uhlig (2019) studied competition between cryptocurrency and national currencies with a two-country economy model. In line with this literature, our model uses the quantity equation of exchange to link the bitcoin price to demand shock.

2   Model Setup

In this section, we develop a continuous-time model to study Bitcoin mining, inspired by the classic exhaustible resource model in Hotelling (1931). We regard all Bitcoin miners as a whole, i.e., the representative miner.[3] The miner chooses a dynamic liquidation rate of bitcoin $\{Q_t\}_{t\geq 0}$ to maximize the expectation of her discounted accumulative profit

$$\int_0^\infty e^{-\beta t}\Big(P_t Q_t - C(Q_t, H_t)\Big)dt, \tag{1}$$

where $\beta > 0$ is a given discount rate, P_t is the bitcoin price at time t, $P_t Q_t$ represents the revenue flow, and $C(Q_t, H_t)$ is the cost function depending on the selling rate Q_t and the miner's inventory level H_t. Next we will specify the price P_t, cost function $C(\cdot, \cdot)$, the dynamics of the inventory level H_t (that depends on the selling rate, Bitcoin reward rate, and transaction fees), and, more importantly, the system constraints on the state and control variables. Note that in the classic

---

[3]In Appendix C, we shall present the optimal selling strategy for an individual miner instead of one representative miner. It is shown that an individual miner's selling strategy is insensitive to her inventory and successful mining probability. Therefore, we may consider an economy with one representative miner.

Hotelling model the control variable is the production rate, while here the control variable is the liquidation rate. Furthermore, we have to impose system specific constraints tailored to the Bitcoin network.

2.1 Bitcoin price and demand

Since we focus on the supply side of Bitcoin mining, we take the demand side and the bitcoin prices essentially as exogenously given, as the determination of the bitcoin price alone is quite challenging itself. In other words, the representative miner essentially takes the demand as given to choose the optimal action in the supply side. However, it should be pointed out that in our model there is an important feedback from the supply side to the demand side, as (9) specifies the impact of the optimal inventory holding on the overall transaction volume on the demand side.

Let X_t be the demand factor and $S_t := \int_0^t b_u du$ be the cumulative supply at time t, where b_u is the block reward rate. We assume that Bitcoin price is determined by the following quantity equation of the medium of exchange (Bolt and Oordt, 2016; Fisher (1911); Friedman (1973)):

$$P_t = \theta_p \frac{X_t}{S_t^{1+\gamma}} \quad \text{for } t \geq 0, \tag{2}$$

where parameter $\gamma \geq 0$ is the elasticity of bitcoin velocity to supply, and parameter $\theta_p > 0$ is determined by the Bitcoin velocity and dollar-value trading volume for one unit of demand. This equation (2) can be derived from the model in Bolt and Oordt (2016).[4] A simple interpretation of equation (2) comes from the basic economic principle that price is determined by demand X and supply S.

---

[4]According to equation (3.3) in Bolt and Oordt (2016), the bitcoin price in USD P_t satisfies $P_t = \frac{\mathcal{T}_t}{S_t \mathcal{V}_t}$, where $\mathcal{T}_t$ is the dollar-value trading volume in goods and services with payments settled in bitcoin at time t, $\mathcal{V}_t$ is the bitcoin velocity, defined as the average number of times each unit of bitcoin is used to purchase real goods and services at time t. For simplicity, we assume $\mathcal{T}_t$ is linearly dependent on the demand level, i.e. $\mathcal{T}_t = \theta_1 X_t$, where θ_1 represents the dollar-value trading volume for one unit of demand level. In addition, we assume that the velocity is positively related to the cumulative supply of bitcoin S_t, i.e., $\mathcal{V}_t = \theta_2 S_t^\gamma, \gamma \geq 0$. Letting $\theta_p = \theta_1/\theta_2$ yields (2).

We assume that X_t has the following dynamics

$$dX_t = \mu(X_t)dt + \sigma(X_t, i_t)dW_t - X_{t-}d\left(\sum_{i=1}^{N_t}(1 - Z_i)\right), \qquad (3)$$

where W_t is a standard Brownian motion, N_t is a Poisson process with intensity λ_J, $\mu(\cdot)$ and $\sigma(\cdot, \cdot) \geq 0$ stand for the adoption term and volatility term, respectively, $1 - Z \in (0, 1)$ refers to the proportional downward-jump size,[5] and $i_t \in \{\mathbb{H}, \mathbb{L}\}$ represent two market states that correspond to high-active and low-active markets,[6] respectively, with transition intensities $\zeta = (\zeta_{\mathbb{H}}, \zeta_{\mathbb{L}})$. Borrowing the idea from marketing science, we use the stochastic Gompertz model[7] to characterize Bitcoin's adoption. Therefore, for a given market state $i \in \{\mathbb{H}, \mathbb{L}\}$, the functions $\mu(\cdot)$ and $\sigma(\cdot, i)$ take the following forms, respectively:

$$\mu(x) = \kappa(\nu - \ln x)x, \quad \sigma(x, i) = \sigma_i x, \qquad (4)$$

where ν is called the log carrying capacity, standing for the stationary mean of the logarithm of demand factor, κ is known as the adoption speed, measuring mean-reverting speed, and $\sigma_i > 0$ is the volatility at regime $i \in \{\mathbb{H}, \mathbb{L}\}$.

2.2 The miner's inventory

The representative miner's inventory level H_t evolves according to

$$dH_t = (b_t + I_t)dt - Q_t dt, \qquad (5)$$

---

[5]In general, $Z \in (0, 1)$ could be a random variable. Here we assume constant jump size for simplicity. As pointed out in Weil (1987), non-government backed money, like bitcoin, is subject to downward-jump risk.

[6]We will use daily mempool transaction count to identify market states; see Fig. 4.

[7]See, e.g., Dixon, 1980; Bass, 1969; Mahajan, Muller, and Bass, 1990; Bass, 2004

where b_t represents the block reward rate, $Q_t \geq 0$ is the miner's selling rate, and I_t represents transaction fees in a unit period[8]. Equation (5) indicates that the miner will receive rewards with the amount of $(b_t + I_t)dt$ at any period $[t, t + dt]$, and meanwhile, the miner sells bitcoins at a controllable rate $Q_t \geq 0$. We will specify how the transaction fee I_t is determined endogenously in Section 2.4.

Since block rewards are predetermined and halve every four years, the reward rate b_t is a deterministic and decreasing function of time t. Moreover, $b_t \equiv 0$ for all $t \geq T$, where T is a predetermined time around the year 2140. Henceforce, the cases before and after the termination of block rewards are called the short-run case and the long-run case, respectively.

2.3 The miner's cost

The miner's cost consists of two parts, mining cost and liquidation cost. The mining cost is mainly from the expense of electricity, which is assumed to be a constant C_m, consistent with Easley, O'Hara, and Basu (2019) and Cong, He, and Li (2018). The liquidation cost includes losses due to price drop and losses of marginal utility upon sale. Parsimoniously, as in the investment literature for adjustment cost or execution cost (see, e.g., Hayashi, 1982; Graewe and Horst, 2017), the liquidation cost is assumed to be convex in the selling rate and decrease in the miner's inventory level. For analytical tractability, we adopt the following form for the total cost: $C_m + C(Q_t, H_t)$, where the liquidation cost

$$C(Q_t, H_t) = \psi P_t Q_t^2 / H_t \tag{6}$$

with a constant parameter ψ. Since we do not impose budget constraint for simplicity, the constant mining cost C_m does not affect the miner's control decision. Therefore, we might as well take $C_m = 0$.

Note that the liquidation cost $C(Q, H)$ is related to the inventory level because Bitcoin can be

---

[8]We assume that the miner is not allowed to purchase bitcoins. The transaction fees in Equation (5) come from verifying and confirming users' transactions, excluding those from the miner's own transactions because (i) only transaction fees from users could increase the miner's inventory, and (ii) the transaction fees from the miner's own transactions are usually tiny compared with transaction fees from users and the miner's selling amount.

viewed as a digital art product with scarcity: the lower the inventory, the higher the liquidation cost could be, as the miner would be less willing to sell her holding. Particularly, when the miner's inventory goes to zero, i.e., $H = 0$, the marginal utility loss tends to infinity. It is also worthwhile pointing out that the cost function is homogeneous[9] of degree one in Q and H, i.e., $C(\delta Q, \delta H) = \delta C(Q, H)$ for $\delta > 0$.

2.4   Endogenous transaction fees

The representative miner's income has two parts, the block rewards determined exogenously by the Bitcoin system, and transaction fees attached to the transactions waiting to be confirmed by the miner. We shall find transaction fees endogenously by solving an optimization problem faced by the miner: Due to capacity constraints, the miner prefers to mine the transactions with higher attached fees to maximize the income.[10]

There is a capacity constraint when mining transactions, i.e. only a fixed number of orders in a unit period can be processed.[11] As such, we denote the system's capacity for the block size to be G.

We assume that for any volume of unconfirmed transaction orders,[12] their attached fee rates share the same distribution with the density function $f(\cdot)$ over the interval $[0, \bar{\phi}]$, where $\bar{\phi}$ is the upper bound of the fee rate determined exogenously by the competition with other payment methods.

We postulate that the volume (in bitcoin) of unconfirmed transaction orders, denoted by L, takes

---

[9]Thanks to the homogeneirty, we can simplify model calibration when extending the model to the case of identical individual miners, also thanks to the fact the individual miners' liquidation strategies are insensitive to their inventory (see Appendix C).

[10]At the beginning of each round of mining, a miner will construct a candidate block by selecting the unconfirmed transactions stored in her node. Miners sort the unconfirmed transactions with respect to the magnitude of the attached fees in mempools and send them into a candidate block as much as possible until the candidate block's capacity is reached.

[11]In the Bitcoin system, each block has limited capacity (i.e., 1MB), which can accommodate about 4000 transaction orders. Since every ten minutes, only one block can be successfully validated and attached to the blockchain, there is a fixed number of orders that can be processed within a unit period.

