An Equilibrium Model of Blockchain-Based Cryptocurrencies [*]

Engin Iyidogan [†]

This version: December 2018
The latest version available here

Abstract

This paper develops an equilibrium model of proof-of-work cryptocurrencies. Equilibrium behaviour of miners and users are characterized for exogenous blockchain protocol metrics. This paper shows that an equilibrium can be achieved in the long run. High fixed mining reward is the reason of instability in current cryptocurrency designs. The equilibrium model has two main implications. First, decentralization and technological improvement in mining are the drivers of low transaction fees and low mining costs. Second, limited block size and mining difficulty, which is endogenously determined, create an incentive mechanism that achieves the sustainability of cryptocurrency in the long run.

JEL Classification: D47, D58, G10, G29

Keywords: Blockchain, Bitcoin, Market Design, General Equilibrium

[*]I am thankful to Franklin Allen, Patrick Bolton, Oleg Chuprinin (discussant), Rustam Ibragimov, Marcin Kacperczyk, Mete Kilic, Andrei Kirilenko, Jan Lukas Korella (discussant), Robert Kosowski, Savitar Sundaresan, and Katrin Tinn for insightful discussions and comments; and as well as seminar and conference participants at Imperial College Business School, Australasian Banking and Finance Conference at UNSW, Developments in Entrepreneurial Finance Workshop at EMLyon, Crowdinvesting Symposium at Max Planck Institute for Innovation and Competition, IFZ FinTech Colloquium, and PhD Symposium at Imperial College London. I acknowledge funding from the Centre for Global Finance and Technology, Brevan Howard Centre for Financial Analysis, and the President's PhD Scholarship Scheme at the Imperial College Business School. All errors are my own.

[†]Imperial College Business School, email: e.iyidogan14@ic.ac.uk

1 Introduction

Blockchain-based cryptocurrencies have become recently popular because of their unorthodox mechanism for securing transactions and decentralizing the payment environment. Despite its enormous potential relevance for practitioners and academics, the literature is still silent about the long term prospects of the cryptocurrency ecosystem. This paper develops a novel equilibrium model of the proof-of-work (PoW) cryptocurrencies to show that an equilibrium can exist and be determined uniquely.[1] In the light of the equilibrium model, I show that higher decentralization and high level of technology in mining allow the cryptocurrency environment to be in a "low mining cost and low transaction fee" regime. I also show that mining difficulty and constraints on the block size give rise to an incentive mechanism that ensures the sustainability of the cryptocurrency.

The model works as follows. There are two agents: miners and users. Users send their transactions onto the blockchain network and attach a fee to each transaction. The proposed transactions by users are collected in a pool of transactions. The transactions wait in the pool until they are added into the blockchain by miners. Miners are responsible for securely writing proposed transactions into a block and adding the block to the blockchain.[2] Miners select and combine transactions to solve a mathematical puzzle to mine a block.[3] To solve the puzzle, miners need computational power.[4] I model the computational power as a function of the unit cost of mining and the level of technology in mining. One can simply think of computational power as an output of a production function, whose inputs are the cost of mining and the level of technology.

Miners compete with one another to solve the puzzle first and are assumed not to coordinate. Once the puzzle is solved they add the mined block to the blockchain. Successful miners are rewarded with the sum of transaction fees from the transactions they added into the block. This amount is called "mining reward". In my model, miners face an exogenous

[1] The PoW consensus algorithm was first introduced by Dwork and Naor (1992) and used by Jakobsson and Juels (1999). The PoW is a consensus algorithm that requires computational work from system verifiers. The computational work generally requires to solve a mathematical puzzle. This paper uses the concept of Bitcoin-type PoW, with periodically adjusted difficulty of the mathematical puzzle. Section 3 explains the PoW consensus algorithm more in detail.

[2] A "block" is a file that contains transactions.

[3] A mathematical puzzle requires miners to find the right combination of transactions and the parameters. They change the parameters in every trial to solve the puzzle. The process of solving a puzzle is called "mining". This puzzle is also named as "mining puzzle".

[4] "Computational power" of a miner is measured by the hash rate the miner produces. Hash rate is the computing speed of a miner. Throughout this paper, I use hash rate and computational power interchangeably.

block size constraint, where a block can include only a limited number of transactions.[5] Hence, miners include transactions with the highest fees into a block in order to maximize their expected mining reward. As a result, transactions with lower fees wait longer in the transaction pools compared to transactions with higher fees. In sum, the block size constraint creates variation in the settlement delay of transactions.

In my model, four factors determine the settlement delay of a transaction. First, the settlement delay is inversely related to the transaction fee, because miners select transactions with higher fees. Second, a higher rate of high-fee transaction flow increases the settlement delay due to congestion. Third, the distribution of transaction fees affects the settlement delay. For instance, the settlement of an average-fee transaction is longer under a left-skewed fee distribution compared to a right-skewed one. The fourth factor is the number of blocks mined per unit of time.

This paper models the number of blocks mined per unit of time as a function of the total computational power of miners and the mining puzzle difficulty. The difficulty level is proportional to the total computational power of miners in the previous mining period. I define a mining period as the time between two consecutive mining difficulty adjustments. Mining difficulty is adjusted after a fixed number of blocks, set in the blockchain protocol, is mined.[6] The intuition works as follows. If the period of mining is shorter (longer) than the pre-set duration of mining a block, the difficulty level increases (decreases) to keep the length of mining period constant at the pre-set level.[7]

Miners derive utility from the mining reward and disutility from the cost of mining. Users derive utility from settling their transaction on the blockchain. Users derive disutility from the transaction fee and the settlement delay of the transaction. My model introduces the unit cost of delay represents the impatience of users with respect to settlement of transactions.

Miners and users interact through the settlement delay of a transaction. This interaction between miners and users creates an incentive mechanism that helps to characterize the equilibrium. This incentive mechanism can be explained as follows. A user pays a higher transaction fee to settle the transaction faster. Higher transaction fees incentivize a miner

[5] In most cryptocurrencies, a block has a limited memory size capacity. The memory size of a Bitcoin block can be at most 1MB, which corresponds to nearly 2000 transactions.

[6] For example, Bitcoin adjusts the difficulty after 2016 blocks are mined. This number varies among the cryptocurrencies.

[7] The pre-set length of mining period is 14 days for 2016 blocks in Bitcoin protocol.

to increase computational power that results in greater probability of mining the next block successfully and receiving the higher mining reward. When total computational power increases, a user is disincentivized to pay higher transaction fees because the frequency of mining a block increases, and the settlement delay of a transaction decreases respectively. Users choose their optimal transaction fee and miners choose their computational power under this incentive mechanism setting.

Equilibrium is characterized by N homogeneous miners and a continuum of users. The optimal transaction fee and the optimal mining cost per miner are a function of the number of miners, the previous period's computational power, the level of technology, the unit cost of delay, and the rate of transaction flow. Equilibrium does exist and the optimal decision of agents is uniquely determined.

I further extend my model to understand the equilibrium behaviour of miners and users in the existence of a fixed mining reward. I rewrite the mining reward such that successful miners receive a fixed mining reward for each block they mine in addition to the sum of transaction fees. I show that equilibrium exists when the fixed mining reward is lower than a threshold that is a function of model parameters. This extension is crucial to understand current cryptocurrency environment. Major PoW cryptocurrencies currently provide a fixed mining reward to the successful miners; however, their protocol is designed to reduce the fixed mining reward to zero in the long run.[8] My analysis suggests that such long-run behaviour is necessary for the survival of PoW cryptocurrencies, as current fixed mining rewards are higher than the threshold that is the upper bound for equilibrium existence. A consequent implication of my model is that dynamic updating of the fixed mining reward can achieve a stable equilibrium.

Finally, the comparative statics of my model shed light on the current discussions about the future of the PoW cryptocurrency ecosystem. First, the model predicts that a high level of decentralization and a high level of technology in mining are key conditions for low transaction fees and low mining costs in the long run. I define high level of decentralization as higher number of non-coordinating miners. Second, the model also predicts that higher mining difficulty, more limited block size, and higher unit costs of delay incentivize miners to increase computational power and users to pay higher transaction fees.

[8]For example, Bitcoin protocol halves the fixed reward nearly every 4 years and the fixed reward is expected to be zero by the end of 2100. For cryptocurrencies that follow a limited money supply model, the fixed mining reward is reduced over time and, in the long run, these cryptocurrencies start to follow the equilibrium model specified in this paper.

This insight about unit cost of delay can be applied to understand user and miner behaviour during the volatile episodes in the cryptocurrency market. In such episodes, users prefer a lower settlement delay to avoid adverse price changes. Hence, they are willing to pay a higher fee to accelerate transactions. Higher fees incentivize miners to increase their hash power. A prominent example of such an episode is the turmoil in the cryptocurrency market at the end of 2017, a period of high price volatility and increasing demand in the market. Both transaction fees and marginal computational power increased during this episode.

The remainder of the paper is outlined as follows. Section 2 reviews the related literature. Section 3 lays out the basics of blockchain and explains how mining works under the PoW algorithm. Section 4 defines the model and characterizes the equilibrium. Section 5 provides comparative statics and numerical analysis of the equilibrium model. Section 6 discusses the implications of the equilibrium model in real life and provides an interpretation of a critical episode in the cryptocurrency market. Section 7 concludes the paper.

2 Related Literature

An excessive literature studies blockchain and cryptocurrency in computer science and is growing in economics and finance. In this section, I first introduce how the literature is evolving on the financial side of blockchain applications. Then I provide an overview of the studies on transaction fee analysis and mining decisions. I show how my paper completes a gap in the literature. The section is finalized by an analysis of some papers from the computer science literature that relate to my paper.

Blockchain technology has caught the attention of both practitioners and academics in the area of finance in recent years. Yermack (2017) presents how blockchain technology and its applications lead to changes in corporate governance. Catalini and Gans (2016) focus on the positive effects of blockchain technology that have led to cost reductions through easy verification and strong network channels. Harvey (2016) provides an overview of cryptofinance and its application in the financial market. Abadi and Brunnermeier (2018) work on ledger competition in blockchain systems through comparing decentralized and centralized systems. Tinn (2017) shows that blockchain technology makes contracts more efficient. The author defines the conditions that make a contract optimal in a blockchain environment. Malinova and Park (2017) argue that the welfare of investors changes when investors choose transparency through blockchain technology. Pagnotta and Buraschi (2018) drive the price

of Bitcoin through network security and user demand. Prat and Walter (2018) preditcs the hash power of Bitcoin by using Bitcoin exchange rate. Chiu and Koeppl (2018) provide a crypto-token price formula that uses platform productivity, user adoption, and user heterogeneity. The theoretical paper of Biais et al. (2018) focuses on the equilibrium setting among miners in case of a predecided hard fork.

