2019 IEEE International Conference on Blockchain (Blockchain)

Bitcoin Mining with Transaction Fees: A Game on the Block Size

Suhan Jiang and Jie Wu
Department of Computer and Information Sciences, Temple University
{Suhan.Jiang and jiewu}@temple.edu

***Abstract*—In a Bitcoin market, miners participate in blockchain mining with an aim to make profits. Until reaching consensus, PoW-valid blocks (including validated transactions and proper PoW solutions) can be viewed as being successfully mined and are rewarded. There are two types of rewards for miners: fixed *block subsidies* and time-varying *transaction fees*. Block subsidies, predetermined by design, are the current major revenue source. Transaction fees, offered by Bitcoin transaction senders to accelerate their transactions, heavily depend on the corresponding transaction size. Thus, a larger-size block tends to contain higher transaction fees and hence more rewards. However, the probability of a miner to successfully mine a block diminishes as the block size increases, since a larger-size block takes a longer time to reach consensus. Thus, the reward included in the block is vitally affected by its size, which is independently decided by a miner. In this paper, we use a game-theoretic approach to study how a miner's payoff, *i.e.*, expected profits, is determined by his block size. More specifically, we derive an expression to characterize the relation between the miner's payoff and block sizes. Besides, we use game theory to analyze how profit-driven miners will manipulate their block sizes to optimize payoff instead of adopting the default block size. We conduct numerical experiments on real-world data collected from Bitcoin to find peaceful equilibrium where miners have no incentive to misbehave. The achieved block sizes thereby give guidelines on the default block size, in order to deter miners from misbehaving. Our analysis suggests a block size of 4 MB.**

***Index Terms*—Bitcoin, blockchain, deviant mining strategy, game theory, transaction fees.**

I. Introduction

As the most successful decentralized digital currency, Bitcoin applies blockchain, a distributed ledger, to record transactions in the form of linked blocks secured by cryptography. The consensus protocol is the core of blockchain, since it regulates how to maintain such an append-only public ledger in a distributed fashion. Bitcoin is built on top of a proof-of-work (PoW) protocol. In the Bitcoin network, agents called miners collect blocks of transactions, verify their integrity, and append them to the blockchain. Miners are required to solve a computationally difficult PoW puzzle, in order to append a block to the blockchain. This mechanism ensures the security and reliability of blockchain, since lots of trial and error is required on average before computing a valid solution to such a puzzle. The process of successfully adding a block to the chain can be viewed as a mining round and the blockchain grows due to continuously repeated mining rounds. Each miner successfully appending a block will receive monetary rewards as a mining incentive.

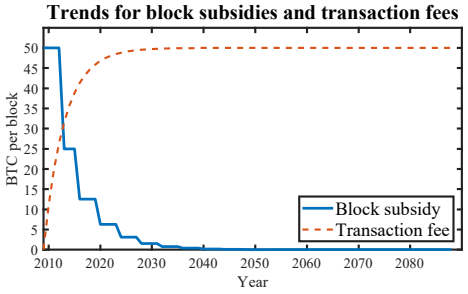


Fig. 1: Block reward evolution trend [10].

A major success factor of Bitcoin is its novel reward mechanism. This mechanism couples, albeit loosely, the extension of the blockchain with newly minted Bitcoins. The creation of Bitcoins is only accompanied by a new block added permanently to the blockchain, as a reward for its creator. However, due to a 21,000,000-unit upper bound of bitcoin supply, starting from 50 BTC, the block subsidy halves every 210,000 blocks and will eventually become zero. Thus, transaction fees, offered by transaction senders, are also introduced to gradually replace block subsidy as the other mining incentive. However, there are two types of rewards in the current Bitcoin market: fixed *block subsidies* and time-varying *transaction fees*. As is shown in Fig. 1, fixed block subsidies for mining will be entirely substituted with transaction fees in the long run. Since the security of Bitcoin's consensus protocol relies on miners behaving correctly, the reward structure of the protocol should encourage honest miners (those who strictly follow the Bitcoin protocol when mining) by ensuring their payoff is proportional to their mining power. However, it cannot always hold due to the increasingly-significant transaction fees in the Bitcoin reward mechanism. More and more miner misbehaviors arise due to transaction fee. To gain more rewards, miners usually have more incentive for transactions with more fees. Thus, chances are high that a transaction without fee could not be processed immediately or might not even be relayed by miners.

There also exist cases where misbehaving miners give up part of available transaction fees in hopes of enhancing his chance to win all other unabandoned rewards. Carlsten *et al.* [1] proposed such a deviant mining behavior called Undercutting. Undercutting attackers always actively fork the head of the chain without claiming all transactions. Those unclaimed transactions (associated with fees) can incentivize more miners to support attackers' blocks instead of an oldest-seen block, since they can collect more transaction fees in their next block

978-1-7281-4693-5/19/$31.00 ©2019 IEEE
DOI 10.1109/Blockchain.2019.00023

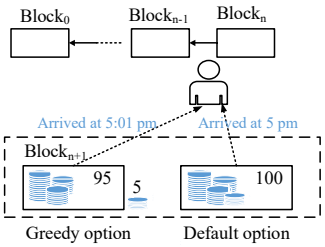


Fig. 2: Two possible options for a miner when accepting a new block.

by mining on an attacker's block. Actually, mining on a block that claims fewer transaction fees instead of a block seen first is also a deviant behavior. Fig. 2 illustrates how these two mining misbehaviors work. Imagine three miners of different types: honest Heidi, greedy Grace, and scheming Sybil. Grace receives two blocks from Heidi and Sybil, respectively, and Sybil's block arrives a little late. Grace has two options: (1) extend the longest chain, mining on Heidi's block and receiving an expected reward of 0; (2) mine on Sybil's block, with an expectation to receive 5 BTC in the next block. The Bitcoin protocol dictates option (1), but quick reasoning suggests that option (2) is more beneficial for Grace.