[12]Here, the transaction orders refer to those submitted by users, as only users' transactions can contribute to the miner's income to increase her inventory.

the following particular form:

$$L(X_t, H_t, i_t; S_t) = \theta_{i_t} [1 - H_t/S_t] S_t^{(1-\alpha)\gamma_s} X_t^\alpha, \quad i_t \in \{\mathbb{H}, \mathbb{L}\}, \tag{7}$$

where S_t is the cumulative supply of Bitcoin, X_t is the demand shock, $\theta_{i_t} > 0$ is a parameter depending on market state i_t, and constants $\alpha \in [0, 1]$ and $\gamma_s > 0$ measure the dependence degree on S_t and X_t.

The function form in Equation (7) captures three important features of the unconfirmed transaction volume: (i) It associates with Bitcoin adoption, which is positively related to S_t. (ii) It depends on demand shock X_t. (iii) A miner does not charge fees for her own transactions. The term[13] $1 - H_t/S_t$ reflects the fact that the higher the miner's bitcoin holding, the lower the unconfirmed transactions.

Note that under (7), the miner's inventory holding H can affect L, which captures a vital feedback from the miner to users in our model of Bitcoin mining. More precisely, the representative miner's liquidating strategy could affect the future income from transaction fees from users.

To maximize the income, during a unit period, the miner chooses unconfirmed transactions with higher fees as much as possible, subject to the capacity constraint. This leads to the following optimization problem for transaction fees I:

$$I = \max_{\phi \in [0, \bar{\phi}]} K(\phi)L \quad \text{subject to} \quad k(\phi)L \le G, \tag{8}$$

where $k(\phi)L$ stands for the volume of selected transactions, G is the system capacity of block size, and

$$k(\phi) = \int_\phi^{\bar{\phi}} f(s)ds \quad \text{and} \quad K(\phi) = \int_\phi^{\bar{\phi}} f(s)s\,ds \tag{9}$$

represent respectively the proportion and fees of selected transactions in one unit volume of unconfirmed transactions.

---

[13]Note that $H_t \le S_t$ for any t.

11
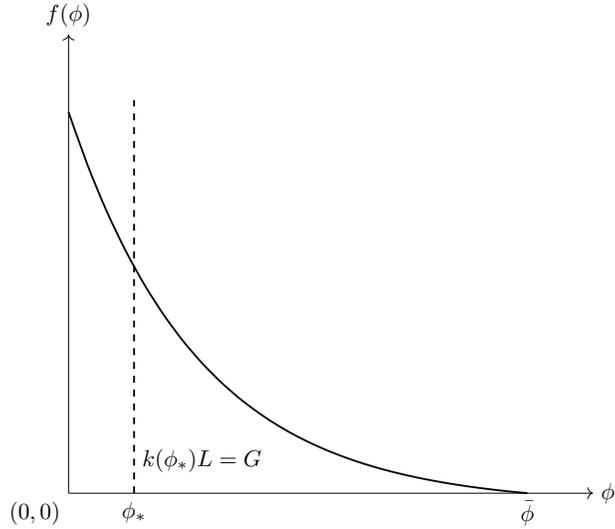
Figure 3: **Distribution of Bitcoin transaction fees and the threshold fee rate** .

The resulting optimal choice of the threshold fee rate, as a function of L, is given by

$$
\phi^*(L) = \begin{cases} F^{-1}(1 - \frac{G}{L}), & \text{if } L > G, \\ 0 & \text{if } L \leq G, \end{cases} \tag{10}
$$

where $F(\cdot)$ is the cumulative distribution function of $f(\cdot)$, $F^{-1}(\cdot)$ stands for the inverse function of $F(\cdot)$; see Fig. 3 for illustration. Therefore, the transaction fees paid to the miner are

$$
I = K(\phi^*(L))L. \tag{11}
$$

The average transaction fee rate that measures the ratio of transaction fees to the validated transaction volume in bitcoin is given as follows:

$$
r = \frac{I}{k(\phi^*)L} = \frac{K(\phi^*)}{k(\phi^*)}. \tag{12}
$$

It is worthwhile pointing out that the above formulation is consistent with the first-price auction problem studied in Basu, Easley, O'Hara, and Sirer (2018), and the miner's optimal fee collection policy is associated with a symmetric Bayes-Nash equilibrium in that paper.

12

In our numerical study, we will choose a Beta distribution for F, with a density

$$f(y) = \frac{\bar{\phi}^{1-a_1-a_2} y^{a_1-1} (\bar{\phi} - y)^{a_2-1}}{B(a_1, a_2)}, \tag{13}$$

where $B(a_1, a_2) = \int_0^1 u^{a_1-1}(1-u)^{a_2-1} du$ is the Beta function, and a_1 and a_2 are constants to be calibrated with market data.

2.5 Miner's optimization problem

In summary, the mining problem is to choose an admissible control strategy $\{Q_t\}_{t \geq 0} \in \mathcal{A}_t$ to maximize the expected present profit (1), namely

$$V_i(t, x, h) = \sup_{\{Q_u\}_{u \geq t} \in \mathcal{A}_t} \mathbb{E}_t \left[\int_t^\infty e^{-\beta(u-t)} \left(P_u Q_u - C(Q_u, H_u) \right) du \right], \tag{14}$$

subject to state dynamics and constraints (2)–(6), and endogenous transaction fees in (11) with the volume of transaction orders in (7) and the function ϕ^* in (10). Here $\mathbb{E}_t$ denotes the expectation conditional on the information up to time t, and $\mathcal{A}_t$ represents the set of admissible strategies starting from $(t, i_t, X_t, H_t) = (t, i, x, h) \in (0, \infty) \times \{\mathbb{H}, \mathbb{L}\} \times (0, \infty) \times [0, S_t]$; a strategy $\{Q_t\}_{t \geq 0}$ is admissible if, for any $t > 0$, $Q_t \geq 0$ is adapted to information filtration up to time t.

3 Theoretical Analysis

3.1 HJB equation and optimal strategy

By the dynamic programming principle, the value function $V_i(t, x, h)$ satisfies the following Hamilton-Jacobi-Bellman (HJB) equation,[14]

$$\frac{\partial V_i}{\partial t} + \mathcal{L} V_i + \max_{q \geq 0} \left\{ \left[\left(b_t + K(\phi^*(L)) L \right) - q \right] \frac{\partial V_i}{\partial h} + Pq - C(q, h) \right\} + \mathcal{J} V_i = \beta V_i \tag{15}$$

---

[14]A verification theorem that the solution of HJB equation (15) equals the value function (14) can be rigorously proved following standard procedures in stochastic control literature, i.e., Cuoco and Liu (2000).

13

for $(x, h) \in (0, \infty) \times [0, S_t]$ and $i \in \{\mathbb{H}, \mathbb{L}\}$, where $P = \theta_p x / S_t^{1+\gamma}$, $L = L(x, h, i; S_t)$ is as given by (7), $K(\cdot)$ and $\phi^*(\cdot)$ are as given in (9) and (10), respectively, and differential operators $\mathcal{L}$ and $\mathcal{J}$ are defined respectively by

$$\mathcal{L}V_i = \frac{1}{2}\sigma^2(x, i)\frac{\partial^2 V_i}{\partial x^2} + \mu(x, i)\frac{\partial V_i}{\partial x}, \tag{16}$$

$$\mathcal{J}V_i = \lambda_J\Big[V_i(t, Zx, h) - V_i(t, x, h)\Big] + \zeta_i\Big[V_\iota(t, x, h) - V_i(t, x, h)\Big] \tag{17}$$

with $\iota \in \{\mathbb{H}, \mathbb{L}\}$ and $\iota \neq i$.

Note that after the termination of block rewards (i.e., in the long-run case $t \geq T$), we have $b_t \equiv 0$ and $S_t \equiv \bar{S} \equiv \int_0^T b_u du$, where $\bar{S}$ represents bitcoin's total available supply and will be scaled to one in our computation.[15] As such, the corresponding value function is independent of time t, i.e., $V_i(t, x, h) = V_i(T, x, h) =: V_i^T(x, h)$ for $t \geq T$, and the corresponding HJB equation (15) reduces to

$$\mathcal{L}V_i^T + \max_{q \geq 0}\left\{\Big(K(\phi^*(L))L - q\Big)\frac{\partial V_i^T}{\partial h} + Pq - C(q, h)\right\} + \mathcal{J}V_i^T = \beta V_i^T \tag{18}$$

for $(x, h) \in (0, \infty) \times [0, S_t]$ and $i \in \{\mathbb{H}, \mathbb{L}\}$, where $L = L(X, H, i; \bar{S})$.

Optimal strategy

Denote by q_i^* the optimal selling rate at state i. If $q_i^* > 0$, then by the HJB equation and the first order condition, we have

$$P = \frac{\partial V_i}{\partial h} + \frac{\partial C}{\partial q} = \frac{\partial V_i}{\partial h} + \frac{2\psi P}{h}q_i^*,$$

which indicates that the optimal (positive) selling rate is chosen such that the marginal value of holding plus marginal liquidation cost must be equal to the bitcoin price. We then obtain the optimal selling rate q_i^* as follows:

$$q_i^* = \frac{h}{2\psi P}\Big(P - \frac{\partial V_i}{\partial h}\Big)^+, \tag{19}$$

---

[15]The true value of $\bar{S}$ is around 21 million.

