TYPE Original Research
PUBLISHED 16 February 2023
DOI 10.3389/fbloc.2023.1067628

OPEN ACCESS

EDITED BY
Akihiro Fujihara,
Chiba Institute of Technology, Japan

REVIEWED BY
Kentaroh Toyoda,
Technology and Research (A*STAR), Singapore
Abhijit Chakraborty,
Kyoto University, Japan

*CORRESPONDENCE
Shoji Kasahara,
kasahara@ieee.org

SPECIALTY SECTION
This article was submitted to Blockchain Technologies,
a section of the journal
Frontiers in Blockchain

RECEIVED 12 October 2022
ACCEPTED 24 January 2023
PUBLISHED 16 February 2023

CITATION
Hiraide T and Kasahara S (2023), Analysis of interaction between miner decision making and user action for incentive mechanism of bitcoin blockchain.
Front. Blockchain 6:1067628.
doi: 10.3389/fbloc.2023.1067628

Analysis of interaction between miner decision making and user action for incentive mechanism of bitcoin blockchain

Takumi Hiraide and Shoji Kasahara*

Division of Information Science, Graduate School of Science and Technology, Nara Institute of Science and Technology, Ikoma, Japan

In Bitcoin blockchain, miner nodes are likely to choose transactions with high fee to be included in a block. This makes transactions with high fee being processed fast, affecting the amount of transaction fee that users want to pay. The reward for a winning miner consists of transaction fee and newly issued coins, and hence the amount of newly issued coins also affects the miner decision to participate in the mining competition. In addition, mining reward also affects the total hash computing power, which plays an important role of Bitcoin security for reducing the success probability of security attack by a malicious miner. In this paper, we develop a mathematical model for analyzing the interaction between miner decision making and user actions in terms of transaction fees, transaction-confirmation time, and security. We analyze the transaction-inclusion process with queueing theory, while decision making processes of miners and users are analyzed in the context of Nash equilibrium. The numerical examples show how the mining costs and newly issued coins affect miner decision making.

KEYWORDS

bitcoin, blockchain, incentive mechanism, decision making, nash equilibrium, newly issued coin, security, confirmation latency

1 Introduction

The blockchain is a decentralized cryptocurrency technology that works securely by incentivizing participants to follow a pre-specified protocol. There are no auspices of a trusted and centralized authority and are open to a variety of security attacks. Therefore, the blockchain protocol is needed to ensure consensus even in the presence of such adversaries. One of the established protocols for ensuring consensus is Proof of Work (PoW), the most common consensus mechanism. PoW supports mainstream cryptocurrencies, including Bitcoin and Ethereum, which account for more than two-thirds of the cryptocurrency market share He et al. (2020).

It is reported in Möser and Böhme (2015) that in the Bitcoin blockchain, transactions with high fees are likely to be included faster in a block than those with low fees. That is, the higher the fee, the faster the transaction is included in a block. Therefore, end users are interested in the fees required for transactions to be processed with acceptable delays, while miners are motivated by high fees included in transactions in order to increase their revenue.

The interplay between users and miners in the blockchain exhibits an intricate dynamic nature of the decentralized system. This paper is concerned with a mathematical model that captures the unique features of cryptocurrency systems, and then using this model to study participant behavior and effect of newly issued coins and mining costs on equilibrium state of the system. Our mathematical model consists of two decision making processes for users and miners. In the user decision making process, a user decides to join the blockchain service according to the expected transaction-confirmation time which is dependant on the fee. In terms of the decision making for miners, a miner decides to perform mining according to the winning reward composed of newly issued coins and total amount of fees in the mined block.

Note that the miner decision making results in the total hash power for mining, which then affects the transaction-confirmation time required for preventing from the security attack. Note also that the transaction-confirmation time affects the user incentive to join the blockchain service. That is, the user decision making interacts with the miner one through the transaction fee and transaction-confirmation time.

For the user decision making, we consider a utility function in which the transaction fee and transaction-confirmation time are taken into consideration. Here, the transaction-confirmation time consists of the transaction-inclusion time and confirmation latency. The mean transaction-inclusion time is analyzed by a single-server queueing model with batch service, while the confirmation latency is determined such that the resulting attack success probability of malicious miners is smaller than certain security level. In terms of the miner decision making, we consider a utility function which includes newly issued coins and the total amount of transaction fee included in the mined block. For both utility functions, we consider Nash equilibrium, investigating the impact of newly issued coins on the equilibrium state of the blockchain system.

The main contribution of the paper is as follows.

1. We develop a mathematical model for the interaction of decision making between users and miners, taking into account fundamental elements of 1) transaction fees, 2) newly issued coins, 3) total hash rate, 4) security, and 5) transaction-confirmation time consisting of transaction inclusion time and confirmation latency. Note that the previous research related to the interplay between users and miners for the blockchain considers some of the five elements listed above, and this is the first work in which all the five elements are considered in the model.
2. We conduct Nash equilibrium analysis for both the user decision making process and miner one, deriving the optimal strategies for users and miners.
3. In numerical examples, we show how the total hash rate and confirmation latency evolves, investigating the existence of convergence points of the two performance measures. We also investigate how the newly issued coins and mining cost affect the existence of convergence points.

The rest of the paper is organized as follows. In Section 2, related work is presented. Section 3 illustrates the mathematical model for details, and equilibrium strategies for users and miners are analyzed in Section 4. Numerical examples are presented in Section 5, and Section 6 concludes the paper.

2 Related work

There has been much literature on the mathematical analysis of the incentive mechanism of blockchains. The literature is categorized into decision making for users and miners, transaction-inclusion delay, and system security.