1) Miners' Misbehaviors on Block Size: The previously-mentioned transaction-fee manipulation can be viewed as miners' misbehaviors on the block size, given the amount of transaction fees included in a block is linearly proportional to its size. Thus, a larger-size block tends to contain more transaction fees. We consider how a miner's mining payoff (expected profits) will be affected by his block size in the long run. The payoff is determined mainly by a miner's winning probability and his expected reward. The expected reward increases as the block grows larger, while the winning probability goes down since smaller blocks tend to reach consensus faster. The Bitcoin protocol itself has requirements on the block size. A block should be bounded within 1 MB and include all valid transactions if available transactions are not enough to fully occupy a 1-MB block. If all miners follow the Bitcoin protocol in an ideal network, then a miner's payoff is proportional to his mining power. However, if a miner dedicatedly designs his block size in order to maximize his payoff, it is possible that he can gain more than his fair share out of total profits, given the current Bitcoin mechanism that includes transaction fees as a source of reward.

2) Our Result: To some extent, transaction fees can be seen as a flaw in Bitcoin as it discourages honest miners and thereby poses an important threat to the stability of Bitcoin network. Manipulating transaction fees is for the purpose of gaining more rewards and essentially is miners' misbehavior on the block size. To analyze the profit-driven miners strategy evolution in transaction-fee regime, we start with how a miner's payoff is determined by his block size. We derive an expression for the distribution and use the law of total expectation to characterize the relation between a miner's payoff and his block size, as well as other parameters. We then discuss how miners with different mining powers can determine their optimal block sizes to maximize payoffs. We find the optimal block size is positively related to the miner's mining power. Based on the observation, we define a game on the block size, where honest miners always follow the default block size, while misbehaving miners play strategies on their own block sizes to optimize payoffs. We investigate our game in different scenarios. Both the game theoretical analysis and numerical results show the existence of peaceful equilibrium where all miners are refrained from misbehaving. We further analyze how different values affect the corresponding equilibria. Since payoff ratios and mining ratios are equivalent in peaceful equilibria, the corresponding block size gives us guidelines on the Bitcoin default block size, which will deter miner's misbehaviors and encourage honest mining. Thus, deviant behaviors in the transaction-fee regime can also be deterred. Our main contributions are summarized as follows:

- We derive expressions to capture relations between miner's expected payoffs and their block sizes.
- We prove a miner with less mining power prefers a smaller block size in order to optimize his payoff.
- We define a block-size game to analyze how misbehaving miners will manipulate their block sizes, instead of following the default block size required in the Bitcoin protocol, in order to maximize payoff.
- We show the Nash equilibria in the proposed game using numerical analysis conducted on the real Bitcoin data.
- The Block sizes achieved in peaceful equilibria give guidelines on the default block size, that would deter misbehaving miners and remove instability caused by transaction fees.

II. Related Work

A vast majority of previous work examines possible types of misbehaviors against the Bitcoin protocol and suggest adaptations of the protocol to encourage honest mining, and thereby ensuring its security. We very briefly mention some of these works here. Usually, misbehaviors at the miners' side tend to be referred to as *Mining attacks*. Eyal and Sirer [4] develop the selfish mining attack, a deviant mining strategy that enables miners to get more than their fair share of rewards. Other works, notably Sapirshtein *et al.* [6] have analyzed selfish mining in more detail using Markov Decision Processes (MDP). Various other attacks have been studied. For example, members of a mining pool can launch a block withholding attack against the pool itself [5], and this harms the victim pool and its other members, but actually increases the revenue of the rest of the network. In [10], the author considers attacks performed between different pools where users are sent to infiltrate a competitive pool giving rise to a pool game. [15] deals with information propagation and Sybil attacks. Most of them are consider a model where the subsidy is the dominant incentive for mining. In this work, we analyze how a miner's behavior differs according to his block size in a reward mechanism with block subsidies and transaction fees. Mser and Bhme [18] review and analyze the history of transaction fees in Bitcoin. They conclude that historically miners prefer to follow the protocol rules rather than optimize their gains.

They predict such a state is sustainable only when fees are a negligible part of the incentive.

There also exists real attacks at the network layer. Each Bitcoin node is connected over TCP to many peers, with a default maximum of 125. The peer-to-peer connections between these nodes can be inferred through various techniques [7, 8]. Heilman *et al.* [9] demonstrated a network-level eclipse attack where a single node monopolizes all possible connections to a victim and eclipses it from the network. Thereby, the eclipsing node can filter the eclipsed node's view of the blockchain. Although a few proposed counter-measures have been implemented that reduce the feasibility of carrying out an eclipse attack by a single node, multiple nodes can collude and still succeed in eclipsing. Besides, Coinscope [7] proposed non-trivial techniques to map out the Bitcoin network topology as well as the mining power of various nodes. This network knowledge can further help a network-level attacker.