14

which implies that selling is optimal if and only if the bitcoin price is strictly greater than the marginal value of holding. Therefore, for a given state $i \in \{\mathbb{H}, \mathbb{L}\}$, we can define the i-Selling region and i-Holding region, respectively, as follows:

$$
\begin{aligned}
i\text{-Selling Region} &= \{(t, x, h) \mid q_i^* > 0\} = \left\{(t, x, h) \,\Big|\, P > \frac{\partial V_i(t, x, h)}{\partial h}\right\}, \\
i\text{-Holding Region} &= \{(t, x, h) \mid q_i^* = 0\} = \left\{(t, x, h) \,\Big|\, P \le \frac{\partial V_i(t, x, h)}{\partial h}\right\}.
\end{aligned}
$$

Numerical algorithm

The HJB equations (15) and (18) do not allow analytical solutions. So, we have to resort to numerical solutions. We employ the finite difference method to numerically solve the HJB equations. We first solve the stationary problem (18), then solve the time-dependent problem (15) backward with the stationary solution as the terminal condition. The detailed algorithm is as given below:

1. Use the finite difference method to solve (18) for $V_i^T(x, h)$, $i \in \{\mathbb{H}, \mathbb{L}\}$.

2. Set the terminal condition $V_i(T, x, h) = V_i^T(x, h)$, $i \in \{\mathbb{H}, \mathbb{L}\}$.

3. Use the finite difference method to solve (15) for $V_i(t, x, h)$, $i \in \{\mathbb{H}, \mathbb{L}\}$ for $t < T$, with the above terminal condition.

Once the value functions V_i are obtained, we can use Equation (19) to find the optimal selling strategy.

3.2 Average transaction fee rate

Proposition 1. *Consider the miner's average transaction fee rate r, as defined in (12).*

(i) If $L \le G$, then $\phi^* = 0$ and $r = K(0)/k(0)$.

(ii) If $L > G$, then ϕ^* and r are strictly increasing with X (or L). In particular, we have

$$
\lim_{X \to \infty} \phi^* = \lim_{X \to \infty} r = \bar{\phi}.
$$

15

Part (i) of Proposition 1 indicates that when the unconfirmed transactions are not enough to fill the miner's capacity, i.e., $L \leq G$, the miner will set $\phi^* = 0$ to take all of the unconfirmed transactions, including those without transaction fees, and the corresponding average transaction fee rate becomes constant according to (12). Since a lower demand leads to a lower volume of unconfirmed transactions, part (i) suggests that the average transaction fee rate can be flat when the Bitcoin demand is sufficiently low. This is consistent with the market observation that in the period of low transaction demand (e.g., the period of 2013-2016, as shown in Fig. 2), the transactions without attaching any fees could be processed, and the individual average fee rate remained constant.

Part (ii) of Proposition 1 suggests that when the number of unconfirmed transactions exceeds the capacity, both the threshold fee rate and individual average fee rate could increase dramatically. This also coincides with the fact that in the period of high transaction demand (e.g., the year 2017, as shown in Fig. 2), users need to pay quite a high fee to ensure their transactions to be processed.

4 Model Calibration

4.1 Data and parameter choices

Denote by r_t^A and H_t^A the average transaction fee rate and aggregate inventory for all miners at time t, respectively. We will use the following available data in the Bitcoin system to calibrate our model:

- Monthly bitcoin price $\{P_t; t = 1, \cdots, T_1\}$ from Jan 2013 to Sep 2020 (see Fig. 2);

- Monthly average transaction fee rate $\{r_t^A; t = 1, \cdots, T_1\}$ from Jan 2013 to Sep 2020 (see Fig. 2);

- Monthly average block size in megabytes $\{\Lambda_t^A; t = 1, \cdots, T_1\}$ from Jan 2013 to Sep 2020.

- Monthly aggregate inventory $\{H_t^A; t = 1, \cdots, T_2\}$ from Jan 2013 to Dec 2015 (see Fig. 1); [16]

---

[16]According to Athey et al. (2016), as more and more miners use mixing strategy to conceal their transactions since 2014, it is difficult to reveal miners' bitcoin holdings by tracking their addresses.

- Daily mempool transaction count in Bitcoin from Apr 2016 to Sep 2020 (see Fig. 4).

Here $t = 1$, $T_1 = 72$, and $T_2 = 36$ correspond to Jan 2013, Sep 2020, and Dec 2015, respectively. It is worthwhile pointing out that the monthly aggregate inventory data, which is not directly observable, is obtained by Athey et al. (2016) and available only from Jan 2013 to Dec 2015.

The bitcoin price P_t is informative to the set of parameters $\Theta_1 = \{\kappa, \nu, \sigma_{\mathbb{H}}, \sigma_{\mathbb{L}}\}$ in (3), while the average fee rate r_t^A, average block size Λ_t^A, and aggregate inventory H_t^A are informative to the set of parameters $\Theta_2 = \{\lambda, \theta_{\mathbb{H}}, \theta_{\mathbb{L}}, \alpha, \gamma_s\}$. Calibrating the parameters in Θ_2 will be elaborated on in Section 4.2.

Our model assumes two regimes in bitcoin transaction: high-active regime and low-active regime. In the high-active regime, the transaction is very active, implying a large number of orders submitted by users and high volatility in bitcoin price. In the low-active regime, the transaction of bitcoin is relatively less active, implying a small number of users' orders and low volatility in bitcoin price. Using the time series of the mempool transaction count,[17] as shown in Fig. 4, we can quickly identify two regimes. Indeed, one can observe that from the end of 2016 to the beginning of 2018, the moving average of the mempool transaction count is much higher than that in the rest periods. Then, we roughly divide the period of 2013 to 2020 into three parts:

- low-active regime from 2013 to 2016 Q3,

- high-active regime from 2016 Q4 to 2017 Q4, and

- low-active regime from 2018 Q1 to 2020 Q3.

Next, we set values for some parameters. We take the discount factor $\beta = 6\%$ that is commonly used in many empirical studies. We normalize the number of bitcoin to be one, i.e., $\bar{S} = 1$. The corresponding block rewards function becomes $b_t = \frac{1}{2^{[t/4]+3}}$ as the block rewards halve every four years. For computational simplicity, we assume that the Bitcoin block rewards will terminate in

---

[17]Mempool is the set of all unconfirmed transactions from users in the Bitcoin network The mempool transaction count refers to the total number of unconfirmed transactions in the mempool, The mempool transaction count data, available at www.blockchain.com, is a good proxy for the number of unconfirmed transactions and is employed to detect the high-active and low-active regimes. A high (low) mempool transaction count suggests a large (small) number of unconfirmed transactions.
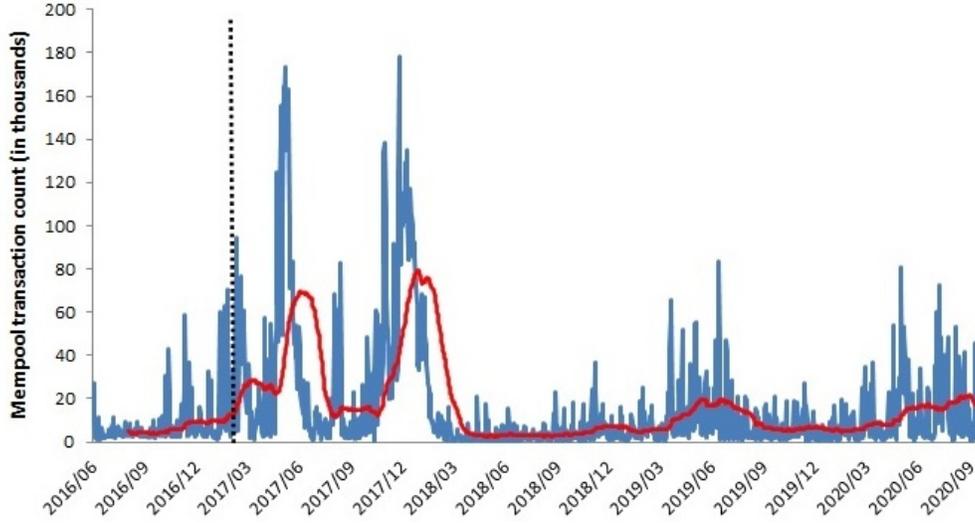
Figure 4: **The high-active and low-active markets suggested by daily mempool transaction count (in thousand) from 2016 to 2020. The red line represents the 60-day moving average.**

2050, after which block rewards will be tiny and can then be neglected. The capacity of blocks per unit of time is chosen as $G = 10$. In fact, the average volume per transaction order since 2016 is around 1.05 bitcoin. Note that each block can accommodate about 4000 transaction orders. This suggests that the capacity of number of orders that the Bitcoin system can process in a year is $4000 \times 6 \times 24 \times 365 = 210,240,000$. Then the normalized capacity per year is $G = 1.05 \times 210,240,000/21,000,000 \approx 10$, where $21,000,000$ is the total actual number of bitcoin. We set $\theta_p = 100$, which implies that one unit change of the demand could lead to a change of 100 billion USD in the bitcoin price. In fact, θ_p plays a role in scaling the demand factor X, so the value of θ_p does not affect our findings. We will choose $\gamma = 0$, as Athey et al. (2016) show that the bitcoin velocity is approximately constant. For the parameters in the Beta distribution in (3.4), we set $(a_1, a_2) = (0.1, 99.9)$ and $\bar{\phi} = 10\%$, which can capture the effect that the average fee rate could increase dozens of times as the bitcoin price changes (see Fig. 2).

We set the transition intensities $\zeta_{\mathbb{H}} = 0.8$ and $\zeta_{\mathbb{L}} = 0.3$, which implies an average duration of 1.25 years for the high-active regime and of 3.33 years for the low-active regime. The durations are consistent with what we observe from the dynamics of the mempool transaction count. Furthermore, we adopt the jump parameters $\lambda_J = 57$ and $Z = 0.9$ estimated by Gronwald (2015), which implies

18

a rough 10% downward jump once a week.

We now use the bitcoin price to estimate the parameters $\Theta_1 = \{\kappa, \nu, \sigma_\mathbb{H}, \sigma_\mathbb{L}\}$ for the Gompertz diffusion model of demand shock (i.e., Gutierrez et al., 2004). Based on the characterization of high-active and low-active regimes from 2016 to 2020, we estimate the annualized volatility for both high-active and low-active regimes and obtain $\sigma_\mathbb{H} = 0.7910$ and $\sigma_\mathbb{L} = 0.6225$, which suggests that the demand shock in the high-active regime is more volatile than in the low-active regime. Using the historical bitcoin prices and (2), we obtain the estimated values of Bitcoin's adoption speed and the log carrying capacity, i.e., $\kappa = 1.2397$ and $\nu = 0.6527$.