My model focuses on the equilibrium behaviour of miners and users in the long run such that miners are only awarded with the sum of the transaction fees they settle. The transaction fee decision of users is analysed using queuing theory, and this idea is also implemented by recent papers to analyse the optimal user decisions in the PoW cryptocurrencies. In particular, Huberman et al. (2017) focus on the optimality of the transaction fee decisions of Bitcoin users and show that congestion is needed to raise revenue. Easley et al. (2017) propose that the number of miners is bounded by transaction fees and the user inclusion is the source of equilibrium in the blockchain environment. Both paper focuses on competitive market of miners, but my paper studies imperfectly competitive market of miners. Li et al. (2018) design a Markovian batch-queuing system that expresses the block creation process in PoW cryptocurrencies. They show that the transaction confirmation time, transaction in the queue, and the block capacity are the sources of a stable system. Chiu and Koeppl (2018) work on a similar problem in a blockchain-based settlement setting. Their paper suggests that the feasibility of such systems depends on the block creation time and block size to generate fees to finance miners. The results of my paper are in line with the findings of these papers on the optimal transaction fee under an exogenously determined mining cost structure. My work focuses on an equilibrium model, with mining difficulty, which is endogenously determined, and settlement delay. The optimal mining cost and the optimal transaction fees are determined as a result of two-sided incentive mechanism.

Kroll et al. (2013) present the first prominent work on mining strategies. They consider mining incentives as a function of the global cost of mining, the individual cost of mining, a fixed mining reward, and an outside option of miners. Their analysis does not capture the effect of transaction fees, while my paper focuses on the long-run where the only source of mining reward becomes the sum of transaction fees. Teo (2015) analyses the decision of miners whether to mine individually, to join a mining pool, or not to mine at all when a fixed mining reward is offered. The author does not include the effect of mining difficulty and transaction fees for the mining strategy, while my model includes these variables to understand equilibrium decisions completely. Houy (2014) analyses how the number of

transactions added into the block affect the strategy of miners under the assumption that each miner is working on a specific set of transactions. The higher technology and high transaction levels rule out their results such that blocks are mined nearly in full capacity now.

Studies also focus on whether cryptocurrency ecosystem can exist without a fixed reward. Kaskaloglu (2014) proposes that transaction fees increase over time because of the volatile exchange rate of Bitcoin against fiat currencies and the adaptation of Bitcoin. This paper suggests that the long-term stability of Bitcoin is achievable under its current design. On the other hand, Carlsten et al. (2016) suggest that Bitcoin has an unstable structure and cannot be successful in the long run without a fixed mining reward. My paper shows that a long-run equilibrium can be achieved without a fixed mining reward or when the fixed mining reward is less than a certain threshold.

The computer science and cryptography literature are extensive, so my focus is narrowed on the works that directly relate to this paper. Eyal et al. (2016) propose a scalable blockchain protocol for Bitcoin, Bitcoin-NG(New Generation), with newly defined metrics. My paper assumes that consensus delay and network latency are infinitely small compared with the block creation time, so the model fits well with both traditional and proposed Bitcoin frameworks. Another assumption of my paper, that selfish mining is not allowed, is supported by the findings of Badertscher et al. (2018). They show that PoW cryptocurrencies are attack-payoff secure under the current transaction fee regime because miners are not incentivized to selfish mining.[9] On the other hand, Saleh (2018) works on the sustainability of Proof-of-Stake (PoS) systems in an equilibrium setting. Although my paper focuses on PoW cryptocurrencies only, it is interesting to analyse equilibrium behaviours of other cryptocurrencies to fully understand the dynamics of the cryptocurrency market in the future.

3 Blockchain Basics

3.1 How Does Blockchain Work?

A blockchain is a mathematically secured and sequential digital database that links data blocks using cryptography.[10] Haber and Stornetta (1990) first proposed the method of stor-

[9]The term “attack-payoff secure” is defined as a “no coordinated incentive” to deviate from the protocol.

[10]The first legislative definition of blockchain technology was made in a proposed bill amendment in Vermont as "mathematically secured, chronological, and decentralized consensus ledger or database, whether

ing data in a sequenced series. They suggested securely timestamping a document and linking this document to the next one in line to ensure the continuum of the database. The security of the system would be ensured through one-way hash function.[11] The hash value of a timestamped document is calculated and it is included in the input of next document. This process ensures that documents are connected to each other through their unique hash values. In addition to the idea of securely connecting the documents in a chronological order, Haber and Stornetta (1990) proposed distributing the chain of documents to all participants in the system. Having multiple copies of a chain mitigates the risk of a "single point of failure". The idea of distributing linked chains is now widely known as a "distributed ledger technology". Bitcoin is the first implementation of this technology to record real-life transactions inside documents.

Blockchain systems can store any type of data from the medical records of patients to worldwide carbon-trading activities. Nakamoto (2008) designed Bitcoin, the first blockchain-based cryptocurrency, to store transactions.[12] In the model of Haber and Stornetta (1990), a central authority is responsible for converting the raw data in documents into a hash value. Doing so makes the blockchain system open to a single point of failure in case of any wrongdoing or failure at the central system. Nakamoto (2008) modelled a decentralized system that allows all participants of the blockchain network to verify transactions and some participants to compete to solve a mathematical puzzle to create the next block for a set of transactions. Each block contains three key elements: hash values of transactions, a timestamp, and the hash value of the previous block. Each block refers to the previous block, that is, the parent block. If block X uses the hash value of block $X-1$ in its mining calculation, block $X-1$ becomes the parent of block X. This ensures a cryptographically secure distributed ledger. Any change in block $X-1$ completely changes the hash value of X.

The process of creating a new block is called mining, and competing participants are called miners. After mining a block, a successful miner broadcasts the newly mined block

maintained via Internet interaction, peer-to-peer network, or otherwise" (Balint (2016)).

[11] One-way hash function maps an alphanumerical input to a fixed-length alphanumeric string. In this function, the recovery of the raw data from the output is not feasibly possible.

[12] Bitcoin only stores transactions in the blockchain. Users have a key for their individual addresses, and the balances are calculated by tracing back all transactions (in-out) to the specific address. Ethereum is another blockchain-based cryptocurrency platform, which launched in 2015, and is designed to perform other functions, such as running smart contracts (Wood (2014)). Ethereum also provides a virtual machine to end users to reach and use these smart contracts.

and waits for the consensus of other miners and nodes. If consensus is achieved among the majority of blockchain miners, the mined block is added into the blockchain. The mining process starts again for the next block.

In most cryptocurrencies, successful miners are rewarded with a predetermined fixed reward and the sum of transaction fees from the transactions they added into the block. The source of fixed rewards are the tokens, or coins, of the digital currencies. These tokens are created each time a block is mined and allocated to the successful miners. The amount of fixed mining reward varies by the different digital currencies.[13]

3.2 How to Mine a Block?

The mining process explained in this section is based on the Bitcoin protocol. The mining process is the same as the one used by Litecoin and Bitcoin Cash but differs by the parameters used. Ethereum and Ethereum Classic have a similar mining design but have additional parameters to consider.

I first explain how a transaction is processed in a PoW cryptocurrency. A transaction is sending an amount of a cryptocurrency from one account to another. Sender and receiver accounts must have a valid address. The transactions are added to the transaction pools after verified.[14] Each miner can have its own transaction pool, and the transactions in two transaction pools may vary because of network latency.[15] The transaction pools are continuously updated. Adding one transaction to the pool does not guarantee that this transaction is added into any block. Hence, transactions in the memory pools can be described as proposed transactions.

Miners choose which transactions they add into their block from the memory pool. After choosing transactions, miners combine hash values of transactions and some other parameters together to obtain a block hash. The required parameters are the hash value of the previous block, the Merkle root, the timestamp, the bits, and the nonce. The hash value of

[13] In Bitcoin, successful miners currently receive 12.5 Bitcoin (BTC) per block mined, and the reward halves every 4 years to control the supply of Bitcoin and for inflation over time. Bitcoin issues coins to successful miners only. Ethereum allocates their coins, Ether (ETH), to both successful miners and the miners who mine valid blocks yet fail in the consensus. Those blocks are called "uncle blocks." This mechanism aims to prevent centralization and lead small miners to compete with others.

[14] In Bitcoin, transaction pools are called "memory pools". Throughout this paper, both term can be used interchangeably.

[15] A network latency, in this concept, is a measure of how much time it takes to broadcast transactions into the different transaction pools.

the previous block is included in the calculation to ensure an unbroken chain structure in the blockchain. The Merkle root is the merged hash value of all transactions included in the block. The nonce is the value that miners add into the merged hash value of other parameters to obtain the hash value of a block. The hash value of a block should satisfy certain requirements. Miners try to find a hash value that satisfies this requirement by changing the nonce value. This process is called solving the mining puzzle.

The cryptographic puzzle requires that the hash value of a new block be lower than a threshold hash value, which is determined by the current difficulty level of the blockchain. The difficulty level is global for the blockchain network, and it ensures that the total number of blocks mined per certain period of time stays same. The process of updating the difficulty level differs between various protocols. In the Bitcoin protocol, the difficulty level is adjusted after every 2016 blocks. The aim is to keep the duration of mining 2016 blocks constant, two weeks.[16] If 2016 blocks are mined shorter (longer) than two weeks, then the protocol increases (decreases) the difficulty proportionally, to keep the block creation rate in the preset level, which is 10 minutes per block.

In the mining process, after deciding which transactions are included in block puzzle, a miner tries every possible nonce value, timestamp, and free choice parameter combinations to find an acceptable hash value. This process is called brute force search. Computational power is mainly required during the application of brute force search.

Miners face various constraints, while choosing the transactions under the limitation of the block size in most blockchain-based platforms.[17] The main determinant of memory size of each transaction is the number of input and output coins used in the transaction. The memory size of a transaction is not proportional to the amount of money sent. Until recently, another constraint that miners faced was the priority of transactions. However, the priority effect became negligible over time, notably in the last few years.

4 Model

This section describes a model of PoW cryptocurrency, the optimal behaviour of miners and users, and their equilibrium behaviour. This section shows that miners and users can reach

[16]The same protocol with different parameters also holds for Litecoin and Bitcoin Cash. Ethereum checks the difficulty level after each block and adjusts the difficulty to keep the block creation frequency between 10-19 seconds.

[17]Bitcoin block size had been fixed to 1 MB for a long time, but discussions regarding block size is still ongoing. Ethereum platform implies a continuous limit on the block size that is updated dynamically.

an equilibrium under certain conditions. Finally, the section provides the equilibrium analysis in the existence of fixed mining reward.

4.1 Model Setup

My model has two types of agents: users and miners. Users, indexed by j and are infinitesimal, broadcast their transactions into the memory pools, and transactions wait in the memory pool until they are included in a block. Each user decides how much fee, $f_j \geq 0$, to add into a transaction. Fees are in units of coin. The memory size of the transactions is the same for all users and is measured in bytes. The transaction fee affects the settlement duration of the transaction because of the limited block size constraint. In particular, transactions with a higher fee-to-memory-size ratio are prioritised by miners to be added into the next available block. The next section details the settlement delay of a transaction.[18]

Miners, indexed by i, $i = 1,2,...,N$, are responsible for adding blocks to the blockchain. Miners are rewarded with the sum of fees of transactions that they added into the block. There is no fixed reward for mining. All miners access the same memory pool.[19] Miners decide which transactions to include into the next block. The main constraint of a miner is the limited memory size of a block, or the transaction capacity. The transaction capacity of a block is exogenously determined in the blockchain protocol. Therefore, miners prefer transactions with a higher transaction-fee-to-memory-size ratio in order to maximize their total reward.