In addition, game theory has been widely applied to analyze Bitcoin attacks. Several recent works have examined the game theoretic consequences of attacks. Kiayias *et al.* [14] performed a theoretical analysis of various selfish mining strategies in the fixed-reward model, and proved that when miners are small enough, the default mining behavior is an equilibrium. See also [11] for a (cooperative) game theoretic analysis regarding pool mining.

III. System Model

In this section, we introduce a realistic Bitcoin mining model used in this paper. As commonly done in blockchain-related analysis, we assume the whole system is in a quasi-static state [14, 21]. That means no miners join or leave, existing miners maintain their behavior, and the system reaches equilibrium. Therefore, in our model, the system comprises a fixed set of miners associated with their mining power.

Suppose there are n miners starting to mine a new block on the top the same block, *i.e.*, there is no fork at the beginning time. All players(miners) are asked to solve the proof-of-work puzzle in order to mine a block. The puzzle can be solved only by using a trial and error strategy, and the occurrence of solving this problem can be well approximated by a random variable following a Poission process. The time for the whole system to find a valid block is exponentially distributed with a fixed rate parameter. Time used to find the first block by any of the miners is the minimum of all finding times by all different miners. The value of the rate parameter is determined by the consensus protocol, such that the expected block time interval is of a constant value. The rate parameter represents the difficulty of the proof-of-work puzzle, and we use the terms difficulty and rate interchangeably. The total mining power affects the value of the rate parameter. The difficulty parameter value is adjusted by the whole system to decrease (or increase) the rate of each miner. In an equilibrium, the rate parameter is fixed as a constant. Currently, the difficulty of finding a block is dynamically adjusted so that it takes $T = 600$ seconds on average. Thus, the mining Poission process has a fixed parameter $1/T$ for the whole network.

We assume that the difficulty of all puzzles is the same. In fact, the difficulty of puzzles at each time is proportional to the total mining power in the Bitcoin network of that time. It is reasonable because in our quasi-static model, the miners and their mining power are fixed, thus there is a stable total mining power. There exists more than one valid solution for each puzzle. It is possible that two or even more miners solve their puzzles for a same-height block, which will result in a blockchain fork. Then, the rest miners have to choose only one to continue mining on. The branch accepted by the majority survives, and the corresponding miner would be rewarded. Thus, we could conclude that, miners who solve a puzzle are not necessarily rewarded, and only the first to make his solved block reach consensus will obtain rewards.

The reward of a mined block comes from two aspects: the fixed block subsidy and the extra fee from transactions included in this block. The block subsidy can be referred to as base reward, which is relatively fixed over time. This reward is comprised of the minting of new currency with the creation of each block. Transaction fees come from the aggregation of newly introduced transactions in the system. This reward is time-dependent. As the time progresses, there are more pending transactions in the system, and the potential fees grow. We follow the assumption made in [1] that transactions (and their associated fees) arrive at a constant and continuous rate. To be more precise, during any time interval t, the sum of fees in the announced transactions is ct, where c is a specific constant. As is emphasized in [1], this assumption helps to simplify analysis on the effects of transaction fees, although there is no guarantee it holds in practice. Thus, the transaction fee density of unverified transactions is also constant.

According to the Bitcoin mining protocol, each miner can decide what and how many transactions to include in their block. Following the assumption in [1], if there are m transaction fees available, a miner can choose to include any real-valued number of transaction fees between 0 and m in his block. That is, a miner can selectively choose a set of transactions whose fees are very close to whatever real-valued target he wants. It is a reasonable approximation due to the large number of transactions per block. Thus, the amount of transaction fees included in a block is proportional to its size. Besides, the set of transactions chosen by each miner has no effects on the time and chance to solve hid puzzle. However, it matters during the block broadcast time. Once a miner finds a block, he needs to broadcast it to the rest of the Bitcoin network. In order to be added permanently to the blockchain, this block must be accepted by the majority. If we take the block transfer delay into consideration, the time used to make a block reach consensus is heavily dependent on its size and hence, the set of transactions in it.

Once a block is mined, all miners move on to find the next block. This process is repeated indefinitely. The profit of a miner for each block is the difference between his total expenses and his total reward. Rational miners strive to maximize their profits, giving rise to a game.

TABLE I: Summary of Parameters.

Symbol	Description
T	Average block arriving interval
R	Block subsidy
α	Transaction fee density
β	Block propagation time per unit
n	Number of miners or players
λ_i	Player i's mining rate
h_i	Player i's mining power where $h_i = {}^{\lambda_i}/_{T}$
B_i	Block size decided by player i
P_i	Payoff for player i to mine a block

IV. Distribution in the Block Size Game

The repeated search for the blocks becomes a series of independent one-shot competitions, and in each competition, only one miner gets the reward but all miners pay expenses. To analyze the expected revenues, rather than considering the individual iterations, we consider a one-shot game played by the miners. A player's strategy is the choice of his block size. The choice of block sizes are made a-priori by all the players.

To find the payoff of each player, we start by analyzing the block finding time probability distribution. This is a function of the players selection of block sizes. We model the block finding time as a random variable denoted X with cumulative distribution function (CDF) and probability density function (PDF) denoted $F_X(t; B, \lambda)$ and $f_X(t; B, \lambda)$, respectively. The corresponding notations are listed in Table I.