4.2 Calibration method for $\Theta_2 = \{\psi, \theta_\mathbb{H}, \theta_\mathbb{L}, \alpha, \gamma_s\}$

It remains to estimate the parameters $\Theta_2 = \{\psi, \theta_\mathbb{H}, \theta_\mathbb{L}, \alpha, \gamma_s\}$ by matching model outputs with the observed data. We will calibrate Θ_2 using the market data $\{(r_t^A, H_t^A), \ t = 1, 2, \cdots\}$ as well as the observed bitcoin prices.

With the observed bitcoin prices, we can recover the demand shock path over time $\{\widetilde{X}_t; t = 1, \cdots, T_1\}$ through Equation (2). Let $\{\iota_t; t = 1, \cdots, T_1\}$ be the observed market states as given by Fig. 4. Given the observed inventory level $\widetilde{H}_t$ and demand level $\widetilde{X}_t$ at time t, we have

$$\widetilde{L}_t \ = \ L(\widetilde{H}_t, \widetilde{X}_t, \iota_t; S_t), \tag{20}$$

$$\widetilde{\phi}_t \ = \ \phi^*(\widetilde{L}_t), \tag{21}$$

$$\widetilde{q}_t \ = \ q_{\iota_t}^*(t, \widetilde{X}_t, \widetilde{H}_t; \Theta_2), \tag{22}$$

where $L(\cdot, \cdot, \cdot; S_t)$ and $\phi^*(\cdot)$ are as given in (7) and (10), respectively, and $q_i^*(\cdot, \cdot, \cdot; \Theta_2), i \in \{\mathbb{H}, \mathbb{L}\}$ is the optimal selling rate given in (19) with a given set of parameters Θ_2 and can be obtained by numerically solving the HJB equation. We then obtain the following average fee rate $\{\widetilde{r}_t, t = 1, \cdots, T_1\}$, average block size $\{\widetilde{\Lambda}_t, t = 1, \cdots, T_1\}$, and inventory $\{\widetilde{H}_t, t = 2, \cdots, T_1\}$ implied by

19

the model:

$$\widetilde{r}_t(\Theta_2) = \frac{K(\widetilde{\phi}_t)}{k(\widetilde{\phi}_t)}, \tag{23}$$

$$\widetilde{\Lambda}_t(\Theta_2) = \widetilde{L}_t/G 1_{\{\widetilde{L}_t < G\}} + 1_{\{\widetilde{L}_t \geq G\}} \tag{24}$$

$$\widetilde{H}_{t+1}(\Theta_2) = \widetilde{H}_t + [b_t + \widetilde{I}_t(\Theta_2)]\delta t - \widetilde{q}_t \delta t, \tag{25}$$

where $\delta t = 1/12$ year as we use monthly data. The dependence of $\widetilde{H}$ on Θ_2 is apparent. We point out that $\widetilde{r}$ also depend on Θ_2 as they implicitly depend on $\widetilde{H}$ through $\widetilde{L}$.

Then we can estimate parameter set Θ_2 by minimizing the weighted least square relative error between model output and observed data:

$$\min_{\Theta_2} \frac{1}{T_1} \sum_{t=1}^{T_1} \left\{ \frac{1}{(r_t^A)^2} (r_t^A - \widetilde{r}_t(\Theta_2))^2 + \frac{1}{(\Lambda_t^A)^2} (\Lambda_t^A - \widetilde{\Lambda}_t(\Theta_2))^2 \right\} + \frac{1}{T_2} \sum_{t=2}^{T_2} \left\{ \frac{1}{(H_t^A)^2} (H_t^A - \widetilde{H}_t(\Theta_2))^2 \right\}.$$

We use the simulated annealing algorithm (Eglese, 1990), which is good at minimizing a function with many local minima, to find the minimum of our objective function.

4.3 Calibration results

The estimated values of Θ_2, together with other parameter values, are summarized in Table 1. As one can see, $\psi = 0.39$, indicating that there is a high cost from liquidation for miners. Such liquidation cost could be higher for a smaller amount of holding, implying that people may view Bitcoin as a kind of digital art with inevitable scarcity and miners may prefer to holding at least a small amount of bitcoins rather than selling all of them. On the other hand, the sensitivity of volume to demand in the high-active regime is $\theta_{\mathbb{H}} = 346.5$, which is much higher than $\theta_{\mathbb{L}} = 62.3$ in the low-active regime. This is consistent with the data that the mempool transaction count in the high-active regime is six times of that in the low-active regime.

In Fig. 5, we plot the model-implied miners' inventory in proportion to the supplied bitcoin (i.e., proportional inventory). One can see that the model-implied proportional inventory (the solid

Table 1: Summary of parameters.

Parameters	Symbol	Value
Discount rate	β	6%
Total supply of bitcoin	$\bar{S}$	1
Capacity of blocks per unit of time	G	10
Hash rate per miner (TH/s)	ω	5.2
Coefficient in quantity equation (Billion USD per unit)	θ_p	100
Elasticity of bitcoin velocity to supply	γ	0
Upper bound of fee rate	$\bar{\phi}$	10%
Beta distribution parameters	(a_1, a_2)	(0.1, 99.9)
Adoption speed of Bitcoin	κ	1.2379
Log carrying capacity	ν	0.6527
Volatility of demand shock in high-active regime	$\sigma_{\mathbb{H}}$	0.7910
Volatility of demand shock in low-active regime	$\sigma_{\mathbb{L}}$	0.6225
State transition intensity	$(\zeta_{\mathbb{H}}, \zeta_{\mathbb{L}})$	(0.8, 0.3)
Jump parameters	(λ_J, Z)	(57, 0.9)
Parameter in liquidation cost	ψ	0.39
Sensitivity of volume to demand in high-active regime	$\theta_{\mathbb{H}}$	346.5
Sensitivity of volume to demand in low-active regime	$\theta_{\mathbb{L}}$	62.3
Shape parameters in L	(α, γ_s)	(0.6, 8)

line) matches the observed one (the dashed line) well from 2013 to 2015. As shown by the dotted line in the figure, the bitcoin price experienced a drastic increase and a gradual decline during this period. This suggests that our model can capture the pattern that miners kept reducing their bitcoin holdings regardless of bitcoin price's drastic fluctuation. The pattern may be attributed to three reasons. First, miners reduce their inventory to make profits and sustain their mining service. Second, as will be shown in Section 5, we find that high jump risk is one of the major forces driving miners to sell their bitcoin holdings at an early stage even when bitcoin prices are relatively low or very volatile (see Fig. 8). Third, we find that transaction fees are another driving force for miners to reduce their inventory. The intuition is quite simple. As users attach transaction fees, the users' bitcoin holding significantly affects the magnitude of transaction fees: the less the miners' inventory, the larger the users' bitcoin holding, and thus the higher the transaction fees (see also Fig. 10). Moreover, as transaction fees will be the miners' unique income source in the long-run, miners have a strong incentive to reduce their inventory in order to make their mining business

21

sustainable.
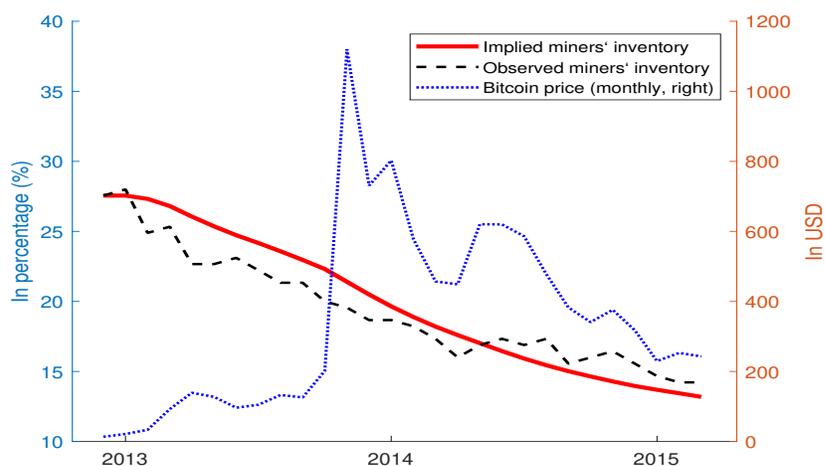
Figure 5: **Implied miner's proportional inventory from 2013 to 2015**. The dashed black line shows the observed miners' proportional inventory based on the estimation from Athey et al. (2016).

In panel A of Fig. 6, we plot the model-implied average fee rate (solid line), which captures the features of the observed data (dashed line): 1) From 2014 to middle 2016, the average fee rate was almost flat; 2) From late 2016 to 2018, the average fee rate rose dramatically. As shown in the panel B of Fig. 6, the model-implied block size (solid line) well matches the observed data (dashed line): 1) In the period 2013-2016, the block size was increasing but lower than 1MB, the block capacity. 2) Since 2017, the blocks were almost full.[18]

Combined with Fig. 6 and Proposition 1, our model can explain the co-movement of the block size and the average fee rate. When Bitcoin demand is low (e.g., 2014-2016), blocks are not full and the miners process all unconfirmed transactions. Then the average fee rate tends to be flat. When the demand is so high (e.g., after 2017) that the volume of unconfirmed transactions significantly exceeds the block capacity, miners should prioritize the validation of unconfirmed transactions with higher fees. Thus, blocks could be almost full and the average fee rate may increase dramatically.[19]

---

[18]Before 2019, the largest capacity for a block was 1MB. Since 2019, the block capacity increased slightly as a new process SegWit was introduced in Bitcoin system; see https://en.wikipedia.org/wiki/SegWit.

[19]There are some slight mismatches between model-implied results and observed data. They may be partially due to the irrational behaviors in Bitcoin mining in an early period (e.g., 2013) and imperfect identification of regimes in Bitcoin transactions.