The interaction of decision making between users and miners in Bitcoin blockchain are considered in Huberman et al. (2017); He et al. (2020); Yan et al. (2020). In Huberman et al. (2017), users make decision to join or opt out the blockchain service in terms of the utility function for the transaction fee and transaction-inclusion time. In terms of the decision making for miners, the hash-power cost and the reward consisting of newly issued coins and transaction fee are taken into consideration. Through the Nash equilibrium analysis, the monopoly pricing issue is discussed in comparison with traditional payment system. In Huberman et al. (2017), however, the impact of security attacks and newly issued coins on decision making for users and miners is not taken into consideration. He et al. (2020) develop the interaction model of Huberman et al. (2017) to the one in which confirmation latency is introduced for the security guarantee of the blockchain service. However, in He et al. (2020), the impact of newly issued coins on the incentive of miners is not also considered. Yan et al. (2020) consider the miner's transaction-selection policy and analyze its effect on the transaction fee with a dynamic game model in which the interaction between user's payment of transaction fee and miner's transaction selection is taken into consideration.

Note that there are five fundamental elements of decision making for users and miners: 1) transaction fees, 2) newly issued coins, 3) total hash rate, 4) security, and 5) transaction-confirmation time. The decision making for users depends on transaction fees, security, and transaction-confirmation time, while that for miners is affected by transaction fees, newly issued coins, and their hash rates. The literature listed above considers some of the five elements, however, no research work takes all the five elements into consideration. Our research scope in this paper is the clarification of how the amount of newly issued coins affects the interaction of decision making between users and miners, which has not been studied in the existing literature.

Another stream of work related to our study focuses on the mechanism for determining transaction fees, comparing the performance of various auction mechanisms with the current "pay your bid" transaction fee mechanism. Within this area, the literature of Lavi et al. (2022); Yao (2020); Basu et al. (2019) considers different auction mechanisms for determining transaction fees.

Transaction fees also affect the transaction-inclusion time, the interval from the time at which a transaction is issued by a user to the time point at which the block including the transaction is eventually added to the blockchain. A typical approach to characterizing the transaction-inclusion time is queueing analysis. In Li et al. (2018) and our previous work Kawase and Kasahara (2017); Kawase and Kasahara (2018); Kasahara and Kawahara (2019); Kawase and Kasahara (2020), a main interest is to characterize the queueing dynamics of transactions in miner nodes. From this point of view, a basic model of the Bitcoin blockchain is a single-server queueing system, in which transactions waiting in the memory pool and block-generation time are taken into consideration. Huberman et al. (2017) and He et al. (2020) consider the M/M^K/1 system for the transaction-inclusion time. In this paper, we use the result of mean transaction-inclusion time of Huberman et al. (2017), applying the priority queueing analysis to the transaction-inclusion time.

There exist much literature on game-theoretic analysis for decision making by miners In Ma et al. (2018), a mining game played by miners is modeled as a dynamic game, and the equilibrium state achieved by Proof-of-Work is analyzed. Selection problem, in which pool managers make decision of how much reward to give to miners while miners decide which mining pool to join. They consider an equilibrium model for mining pools and its symmetric subgame perfect equilibria, discussing how risk-sharing affects the mining-pool centralization and global hash rate.

Capponi et al. (2021) develop a two-stage game model to analyze the correlation nature of the hardware investment and mining competition. In the first stage of the model, miners decide how much to invest in mining equipment, while in the second stage, miners make decision on hash rates to win mining competition. The authors analyze the Nash equilibrium for the model, discussing centralization in mining and the impact of the equipment investment and mining reward on the decentralization in mining.

In Altman et al. (2020), focusing on the miner decision making, the authors consider multiple blockchain services supported by edge computing service providers, where a miner chooses which service provider to use and which blockchain to mine. They model the miner's decision making as a non-cooperative game, investigating its Nash equilibrium.

The security threat is also an important issue of the decision making for users and miners. Chiu and Koeppl (2017) consider a mining game model in which miners are classified into honest and malicious ones, and the incentives of malicious miners to conduct double spending attack are analyzed in terms of the total hash rate. In Pagnotta (2018), focusing on the token economy of Bitcoin blockchain, the authors consider the evolution process of Bitcoin price under mining competition, in which security threat is taken into consideration. Chatterjee et al. (2018) propose concurrent ergodic games for modeling long-term economic aspects of security violations.

In Prat and Walter (2018), a miner-entry decision model based on real options theory is proposed, in which the interaction between Bitcoin/US dollar exchange rate and the hash power of the Bitcoin network is taken into consideration. The authors analyze the equilibrium of the payoff rate for miners, discussing how miners response to the price evolution of Bitcoin.

Wang and Liu (2015) propose a formula to estimate the total hash power based on the number of blocks created in a day and the difficulty. Pagnotta and Buraschi (2018) address the valuation of Bitcoin and other blockchain tokens in a decentralized financial network. In their model, total hash rate and the bitcoin price are jointly determined.

In terms of the analysis of the security attack by malicious miners, Goffard (2019) model a public blockchain and a malicious blockchain as two independent counting processes, analyzing the probability distribution of the time at which the malicious chain catches up the public blockchain.

3 Model

In this section, we present a mathematical model that incorporates the operational features of blockchain systems, the interplay between miners and users, and the security issue associated with the decentralized nature of the blockchain system.

In our model, we assume zero latency for transactions to propagate through the network. This implies that a transaction issued by a user immediately arrives at the memory pool of all miner nodes. Suppose that transactions arrive at the memory pool according to a Poisson process with arrival rate λ. The miners select transactions from the memory pool in order of highest fee and processes up to K transactions into a block during a process called hashing or mining. We assume that the time interval between consecutive blocks follows an exponential distribution with rate μ. Then the blockchain system is modeled as a single-server queue with batch service M/M^K/1.