A. Distribution Analysis

The first step towards analyzing the system is to derive an expression for the distribution, namely $F_X(t; B, \lambda)$ and $f_X(t; B, \lambda)$. We begin with the distribution of a single player i with mining rate λ_i. Assume i's block size is B_i, thus, his propagation time is $p_i = \beta B_i$. Denote the time this player requires for successfully mining a block as a random variable X_i. The probability density function (PDF) of X_i is

$$f_{X_i}(t; B_i, \lambda_i) = \begin{cases} 0 & t < p_i \\ \lambda_i e^{-\lambda_i (t-p_i)} & t \geq p_i \end{cases}, \tag{1}$$

which describes the probability of player i, whose mining rate is λ_i, to successfully mines a block of size B_i at time t. And the corresponding cumulative density function (CDF) is

$$F_{X_i}(t; B_i, \lambda_i) = \begin{cases} 0 & t < p_i \\ 1 - \ e^{-\lambda_i (t-p_i)} & t \geq p_i \end{cases}, \tag{2}$$

defining i's accumulated winning probability until time t.

As $F_{X_i}(t; B_i, \lambda_i) = Pr(X_i \leq t) = 1 - Pr(X_i \geq t)$, we can obtain that

$$Pr(X_i \geq t) = \begin{cases} 1 & t < p_i \\ e^{-\lambda_i (t-p_i)} & t \geq p_i \end{cases}. \tag{3}$$

Since all the players are competing on mining the next block, any player with the minimal value of X_i is the first one to find the next block. Therefore, the time required for finding the next block is $X = \min_{i \in \{1,2,\cdots,n\}} X_i$.

We use a boolean variable $active_i(t)$ to capture a player i's winnablility at time t, which is expressed in the below:

$$active_i(t) = \begin{cases} 0 & t < p_i \\ 1 & t \geq p_i \end{cases}. \tag{4}$$

It is obvious that, i has zero winnablility before time p_i, even if he could solve his PoW puzzle at $t = 0$. After p_i, i starts to hold a probability to win. Besides, we define $active(t)$ as the set of any player who is likely to win at time t. That is, $active(t) = \{i \mid active_i(t) = 1, \forall i\}$.

The probability that none of the players have found a block by time t, $Pr(X > t)$, is the product of $Pr(X_i > t)$ for all i (as players are independent of each other), shown in Eq.(5).

$$\begin{aligned} Pr(X > t) &= \bigcap_{i \in \{1,2,\cdots,n\}} Pr(X_i > t) = \prod_{i=1}^{n} Pr(X_i > t) \\ &= e^{\sum_{i \in active(t)} [-\lambda_i (t-p_i)]} \end{aligned} \tag{5}$$

Thus, X's corresponding CDF and PDF are shown below,

$$\begin{aligned} F_X(t; B, \lambda) &= 1 - Pr(X > t) \\ &= 1 - e^{\sum_{i \in active(t)} [-\lambda_i (t-p_i)]}, \\ f_X(t; B, \lambda) &= (\sum_{i \in active(t)} \lambda_i) \cdot e^{\sum_{i \in active(t)} [-\lambda_i (t-p_i)]}. \end{aligned} \tag{6}$$

B. Proof of A Valid PDF

Theorem 1. *$f_X(t; B, \lambda)$ is a valid probability density function to express the probability of finding a block as time passes in the whole blockchain mining network.*

Proof. We present the full verification process in the below by checking that $\int_{-\infty}^{+\infty} f_X(t; B, \lambda) \mathrm{d}t = 1$ holds.

$$\begin{aligned} &\int_{-\infty}^{+\infty} f_X(t; B, \lambda) \mathrm{d}t = \sum_{l=1}^{l=n} \int_{p_l}^{p_{l+1}} f_X(t; B, \lambda) \mathrm{d}t \\ &= \sum_{l=1}^{l=n} \int_{p_l}^{p_{l+1}} \lambda |active(p_l)| e^{\sum_{j \in active(p_l)} [\lambda_j (t-p_l)]} \mathrm{d}t \\ &= \sum_{l=1}^{l=n} \int_{p_l}^{p_{l+1}} \lambda x_l e^{-x_l \lambda t} e^{\sum_{j \in active(p_l)} p_j} \mathrm{d}t \\ &= e^{-\lambda} \sum [e^{\sum_{j \in active(p_l)} (p_l - p_j)} - e^{\sum_{l \in active(p_l)} (p_{l+1} - p_j)}] \\ &= e^{-\lambda} [e^{\sum_{j \in active(p_1)} (p_1 - p_j)} - e^{\sum_{j \in active(p_\infty)} (p_\infty - p_j)}] \\ &= e^{-\lambda} (e^0 - e^{+\infty}) = 1 \end{aligned} \tag{7}$$

□

Thus, the PDF we use is valid, hence our model is as well.