Miners solve a mining puzzle. The transactions included in a block do not affect the probability of solving calculations.[20] The length of the transaction selection process is infinitely shorter compared to the application of brute force to solve the mining puzzle. Therefore, the number of transactions included in a block does not affect the probability of solving the puzzle first. Brute force calculation for previous block puzzle has no effect on current block puzzle.

[18] In this model, a transaction is considered to be settled if it is successfully included in a block. However, some merchants or exchanges accept a transaction if a certain number of block is added to the blockchain after the transaction is included in the blockchain. The aim is to prevent any double spending attempt in real life. For example, a merchant may accept a transaction if six more blocks mined after the block that transaction is included into the blockchain.

[19] In practice, transactions are different between various memory pools, and each miner works on different transactions. Network latency determines how fast a memory pool updates. Even though transaction-picking strategies of the miners are the same, the probability of finding a block is determined by the hash rate.

[20] Different transaction combinations create a different Merkle root. The probability of solving the puzzle is independent of the Merkle root.

Following these constraints and the main objective of the miners, the best response of a miner to maximize her total reward is to sort all available transactions with respect to their fee-to-size ratios. A miner would then choose the maximum number of transactions from the top of the list, while satisfying the limited block size constraint. Successful miners, those who solve mathematical puzzle and whose block added into the main chain after consensus, earn

$$F = \sum_{j=1}^{M} f_j, \tag{1}$$

where M is the maximum number of transactions that a block can contain. In other words, this is the transaction capacity of a block. I assume that memory pools always contain more than M transactions. Other miners who find a valid block that is not accepted into the main chain do not receive a mining reward. Only successful miners are rewarded.[21]

The model is set in unevenly spaced mining periods. A mining period starts with a change in the global mining difficulty. Difficulty is adjusted after K number of blocks mined. K is exogenously determined in the blockchain protocol, and it is the number of blocks need to be mined to adjust difficulty. In other words, after K blocks mined in period $t-1$, difficulty is adjusted from d_{t-1} to d_t, and a new period t starts. Difficulty is adjusted to keep the duration of mining a block constant. The theoretical duration of mining a block is also exogenous, and it is ω.[22] Difficulty is calculated as a function of the previous period's difficulty and the length of the previous period.

$$d_t = d_{t-1} \frac{K\omega}{\Delta_{t-1}}, \tag{2}$$

where Δ_{t-1} is the length of time period $t-1$. The length of a mining period is a function of current period total hash rate, $H_{I,t}$, previous period total hash rate, $H_{I,t-1}$, and K:

$$\Delta_t = \frac{H_{I,t-1}}{H_{I,t}} K\omega, \tag{3}$$

[21] Ethereum pays a certain amount of fixed reward to miners who successfully mine a valid block yet are not included in the main chain. The underlying idea is to incentivize small miners and prevent the system from centralization over time (Wood, 2014).

[22] As mentioned before, this rate is 10 minutes for Bitcoin and 15–17 seconds for Ethereum.

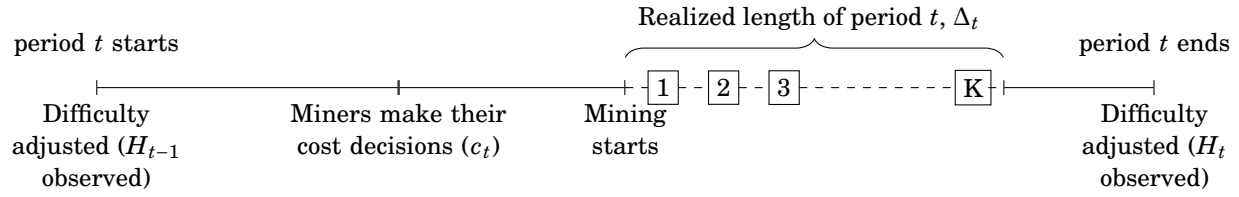

Figure 1: Timeline of Mining

and the average duration of mining a block in period t becomes

$$\omega_t = \frac{H_{I,t-1}}{H_{I,t}}\omega. \tag{4}$$

The hash rate is a unit of processing power per unit of time. Each miner has a hash power, $h_{i,t}$, and the total hash rate in the blockchain is the sum of the hash rate in that period:

$$H_{I,t} = \sum_i h_{i,t}. \tag{5}$$

If total hash power increases, the probability of solving a mining puzzle per unit of time increases as well. It eventually reduces the length of time spent mining a block for that period. Therefore, the average duration of mining a block is scaled by a higher total hash rate. The total hash rate at period $t-1$ determines the mining difficulty in period t and effectively the average duration of mining a block in period t.

Miners make their hash rate decision at the beginning of each period t. Miners cannot adjust their hash rate during the same period. The mining cost includes the cost of equipment, the electricity cost, and the operating cost. The unit of cost is the coin per unit of time. Miners do not pay any entry cost. Figure 1 shows the time span of the mining period.

4.2 Transaction Delay and Optimal Fee

This subsection characterizes the fee decision of users and works on how the transaction fee distribution in the memory pool affects the optimal fee decision of each user. Each user broadcasts one transaction at each period t. For simplicity, I use subscript j interchangeably such that user j broadcasts transaction j. Users derive utility from the settlement of transactions into the blockchain, $\theta_{j,t} \geq 0$. The sources of positive utility may vary and its specification is beyond the scope of this paper. In this model, $\theta_{j,t}$ is exogenously given. Users derive disutility from the settlement delay of the transaction, $\tau_{j,t}$, and transaction fee, $f_{j,t}$.

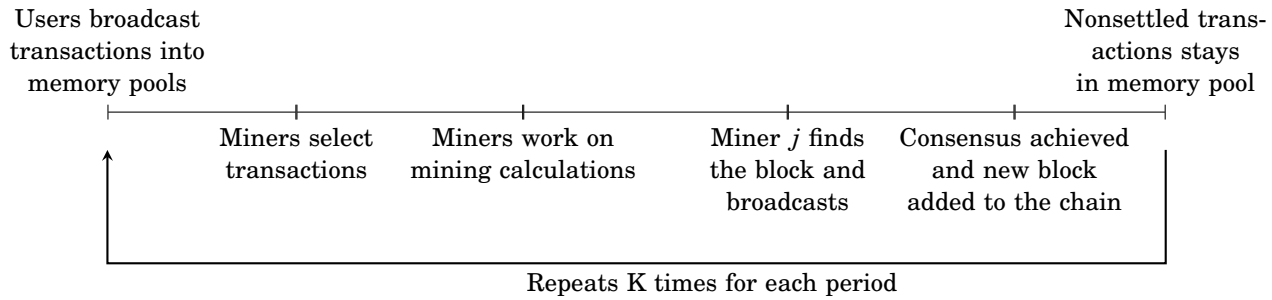

Figure 2: Timeline of Block Creation (Queuing Game)

The utility function can be summarized as

$$U_{j,t} = \theta_{j,t} - f_{j,t} - a_j \tau_{j,t}, \tag{6}$$

where a_j is the cost of settlement delay for user j and $a_j > 0$.

The settlement delay of a transaction is measured by stochastic priority queueing. The queueing game in the PoW cryptocurrencies proceeds as follows. Users send their transactions into the transaction pool with the rate of λ_t. Each transaction is sent with a transaction fee, $f_j \geq 0$. Miners queue all transactions with respect to fees. Miners can include at most M transactions in their mining calculation because of the limited transaction capacity of each block that is pre-determined in the blockchain protocol. After miners the transactions, they combine these transactions together to solve a mathematical puzzle. Miners apply brute force calculation to solve this puzzle. When the first miner solves the puzzle, she broadcasts the successful next block to obtain consensus from the other miners. The model assumes that consensus is immediately achieved. After consensus is achieved, the successful block is added to the chain of blocks, in other words blockchain. After a block is added into the blockchain, all non-settled transactions, along with newly arriving transactions, queue again for the next mining calculation. Miners start the mining calculation with the available transactions waiting in the queue. The game repeats for each block in every period, which is equal to K times per period. Figure 2 shows the timeline of the queuing game.[23]

The next step measures the settlement delay for a transaction with fee $f_{j,t}$ at period t.

[23] In the blockchain environment, memory pools are more frequently updated, and transactions not settled for a long time are dropped from memory pools. Some economic nodes even put a threshold expiry time and automatically drop transactions from memory pools.

Transactions arrive in the memory pool with a rate of λ_t such that λ number of transactions arrive per unit block time, ω. The transaction arrival rate stays constant over period t. $G(.)$ is the equilibrium distribution function of the transaction fees, whose support is $[0, \bar{f}]$. $\bar{f}$ represents the highest fee paid for a transaction at period t and $0 < \bar{f} \leq \infty$. $G(.)$ is strictly increasing and continuous. Blocks are mined with the rate of ω_t as find in equation (4). According to queuing theory (Little (1961) and Kleinrock (1975)), the settlement delay of a transaction with fee $f_{j,t}$ follows:

$$\tau_{j,t} = \begin{cases} \dfrac{\omega_t}{1-\rho_t(1-G(f_{j,t}))} & \text{if } 0 \leq \rho_t(1-G(f_{j,t})) < 1 \quad \text{and} \quad K\rho_t(1-G(f_{j,t})) > 1 \\ \infty & \text{if } \rho_t(1-G(f_{j,t})) \geq 1 \qquad \text{or} \quad K\rho_t(1-G(f_{j,t})) \leq 1, \end{cases} \tag{7}$$

where

$$\rho_t = (\lambda_t \omega_t)/M$$

is called the utilization factor of the system. $\rho_t(1-G(f_{j,t}))$ is the utilization factor of transaction $f_{j,t}$, in a given $G(.)$ set. This term can be called an adjusted utilization factor. The second multiplier of the adjusted utilization factor, $1-G(f_{j,t})$, is the proportion of transactions that propose fees higher than $f_{j,t}$, in other words, transactions with a higher priority.

If the adjusted utilization factor is equal to zero, the settlement delay would be equal to the block creation duration, $\tau_{j,t} = \omega_t$. This factor is zero only for $G(f_{j,t}) = 1$, which implies that user j pays the highest fee in period t, and her transaction will be the first in line. Hence, the expected waiting time is equal to the block creation frequency of period t.