As miners seek to increase their own revenue, service discipline is prioritized by the fee b that a user is willing to pay to process his/her transaction; the higher the fee, the more quickly the transaction will be selected and processed. Each miner generates a new block with transactions in the memory pool up to the block limit K. The miner that wins the mining competition is awarded the sum of the total fees in the block and the new coins issued. Let B denote the amount of new coins issued in one-block mining. Assuming that the mined block includes K transactions, miners revenue is given by the sum of B and the mean amount of total fees in the block $K\int_{\underline{b}}^{\infty} b\, dG_u^*(b)$. Note that the mean amount of total fees in the mined block depends on the user decision making.

We define q as the hash power of a miner. Since miners are likely to replace mining machines and sometimes leave mining operations, we assume that q follows a distribution function G_M. We also assume that a miner with the hash power q incurs the mining cost $C_M(q)$ for one-block mining. The incentive for miners to participate in the mining competition increases or decreases depending on the total fees from users. We model the miner's decision making by (p_M, G_M), where p_M is the probability a miner will join the mining competition of the blockchain system. We assume that miners are homogeneous, i.e., all the miners make decision according to (p_M, G_M).

When a user sends a transaction, the user pays the transaction fee b. The transaction fee b $(\in \underline{b}, \infty))$ is independent and identically distributed (i.i.d.) with a distribution function G_u. Here, $\underline{b}$ is the minimum fee of a transaction required to be accepted by miners. Assume that the user incurs the waiting cost c per unit time. Then the user waiting cost is given by cW_u, where W_u is the transaction confirmation time as W_u. Here, the transaction-confirmation time W_u consists of the transaction-inclusion time and confirmation latency. The transaction-inclusion time is the time interval from the time epoch when the transaction is sent by a user to the time point at which the block including the transaction is added to the blockchain. The transaction-confirmation latency is the time after which the block including the transaction is confirmed as the longest chain. Let z denote the number of blocks which are added to the blockchain after the block including the transaction. Then, the mean transaction-confirmation latency is given by z/μ. Note that z is determined such that the probability of malicious miner's tampering with the blockchain, e.g., double spending attack, is smaller than a prespecified value.

We assume that the user gains R_u when the transaction is confirmed. Note that a user makes decision to send transactions according to the utility in terms of the user gain R_u, the minimum entrance fee $\underline{b}$, and the waiting cost cW_u. We model the user's decision making by (p_u, G_u), where p_u is the probability that a user sends a transaction to the system, and G_u is the distribution of the transaction fee b. That is, a user with decision making (p_u, G_u) decides to send a transaction with probability p_u and to pay its fee b distributed with $G_u(b)$. Suppose that there exist a fixed number of users joining the blockchain network. We define Λ_u as the overall transaction-arrival rate and suppose that users' decision making is homogeneous, i.e., all the users in the system make decision to issue transactions according to (p_u, G_u). Since a user joins the blockchain system with probability p_u, the overall transaction-arrival rate to the blockchain λ is given by $p_u\Lambda_u$.

Let $\mathcal{H}_{total}$ denote the total hash rate of miners joining the blockchain network. We assume that mining difficulty is immediately adjusted[1] and that $\mathcal{H}_{total}$ is independent of the block-

[1] In the real world, the difficulty target assigned for each block is fixed, and the reward provided for a unit hash power is fixed (i.e., independent of other miners' activities).

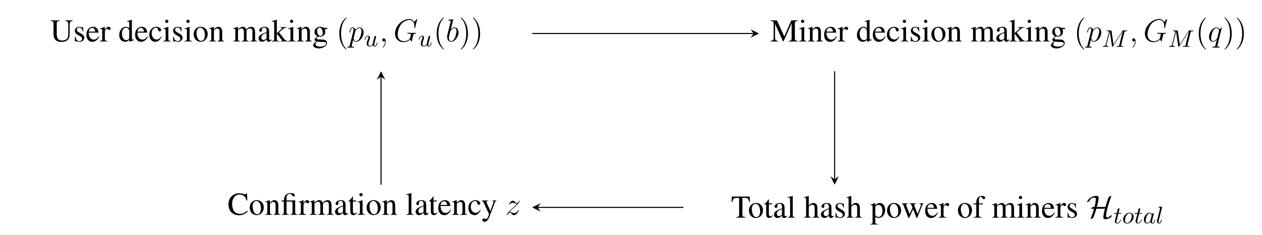
User decision making $(p_u, G_u(b))$
Miner decision making $(p_M, G_M(q))$
Confirmation latency z
Total hash power of miners $\mathcal{H}_{total}$

FIGURE 1
Transition of equilibrium state.

generation rate μ. Note that from this assumption, $\mathcal{H}_{total}$ does not affect the transaction-inclusion time, i.e., the transaction-sojourn time in the memory pool. On the contrary, $\mathcal{H}_{total}$ affects the transaction-confirmation latency z/μ required to prevent double spending attack. We define A and η as the malicious miner's hash rate and the probability that the malicious miner succeeds double spending attack. When the malicious miner's hash rate A is relatively large in comparison with $\mathcal{H}_{total}$, this increases η and the malicious miner is likely to succeed double spending attack. In such case, we need to increase z in order to make η small in order to prevent the double spending attack.

As a summary, our model consists of the following four phases.

1. The total hash power $\mathcal{H}_{total}$ affects the number of subsequent blocks z required for block approval.
2. z affects the user's decision making (p_u, G_u).
3. The user decision making (p_u, G_u) affects the miner's revenue.
4. The miner's revenue affects the miner's decision (p_M, G_M), which determines the total hash power $\mathcal{H}_{total}$ of miners joining the blockchain network.

We illustrate the transitions of decision making for users and miners in Figure 1.