V. Payoff in the Block Size Game

A. Payoff Analysis

The payoff is defined as the expected profit of player i. We use the variable $profit_i$ to represent i's profit and hence at time t, i's expected profit is denoted as $E(profit_i | X = t)$. We model the profit of a block consisting of the fixed block subsidy and transaction fees inside that block, which is proportional to the block size. Thus, for a specific player i, the total available profit is $R + \alpha B_i$. Recall that, in expectation, the probability that a specific active player will find a block is his mining power divided by the total mining power owned by all the active players. Thus, if a block was found at time t, then the expected profit of player i is shown below.

$$E(profit_i | X = t) = \frac{active_i(t) \cdot \lambda_i}{\sum_{j \in active(t)} \lambda_j} (R + \alpha B_i) \tag{8}$$

Since we define the player i's payoff as the expectation of his profit, we express it in Eq.(9),

$$\begin{aligned} P_i &= E(profit_i) = E(E(profit_i|X=t)) \\ &= \int_{-\infty}^{+\infty} E(profit_i|X=t)\cdot f_X(t;B,\lambda)\mathrm{d}t \\ &= \lambda_i(R+\alpha B_i)\sum_{l=i}^{n}\frac{e^{\sum\lambda_j(p_j-p_l)}-e^{\sum\lambda_j(p_j-p_{l+1})}}{\sum\lambda_j} \end{aligned} \tag{9}$$

where $j \in active(p_l)$ for all valid l.

1) Impacts of Individual Block Size on Self-payoff: A player can improve his expected payoff by two means - increasing either (i) his expected reward or (ii) his chance of being rewarded. Although both of them are implemented by adjusting the block size, they are in conflicting directions. When a player chooses a big block size, he prefers to increase his potential transaction fee reward by including more transactions, at the cost of lowering his chance to be rewarded (since a bigger block incurs a longer propagation time). When a player chooses a small block size, he prefers to increase his chance for receiving a reward by shortening the propagation time of his block (therefore prolonging his mining time), at the cost of decreasing his reward amount from transaction fees.

2) Impacts of Individual Block Size on Others' Payoffs:

Theorem 2. *A player indirectly increases each of his rivals' payoff by increasing his own block size.*

Proof. We calculate the first-order derivatives of player k's payoff over B_i:

$$\frac{\partial P_k}{\partial B_i} = \beta\lambda_i\lambda_k(R+\alpha B_k)\sum_{l=max\{i,k\}}^{n}\frac{e^{\sum\lambda_j(p_i-p_l)}-e^{\sum\lambda_j(p_j-p_{l+1})}}{\sum\lambda_j}. \tag{10}$$

where $k\neq i$ and $j\in active(p_l)$ for all valid l.

Obviously, ${}^{\partial P_k}/_{\partial B_i} \geq 0$ always holds. This result can be interrupted as follows. When any player increases his own block size, it brings external benefits to other players. This is because the player lengthens his own propagation time, allowing others to mine for a longer time. This increases their probability of finding a valid PoW solution. □

B. Optimal Block Size and Mining Power

According to Eq.(9), a player's expected payoff is related to the block sizes selected by all the players, as well as the mining power distribution in the whole Bitcoin network. Now, we are interested in finding out how a player's mining power would affect his decision on the block size. Intuitively,

Theorem 3. *A player's optimal block size is positively related to his mining power.*

Proof. We assume two heterogeneous players: player 1 with lower mining power and player 2 with higher mining power. Besides, we assume there is no bound on the block size. Thus, players are allowed to put as many transactions as they want in the block. We define player 1's mining power as h_1 and player 2's mining power as h_2 , respectively. Given $h_1+h_2=1$ and $h_1<h_2$, then we can see $\lambda_1={}^{h_1}/_{T}$ and $\lambda_2={}^{h_2}/_{T}$. We analyze these two players' payoffs under two possible conditions: (1) $B_1<B_2$ and (2) $B_1>B_2$, respectively.

(1) $B_1<B_2$: This means player 1 with lower mining power would choose a smaller block size than player 2. Then, each player's expected payoff can be expressed as

$$\begin{aligned} P_1 &= (R+\alpha B_1)\left[1-(1-h_1)e^{-{}^{h_1\beta(B_2-B_1)}/_{T}}\right] \\ P_2 &= (R+\alpha B_2)h_2 e^{-{}^{(1-h_2)\beta(B_2-B_1)}/_{T}}. \end{aligned} \tag{11}$$

To figure out each player's optimal block size, we calculate the first-order derivative of P_j over B_j in Eq.(12).

$$\begin{aligned} \frac{\partial P_1}{\partial B_1} &= \alpha\left[1-h_2 e^{\frac{-h_1\beta(B_2-B_1)}{T}}\right]-\frac{h_1h_2}{T}\beta(R+\alpha B_1)e^{\frac{-h_1\beta(B_2-B_1)}{T}} \\ \frac{\partial P_2}{\partial B_2} &= \alpha h_2 e^{\frac{-h_1\beta(B_2-B_1)}{T}}-\frac{h_1}{T}\beta(R+\alpha B_2)h_2 e^{\frac{-h_1\beta(B_2-B_1)}{T}} \end{aligned} \tag{12}$$

Let ${}^{\partial P_2}/_{\partial B_2}=0$, then $B_2={}^{T}/_{\beta(1-h_2)}-{}^{R}/_{\alpha}$. Let $B_2^*=\underset{B_2\geq 0}{\operatorname{argmax}} P_2$, thus we conclude that

$$B_2^* = \begin{cases} 0 & \text{if } \frac{R}{\alpha}\geq\frac{T}{\beta(1-h_2)} \quad \text{case (a)} \\ \frac{T}{\beta(1-h_2)}-\frac{R}{\alpha} & \text{otherwise} \quad \text{case (b)} \end{cases}$$