Transaction j cannot be settled in two cases and drops from the memory pool at the end of the mining period t. First, if the adjusted utilization factor is greater than or equal to unity for transaction j, $\rho_t(1-G(f_{j,t})) > 1$, miners do not add transaction j into their block calculation, because M transactions with a higher transaction fee always will be in the memory pool. Second, if the settlement delay of transaction j is greater than the duration of period t, $\Delta_t > \omega_t(\rho_t(1-G(f_{j,t})))^{-1}$, transaction j drops from the memory pool at the end of period t, so the settlement delay would be infinite. Therefore, I concentrate on transactions that ensure both $0 \leq \rho_t(1-G(f_{j,t})) < 1$ and $K\rho_t(1-G(f_{j,t})) > 1$.

Equation (7) states that settlement delay is a function of average block creation frequency and adjusted utilization factor. When there are fewer transactions with a higher fee

than $f_{j,t}$, the adjusted utilization factor of transaction j becomes close to zero. Less competition among transactions drives the settlement delay to lower values. In contrast, when the adjusted utilization factor of transaction j is close to 1, the length of the queue would be longer compared to the previous case. Hence, this factor is a proxy of congestion for transaction j. Huberman et al. (2017) model the behaviour of users in a similar way. They use the congestion queuing game approach for batch system arrivals and users with different delay costs.

I can now calculate the optimal transaction fee for users. For tractability, let transaction fees be uniformly distributed on the interval $[0, \bar{f}_t]$ for $\bar{f}_t < \infty$ under some equilibrium for the distributions of θ_j and a_j. The model assumes that the equilibrium distribution of fees stay uniform, but it allows a change in parameters, such as f_t. The equilibrium cumulative distribution function follows $G(f_{j,t}) = \frac{f_{j,t}}{\bar{f}_t}$ with boundary conditions of $G(0) = 0$ and $G(\bar{f}_t) = 1$. Definition of the settlement delay and the utility function yield the optimal transaction fee for user j:

$$f^*_{j,t} = \left(\frac{M a_{j,t} \bar{f}_t}{\lambda_t}\right)^{0.5} - \frac{M \bar{f}_t}{\lambda_t \omega_t} + \bar{f}_t. \tag{8}$$

Appendix A.2 provides detailed calculations and necessary conditions for the optimal transaction fee. I show the explicit solution for the general case in which transaction fees are not distributed uniformly. Uniform distribution satisfies the optimal conditions.

Equation (8) states that the optimal transaction fee increases with the highest transaction fee paid between users in that period, the unit cost of delay of user j, and the average block creation duration in period t. The highest transaction fee paid between users in that period, $\bar{f}_t$, represents the higher competition, because more users are willing to pay higher fees to be settled earlier. In this case, the optimal transaction fee for user j increases until $U(f^*_{j,t}) = 0$. The unit cost of delay of a user represents the patience of the user, and higher $a_{j,t}$ implies higher $f^*_{j,t}$ to maximize utility. The average block creation frequency depends on the cost decision of miners. If the average block mining frequency becomes longer, the optimal fee for user j increases until $U(f^*_{i,t}) = 0$. It is worth stressing that equation (8) only holds for the condition of positive user utility, $U(f^*_{j,t}) \geq 0$. Otherwise, a user prefers not to make a transaction on the blockchain. Section 4.4 details how transaction fees incentivize miners to reduce block creation frequency.

4.3 Optimal Mining Cost

This subsection characterizes the value maximization problem of miners and finds the optimal cost for miners. Miner i decides how much computational power generates at period t according to the following cost function at period t. The hash rate of the miner i, $h_{i,t}$, is the unit of computational power.

$$\left(\frac{h_{i,t}}{A_{i,t}}\right)^{\sigma_{i,t}} = c_{i,t}, \tag{9}$$

where $c_{i,t}$ is the cost of mining per unit of time and A_t is the the level of technology in mining at period t. The unit of time is the hypothetical block mining duration, ω, in this setting. $\sigma_{i,t}$ is the elasticity of cost with respect to the hash rate for miner i. I scale $\sigma_{i,t}$ to be greater than unity. Technology is a nondecreasing function of time, $A_t \geq A_{t-1}$. The interpretation of this model choice is that miners produce higher hash rates with lower cost over time. The assumption $\sigma > 1$ implies that miners cannot produce computational power without any friction. This assumption brings the model close to real-life mining.[24]

Miners compete with each one another to mine the next block in the blockchain. The probability of mining a block by miner i is proportional to her hash rate, $h_{i,t}$. Hence, the probability of mining the next available block for miner i in a blockchain is

$$Pr(h_i, H_I) = \frac{h_i}{h_i + \sum_{j \neq i} h_j} = \frac{h_i}{H_I}, \tag{10}$$

where H_I denotes the total hash rate of the blockchain. In other words, this is the sum of hash rates of all miners mining in the blockchain. Miners are risk-neutral profit maximizers, and they decide their own hash rate to maximize their profit per unit of time. Expected total earning of miner i at period t is as follows:

$$Pr(h_{i,t}, H_{I,t}) KF_t = \frac{h_{i,t}}{H_{I,t}} KF_t, \tag{11}$$

where F_t represents expected earnings per block during period t. This formula is the multiplication of probability of mining a block at period t for miner i and the expected total

[24]The mining cost is the sum of machinery, electricity, cooling down, shipping cost, and broadband costs. The main driver of computational power is machinery and electricity cost. This model only focuses on cost per unit of time without a cost breakdown.

transaction fee. Hence, miner maximize the following profit function:

$$V_{i,t} = \frac{\frac{h_{i,t}}{H_{I,t}} K F_t}{\Delta_t} - c_{i,t}, \tag{12}$$

where Δ_t defined in equation (3) and represents the length of period t. The interpretation of the profit function of miner is as follows. The first term is the total amount of transaction fees earned per unit of time at period t. It is found by dividing the expected sum of transaction fee earnings per period by the period's duration. The second term is the cost of mining per unit of time. The maximization problem can be simplified using the production function and the period's duration:

$$V_{i,t} = \frac{c_{i,t}^{1/\sigma_{i,t}} A_{i,t}}{H_{I,t-1}}, \frac{F_t}{\omega} - c_{i,t}$$

Following from miner's value function and using the first-order condition, the optimal cost of mining at period t becomes

$$c_{i,t}^* = \left(\frac{A_{i,t} F_t}{\omega H_{I,t-1} \sigma_{i,t}} \right)^{\frac{\sigma_{i,t}}{\sigma_{i,t}-1}}, \tag{13}$$

where the appropriate second-order condition, $\frac{\partial^2 V_{i,t}}{\partial c_{i,t}^2} < 0$, is satisfied for any $\sigma_{i,t} > 1$. Equation (13) only holds if the value function of miner i is nonnegative, $V_{i,t} \geq 0$.

4.4 Equilibrium between Miners and Users

This section addresses the equilibrium behaviour of miners and of users. The equilibrium is characterized by the relation between the cost decision of miners and the fee decision of users. To keep the model tractable, the equilibrium fee, f_t^* is defined for the pivotal user. Transaction fees in memory pools are uniformly distributed under some equilibrium. The pivotal user has a unit cost of delay of $a_{j,t} = a_t$ and utility of settlement $\theta_{j,t} = \theta_t$ such that the expected sum of transaction fees can be written as follows:

$$F_t^* = M f_t^*. \tag{14}$$

The equilibrium cost, c_t^*, is defined for N homogeneous miners with the same rate of access to the technology in mining, $A_{i,t} = A_t$. The definition of homogeneous miners implies that miners have the same elasticity rate from cost to hash rate, $\sigma_{i,t} = \sigma_t$. The problem is similar to the one introduced by Orda et al. (1993) and Rosen (1965) under symmetrical miners with the same maximization objective. The concavity of the utility function of miners implies a unique symmetric Nash equilibrium, and all miners choose the same hash rate, $h_{i,t}^* = h_t^*$, to mine the next block. The total hash rate of the system becomes

$$H_{I,t}^* = N h_t^* = N(c_t^*)^{1/\sigma_t}(A_t). \tag{15}$$

To complete the description of equilibrium, I specify the optimal transaction fee and the optimal mining cost. Substituting the total hash value into equilibrium yields the following optimal transaction fee, which is paid by the pivotal user:

$$f_t^* = K_1 - K_2 N (c_t^*)^{\frac{1}{\sigma_t}}, \tag{16}$$

where

$$K_1 = \left(\frac{a_t \bar{f}_t M}{\lambda_t}\right)^{0.5} + \bar{f}_t,$$
$$K_2 = \frac{\bar{f}_t M A_t}{\lambda_t \omega H_{I,t-1}}.$$

Substituting the expected total transaction fee into equilibrium yields the following optimal mining cost for each miner:

$$c_t^* = (K_3 f_t^*)^{\frac{\sigma_t}{\sigma_t - 1}}, \tag{17}$$

where

$$K_3 = \frac{\lambda_t}{\bar{f}_t \sigma_t} K_2.$$

These results are summarized in the following proposition.

Proposition 1. *i) The equilibrium transaction fee paid by the pivotal user solves the follow-*

ing equation and it is unique:

$$f_t^* + K_2(K_3)^{\frac{1}{\sigma_t - 1}} N (f_t^*)^{\frac{1}{\sigma_t - 1}} - K_1 = 0. \tag{18}$$

ii) The equilibrium mining cost incurred by each homogeneous miner solves the following equation, and it is unique:

$$(c_t^*)^{\frac{\sigma_t - 1}{\sigma_t}} + K_2 K_3 N (c_t^*)^{\frac{1}{\sigma_t}} - K_1 K_3 = 0. \tag{19}$$

Proposition 1 states that miners and users can reach equilibrium for given long-run conditions. The final form of equations is the immediate result of solving equations (16) and (17) together. The appendix proves the uniqueness and existence of an optimal transaction fee and the equilibrium mining cost.

4.5 Extension of Fixed Reward

So far, the model includes transaction fees as the only source of a mining reward. Most cryptocurrencies are currently providing a fixed reward to miners for each successfully mined block. The reward scheme may differ by cryptocurrencies. Section 3.2 explains the main structure in more detail. This subsection focuses on how a fixed reward affects the equilibrium behaviour of miners and users.

Recall the value function of miners and include a fixed reward, R, in the total expected earning per block as

$$V_{i,t} = \frac{c_{i,t}^{1/\sigma_{i,t}} A_{i,t}}{H_{I,t-1}} \frac{(F_t + R)}{\omega} - c_{i,t},$$

and, also, recall the corresponding optimal mining cost:

$$c_{i,t}^* = \left(\frac{A_{i,t}(F_t + R)}{\omega H_{I,t-1} \sigma_{i,t}} \right)^{\frac{\sigma_{i,t}}{\sigma_{i,t} - 1}}.$$

In this case, the optimal mining cost in equilibrium becomes

$$c_t^* = (K_3 f_t^* + \frac{K_3 R}{M})^{\frac{\sigma_t}{\sigma_t - 1}}.$$

Notice that a fixed reward incentivizes miners to mine in the blockchain even without transaction fees. Therefore, in the existence of a fixed reward, users may opt out to pay any transaction fee because the transaction fee they pay would not create enough incentive for miners. Hence, an equilibrium transaction fee solves the following equation:

$$f_t^* + K_2 N (K_3 f_t^* + \frac{K_3 R}{M})^{\frac{1}{\sigma_t - 1}} - K_1 = 0.$$

if and only if the following condition holds:

$$R \leq \big(\frac{K_1}{K_2 N}\big)^{\sigma_t - 1} \frac{M}{K_3}. \tag{20}$$

These results are summarized in the following proposition.