4 Equilibrium analysis of optimal strategies for users and miners

4.1 User's optimal strategy

The analysis of the user's optimal strategy in this section follows He et al. (2020); Huberman et al. (2017). In our model, the transaction-confirmation time for a user, W_u, consists of the transaction-inclusion time and confirmation latency. Since the transaction-inclusion process is M/M^K/1, the mean transaction-inclusion time is given by the mean sojourn time of a transaction in M/M^K/1. Denoting $W_{queue}(\lambda)$ the mean transaction-inclusion time, we have (Huberman et al. (2017), Lemma A2)

$$W_{queue}(\lambda) = \frac{1}{(1-x_0)\{\mu+\lambda-\mu(k+1)x_0^K\}},$$

where x_0 is given as unique solution of the following polynomial equation in the interval [0,1) (Kleinrock (1975)).

$$x^{K+1} - \left(\frac{\lambda}{\mu}+1\right)x + \frac{\lambda}{\mu} = 0.$$

We consider a transaction-inclusion process in which transactions with high fee are included into a block faster than those with low fee. Note that the arrival rate of the transactions whose fee is greater than b is given by $\lambda(1-G_u(b))$. Noting also that the overall transaction-arrival rate to the blockchain λ is given by $p_u\Lambda_u$, the mean transaction-inclusion time for such transactions is given by $W_{queue}\, p_u\Lambda_u(1-G_u(b))$.

Assume that W_u is the function of transaction fee b given that the user decision making is (p_u, G_u) and that the number of blocks regarded as the longest chain is z, denoted as $W_u(b|(p_u, G_u), z)$. Then we have

$$W_u(b|(p_u,G_u),z) = W_{queue}(p_u\Lambda_u(1-G_u(b))) + \frac{z}{\mu}. \qquad (1)$$

Let f_u denote the utility function of a user with decision making (p_u, G_u), defined as

$$f_u(p_u,G_u,b) = R_u - b - cW_u(b|(p_u,G_u),z).$$

Let $U((p_u,G_u)|(p_u',G_u'),z)$ denote the utility function of a user who takes the strategy (p_u, G_u) when the strategy of all other users is (p_u',G_u'). We obtain

$$U((p_u,G_u)|(p_u',G_u'),z) = p_u\int_{\underline{b}}^{\infty} f_u(p_u',G_u',b)dG_u(b).$$

Let $(p_u^\star,G_u^\star)$ be the user's strategy in Nash equilibrium, then $(p_u^\star,G_u^\star)$ satisfies

$$U((p_u^\star,G_u^\star)|(p_u^\star,G_u^\star),z) = \sup_{(p_u,G_u)} U((p_u,G_u)|(p_u^\star,G_u^\star),z).$$

From Appendix, the optimal user's strategy $(p_u^\star,G_u^\star)$ satisfies

$$\frac{d}{db}f_u(p_u^\star,G_u^\star,b) = 0.$$

Thus, the following equation holds.

$$f_u(p_u^\star,G_u^\star,\underline{b}) = f_u(p_u^\star,G_u^\star,b),$$

which yields

$$R_u - \underline{b} - cW_u(\underline{b}|(p_u^\star,G_u^\star),z) = R_u - b - cW_u(b|(p_u^\star,G_u^\star),z). \qquad (2)$$

Applying 1) to 2) and noting $G_u(\underline{b}) = G_u^\star(\underline{b}) = 0$ yield

$$\underline{b} + c\left(W_{queue}(p_u^\star\Lambda_u) + \frac{z}{\mu}\right) = b + c\left(W_{queue}(p_u^\star\Lambda_u(1-G_u^\star(b))) + \frac{z}{\mu}\right). \qquad (3)$$

If $f_u(p_u^\star,G_u^\star,b) > 0$, the utility of a user is positive and the user joins the system, which implies $p_u^\star = 1$. If $f_u(p_u^\star,G_u^\star,b) < 0$, the user decides not to join the system, i.e., $p_u^\star = 0$. If $0 < p_u^\star < 1$, on the other hand, the following equation holds.

$$R_u - \underline{b} - c\left(W_{queue}\left(p_u^\star \Lambda_u\right) + \frac{z}{\mu}\right) = 0. \quad (4)$$

From (4), the equilibrium user's probability to participate is given as

$$p_u^\star = \min\left\{\frac{1}{\Lambda_u} W_{queue}^{-1}\left(\frac{R_u - \underline{b}}{c} - \frac{z}{\mu}\right), 1\right\}. \quad (5)$$

From (3), the equilibrium fee distribution $G_u^\star$ is obtained as

$$G_u^\star(b) = 1 - \frac{1}{p_u^\star \Lambda_u} W_{queue}^{-1}\left(W_{queue}\left(p_u^\star \Lambda_u\right) - \frac{b - \underline{b}}{c}\right). \quad (6)$$

Let $\Phi^\star$ denote the equilibrium total fee included in the mined block when user decision making is $(p_u^\star, G_u^\star)$. Noting that $\Phi^\star$ depends on the minimum fee $\underline{b}$, we obtain (He et al. (2020), A.3)

$$\begin{aligned}\Phi^\star(\underline{b}) &= p_u^\star \Lambda_u \int_{\underline{b}}^{\infty} b\, dG_u^\star(b) \\ &= p_u^\star \Lambda_u \min\left\{R_u, \underline{b} + c\left(W_{queue}(\Lambda_u) + \frac{z}{\mu}\right)\right\} - c\int_0^{p_u^\star \Lambda_u} d\lambda \left(W_{queue}(\lambda) + \frac{z}{\mu}\right).\end{aligned} \quad (7)$$

When $R_u - c\ (W_{queue}\ (\Lambda_u) + z/\mu) < 0$ holds, we have

$$\Phi^\star(\underline{b}) = p_u^\star \Lambda_u R_u - c\int_0^{p_u^\star \Lambda_u}\left(W_{queue}(\lambda) + \frac{z}{\mu}\right) d\lambda. \quad (8)$$