Now we discuss the optimal $B_1^*=\operatorname{argmax}_{0\leq B_1\leq B_2^*} P_1$. B_1^* is dependent on B_2^*. Given player 2's dominant strategy, player 1 should choose his best response. In case (a), $B_2^*=0$, then

$$\frac{\partial P_1}{\partial B_1}=\alpha\left[1-h_2 e^{{}^{h_1\beta B_1}/_{T}}\right]-\frac{h_1h_2}{T}\beta(R+\alpha B_1)e^{{}^{h_1\beta B_1}/_{T}}.$$

For any $B_1\geq 0$, ${}^{\partial P_1}/_{\partial B_1}\leq 0$ always holds. Thus, $B_1^*=0$. In the case (b), $B_2^*={}^{T}/_{\beta(1-h_2)}-{}^{R}/_{\alpha}$, and the payoff function P_1 for player 1 is concave in B_1 since ${}^{\partial^2 P_1}/_{(\partial B_1)^2}<0$ always holds. As ${}^{\partial P_1}/_{\partial B_1}|_{B_1=B_2}<0$ holds if ${}^{R}/_{\alpha}<{}^{T}/_{\beta(1-h_2)}$, there is a unique B_1^*, satisfying $B_1^*<B_2^*$. Obviously, the analysis result is consistent with the condition $B_1<B_2$.

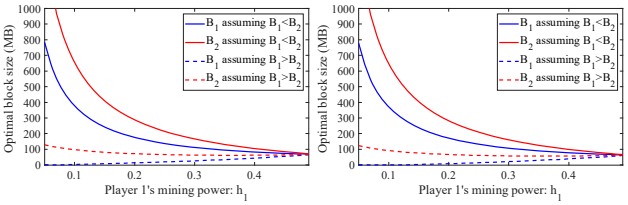
(2) $B_1>B_2$: This means player 1 with lower mining power would choose a bigger block size than player 2. Now, each player's expected payoff can be expressed as

$$\begin{aligned} P_1 &= (R+\alpha B_1)h_1 e^{-{}^{(1-h_1)\beta(B_1-B_2)}/_{T}} \\ P_2 &= (R+\alpha B_2)\left[1-(1-h_2)e^{-{}^{h_2\beta(B_1-B_2)}/_{T}}\right]. \end{aligned} \tag{13}$$

Then by calculating $\partial P_1/\partial B_1=0$, we obtain the optimal block size B_1^* for player 1, which is listed below.

$$B_1^* = \begin{cases} 0 & \text{if } \frac{R}{\alpha}\geq\frac{T}{\beta(1-h_1)} \quad \text{case (a)} \\ \frac{T}{\beta(1-h_1)}-\frac{R}{\alpha} & \text{otherwise} \quad \text{case (b)} \end{cases}$$

We verify if $B_2^*<B_1^*$ holds. We begin with case (a), where ${}^{R}/_{\alpha}\geq{}^{T}/_{\beta(1-h_1)}$ and $B_1^*=0$. Thus, ${}^{\partial P_2}/_{\partial B_2}=\alpha\left(1-h_1 e^{{}^{h_2\beta B_2}/_{T}}\right)-({}^{h_1h_2}/_{T})\beta(R+\alpha B_2)e^{{}^{h_2\beta B_2}/_{T}}$. When $B_2=0$, we obtain ${}^{\partial P_2}/_{\partial B_2}|_{B_2=0}=(\alpha-{}^{h_1}/_{T}\beta R)h_2$. Based on ${}^{R}/_{\alpha}\geq{}^{T}/_{\beta(1-h_1)}$, we can see $B_2^*=0$ if $\alpha\leq{}^{R\beta h_1}/_{T}$ (since ${}^{\partial P_2}/_{\partial B_2}|_{B_2=0}\leq 0$), and $B_2^*>0$ if ${}^{R\beta h_1}/_{T}\leq\alpha\leq{}^{R\beta h_2}/_{T}$ (since ${}^{\partial P_2}/_{\partial B_2}|_{B_2=0}>0$). Thus, $B_2^*\geq B_1^*$ holds in case (a). We proceed with case (b), where ${}^{R}/_{\alpha}<{}^{T}/_{\beta(1-h_1)}$ and $B_1^*={}^{T}/_{\beta(1-h_1)}-{}^{R}/_{\alpha}$. When $B_2=B_1^*$, we obtain ${}^{\partial P_2}/_{\partial B_2}|_{B_2=B_1^*}=(1-{}^{h_1}/_{h_2})\alpha h_2$, which is bigger than 0 given $h_1<h_2$ and P_2 is a concave function in B_2 as ${}^{\partial^2 P_2}/_{(\partial B_2)^2}<0$ holds, then $B_2^*>B_1^*$. Thus, the result violates the condition $B_1>B_2$.



(a) $R = 12.5, \alpha = 0.16, \beta = 8.2$ (b) $R = 25, \alpha = 0.3, \beta = 8.2$

Fig. 3: Player with lower mining power will have smaller optimal block size.