22
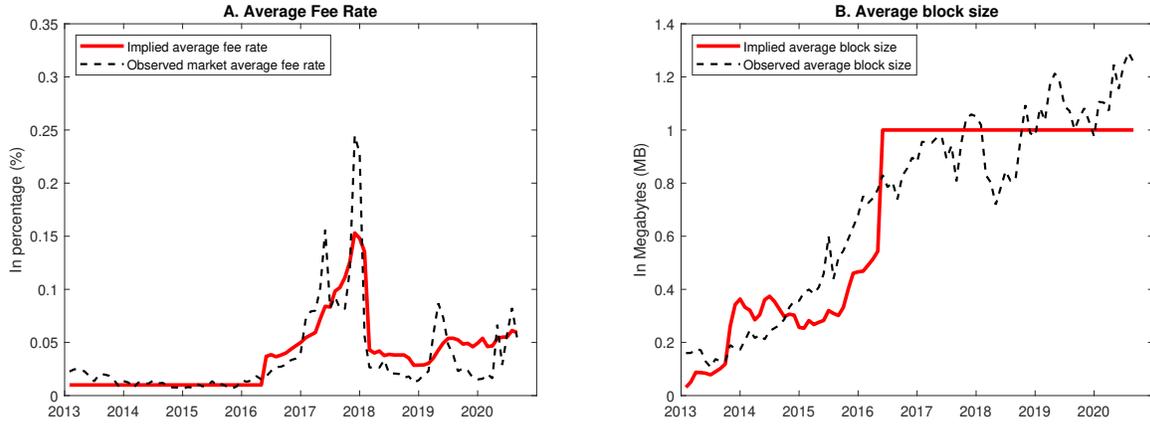
Figure 6: **Implied average fee rate and implied average block size from 2013 to 2020**. The dashed line in panel A represents the monthly observed average fee rate. The dashed line in panel B represents the monthly observed average block size.

5 Quantitative Analysis

We shall conduct an quantitative analysis in this section with the parameter values of Table 1 as default values.

5.1 The miner's optimal strategy
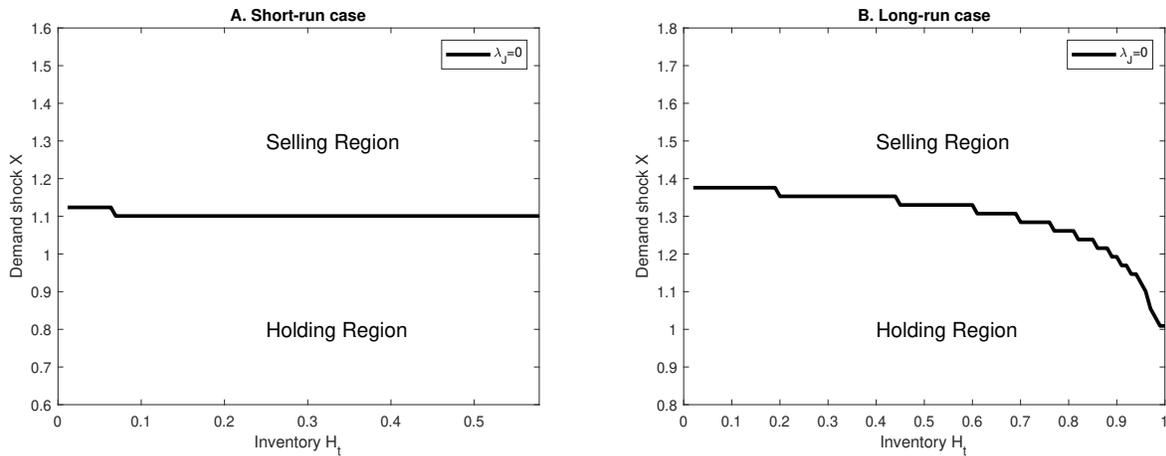
Figure 7: **Selling and holding regions in the high-active regime with no jump risk** ($\lambda_J = 0$). Parameter values are based on Table 1. The left panel shows the short-run case, i.e., with block rewards, $t = 2014$ and $S_t = 0.5871$. The right panel shows the long-run case in which the block rewards are terminated, i.e., $t = 2140$.

23

Optimal selling barrier, selling region, and holding region. Fig. 7 shows the miner's liquidating strategies for the short-run case (t = 2014, the left panel) and the long-run case (the right panel), where the high-active regime with no jump risk ($\lambda_J = 0$) is assumed, the cumulative supply of bitcoin is $S_t = 0.5871$ for the short-run case, and other default parameters are reported in Table 1. Numerical results for the low-active regime are quite similar and are thus omitted here. It shows that there exists an optimal selling barrier, splitting the solution region into a holding region and a selling region in which the miner holds and sells her inventory, respectively. For a fixed inventory level, the selling region is below the (optimal) selling barrier because the miner is inclined to reduce her inventory when the demand shock is lower enough.

It can be observed from Fig. 7 that the selling barrier decreases as the inventory level increases partially because a higher inventory prompts miners to reduce their inventory earlier in order to receive higher transaction fees in the future. Note that the selling barrier slightly decreases with inventory in the short-run case (the left panel of Fig. 7), as block rewards significantly prevail over the transaction fee income in this case. As shown by the right panel of Fig. 7 for the long-run case, the selling barrier exhibits a clear downtrend against inventory. This is because in the long run, transaction fees are the unique source of miners' income, and miners are inclined to reduce their inventory to increase potential transaction fee income.

Jump risk or high volatility? The jump intensity λ_J and the volatility $\sigma_{\mathbb{H}}$ ($\sigma_{\mathbb{L}}$) impact the miner's optimal selling strategy quite differently. In particular, we shall point out a reasonably high volatility cannot explain why miners kept selling their inventory in 2014-2015..

Fig. 8 plots the selling barrier against jump intensity λ_J for the short-run case (t = 2014), where the high-active regime is assumed, $S_t = 0.5871$, $H_t/S_t = 0.1$, and other default parameter values are given in Table 1. As jump intensity increases from 0 to 57, the selling barrier decreases from around 1.6 to 0. This implies that jump risk could hasten miners' selling of bitcoin holdings. In particular, for a high jump risk, e.g., $\lambda_J = 57$, miners keep selling their bitcoin holdings. We then infer that the jump risk is a primary factor determining miners' optimal selling timing. This also explains why miners started to sell their holdings to market at the inception of Bitcoin even
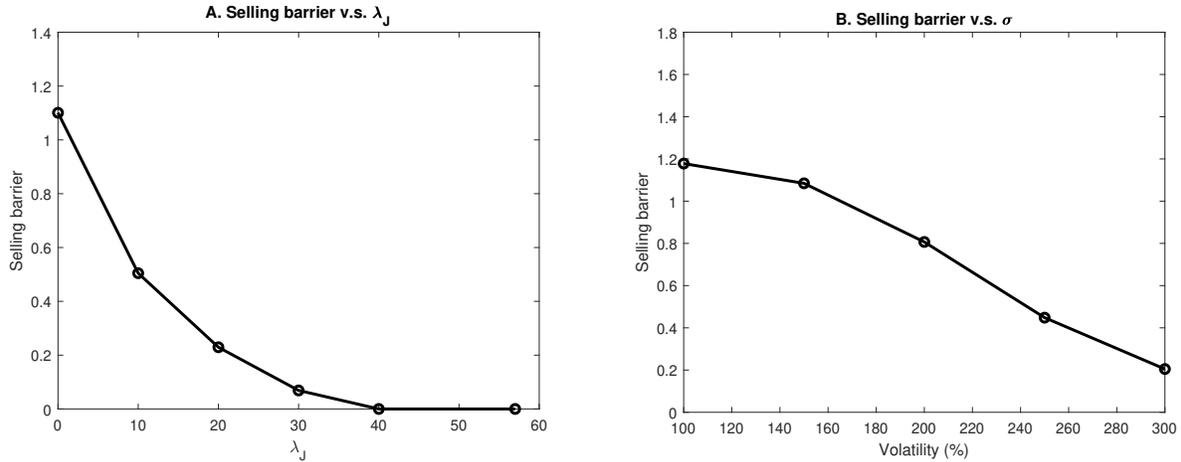
Figure 8: **Impact of jump intensity λ_J and volatility $\sigma_{\mathbb{H}}$ ($\sigma_{\mathbb{L}}$) on the selling barrier for the short-run case in the high-active regime**. Parameter values are based on Table 1. For panel B, we assume $\sigma_{\mathbb{H}} = \sigma_{\mathbb{L}} = \sigma$ varying from 100% to 300%. We choose $t = 2014$ and $H_t/S_t = 0.1$ with $S_t = 0.5871$.

when bitcoin prices and demands were extremely low. Note that the demand level implied from bitcoin price could be as low as 0.073 in 2014-2015 and increased to 4.03 in 2017. In contrast, a reasonably high volatility in Bitcoin demand shock could not drive miners to sell when the bitcoin demand was so low in 2014-2015. For example, as shown in the right panel of Fig. 8, even for the volatility of 300%,[20] the selling barrier is higher than 0.2, which is much higher than the demand level 0.073 in 2014-2015. Therefore, a reasonably high volatility cannot explain why miners kept selling their inventory in 2014-2015.

Optimal selling rate. Fig. 9 depicts the miner's optimal selling rate against demand shock and inventory level for the short-run case ($t = 2014$) in a high-active regime with no jump risk ($\lambda_J = 0$). The optimal selling rate appears to be smooth and non-decreasing with respect to both inventory and demand levels.

---

[20]Note that Liu and Tsyvinski (2018) estimate the bitcoin price volatility with daily, weekly, and monthly data and find the annualized volatility varies from 106.03% to 240.61%.