We can easily verify that $\Phi^\star$ of (8) is a decreasing function of $\underline{b}$. On the contrary, when $R_u - c\ (W_{queue}\ (\Lambda_u) + z/\mu) \geq 0$, we have

$$\Phi^\star(\underline{b}) = \begin{cases} \Lambda_u\left\{\underline{b} + c\left(W_{queue}(\Lambda_u) + \frac{z}{\mu}\right)\right\} & \\ -c\int_0^{\Lambda_u}\left(W_{queue}(\lambda) + \frac{z}{\mu}\right) d\lambda, & \text{if } R_u \geq \underline{b} + c\left(W_{queue}(\Lambda_u) + \frac{z}{\mu}\right), \\ p_u^*(\underline{b})\Lambda_u R_u - c\int_0^{p_u^*(\underline{b})\Lambda_u}\left(W_{queue}(\lambda) + \frac{z}{\mu}\right) d\lambda, & \text{otherwise.}\end{cases} \quad (9)$$

From (9), we can see that $\Phi^\star$ is a linear function of $\underline{b}$ if $R_u \geq \underline{b} + c(W_{queue}(\Lambda_u) + z/\mu)$. We can also verify easily that $\Phi^\star$ is a decreasing function of $\underline{b}$ if $R_u < \underline{b} + c(W_{queue}(\Lambda_u) + z/\mu)$.

From (8) and 9, the minimum entrance fee $\underline{b}$ that maximizes user's total fee is obtained as follows.

$$\arg\max_{\underline{b}} \Phi^\star(\underline{b}) = \begin{cases} R_u - c\left(W_{queue}(\Lambda_u) + \frac{z}{\mu}\right), & R_u - c\left(W_{queue}(\Lambda_u) + \frac{z}{\mu}\right) \geq 0. \\ 0, & R_u - c\left(W_{queue}(\Lambda_u) + \frac{z}{\mu}\right) < 0.\end{cases} \quad (10)$$

4.2 Miner's optimal strategy

Let Λ_M denote the population size of miners. Remind that the miner's decision making is expressed with (p_M, G_M) where p_M is the probability that the miner will join the mining competition and G_M is the distribution function of hash power. Let (p_M', G_M') be the strategy of all other miners, and denote $U_M((p_M, G_M)|(p_M', G_M'))$ as the utility of the miner with strategy (p_M, G_M). Since the difficulty adjustment is immediate, the block generation rate is constant. We have

$$U_M((p_M, G_M)|(p_M', G_M')) = p_M \int_0^\infty \left\{\frac{q\left(K\int_{\underline{b}}^\infty b\, dG_u^*(b) + B\right)}{q + p_M'(\Lambda_M - 1)\int_0^\infty \xi d\, G_M'(\xi)} - C_M(q)\right\} dG_M(q). \quad (11)$$

The first term in the integral of (11) is the mean reward earned by a miner with hash power q during one-block mining period. $C_M(q)$ is the mining cost per one-block mining period, which is the function of hash power q. Assuming that the mined block includes K transactions, the revenue of the winning miner is given by the sum of the mean value of the total fees included in the mined block $K\int_{\underline{b}}^\infty b\, dG_u^\star(b)$ and the newly issued coins B. Then the equilibrium strategy $(p_M^\star, G_M^\star)$ is formulated by

$$U_M((p_M^\star, G_M^\star)|(p_M^\star, G_M^\star)) = \sup_{(p_M, G_M)} U_M((p_M, G_M)|(p_M^\star, G_M^\star)). \quad (12)$$

We consider the optimal strategy $(p_M^\star, G_M^\star)$ from the miner's utility (11). Similarly to the user's optimal policy of $(p_u^\star, G_u^\star)$, we define f_M as

$$f_M(p_M, G_M, q) = \frac{q\left(K\int_{\underline{b}}^\infty b\, dG_u^\star(b) + B\right)}{q + p_M(\Lambda_M - 1)\int_0^\infty \xi\, dG_M(\xi)} - C_M(q), \quad q \in [0, \infty). \quad (13)$$

From Appendix, the optimal miner's strategy $(p_M^\star, G_M^\star)$ satisfies

$$\frac{d}{dq} f_M(p_M^\star, G_M^\star, q) = 0. \quad (14)$$

Assuming a large population of miners, i.e., $\Lambda_M \gg 0$, we can approximate the denominator of the first term in (13) with

$$q + p_M^\star(\Lambda_M - 1)\int_0^\infty \xi\, dG_M^\star(\xi) \approx p_M^\star \Lambda_M \int_0^\infty \xi\, dG_M^\star(\xi). \quad (15)$$

From (14) and (15), we obtain

$$\frac{d}{dq} C_M(q) = \frac{K\int_{\underline{b}}^\infty b\, dG_u^\star(b) + B}{p_M^\star \Lambda_M \int_0^\infty \xi\, dG_M^\star(\xi)}, \quad q \in [0, \infty). \quad (16)$$

Integrating (16) with q and noting that $C_M(0) = 0$, we obtain

$$C_M(q) = \frac{q\left(K\int_{\underline{b}}^\infty b\, dG_u^\star(b) + B\right)}{p_M^\star \Lambda_M \int_0^\infty \xi\, dG_M^\star(\xi)}.$$

Note that the above equation of $C_M(q)$ is the necessary condition of the existence of Nash equilibrium, implying that the mining cost $C_M(q)$ of a miner with hash power q has a form proportional to q. For simplicity, we write $C_M(q) = C_M \cdot q$ where C_M is constant and given by

$$C_M = \frac{K\int_{\underline{b}}^\infty b\, dG_u^\star(b) + B}{p_M^\star \Lambda_M \int_0^\infty \xi\, dG_M^\star(\xi)}.$$