Proposition 2. *Users and miners can reach equilibrium in the existence of a fixed reward if and only if the fixed reward is less than or equal to a threshold level, $\bar{R}$. $\bar{R}$ is written as*

$$\bar{R} = \big(\frac{K_1}{K_2 N}\big)^{\sigma_t - 1} \frac{M}{K_3}. \tag{21}$$

The appendix provides the proof of the proposition. Proposition 2 states that a fixed reward in mining creates an incentive for miners, yet it makes the system unstable after a certain threshold. The fixed reward changes the cost decision of miners, and, as a result, the frequency of mining a block in that period. If the fixed reward is above a certain threshold, optimal transaction fees are not enough to incentivize miners to mine the block faster to increase block creation frequency. In this case, miners are only incentivized by fixed rewards, and the optimal mining fee for the pivotal user goes to zero.

5 Model Analysis

This section provides comparative statics of the model to explain how equilibrium behaviours change with model parameters and their importance for cryptocurrencies environment. The main parameters of interests are the level of technology in mining, the number of miners, previous period hash-rate, and the unit cost of delay. To this end, I summarize the impacts of these parameters under two significant concepts: (1) the low transaction fee and low mining cost regime in a cryptocurrency environment, and (2) a stronger incentive mechanism that ensure the sustainability of a PoW cryptocurrency. The section ends with a numerical analysis.

5.1 Low Transaction Fee - Low Mining Cost Regime

This part discusses how low transaction fee and low mining cost per miner can be achieved in an equilibrium setting. I begin with the following proposition, which characterizes the effect of the level of technology on the individual mining cost and transaction fees.

Proposition 3. *f_t^* decreases with A_t. c_t^* decreases with A_t if $K_1 < 2K_3N(c_t^*)^{\frac{1}{\sigma}}$ and, otherwise, increases with A_t.*

The appendix details the proof of the proposition. The first statement of Proposition 3 relates the level of technology to the optimal transaction fees paid by the pivotal user. Improved technology enables miners to increase their hash rate at a lower mining cost. The total hash rate Nc_t^* increases in equilibrium, and the average block creation duration lessens, which increases the tendency of users to pay fewer transaction fees to incentivize miners.

While the total hash rate increases with the level of technology, the optimal mining cost per miner depends on the condition stated in the second part of Proposition 3. As the level of technology increases the mining incentive to compete, the high number of miners in the blockchain reduces the individual mining incentive to compete. The left-hand side and the right-hand side of the condition represents how the Nash equilibrium setting affects the utility of individual miners. The direction of inequality is mainly driven by the number of miners, N. If the number of miners increases, the optimal cost of mining decreases with the level of technology.

A higher number of miners are already reducing the optimal mining cost under the conditions satisfied in the second part of Proposition 3. The following result describes the effect of the number of total miners on the equilibrium mining cost and transaction fees.

Proposition 4. *f_t^* and c_t^* decreases with N under equilibrium.*

The appendix provides the proof of the proposition. In principle, the number of miners affect the Nash equilibrium strategy of miners, where all miners are homogeneous in their elasticity of production function σ and have the same access to the technology A_t. A higher number of miners or mining pools in practice reduces the earning share for each miner, and, hence, the best response of individual miners is to reduce the mining cost.

Even though the optimal mining cost per miner decreases over time, the total hash rate increases, because an increase in N is faster in number than the decrease in the individual mining cost, c_t^*. A higher total hash rate increases the tendency of users to reduce their

optimal transaction fees. This result, along with Proposition 3, implies that, under higher level of technology and a high number of miners, the equilibrium mining cost per miner decreases.

5.2 Sustainability of a PoW Cryptocurrency

In this paper, the sustainability of a cryptocurrency is described such that miners are incentivized to incur higher computational work and users are incentivized to pay higher fees. The first proposition shows that having difficulty in mining built into the cryptocurrency is necessary for sustainability. The equilibrium model captures the effect of difficulty with the previous period's hash rate, $H_{I,t-1}$.

Proposition 5. *f_t^* increases with $H_{I,t-1}$ until $V_t = 0$. c_t^* increases with $H_{I,t-1}$ if $K_1 < 2K_3N(c_t^*)^{\frac{1}{\sigma}}$ and, otherwise, decreases with $H_{I,t-1}$.*

The appendix provides the proof of Proposition 5. The first part of Proposition 5 states that the pivotal user increases his or her transaction fee when the previous period's total hash rate, $H_{I,t-1}$, was higher. The reason is to incentivize miners to increase their mining cost, c_t, to reduce block creation duration for period t, ω_t. When the total hash rate of period $t-1$ increases, the difficulty of the mathematical puzzle in period t adjusts accordingly, and the duration of the average block creation become longer. Miners are not willing to deviate from the decisions of the previous period or even reduce their mining cost if transaction fees stay the same over period t. Hence, users increase their transaction fees at period t to reduce the average block creation duration until $V_{i,t}$. The utility of users decreases, yet the incentive mechanism works in favour of sustainable cryptocurrency.

The second part of Proposition 5 states that if there is a high number of miners, or higher competition, the mining cost increases with the previous period's hash rate. The rationale of this finding is that the user's transaction fee provides enough incentive for competition. Otherwise, when the number of miners is less than a certain level, the transaction fee is not enough to incentivize miners to compete.

The next proposition explains how the unit cost of delay of the user affects the equilibrium behaviour of miners and of users. It is worth to note that fixed mining block size and the unit cost of delay are observationally equivalent in the sense that they give the same result in the comparative statics. Hence, I decided to use only one of them in the following

proposition to examine their effect on equilibrium decision of agents. I prefer to use the unit cost of delay because it has an empirical counterpart that changes dynamically over time.

Proposition 6. *f_t^* increases with a_t until $V_t = 0$, and c_t^* increases with a_t.*

Proposition 6 shows that higher unit cost of delay of the pivotal user lead to an increase in both equilibrium transaction fee paid and equilibrium mining cost per miner.

K_1 term is the source of increase in both terms and this term derives from the level of congestion in the transaction pools. Being that cryptocurrencies are still in the early adoption period, even under a high fixed mining reward regime, this effect can be seen during the volatile periods in the cryptocurrency market. Currently, most users in the cryptocurrency market are traders, either individual or institutional. These users prefer settling their transactions as soon as possible to avoid from any loss due to rapid price changes, which is represented by high a_t in my model. Hence, users increase the transaction fee. This incentivizes miners to put higher computational power to increase the chance of mining a block and receive corresponding higher mining reward.

This phenomenon can be seen from August 2017 to early January 2018 in the Bitcoin market. During this period, the daily volatility of the Bitcoin price was higher than average. The unit cost of delay in the market was high. As a result, transaction fees added into the transactions raised abruptly. The observable hash rate over also increased over 5 consecutive months without any significant change in the level of technology in mining.

5.3 Numerical Analysis

I conclude this section with numerical analysis. My aim is to illustrate how the optimal equilibrium decisions of miners and of users change with the variable of interests. The parametrization of variables is neither cryptocurrency specific nor particular to a design protocol.

For the sake of illustration, I keep the unit of block creation time equal to unity, $\omega = 1$. The unit of fee is coins. The unit of cost is coin per block creation time. I assume the transaction capacity of a block is 2,000, and the rate of transaction flow per unit of time is 2,300. The highest transaction fee paid is capped at 3 coin units, $\bar{f}_t = 3$. The number of miners represent the number of mining pools in real life. Figure 3 shows how the level of technology affects the equilibrium decision of miners and users. The results are in line with Proposition 3.

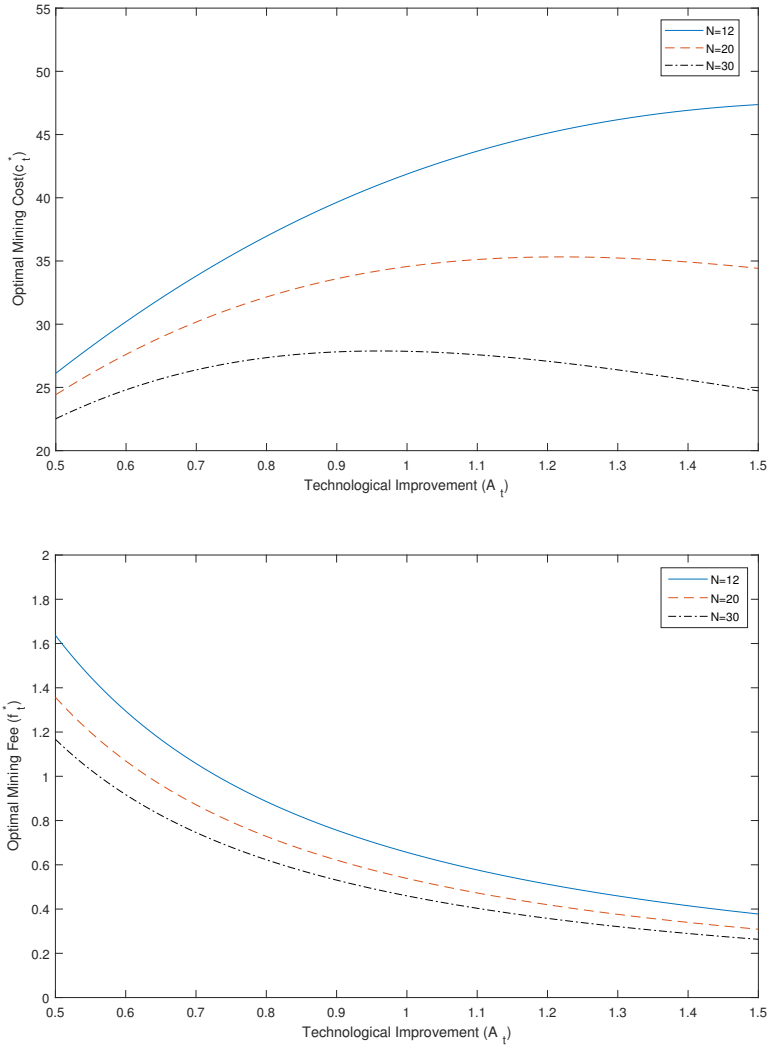

Figure 3: The upper figure shows the change in optimal mining cost per unit of time for each miner with the level of technology. The bottom figure shows the change in optimal transaction fee for users with the level of technology. $\alpha_t = 10$ and $H_{I,t-1} = 200$.