25
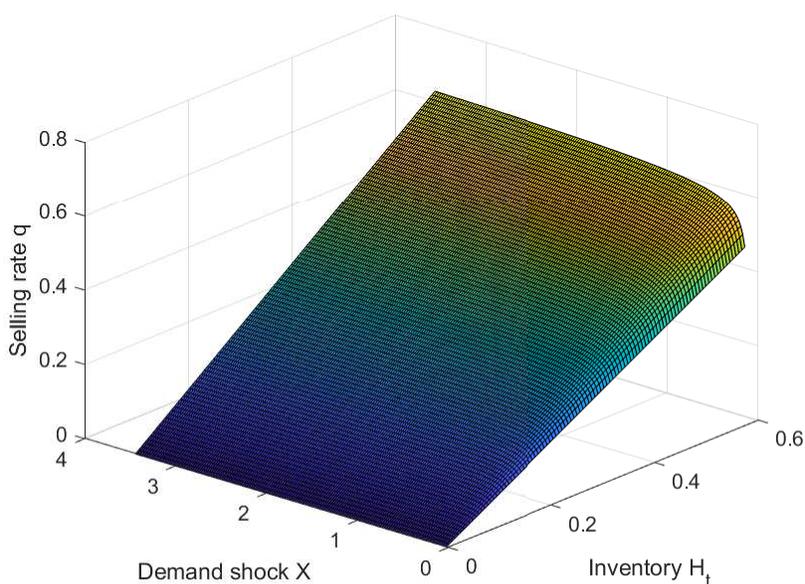
Figure 9: **Optimal selling rate against demand shock and inventory for the short-run case in the high-active regime with no jump risk** $\lambda_J = 0$. Here $t = 2014$ with $S_t = 0.5871$, and other default parameter values are as given in Table 1.

5.2 Average transaction fee rate

Now let us investigate the properties of the average transaction fee rate. Fig. 10 plots the miner's average transaction fee rate against the demand shock in the high-active regime (panel A) and the low-active regime (panel B), respectively. It can be seen that consistent with Proposition 1, the average transaction fee rate in both the long-run case (solid lines) and the short-run case (dashed lines) is non-decreasing in demand shock, as a higher demand shock results in a larger volume of unconfirmed transactions. Moreover, as predicted by part (i) of Proposition 1, the average transaction fee rate is likely flat when the demand shock is sufficiently low. One can also observe that the average fee rate in the long-run is always no lower than in the short-run, which is not surprising because, ceteris paribus, there are more circulated bitcoins and thus more transactions in the long-run than in the short-run. In addition, the average fee rate in the low-active regime is lower than or equal to that in the high-active regime, as more transactions occur in the high-active regime.

26
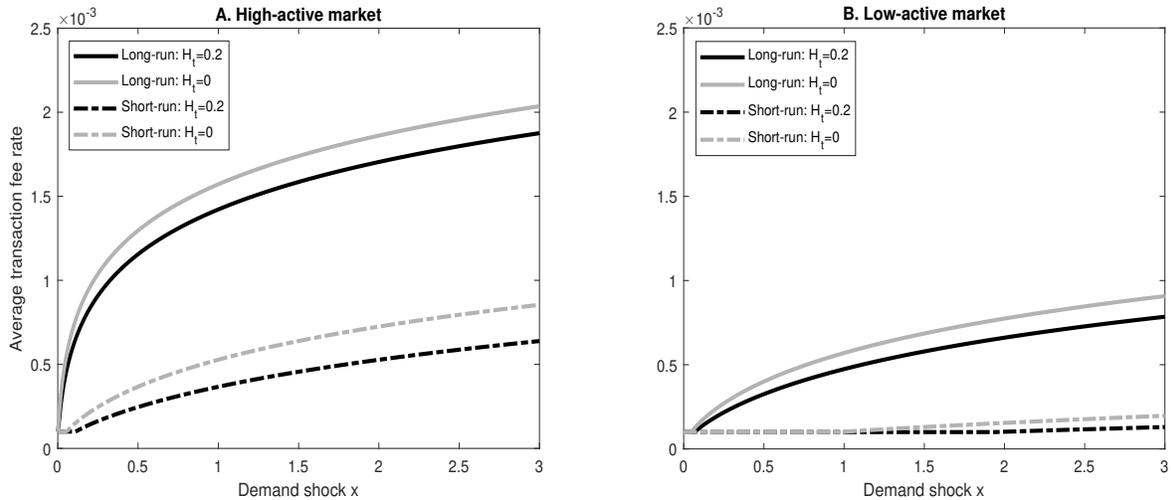
Figure 10: **The average fee rate against demand shock for different inventory**. The short-run case is at $t = 2014$. The left panel is for the high-active regime, while the right panel is for the low-active regime.

We further examine how the miner's holding affects transaction fees. As shown in Fig. 10, the average fee rate with $H = 0.2$ (black lines) is always lower than that with $H = 0$ (gray lines). Intuitively, ceteris paribus, the more bitcoins held by miners, the fewer bitcoins held by users, and the fewer users' unconfirmed transactions as a result. Combined with Proposition 1, this explains why a higher miner's inventory could induce a lower average fee rate.

5.3 The miner's value function

We now examine how transaction fees and the declining block rewards affect the miner's value in Bitcoin mining in both short run (with block rewards) and in long run (without block rewards). For computational simplicity, the block rewards are assumed to terminate in 2050, as there are very few block rewards from 2050 and ultimately no block rewards from 2140. Fig.11 presents the miner's value against time without (solid line) and with jump risk (dashed line), respectively. The dashed line is always below the solid line because jump risk hurts the miner's value.

Note that in both cases, the miner's value against time is U-shaped, which can be attributed to the declining block rewards and endogenous Bitcoin transaction fees. Indeed, at the early stage of the Bitcoin system when the transaction volume is low while block rewards are high, the majority of

27

a miner's income comes from block rewards. As such, the declining block rewards predetermined by the system lead the miner's value to be decreasing with time at the early stage, *ceteris paribus*. As time goes up, endogenous transaction fees would eventually dominate the miner's value, even before the termination of block rewards, which explains the increasing part of the miner's value.
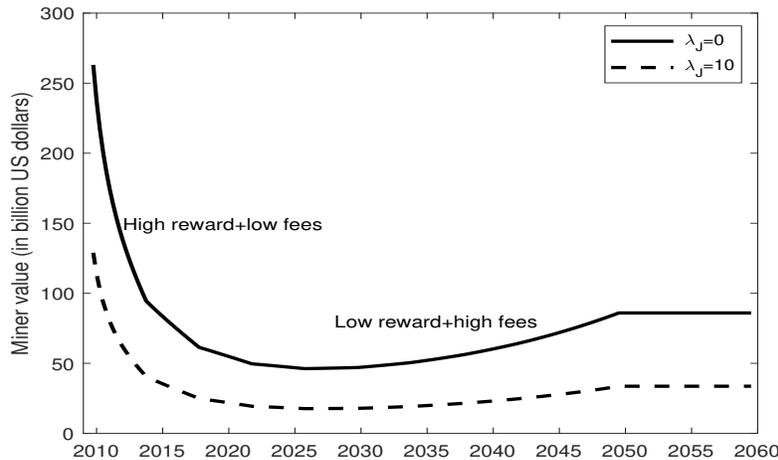
Figure 11: **The miner's value function across time in the high active regime.** Here the initial demand $X = 1$ and initial inventory 0. Note that in the beginning the block rewards are high but the endogeneuous transaction fees are low, while in the long run the block rewards diminish but the endogenous transaction fees become high.

6 Conclusion

We develop a continuous-time dynamic model to study the economics of the supply side of bitcoin mining, inspired by the classic Hotelling model for exhaustible resources. The model is rich enough to incorporate endogenous transaction fees, the miners' liquidation policies, endogenous inventory holdings, declining system block rewards, and stochastic demand. We find that high jump risk and transaction fees are major forces driving miners to reduce their inventory even when bitcoin prices are extremely low, consistent with empirical observations. The model gives an explanation for the observed co-movements of average transaction fee rate, average block sizes, and Bitcoin prices, especially why the average transaction fee rate stays flat from 2014 to 2016 and increases dramatically in 2017.

28

References

Alsabah, H. and Capponi, A. 2019. Pitfalls of Bitcoin's Proof-of-Work: R and D Arms Race and Mining Centralization. mimeo Columbia University.

Athey, S., Parashkevov, I., Sarukkai, V., and Xia, J. 2016. Bitcoin pricing, adoption, and usage: Theory and evidence. Working paper.

Bass, M. F. 1969. A new product growth for model consumer durables. *Management Science* **15** 215-227.

Bass, M.F. 2004. Comments on "A new product growth for model consumer durables": the Bass model. *Management Science* **50** 1833-1840.

Basu, S., Easley, D., O'Hara, M., and Sirer, E. G. 2018. Towards a Functional Fee Market for Cryptocurrencies. Working paper.

Ben-Or, M. (1983). Another advantage of free choice: completely asynchronous agreement protocols. *Proceedings of ACM PODC 1983*.

Benigno, P., Schilling, L., and Uhlig, H. 2019. Cryptocurrencies, Currency Competition, and the Impossible Trinity. *Working paper*.

Biais, B., Bisière, C., Bouvard, M., Casamatta, C., and Menkveld, A. 2018. Equilibrium Bitcoin pricing. TSEWorking Paper.

Biais, B., Bisière, C., Bouvard, M., and Casamatta, C. 2019. The Blockchain Folk Theorem. *Review of Financial Studies* **32** 1662-1715.

Bohme, R., Christin, N., Edelman, B., and Moore, T. 2015. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives* **29** 213-238.

Bolt, W. and Oordt, M. 2016. On the value of virtual currencies. *Working Paper*.

Catalini, C. and Gans, J.S. 2016. Some simple economics of the blockchain, *National Bureau of Economic Research* Technical report.

Chaum, D. (1983). Blind signatures for untraceable payments. Working Paper.

Chiu, J. and Koeppl, T. 2017. The economics of cryptocurrencies-Bitcoin and beyond. *Working paper*.

Cong, L., He, Z., and Li, J. 2018. Decentralized mining in centralized pools. *Forthcoming at Review of Financial Studies*.

Cong, L., Li, Y., and Wang, N. 2019. Tokenomics: Dynamic Adoption and Valuation. *Forthcoming at Review of Financial Studies*.

Detzel, A., Liu, H., Strauss, J., Zhou, G., and Zhu, Y. 2018. Bitcoin: Learning and Predictability via Technical Analysis. *Working paper*.