$\mathcal{H}_{total}$, the total hash rate of miners joining the blockchain network, is given by[2]

$$\mathcal{H}_{total} = p_M^\star \Lambda_M \int_0^\infty \xi\, dG_M^\star(\xi) = \frac{1}{C_M}\left\{K\int_{\underline{b}}^\infty b\, dG_u^\star(b) + B\right\}. \quad (17)$$

Let ζ denote the probability that a malicious miner wins a mining competition. We define $\gamma(\zeta, z)$ as the probability that a malicious miner with winning probability ζ succeeds in tampering with the

[2] The equation (17) shows that the total hash rate is proportional to the miners' revenue. In Appendix, we report the proportional relationship between miners' revenue and the total hash rate, which is based on the data from blockchain.com. See Supplementary Appendix Figure 3.

TABLE 1 Parameter setting.

Parameter	Description	Value
B	Newly issued coin [BTC]	0, 12.5
C_M	Electricity cost of mining [BTC/Mh]	1.5×10^{-12}, 3.8×10^{-12}
R_u	User gain [BTC]	2.4×10^{-2}
Λ_u	Overall transaction arrival rate [transaction/sec]	5.5
μ	Block generation rate [block/sec]	1.67×10^{-3}
A	Malicious miner's hash rate [Mh/sec]	6×10^{11}
K	Block size (Upper bound on the number of transactions in one block)	4,400
c	User waiting cost [BTC/sec]	6×10^{-6}
η	Upper bound on the success probability of a double spending attack	0.001

blockchain under confirmation latency z. Assuming that mining competitions are independent, we obtain (Rosenfeld (2014))

$$\gamma(\zeta, z) = \sum_{k=0}^{z-1} \binom{z+k-1}{z-1} \zeta^z (1-\zeta)^k + \sum_{k=z+1}^{\infty} \binom{z+k-1}{z-1} \zeta^k (1-\zeta)^z. \tag{18}$$

Since the hash power of the malicious miner is A and the total hash power is $\mathcal{H}_{total}$, ζ is given by $\zeta = A/\mathcal{H}_{total}$. Given A and $\mathcal{H}_{total}$, the confirmation latency z^* can be calculated by

$$z^* = \min_{z \in \mathbb{N}} \left\{ z: \gamma\left(\frac{A}{\mathcal{H}_{total}}, z\right) < \eta \right\}, \tag{19}$$

where η is a prespecified constant for security requirement.

5 Numerical results

In this section, we show some numerical examples for analytical results. In our numerical experiments, we used the parameter values of He et al. (2020). Table 1 shows the parameter setting for numerical experiments.

In terms of the reality of parameter setting in Table 1, the amount of newly issued coin $B = 12.5$ is the value during 2016–2020. The inverse number of the block-generation rate $\mu = 1.67 \times 10^{-3}$ is almost 10 min, following the real Bitcoin protocol. In terms of the block size K, it is reported that the median transaction size is around 226 bytes[3]. Since the upper limit of block size is 1 Mbytes, the upper limit of the number of transactions in one block is estimated as $10^6/226 \approx 4{,}400$ transactions.

5.1 Minimum entrance fee that maximizes user's total fee

In this subsection, we investigate the relation of the minimum transaction fee $\underline{b}$ with the total fees paid by users $\Phi^*(\underline{b})$ and user's waiting cost c.

Supplementary Appendix Figure 1A shows the total fees paid by users $\Phi^*(\underline{b})$ against the minimum transaction fee $\underline{b}$. We calculate $\Phi^*(\underline{b})$ from (7) in cases of user's waiting cost c from 4×10^{-7} to 1×10^{-6} in 2×10^{-7} increments. We also plot the case of $c = 6 \times 10^{-6}$. In this figure, $\Phi^*(\underline{b})$ linearly grows with increase in $\underline{b}$ and then decreases, achieving certain maximum value for each c case. The increase of the minimum entrance fee grows the total fee linearly. However, a high entrance fee demotivates users to use the blockchain service, and when the minimum entrance fee exceeds the acceptable range of users, they stop the use of the blockchain. This is why the total fee achieves the maximum. It is also observed in this figure that a small c results in a small $\Phi^*(\underline{b})$ when $\underline{b}$ is small. This is because a low transaction-waiting cost makes users tolerate to a long transaction-confirmation time, resulting in users' low-fee payment. On the contrary, a small c results in a large $\Phi^*(\underline{b})$ for large $\underline{b}$. This suggests that lowering the transaction waiting cost is effective to increase the miners' revenue.

Supplementary Appendix Figure 1B illustrates the minimum transaction fee $\underline{b}$ against the user waiting cost c. We calculate $\underline{b}$ from (10). This figure shows that as the user's waiting cost c increases, the minimum transaction fee set by the miner decreases. This is because when users are less incentivized to join the blockchain service due to a large user waiting cost. This result also implies that when the user's waiting cost is high, miners are likely to encourage users to join the blockchain service by lowering the minimum transaction fee.

5.2 Equilibrium point transition for attack success probability and confirmation latency

In this subsection, we show how user decision making interacts with miner one, by illustrating the evolution of equilibrium points of the ratio of the malicious miner's hash rate to the total one $A/\mathcal{H}_{total}$ and confirmation latency z. Note that $A/\mathcal{H}_{total}$ is equivalent to the attack success probability. The procedure of this numerical experiment is as follows.

1. The transaction-confirmation time $W_u(b|(p_u, G_u), z)$ is calculated from (1).
2. The optimal user decision making (p_u^*, G_u^*) is determined by (5) and (6).

[3] https://bitcoinvisuals.com/chain-tx-size.