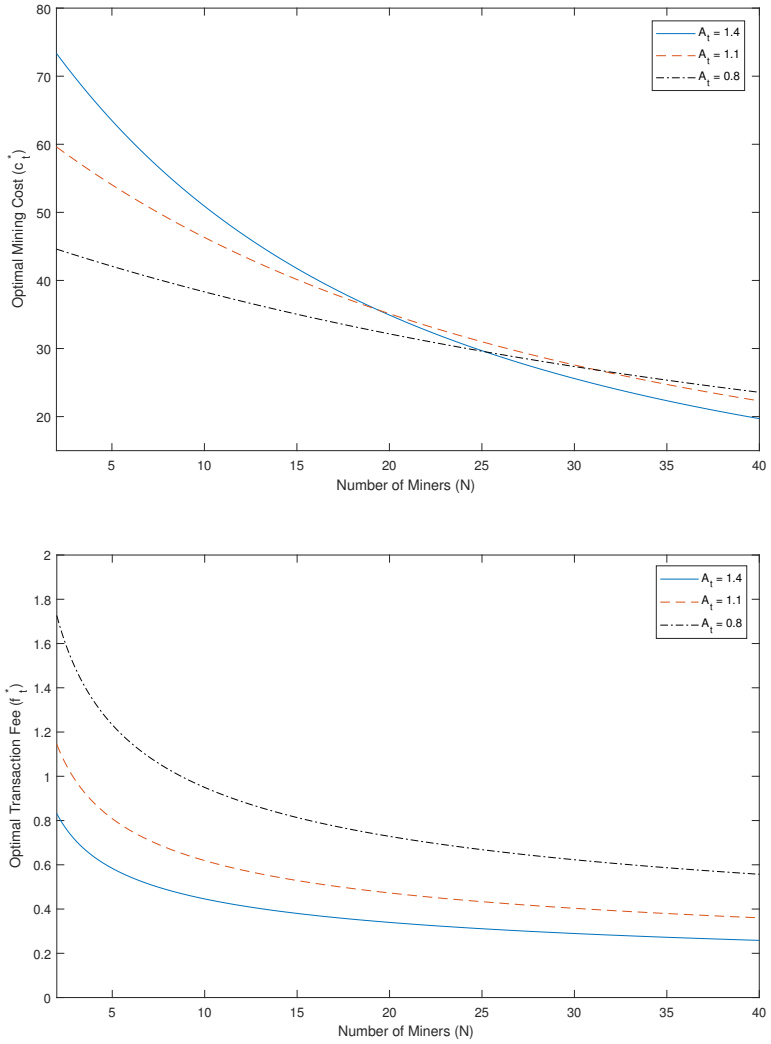

Figure 4: The upper figure shows the change in optimal mining cost per unit of time for each miner with a number of miners. The bottom figure shows the change in optimal transaction fee for each user with a number of miners. $\alpha_t = 10$ and $H_{I,t-1} = 200$.

Figure 4 shows that the number of miners reduce the optimal mining cost with higher level of technology, because each miner extracts less profit because of competition. The left graph of Figure 3 shows this effect. Figure 5 illustrates how the incentive mechanism is achieved under increasing unit cost of delay. If the settlement delay of users increase over time, optimal transaction fee increases to incentivize miners to reduce the average block creation duration, which reflects the Proposition 6. Miners compete with each other to receive higher rewards with increasing transaction fee and, as a result, optimal mining cost increases.

6 Discussion

In this section, I discuss two key points that relate the equilibrium model to real life. The first part focuses on the cryptocurrency design and the future of dominant cryptocurrencies in the market. The second part discusses the effects of sharp price movements on transaction fees in the context of the equilibrium model of this paper. The discussion in the second part uses the volatile price episode of cryptocurrencies in late 2017 as an empirical case study.

6.1 Implications of the Model

The equilibrium model provides a number of implications that can be useful in the cryptocurrency market and in future research. First, the model predicts that equilibrium cannot be reached with the existence of a high fixed mining reward. The rationale behind this finding is that a fixed mining reward already provides enough incentive to miners to mine faster. The amount of transaction fee required for an additional mining incentive makes user utility negative. The model in this paper assumes that the user base already exists. Without a user base, miners need to be incentivized with a fixed mining reward. The question here is: Does a fixed mining reward need to be dynamically updated? Bitcoin halves the fixed mining reward after 210,000 blocks mined, roughly a 104 mining period.[25] Ethereum does not put any cap on the circulated supply of coin, and, hence, the fixed mining reward does not change until the mining community changes the protocol. Monero, on the other hand, determines the fixed mining reward for each block by penalizing the reward if the

[25] In Bitcoin platform, the mining difficulty adjusted after 2016 blocks mined. My model defines mining period as the period between two consecutive mining difficulty adjustments. Hence, 210,000 blocks are mined in 210,000/2016 = 104.16 mining period.

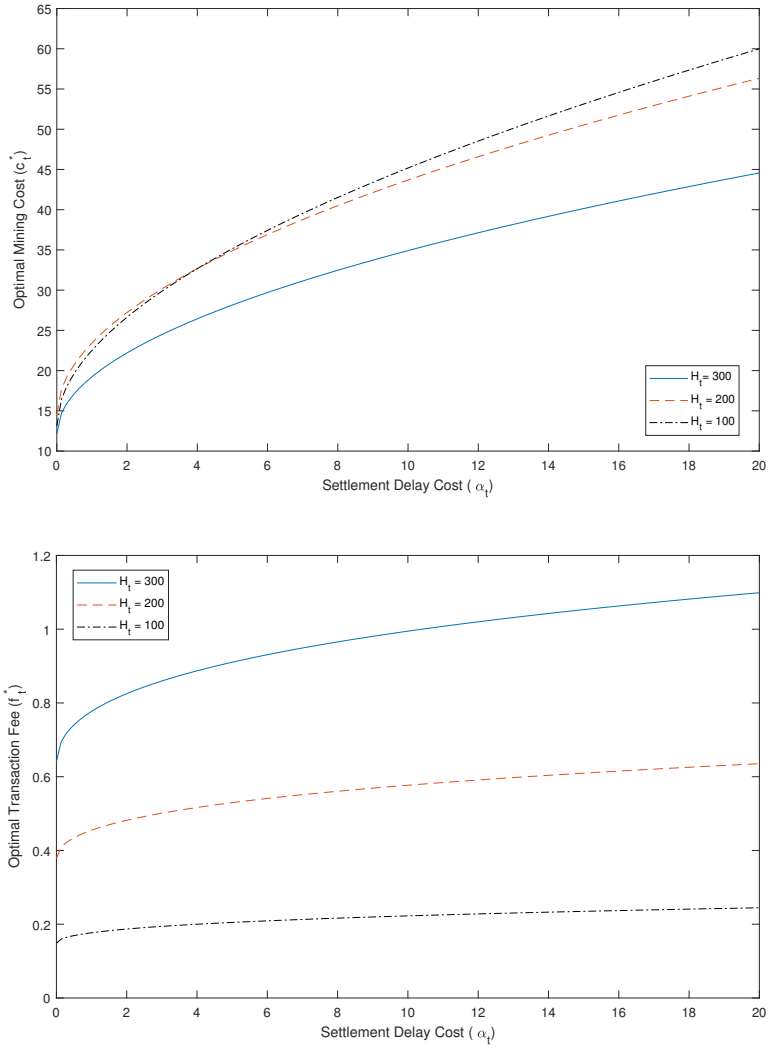

Figure 5: The upper figure shows the change in optimal mining cost per unit of time for each miner with different levels of unit cost of delay. The bottom figure shows the change in optimal transaction fee for users with different levels of unit cost of delay. $N = 12$ and $A_t = 1.1$.

block size passes a certain threshold. The result of Proposition 2 can be implemented in a newly proposed cryptocurrency. Instead of a fixed mining reward, the mining reward can be updated every mining period to achieve a sustainable incentive mechanism according to the threshold specified in the proposition.[26]

Second, the model shows that the level of technology in the production function reduces the optimal mining cost per miner when the number of competing miners is higher. Mining in a less competitive market reduces the positive impact of higher level of technology in the cost of mining per miner. Monopolistic or oligopolistic mining creates a less cost-efficient system. The results hold both for individual miners and mining pools. Even though the number of individual miners inside the mining pools varies, competition runs between the centralized mining pools. Hence, each mining pool can be seen as a single entity that competes for mining. Currently, 86% of blocks are mined by 10 major mining pools in Bitcoin, and 82% of blocks are mined by 8 major mining pools in Ethereum.[27] These numbers can be interpreted as being roughly 10 miners who compete to mine the next block in both dominant cryptocurrencies. To achieve higher cost-efficient systems, the number of mining pools should satisfy the condition in Proposition 3. The condition updates after each mining period theoretically, but the change is limited. Importantly, the same condition is the source of incentive mechanism that enables the sustainability of blockchain under high mining difficulty.

6.2 Interpretation of Late 2017 Episode

In this section, I discuss the decisions of miners and users during the volatile periods in the cryptocurrency market in the light of this paper's model findings. In my model, the unit cost of delay of a user determines how much the user suffer from the settlement delay. Proposition 6 shows that transaction fees are increasing with higher unit cost of delay. The unit cost of delay is mainly determined by two factors: the amount of money transferred and the volatility of exchange rate of corresponding crytocurrency. The model presented in this paper uses the unit of coins while presenting transaction fees and mining costs. In other

[26] One might find it difficult to implement in practice, because the number of miners, changes in the level of technology in mining, and σ_t cannot be easily detectable. These variables are included in the threshold equation of fixed reward. Further research is needed to estimate this parameter in a decentralized protocol.

[27] The data can be found in blockchain.com/en/pools for Bitcoin and investoon.com/charts/mining/eth for Ethereum. The hash rate distribution of mining pools is calculated as the ratio of the number of blocks mined by a mining pool to the total number of mined block for a given period of time.

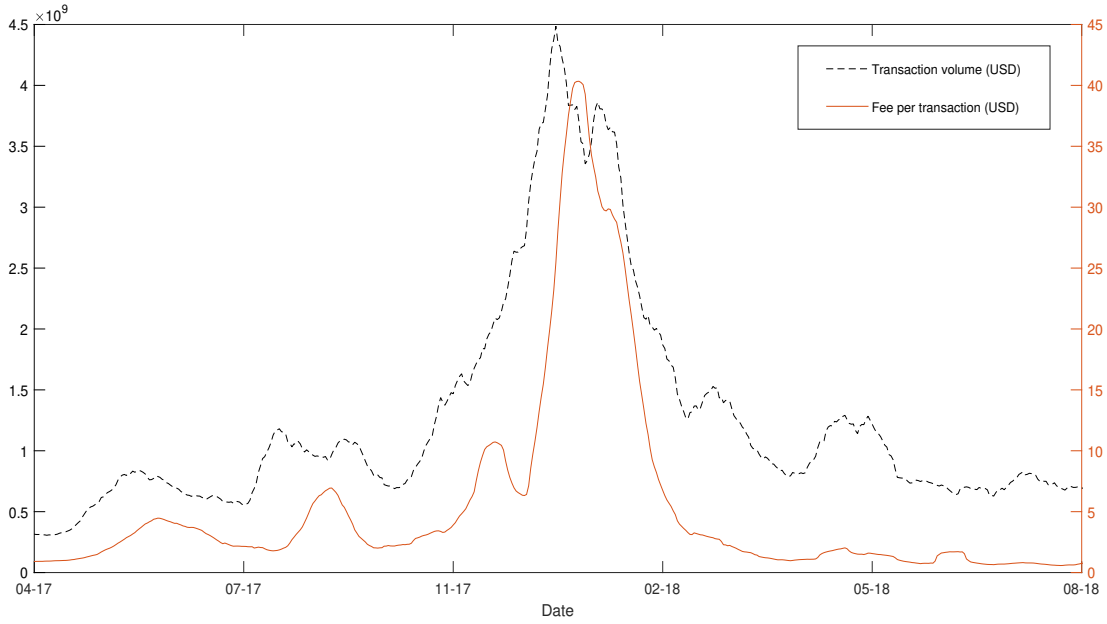

Figure 6: The left panel shows the daily transaction volume in USD in the Bitcoin platform. The right panel shows the average transaction fee per transaction in USD.

words, the model calculations do not include any exchange rate of a cryptocurrency to a fiat currency. However, fiat currencies are still dominating the currency market at the moment. Therefore, the exchange rate of cryptocurrencies also affect the behaviour of users.