Dixon, R. 1980. Hybrid Corn Revisited. *Econometrica* **48** 1441-1451.

Cuoco, D. and Liu, H. 2000. Optimal consumption of a divisible durable good. *Journal of Economic Dynamics and Control*. **24** 561-613.

Dwork, C. and Naor, M. 1992. Pricing via processing or combating junk email. *Proceedings of CRYPTO 1992*, 139-147.

Easley, D., O'Hara, M., and Basu, S. 2019. From mining to markets: the evolution of transaction fees. forthcoming in *Journal of Financial Economics*.

Fischer, M. J., Lynch, N. A. and Paterson, M. S. 1985. Impossibility of Distributed Consensus with One Faulty Process. *Journal of the ACM*. **32** 374–382.

Gronwald, Marc. 2015. The Economics of Bitcoin-News, supply vs. Demand nd Jumps. *Working paper*.

Gutierrez, R., Nafidi, A., and Sanchez, R. 2004. Inference in the stochastic Gompertz diffusion model with continuous sampling. *Monografias del Seminario Matematico Garcia de Galdeano* **21** 347-353.

Haber, S. and Stornetta, W.S. 1991. How to time-stamp a digital document. *Journal of Cryptology* **3** 99–111.

Hayashi, Fumio. 1982. Tobin's marginal q and average q: A neoclassical interpretation. *Econometrica* **50** 215-224.

Hotelling, H. 1931. The Economics of Exhaustible Resources. *Journal of Political Economy* **39** 137-175.

Graewe, P. and Horst, U. 2017. Optimal trade excution with instantaneous price impact and stochastic resilience. *SIAM J. Control and Optimization* **56** 3707-3725.

Hayes, S. Adam. 2017. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing Bitcoin. *Telematics and Infomatics* **34** 1308-1321.

Huberman, G., Leshno, J. D., and Moallemi, C. 2017. Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *Working paper*.

Lamport, L., Shostak, R., and Pease, M. 1982. The Byzantine generals Problem. *ACM Transactions on Programming Languages and Systems* **4** 387–389.

Levhari, D. and Pindyck, S.R. 1981. The Pricing of Durable Exhaustible Resources. *Quarterly Journal of Economics* **96** 365-377.

Liu, Y. and Tsyvinski, A. 2018. Risks and Returns of Cryptocurrency. NBER Working Paper No. w24877.

Mahajan, V., Muller, E., and Bass, M.F. 1990. New product diffusion models in marketing: a review and directions for research. *Journal of Marketing* **54** 1-26.

Malueg, A.D. and Solow, L.J. 1990. Monopoly Production of Durable Exhaustible Resources. *Economica* **57** 29-47.

Nakamoto, S. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved at https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. 2016. Bitcoin and cryptocurrency technologies, Princeton University Press.

Eglese, R. W. 1990. Simulated annealing: A tool for operational research. *European Journal of Operational Research* **46** 271-281.

Fisher, I. 1911. The purchasing power of money: Its determination and relation to credit, interest and crises. Macmillan, New York.

Friedman, M. 1973. A theoretical framework for monetary analysis. *Journal of Political Economy* **78** 193-238.

Prat, J. and Walter, B. 2018. An equilibrium model of the market for bitcoin mining, *Working paper*.

Weil, Philippe. 1987. Confidence and the real value of money in an overlapping generations economy. *Quarterly Journal of Economics* **102** 1-22.

Sapirshtein, A., Sompolinsky, Y., and Zohar, A. 2016. Optimal selfish mining strategies in Bitcoin, *International Conference on Financial Cryptography and Data Security* Springer 515-532.

Schilling, L. and Uhlig, H. 2019. Some simple bitcoin economics. *Journal of Monetary Economics*.

Schilling, L. and Uhlig, H. 2019. Currency Substitution under Transaction Costs. *AEA Papers & Proceesdings* **109**.

Stewart, M.B. 1980. Monopoly and the Inter-temporal Production of a Durable Extractable Resource. *Quarterly Journal of Economics* **94** 99-111.

32

Yermack, D. 2013. Is Bitcoin a real currency? an economic appraisal. *National Bureau of Economic Research* Technical report.

From Hotelling to Nakamoto:
How Do Miners Liquidate Their Bitcoins?

Appendices

A   Background of Bitcoin Mining

Bitcoin system in Nakamoto (2009) is a decentralized online payment system with an embedded crypto-currency, bitcoin. Capped at 21 million in total number, bitcoins are supplied in terms of block rewards that will terminate in 2140. There are two groups of fundamental participants in the Bitcoin system: users and miners. Compensated by block rewards and/or transaction fees as an incentive, miners play an indispensable role in the system by validating users' transactions and updating the distributed ledger (i.e., the blockchain) through a particular type of proof-of-work.

Once a miner's candidate block is successfully attached to the blockchain, the miner will get two sources of income, block rewards predetermined by the system and the transaction fees attached to the block. The two sources have distinct features: Block rewards are *deterministic* and *exogenous*, as the amount of block rewards is halved after every four years and will vanish after the year 2140; see the left panel of Fig. 12. Hence, bitcoin's total supply is fixed and finite, and scarcity is one of bitcoin's most distinctive features. In contrast, transaction fees are *stochastic* and *endogenous*, as miners can select which transactions are included in the mining block according to the transaction fees attached by users. Consequently, the higher the transaction fees attached to a transaction, the more likely the transaction will be added to a block for mining.

Note that the only way to generate new bitcoins is through the mining record, and the total number of available bitcoins is 21 million, resulting in the termination of supplying new bitcoin in the year 2140. The unique pattern of block rewards suggests that the Bitcoin system's lifetime
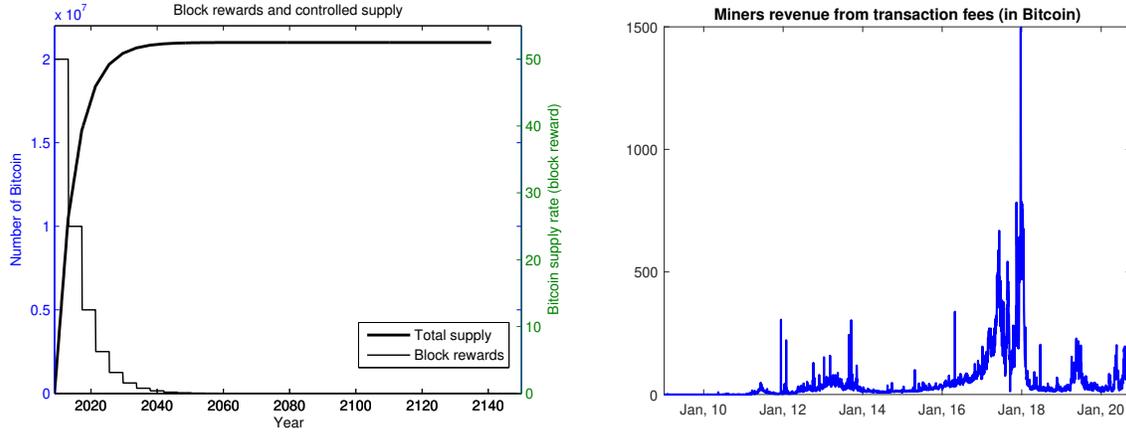
Figure 12: **Two types of miner's revenue: block rewards and transaction fees**. The left figure shows the predetermined block rewards for each successfully mined block, which gets halved every four years and will terminate in the year 2140. The right figure shows the daily transaction fees in terms of bitcoin from 2009 to 2020.

can be divided into two stages: the short-run period (i.e. before the termination of bitcoin supply in 2140) and the long-run period (i.e., after the termination of bitcoin supply in 2140). In the long-run, miners' activities are only compensated by transaction fees.

B Proof of Proposition 1

Proof. By definition, it is easy to check that $K' < 0$ and $k' < 0$. The optimal strategy of problem (8) is given by (10). Assertion (i) thus follows by (10) immediately. For assertion (ii), the first part follows from a direct calculation

$$\frac{\partial r}{\partial X} = \frac{\partial}{\partial X}\left(\frac{K(\phi^*)}{k(\phi^*)}\right) = \left(\frac{K(\phi^*)}{k(\phi^*)}\right)'\frac{\partial \phi^*}{\partial X} = \frac{f(\phi^*)\int_{\phi^*}^{\bar{\phi}}(u - \phi^*)f(u)du}{k^2(\phi^*)}\frac{\partial \phi^*}{\partial X} > 0.$$

and the fact that L is an increasing function of X. The second part follows by a direct application of L'Hôpital's rule. □

C An Individual Miner

For simplicity, we assume no regime-switching in the demand shock of Bitcoin. We consider an economy with identical miners that are endowed with certain computation powers and face the same mining cost per unit of computational power. Let ω TH/s be the computing power of a miner in terms of hash rate, and denote by π the probability that the miner can successfully mine a block and win rewards/fees in 10 minutes. The winning probability π is approximate to be, according to Hayes (2017),

$$\pi = \frac{\omega}{D \times 2^{23}/600},\tag{26}$$

where D is the difficulty level, and $D \times 2^{32}/600$ is called the network hash rate of Bitcoin system.