3. The miner revenue is calculated and total hash rate $\mathcal{H}_{total}$ is estimated from (17), resulted from the optimal miner decision making $(p_M^\star, G_M^\star)$.
4. The confirmation latency z is calculated from (19).
5. Go to step 1 with updating z.

The above steps are repeated until the point of $(z, A/\mathcal{H}_{total})$ converges or the termination condition is satisfied.

Supplementary Appendix Figure 2A shows the equilibrium state transitions when $B = 0$ and $C_M = 1.5 \times 10^{-12}$. We consider two cases for the initial value of z, $z = 4$ and 5. The blue points are calculated from Step 3, while the red ones are from Step 4. When the z is initially set to three or 4, $(z, A/\mathcal{H}_{total})$ moves to the points in which both the confirmation latency and the hash-rate ratio decrease, and finally converges to the point (2, 0.024). Note that the decrease in the hash-rate ratio implies the increase in the total hash rate. When the initial value of z is set to 5, on the contrary, no transition occurs. In this case, the confirmation latency of $z = 5$ is large for users, causing that users leave the blockchain service. This also decreases the number of miners to join the mining competition.

Supplementary Appendix Figure 2B shows the equilibrium state transitions when $B = 0$ and $C_M = 3.8 \times 10^{-12}$. In this figure, the initial value of z is 2. We observe that $(z, A/\mathcal{H}_{total})$ moves to the points in which both elements increase and diverge. This implies that if mining cost is high, miners will not join the mining competition and the confirmation latency is required to be increased to prevent from malicious miner's attack. This results in a large transaction-confirmation time, making the number of users joining the blockchain service small.

Supplementary Appendix Figure 2C shows the equilibrium state transitions when $B = 12.5$ and $C_M = 1.5 \times 10^{-12}$. We observe in this figure that any initial value of z greater than or equal to two induces in the convergence point (2, 0.018). This is because of high amount of newly issued coins B. In this situation, there exist a certain number of miners who are incentivized with newly issued coins regardless of the total fees.

Supplementary Appendix Figure 2D illustrates the equilibrium state transitions when $B = 12.5$ and $C_M = 3.8 \times 10^{-12}$. In this case, interestingly, we observe four convergence points of $(z, A/\mathcal{H}_{total})$. Note that when initial value of z is smaller than or equal to three, $(z, A/\mathcal{H}_{total})$ converges to (3,0.057). When the initial value of z is four or 5, the value of z for the convergence point is the same as the initial value.

When the initial value of z is greater than 5, $(z, A/\mathcal{H}_{total})$ converges to the convergence point (10, 0.18). This is because of the high mining cost of C_M. Consider the case of the initial value of z equal to seven for instance. There are some miners who are incentivized with the newly issued coins B. However, due to the high mining cost of C_M, there are a certain number of the miners who decide to leave the mining competition. This makes the confirmation latency z large. The convergence point (10, 0.18) is also a situation where all users no longer submit transactions due to the large confirmation latency $z = 10$.

5.3 Impact of newly issued coins

Comparing Supplementary Appendix Figure 2A, C, when the initial confirmation latency is 6, the total hash rate $\mathcal{H}_{total}$ continues to increase and converge to a stable equilibrium point when the newly issued coin is 12.5 [BTC] (Supplementary Appendix Figure 2C). When the newly issued coin decreases to 0 [BTC] (Supplementary Appendix Figure 2A), on the other hand, the fraction of the hash rate of malicious miners $A/\mathcal{H}_{total}$ is too large and there is no confirmation latency that can reduce the probability of success of a double spending attack below 0.001.

Comparing Figures 2B,D, when the newly issued coin is 12.5 [BTC] (Supplementary Appendix Figure 2D), $A/\mathcal{H}_{total}$ converges to one of four stable equilibrium points. On the other hand, when the newly issued coins decrease to 0 [BTC] (Supplementary Appendix Figure 2B), the total hash rate decreases and the confirmation latency continues to increase, regardless of the initial confirmation latency.

These results imply that the decrease of newly issued coins significantly causes security issues such as selfish mining and double spending attack. Supplementary Appendix Figure 2A suggests that if the mining cost is small, setting a small confirmation latency is effective to prevent these security problems. However, we observe from Supplementary Appendix Figure 2B that in case of a large mining cost, adjusting the confirmation latency cannot work well against the security issues. More careful investigation is needed for clarifying the relation between the incentive mechanism and security issues.

6 Conclusion

In this paper, we developed a blockchain model that describes the interaction between user decisions and miner ones, taking into account the transaction fees, mining costs, newly issued coins, minimum entrance fee, and security. In numerical results, we investigated the relationship between minimum entrance fee that miners set to increase reward and user's waiting cost. We found that the minimum entrance fee decreases linearly with respect to waiting costs.

In our proposed model, we implicitly assumed that transactions sent by users immediately arrive at miners. If transactions arrive at miners with large delay, the resulting transaction-confirmation time increases. Note that users cannot identify what causes the large transaction-confirmation time. If the transmission delay is smaller than the block-generation time, users are likely to pay high fee for sending transactions. If the transmission delay is larger than the block-generation time, on the contrary, users find that high-fee payment is not effective for reducing the transaction-confirmation time, being discouraged from sending transactions.

In terms of the decision making for miners, the utility function for miners does not include some heterogeneity factors that capture changes in miners' situation. We need to refine the cost function of miners in which changes in miners' situation are capture in a realistic sense.