Based on the previous discussion, it is obvious to see that, given $h_1 < h_2$, $B_1^* < B_2^*$ always holds. □

We also use real-world data from the Bitcoin network to validate our conclusions. The numeric results can be seen in Fig. 3. We plot the optimal block sizes for both players under different conditions. In Fig. 3(a), the solid lines represent B_1^* and B_2^* under the condition $B_1 < B_2$. The red solid line is above the blue solid line, which is consistent with the condition $B_1 < B_2$. As h_1 increases, *i.e.*, h_1 is close to h_2, these two solids approach and finally intersect when $h_1 = h_2$. However, the result reflected by the dashed lines violates the condition $B_1 > B_2$ (the blue dashed line is below the red one). In the Fig. 3(b), we modify the Bitcoin network settings by changing the block subsidy, transaction fee density and the network delay, but we still get the same trend. Thus, a player with low mining power should choose a small block size while a player with high mining power should choose a big one.

VI. System Equilibrium Analysis and Search

The payoff presented in Eq.(9) is derived given all players' strategies. If a player changes his strategy, then the payoffs of all the other players will also be affected. We are interested in finding equilibria, *i.e.*, strategies of all players such that no player can improve its payoff by changing its strategy. It is infeasible to express a player's payoff in a symbolic manner, since it is a function of all players' strategies as well as the difficulty parameter, which is expressed as an implicit function. Therefore, we use numerical analysis to find equilibria in the system.

We implement an equilibrium-search-tool, a tool we use to numerically search for an equilibrium, and that works in the following manner. The equilibrium-search-tool receives as an input for the system income and expenses parameters, as well as a list of tuples representing all players strategies. Each tuple of that list is in the form of $\{i, h_i, B_i\}$, where i is a players index, h_i is the mining power controlled by player i, and B_i is the block size selected by player i.

Iteratively, the equilibrium-search-tool randomly chooses an input tuple $\{i, h_i, B_i\}$, and searches what value of a block size B_i will result in maximal payoff for player i. This process is repeated until no player increases its payoff by changing any of its rigs, meaning an equilibrium is reached. Note that all equilibria found by such process are only ϵ-Nash equilibria, as they are limited by the numerical precision of the calculation. To counter that predicament, we repeat the search process with different random start times and different optimizing order. In all conducted experiments, the randomness introduced had no effect on the output equilibrium. That strengthens our analysis of an equilibrium.

VII. One Misbehaving Miner

We begin our analysis with an assumption that there is exactly one miner with misbehavior. For simplicity, we assume that miners are divided into two groups, a corrupted pool A controlled by the misbehaving miner, and the rest of the miners M behaving heuristically. It is irrelevant whether M operates as a single pool, as a collection of pools, or individually. Each miner in M always honestly mines with the default block size $\overline{B}$ ($1MB$ at the time of writing this paper), while A manipulates his block size B_A to optimize his expected payoff.

A. Attacker's Expected Payoff

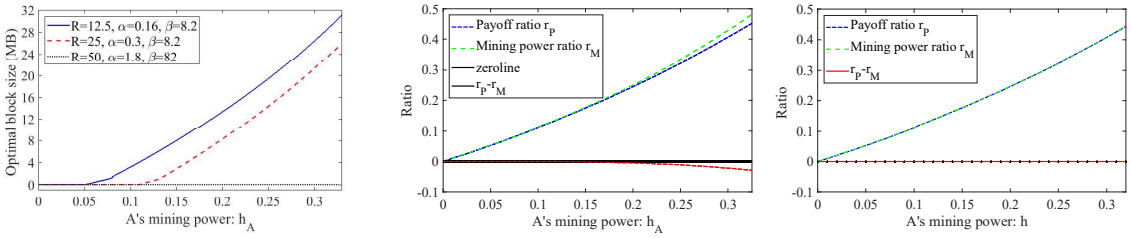
Let A's mining power equal to h_A, then M controls $h_M = 1–h_A$ of the total mining power. Based on Eq.(9), we calculate A's expected payoff in Eq.(14).

$$P_A = \begin{cases} (R + \alpha B_A)\left[1 - (1 - h_A)e^{-h_A\beta(\overline{B} - B_A)/T}\right] & \text{if } B_A \leq \overline{B}. \\ (R + \alpha B_A)h_A e^{-(1-h_A)\beta(B_A - \overline{B})/T} & \text{otherwise.} \end{cases} \quad (14)$$

B. Numerical Analysis on One-Sided Misbehavior

The expected payoff presented in Eq.(14) is derived given A's mining power and block size. In fact, A's optimal block size B_A^* can be decided according to $\partial P_A / \partial B_A = 0$, and is an implicit function related to h_A. Now, we focus on how A's mining power h_A would influence his decision on B_A. Thus, we allow A to put as many (or few) transactions as he wants in the block. Since it is infeasible to express B_A^* in a symbolic manner, we use numerical analysis to find B_A^* under different values of h_A, in hopes of finding out a unified and reasonable explanation to these numerical results.

Fig. 4(a) shows how A's optimal block size B_A^* is related to his mining power h_A, given $\overline{B} = 1$ and $T = 600$. We fix the parameters R, α, and β and vary the parameter h_A. Values of each set (R, α, β) are based on the real-time information from [16]. From the black dashed line we can see A always puts few transactions in his block. $B_A^* = 0$ is reasonable due to the huge network delay, *i.e.*, $\beta = 82$. When we set the network delay to a normal level ($\beta = 8.2$), we find A's optimal block size becomes larger as his mining power increases. We can also see that decreasing the block subsidy motivates A to increase his block size to optimize payoff, even if the transaction fee density decreases. Thus, we could predict that, once the transaction fee dominates the Bitcoin reward mechanism, optimal block size increases for each player no matter what his mining power is. Results in Fig. 4(b)-(c) show that, the payoff ratio is equivalent to the mining ratio between A and M when A adopts his optimal block size while M follows default block size. In fact, if only A seeks to gain more by manipulating his block size, we could see the payoff distribution between A and M still follows the fairness requirement: the payoff should be distributed proportionally to the mining power in the long run.