To relate the results of model analysis to the current cryptocurrency market, I use data from Bitcoin platform. Figures 6 and 7 show that transaction fees paid per transaction are in line with the volatility of Bitcoin price and the average daily transaction volume. All variables are calculated for a 14-day moving average window.[28] Transaction fee per transaction increase with the daily transaction volume and the daily price volatility in late 2017. When the transaction volume and daily price volatility start to tumble in early 2018, transaction fees follow a downward trend as well.

During the same period, the number of transactions in the queue also peaked. The model can also explain the increase in transaction fees as a result of high transaction inflow, λ. High transaction inflow reduces the adjusted utility factor, $\rho(1-G(f))$, and the settlement delay increases as explained in Section 4.2. Miners choose the transactions with high

[28]The rationale is that the mining period for Bitcoin is close to 14 days. In Bitcoin protocol, $\omega = 10$ min and $K = 2016$. Hence, $\Delta = \omega K = 20160$ min $= 14$ days. Data are open source and can be obtained from blockchain.com

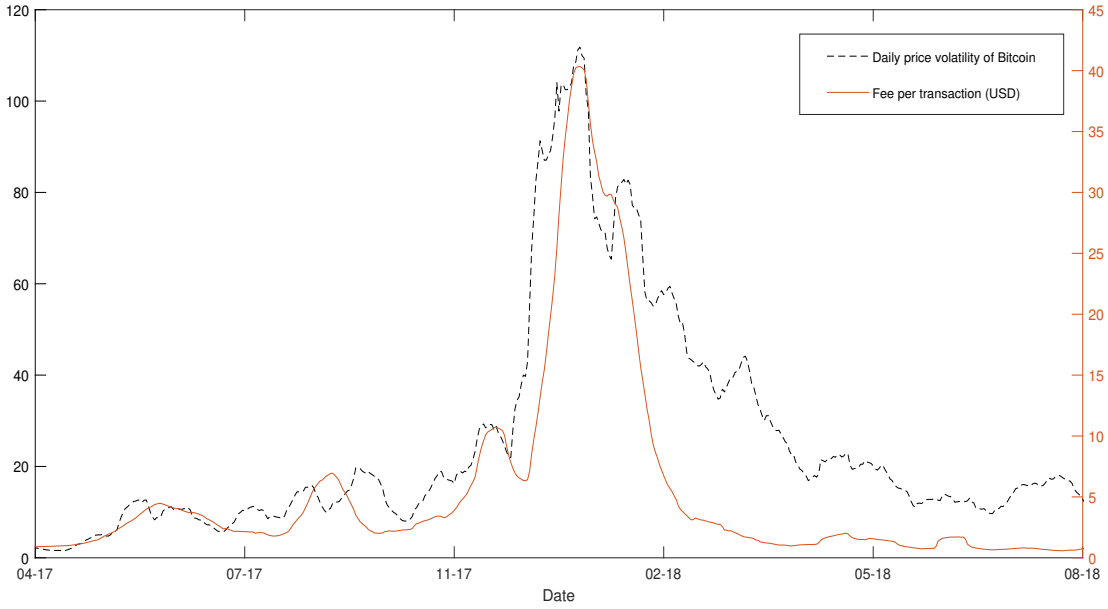

Figure 7: The left panel shows the daily volatility of BTC/USD exchange rate. The right panel shows the average transaction fee per transaction in USD.

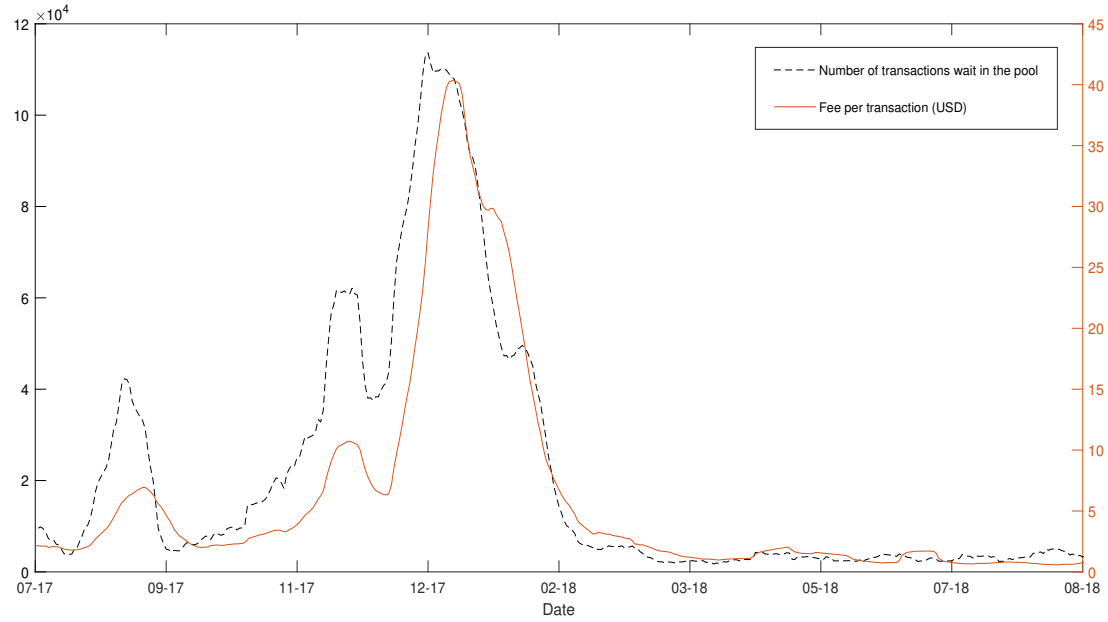

Figure 8: The left panel shows the average number of transactions that wait to be settled in the memory pool per day. The right panel shows the average transaction fee per transaction in USD. Both variables are calculated for 14-days moving average window.

transaction fees, and the transactions with low fees were removed from the mining pools over time. The settled transactions represent users with the high unit cost of delay, α. Figure 8 shows how transaction fee per transaction changed over time as the average number of transactions waiting in the memory pool per day changes.

7 Concluding Remarks

In this paper, I present a model of PoW cryptocurrencies to show that an equilibrium can be achieved in the long run. The key mechanism is that while miners incur the cost of mining to settle transactions securely, users incentivize them with proposed transaction fees. Equilibrium does not exist in a fixed-mining reward regime until the fixed reward is below some threshold.

The equilibrium has two main implications. First, high level of decentralization, with a large number of miners, and high level of technological improvements in mining reduce transaction fees and the mining cost per miner. Without decentralization, the high level of technology in mining have an adverse effect on the mining costs. Second, lower transaction capacity of a block and higher mining difficulty incentivize miners to invest more in computational power and users to pay higher transaction fees.

Starting from this study, further research can be conducted in the area of second layer protocols and their interaction with the decentralised payment systems. To my knowledge, the second layer protocols plan to create a decentralized environment among users and it would be interesting to explore the relative advantage of these systems in the future.

A Appendix

A.1 Transaction Fees and Mining Cost

Below, I extend the analysis to the general case in which transaction fees are not necessarily uniformly distributed over the period and the cumulative distribution function is strictly increasing. In this case, the optimal transaction fee must solve the following ordinary differential equation (ODE):

$$G(f_t^*) = \frac{\rho_t - 1 + (a_t \omega_t \rho_t G'(f_t^*))^{0.5}}{\rho_t}. \tag{22}$$

The second-order condition for local maximum,

$$\frac{\partial^2 U}{\partial f^2} = \frac{a_t \omega_t \big(\rho_t G''(f))(1-\rho_t(1-G(f))) - 2(\rho_t G'(f))^2\big)}{(1-\rho_t(1-G(f)))^3} < 0,$$

is satisfied for any $f \geq 0$ when the following conditions hold:

$$G''(f) \leq 0 \tag{23}$$

$$1-\rho_t(1-G(f)) > 0. \tag{24}$$

The existence of solution requires the concavity of the distribution of transaction fees. The uniform distribution function is also strictly increasing and satisfies $G''(f) \leq 0$. Hence, all these findings for the general case hold for the specific case, where transaction fees are uniformly distributed.

A.2 Proofs of Propositions

Proof of Proposition 1:
i) Define $y(f_t^*)$ such that

$$y(f_t^*) = f_t^* + K_2 (K_3)^{\frac{1}{\sigma_t - 1}} N(f_t^*)^{\frac{1}{\sigma_t - 1}} - K_1,$$

where the roots of this function are the equilibrium transaction fee. K_1, K_2, and K_3, which are defined in Section 4.4, are all positive. Clearly, $y(0) = -K_1 < 0$ and $\lim_{f_t^* \to \infty} y(f_t^*) = \infty > 0$. Also, $y(f_t^*)$ is a continuous function in the interval of $f_t^* = [0, \infty]$. By the intermediate value theorem, there is at least one strictly positive root. Because $y'(f_t^*) > 0$ for all f_t^* in this interval, only one unique strictly positive f_t^* exists.
ii) The proof is the same as the first part.

Proof of Proposition 2:
The proof is similar to the proof of Proposition 1. Redefine $y(f_t^*)$ with fixed reward included such that

$$y(f_t^*) = f_t^* + K_2 N(K_3 f_t^* + \frac{K_3 R}{M})^{\frac{1}{\sigma_t - 1}} - K_1,$$

which has at least one nonnegative root if $y(0) \leq 0$ because $\lim_{f_t^* \to \infty} y(f_t^*) = \infty > 0$ and

$y'(f_t^*) > 0$ for all $f_t^* > 0$. The largest fixed reward, $\bar{R}$, that satisfies $y(0) \leq 0$ is

$$R \leq \left(\frac{K_1}{K_2 N}\right)^{\sigma_t - 1} \frac{M}{K_3},$$

and the proof is completed.