Recently, the Bitcoin mining is conducted by several mining pools, and hence mining pool selection for miners is also an important incentive mechanism issue. For future work, we develop our mathematical model to the one in which mining pool selection is taken into consideration.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

Funding

The research in Sections 3 and 4 was supported in part by Japan Society for the Promotion of Science under Grant-in-Aid for Scientific Research A) No. 19H01103, and Grant-in-Aid for Challenging Research (Exploratory) No. 22K19776. The research in Section 5 was supported in part by the joint project of Kyoto University and Toyota Motor Corporation, titled Advanced Mathematical Science for Mobility Society.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher’s note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fbloc.2023.1067628/full#supplementary-material

References

Altman, E., Menasché, D., Reiffers-Masson, A., Datar, M., Dhamal, S., Touati, C., et al. (2020). Blockchain competition between miners: A game theoretic perspective. *Front. Blockchain* 2, 26. doi:10.3389/fbloc.2019.00026

Basu, S., Easley, D., O’Hara, M., and Sirer, E. (2019). Towards a functional fee market for cryptocurrencies. *SSRN Electron. J.* doi:10.2139/ssrn.3318327

Capponi, A., Olafsson, S., and Alsabah, H. (2021). Proof-of-work cryptocurrencies: Does mining technology undermine decentralization? *SSRN Electron. J.* doi:10.2139/ssrn.3869144

Chatterjee, K., Goharshady, A. K., Ibsen-Jensen, R., and Velner, Y. (2018). Ergodic mean-payoff games for the analysis of attacks in crypto-currencies. arXiv preprint arXiv: 1806. doi:10.48550/ARXIV.1806.03108

Chiu, J., and Koeppl, T. V. (2017). The economics of cryptocurrencies bitcoin and beyond. *SSRN Electron. J.* doi:10.2139/ssrn.3048124

Goffard, P. O. (2019). Fraud risk assessment within blockchain transactions. *Adv. Appl. Probab.* 51, 443–467. doi:10.1017/apr.2019.18

He, J., Zhang, G., Zhang, J., and Zhang, R. (2020). An economic model of blockchain: The interplay between transaction fees and security. *SSRN Electron. J.* doi:10.2139/ssrn.3616869

Huberman, G., Leshno, J. D., and Moallemi, C. C. (2017). Monopoly without a monopolist: An economic analysis of the bitcoin payment system. *Rev. Econ. Stud.* 88, 3011–3040. doi:10.2139/ssrn.3025604

Kasahara, S., and Kawahara, J. (2019). Effect of bitcoin fee on transaction-confirmation process. *J. Industrial Manag. Optim.* 15, 365–386. doi:10.3934/jimo.2018047

Kawase, Y., and Kasahara, S. (2018). “A batch-service queueing system with general input and its application to analysis of mining process for bitcoin blockchain,” in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July 2018 - 03 August 2018 (IEEE), 1440–1447. doi:10.1109/Cybermatics_2018.2018.00245

Kawase, Y., and Kasahara, S. (2020). Priority queueing analysis of transaction-confirmation time for bitcoin. *J. Industrial Manag. Optim.* 16, 1077–1098. doi:10.3934/jimo.2018193

Kawase, Y., and Kasahara, S. (2017). “Transaction-confirmation time for bitcoin: A queueing analytical approach to blockchain mechanism,” in *Queueing Theory and Network Applications*. Editor W. Yue, Q.-L. Li, S. Jin, and Z. Ma (Cham: Springer International Publishing), 75–88. doi:10.1007/978-3-319-68520-5_5

Kleinrock, L. (1975). *Queueing Systems Volume I: Theory*. Wiley-Interscience.

Lavi, R., Sattath, O., and Zohar, A. (2022). Redesigning bitcoin’s fee market. *ACM Trans. Econ. Comput.* 10, 1–31. doi:10.1145/3530799

Li, Q. L., Ma, J. Y., and Chang, Y. X. (2018). “Blockchain queue theory,” in *Computational data and social networks* (Springer International Publishing). doi:10.1007/978-3-030-04648-4_3

Ma, J., Gans, J. S., and Tourky, R. (2018). Market structure in bitcoin mining. *SSRN Electron. J.* doi:10.2139/ssrn.3103104

Möser, M., and Böhme, R. (2015). “Trends, tips, tolls: A longitudinal study of bitcoin transaction fees,” in *Financial cryptography and data security* (Berlin Heidelberg: Springer), 19–33. doi:10.1007/978-3-662-48051-9_2

Pagnotta, E. (2018). Bitcoin as decentralized money: Prices, mining rewards, and network security. *SSRN Electron. J.* doi:10.2139/ssrn.3264448

Pagnotta, E., and Buraschi, A. (2018). An equilibrium valuation of bitcoin and decentralized network assets. *SSRN Electron. J.* doi:10.2139/ssrn.3142022

Prat, J., and Walter, B. (2018). An equilibrium model of the market for bitcoin mining. *J. Political Econ.* 129, 3143410. doi:10.2139/ssrn.3143410

Rosenfeld, M. (2014). Analysis of hashrate-based double spending. arXiv preprint arXiv: 1402. doi:10.48550/ARXIV.1402.2009

Wang, L., and Liu, Y. (2015). “Exploring miner evolution in bitcoin network,” in *Passive and Active Measurement*. Editor J. Mirkovic and Y. Liu (Cham: Springer International Publishing), 290–302.

Yan, G., Wang, S., Yang, Z., and Zhou, Y. (2020). Dynamic game model for ranking bitcoin transactions under gsp mechanism. *IEEE Access* 8, 109198–109206. doi:10.1109/access.2020.3001157

Yao, A. C. (2020). “An incentive analysis of some bitcoin fee designs (invited talk),” in *47th international colloquium on automata, languages, and programming, ICALP 2020, july 8-11, 2020, saarbrücken, Germany (virtual conference)*. Editors A. Czumaj, A. Dawar, and E. Merelli (Schloss Dagstuhl: Leibniz-Zentrum Informatik). doi:10.4230/LIPIcs.ICALP.2020.1