Let $\pi \in (0, 1]$ be the probability that the miner can successfully mine a block and win rewards/fees in 10 minutes. Then the individual's miner's inventory level H_t evolves according to

$$dH_t = (b_t + I_t)\pi dt - Q_t dt.\tag{27}$$

For an individual miner with inventory level H_t at time t, the system naturally imposes a constraint

$$0 \leq H_t \leq S_t.\tag{28}$$

In fact, only transaction orders submitted by users and other miners could contribute to the miner's transaction fees and thus be regarded as effective orders to the miner. In addition, the volume of effective orders shall depend on Bitcoin adoption, which is represented by S_t, and demand level X_t. Thus, we take the following function form of L:

$$L(H_t, X_t; S_t) = \theta[1 - H_t/S_t]S_t^{(1-\alpha\gamma_s)}X_t^{\alpha}.\tag{29}$$

Given different successful mining probabilities, Fig. 13 depicts the impact of λ_J and proportional inventory H_t/S_t, on q_t^*/H_t, the ratio of the optimal selling rate to inventory, for the short-run case ($t = 2014$) in the high-active regime, where $S_t = 0.5871$ and for the long-run case. As shown in all graphs in Fig. 13, by comparing the dark solid line and dark dashed line (red dot-dashed

A–3
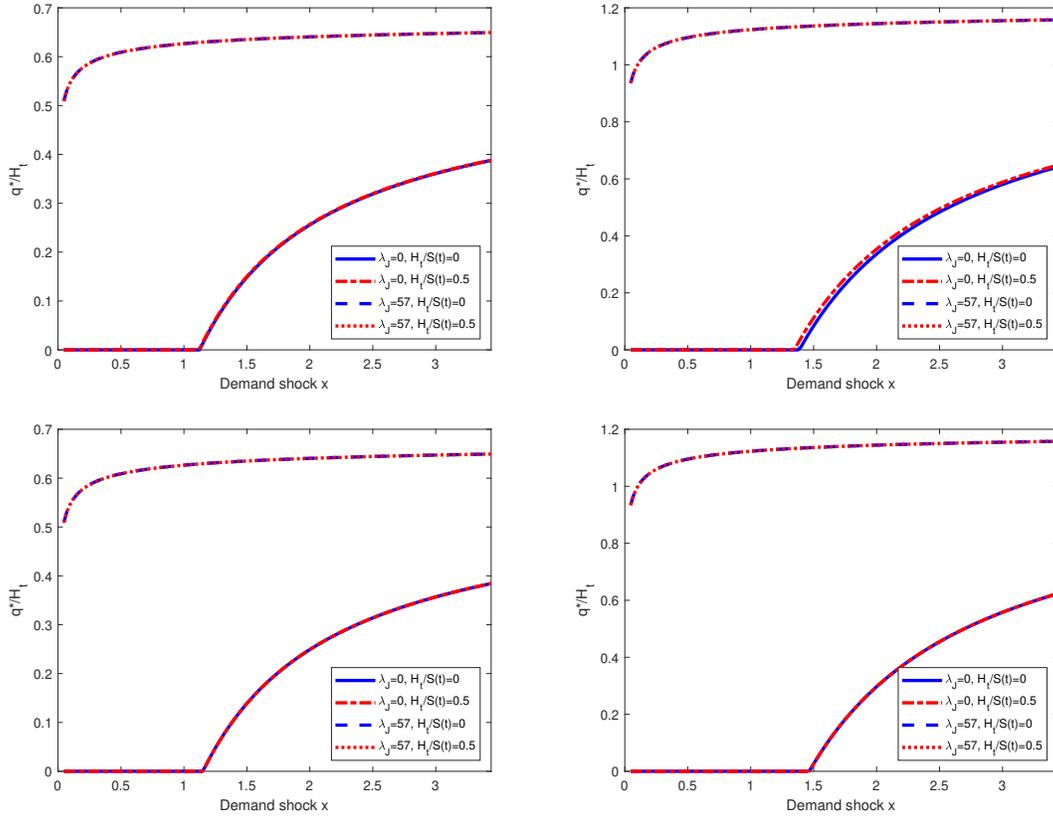
Figure 13: **The ratio of optimal selling rate to inventory in the high-active regime**. The upper two panels are for $\pi = 1$, while the lower two panels are for $\pi = 1/100$. The left two panels shows the short-run case at $t = 2014$ with $S_t = 0.5871$ and the right two panels show the long-run case, i.e., $t = T$. Other parameter values are based on Table 1.

line and red dotted line), we find that jump risk could increase the selling rate significantly. By comparing the dark solid line and red dotted line (dark dashed line and red dot-dashed line), we find that with different levels of jump risk q_t^*/H_t is insensitive to the change in H_t/S_t.

In summary, all miners approximately follow the same strategy regardless of their inventory and successful mining probability. The conclusion is robust to different levels of successful mining probability. This finding helps to justify the representative miner in our model.

D An Individual Miner With An Exit Option

Our model can be extended to include an individual miner's optimal exit decision. The miner

A–4

with an exit option aims to choose optimal stopping time τ_o and optimal selling rate to maximize her present value of accumulated profits:

$$\sup_{\{Q_u\}_{u \geq t} \in \mathcal{A}_t} \mathbb{E}\left[\int_t^{\tau_o} e^{-\beta(u-t)}\left(P_u Q_u - C(Q_u, H_u)\right)du + e^{-\beta(\tau_0 - t)}W(X_{\tau_0}, H_{\tau_0})\right], \qquad (30)$$

subject to (2)-(3), (27), (6), (10)–(7), where $W(X_t, H_t)$ is the value for the miner after exercising the exit option. As before, the miner's cost satisfies $C(Q_t, H_t) = C_m + \psi P_t Q_t^2/H_t$. In our baseline model, the constant mining cost C_m does not affect the miner's decision and is thus assumed to be 0. In the model with an exit option, the constant mining cost C_m cannot be ignored as it does affect the exit decision.[21] Actually, a miner who faces an exit option weighs mining returns and costs and may consider leaving the mining business to avoid losses.

Once the miner decides to exit the mining business, she will liquidate her inventory to realize her profit facing liquidation cost $\psi P_u Q_u^2/H_u$, and in this case, her inventory will only be affected by selling. Therefore, the miner's value function is given by

$$W(X_t, H_t) = \sup_{\{Q_u\}_{u \geq t} \in \mathcal{A}_t} \mathbb{E} \int_t^\infty e^{-\beta(u-t)}\left(P_u Q_u - \psi P_u Q_u^2/H_u\right)du, \qquad (31)$$

where the inventory H_t satisfies $dH_t = -Q_t dt$.

We characterize the miner's strategy by two regions: the mining region and the exit region. As shown in Fig. 14, when demand shock is high, the return from the mining business is high and the miner is in the mining region. Once the demand shock is too low to cover the operational cost, the miner could be in the exit region and optimally leave the mining business. Moreover, a miner with higher bitcoin holding faces a broader exit region because she faces a higher liquidation cost. Therefore, a miner with higher holding requires a higher return to stay in the mining business. In addition, we plot in Fig. 15 the impacts of λ_J, π, C_m on the exit barriers for the short-run case.

---

[21]The mining cost, mainly electricity cost in mining business, can be estimated with average electricity cost and average energy efficiency of mining machines. According to www.eia.gov, the average electricity cost in USA from 2013 to 2018 is 10.3092 cents per Kilowatthour. On the other hand, according to Hayes (2017), the average energy efficiency across the mining network is around 0.4 Watt per GH/s. Hence the mining cost per TH/s is about $C_m = 3.61 \times 10^{-7}$ Billion USD per year.
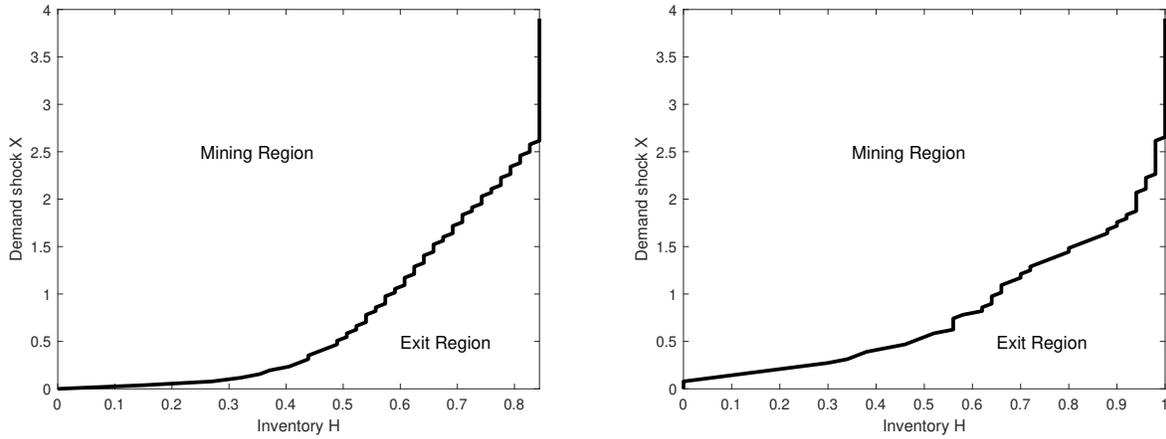
Figure 14: **Exit and mining regions**. We assume $\lambda_J = 0.1$, $\pi = 1e - 7$, $C_m = 3.61e - 7$ (Billion USD), and other default parameter values are from Table 1 with the high-activity market. The left panel is for the short-run case, i.e., $t = 2018$ with $S_t = 0.8438$, while the right panel is for the long-run case.
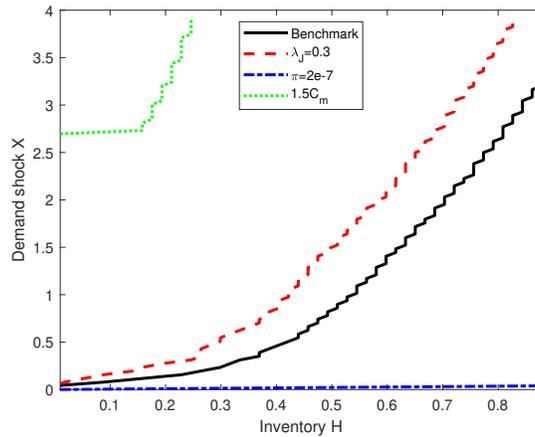
Figure 15: **Impact of λ_J, π, and C_m on exit barriers for the short-run case**. We use the exit barrier in Fig. 14 as the benchmark, compared with the barriers for different values of λ_J, π, and C_m. Specifically, we consider the three cases: jump risk λ_J is tripled, the probability of successful mining π is doubled, and the mining cost C_m is increased by 50%, respectively. The short-run case is at $t = 2018$ with $S_t = 0.8438$.

A–6

We find that increasing jump risk and operational cost could hasten the miner's exit choice, while increasing in probability of successful mining could delay the miner's exit choice.