Proof of Proposition 5:
I present the proof of Proposition 3 after the proof of Proposition 5. Before moving onto the proof, I show that $f_t^* > 0$, $c_t^* > 0$, $K_1 > 0$, $K_2 > 0$, and $K_3 > 0$. The first part of the proof starts by taking derivative of equation (18) with respect to $H_{I,t-1}$:

$$\frac{\partial f_t^*}{\partial H_{I,t-1}}\left(1 + \frac{1}{\sigma - 1}(f_t^*)^{\frac{2-\sigma}{\sigma-1}} N K_2 K_3^{\frac{1}{\sigma-1}}\right) = -\frac{\partial K_2}{\partial H_{I,t-1}}\left(K_3^{\frac{1}{\sigma-1}} N (f_t^*)^{\frac{1}{\sigma-1}}\right) - \frac{\partial K_3}{\partial H_{I,t-1}}\left(\frac{1}{\sigma-1} K_3^{\frac{1}{\sigma-1}} K_2 N (f_t^*)^{\frac{2-\sigma}{\sigma-1}}\right).$$

Because both $\frac{\partial K_2}{\partial H_{I,t-1}} < 0$ and $\frac{\partial K_3}{\partial H_{I,t-1}} < 0$, the right-hand side of the equation becomes less than zero. The term multiplied by $\frac{\partial f_t}{\partial H_{I,t-1}}$ is greater than zero followed by $\sigma \geq 0$. Hence, $\frac{\partial f_t}{\partial H_{I,t-1}} > 0$ completes the proof.
The second part of the proof uses the same chain rule to differentiate equation (19) with respect to $H_{I,t-1}$ to obtain

$$\frac{\partial c_t^*}{\partial H_{t-1}}\left(\frac{\sigma}{\sigma-1}(c_t^*)^{-\frac{1}{\sigma}} + \frac{1}{\sigma} K_2 K_3 N (c_t^*)^{\frac{1-\sigma}{\sigma}}\right) = -\frac{\partial K_3}{\partial H_{I,t-1}}\left(K_2 N (c_t^*)^{\frac{1}{\sigma}} - K_1\right) - \frac{\partial K_2}{\partial H_{I,t-1}}\left(K_3 N (c_t^*)^{\frac{1}{\sigma}}\right).$$

The term multiplied by $\frac{\partial c_t^*}{\partial H_{I,t-1}}$ is greater than zero, followed by $\sigma \geq 0$. Hence,

$$sgn\left[\frac{\partial c_t^*}{\partial H_{I,t-1}}\right] = sgn\left[-\frac{\partial K_3}{\partial H_{I,t-1}}\left(K_2 N (c_t^*)^{\frac{1}{\sigma}} - K_1\right) - \frac{\partial K_2}{\partial H_{I,t-1}}\left(K_3 N (c_t^*)^{\frac{1}{\sigma}}\right)\right],$$

where sgn represents the sign of the variable. The right-hand side simplifies to

$$sgn\left[\frac{A_t M}{\omega\sigma (H_{I,t-1})^2}\left(2K_3 N (c_t^*)^{\frac{1}{\sigma}} - K_1\right)\right] = sgn\left[2K_3 N (c_t^*)^{\frac{1}{\sigma}} - K_1\right],$$

because $\frac{A_t M}{\omega\sigma (H_{I,t-1})^2} > 0$. This completes the proof such that c_t^* is increasing function of H_{t-1} if $2K_3 N (c_t^*)^{\frac{1}{\sigma}} > K_1$ and decreasing function of H_{t-1} otherwise.

Proof of Proposition 3:

The proof is very similar to the proof of Proposition 5, because A_t only shows in K_2 and K_3, as $H_{I,t-1}$. The only difference is that $\frac{\partial K_2}{\partial A_t} > 0$ and $\frac{\partial K_3}{\partial A_t} > 0$. Therefore, the sign changes, $\frac{\partial f}{\partial A_t} < 0$.

The same holds for the second part of the proof. The sign of the condition reverses such that c_t^* increases if $2K_3 N (c_t^*)^{\frac{1}{\sigma}} < K_1$.

Proof of Proposition 4 :

Now observe that $\frac{\partial K_1}{\partial N} = \frac{\partial K_2}{\partial N} = \frac{\partial K_3}{\partial N} = 0$. Differentiating equation (18) with respect to N gives

$$\frac{\partial f_t^*}{\partial N}\left(1 + \frac{1}{\sigma - 1} K_2 K_3^{\frac{1}{\sigma-1}} N (f_t^*)^{\frac{2-\sigma}{\sigma-1}}\right) = -K_2 K_3^{\frac{1}{\sigma-1}} (f_t^*)^{\frac{1}{\sigma-1}},$$

and $\sigma > 1$ makes the term multiplied by $\frac{\partial f_t^*}{\partial N}$ positive. The left-hand side of the equation is always positive for $f_t^* > 0$. Therefore, $\frac{\partial f_t^*}{\partial N} < 0$.

The second part of the proof uses the result in the first part. Taking the derivative of (17) with respect to N gives

$$\frac{\partial c_t^*}{\partial N} = \frac{\sigma}{\sigma - 1} (c_t^*)^{\frac{1}{\sigma}} K_3 \frac{\partial f_t^*}{\partial N},$$

because $\sigma > 1$ and $c_t^* > 0$, and

$$sgn[\frac{\partial c_t^*}{\partial N}] = sgn[\frac{\partial f_t^*}{\partial N}]$$

completes the proof of $\frac{\partial c_t^*}{\partial N} < 0$, following the result of first part, $\frac{\partial f_t^*}{\partial N} < 0$.

Proof of Proposition 6 :

K_1 is a function of a_t, and $\frac{\partial K_1}{\partial a_t} > 0$. Differentiating equation (18) with respect to a_t gives

$$\frac{\partial f_t^*}{\partial a_t}\left(1 + \frac{1}{\sigma - 1} K_2 K_3^{\frac{1}{\sigma-1}} N (f_t^*)^{\frac{2-\sigma}{1-\sigma}}\right) = \frac{\partial K_1}{\partial a_t}.$$

Notice that the second multiplier of the left-hand side is always positive for $\sigma > 1$. Therefore,

$$sgn[\frac{\partial f_t^*}{\partial a_t}] = sgn[\frac{\partial K_1}{\partial a_t}]$$

and $\frac{\partial f_t^*}{\partial a_t} > 0$.
The proof of the second part directly follows from differentiating equation (17) with respect to a_t:

$$\frac{\partial c_t^*}{\partial a_t} = \frac{\sigma}{\sigma - 1}(c_t^*)^{\frac{1}{\sigma}} K_3 \frac{\partial f_t^*}{\partial a_t},$$

because $\sigma > 1$ and $c_t^* > 0$, and

$$sgn[\frac{\partial c_t^*}{\partial a_t}] = sgn[\frac{\partial f_t^*}{\partial a_t}]$$

completes the proof of $\frac{\partial c_t^*}{\partial a_t} > 0$, following the result of first part, $\frac{\partial f_t^*}{\partial a_t} > 0$.

References

Abadi, J., and Brunnermeier, M. (2018). *Blockchain Economics* (Tech. Rep.). Princeton University.

Badertscher, C., Garay, J., Maurer, U., Tschudi, D., and Zikas, V. (2018). But Why does it Work? A Rational Protocol Design Treatment of Bitcoin. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 34–65).

Balint, S. (2016). Sec. i.1. 12 v.s.a. code 1913. *Vermont State Legislator*, H.868.

Biais, B., Bisiere, C., Bouvard, M., and Casamatta, C. (2018). The Blockchain Folk Theorem. *Working Paper*.

Carlsten, M., Kalodner, H., Weinberg, S. M., and Narayanan, A. (2016). On the Instability of Bitcoin Without the Block Reward. In *Proceedings of the 2016 acm sigsac conference on computer and communications security* (pp. 154–167).

Catalini, C., and Gans, J. S. (2016). *Some Simple Economics of the Blockchain* (Tech. Rep.). National Bureau of Economic Research.

Chiu, J., and Koeppl, T. V. (2018). Blockchain-based Settlement for Asset Trading. *Working Paper*.

Dwork, C., and Naor, M. (1992). Pricing via Processing or Combatting Junk Mail. In *Annual international cryptology conference* (pp. 139–147).

Easley, D., O'Hara, M., and Basu, S. (2017). From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Working Paper*.

Eyal, I., Gencer, A. E., Sirer, E. G., and Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In *Nsdi* (pp. 45–59).

Eyal, I., and Sirer, E. G. (2014). Majority is not Enough: Bitcoin Mining is Vulnerable. In *International conference on financial cryptography and data security* (pp. 436–454).

Haber, S., and Stornetta, W. S. (1990). How to Time-stamp a Digital Document. In *Conference on the theory and application of cryptography* (pp. 437–455).

Harvey, C. (2016). Cryptofinance. *Working Paper*.

Houy, N. (2014). The Economics of Bitcoin Transaction Fees. *Working Paper*.

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

Jakobsson, M., and Juels, A. (1999). Proofs of Work and Bread Pudding Protocols. In *Secure information networks* (pp. 258–272). Springer.

Kaskaloglu, K. (2014). Near Zero Bitcoin Transaction Fees cannot Last Forever. In *The international conference on digital security and forensics (digitalsec2014)* (pp. 91–99).

Kleinrock, L. (1975). *Queueing Systems, volume 2: Computer Applications*. Wiley New York.

Kroll, J. A., Davey, I. C., and Felten, E. W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In *Proceedings of weis* (Vol. 2013).

Li, Q.-L., Ma, J.-Y., and Chang, Y.-X. (2018). Blockchain Queueing Theory. *Working Paper*.

Little, J. D. (1961). A Proof for the Queuing Formula: L= λ W. *Operations research*, *9*(3), 383–387.

Malinova, K., and Park, A. (2017). Market Design with Blockchain Technology. *Working Paper*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer Electronic Cash System. *Unpublished manuscript*.

Orda, A., Rom, R., and Shimkin, N. (1993). Competitive Routing in Multiuser Communication Networks. *IEEE/ACM Transactions on Networking (ToN)*, *1*(5), 510–521.

Pagnotta, E., and Buraschi, A. (2018). An Equilibrium Valuation of Bitcoin and Decentralized Network Assets. *Working Paper*.

Prat, J., and Walter, B. (2018). *An Equilibrium Model of the Market for Bitcoin Mining* (Tech. Rep.). CESifo Working Paper.

Rosen, J. B. (1965). Existence and Uniqueness of Equilibrium Points for Concave n-person Games. *Econometrica: Journal of the Econometric Society*, 520–534.

Saleh, F. (2018). Blockchain without Waste: Proof-of-Stake. *Working Paper*.

Teo, E. G. (2015). Emergence, Growth, and Sustainability of Bitcoin: The Network Economics Perspective. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, 191.

Tinn, K. (2017). Blockchain and the Future of Optimal Financing Contracts. *Working Paper*.

Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*, *151*.

Yermack, D. (2017). Corporate Governance and Blockchains. *Review of Finance*, *21*(1), 7–31.