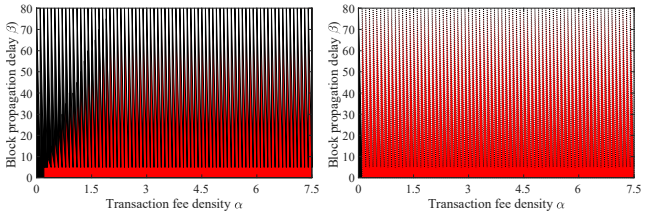


(a) Optimal block size using different sets of (R, α, β).

(b) Payoff ratio Vs Mining power ratio between A and M when $R = 12.5$.

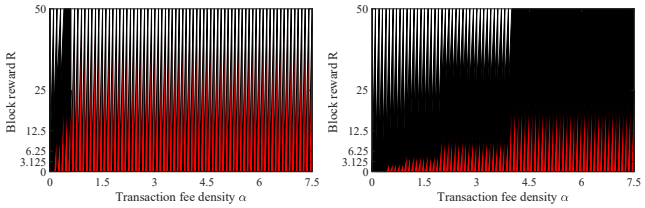
(c) Payoff ratio Vs Mining power ratio between A and M when $R = 25$.

Fig. 4: Numerical analysis based on real-time information from [10].



(a) $R = 12.5$ (b) $R = 0$

Fig. 5: Existence of the peaceful equilibrium when R is fixed.



(a) $\beta = 8.2$ (b) $\beta = 82$

Fig. 6: Existence of the peaceful equilibrium when β is fixed.

Since any block over 1 MB will be denied in the real Bitcoin network, we are interested in finding peaceful equilibria which refrain A with any h_A from manipulating his block size. That is, we want to find on what conditions, A can optimize his payoff by always filling up his 1-MB block. Obviously, $B_A^* \geq 1$ must hold on those conditions, such that A is forced to fill up his block, in order to maximize his expected payoff (although it is still not his optimal payoff due to the $1MB$ limitation).

In Fig. 5(a), we firstly fix the parameter R as 12.5, and we vary the parameters α and β. The red shaded areas represent the existence of peaceful equilibria given different values of α and β (if you are reading this paper in a black-and-white version, those grey parts represent equilibria). The figure shows that, a peaceful equilibrium tends to appear when α is high and β is low. That is, if the transaction fee density is high enough and the network delay is within a low range, A's optimal block size is always over 1 MB, which forces him to maximize his obtainable payoff by choosing his block size as the default 1 MB. In Fig. 5(b), we assume the block reward runs dry, *i.e.*, $R = 0$, and we cannot observe a peaceful equilibrium unless either $\alpha \to 0$ or $\beta \geq 600$ (which is impossible in reality unless a delay attack exists). This is reasonable since transaction fees are the only incentive.

In Fig. 6, we fix the parameters β (81.92 in (a) and 8.192 in (b)), and we vary the parameters R and α. These figures show that if R is low and α is high, then a peaceful equilibrium is possible; however, if either of these parameters is deviant, then there can be no peace. This further confirms the result in Fig. 5(b), as the block subsidy goes low (even dry), the transaction fee dominates, A with any mining power has the motivation to choose a larger block size. Besides, Fig. 6 also implies β is especially important. As we can compare, the red shaded area obviously shrinks as β goes up. That is, dramatic increase on the network delay will lead A to choose a block size smaller than 1 MB. In practice, if someone issues a delay attack (which can delay a message for at most 20 minutes), then players may have no incentive to collect transactions in their blocks. This would be a disaster for the liveness of Bitcoin.

VIII. Two Pools

We proceed to analyze the case with two misbehaving miners where miner L has a small pool and miner H has a big pool. By size comparison, we simply mean that L has less mining power than H. Obviously, $B_L^* \leq B_H^*$. A third entity M represents the rest of the Bitcoin mining market and behaves heuristically, using the default block size $\overline{B}$.

A. Peaceful Equilibria

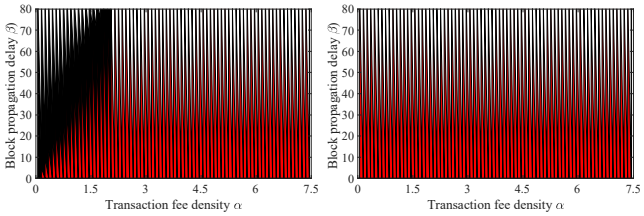
First, we are interested in finding peaceful equilibria which refrain both L and H from deviating from $\overline{B}$. On these conditions, both B_L^* and B_H^* must be no less than $\overline{B}$ so that if L and H want to maximize their expected payoffs, they have to fill up their blocks. The payoff functions of L and H under the condition of $\overline{B} \leq B_L \leq B_H$ are listed in Eq.(15):

$$P_L = (R + \alpha B_L)\frac{h_L}{h_M + h_L} \times \left[e^{-h_M \beta (B_L - \overline{B})/T} - h_H e^{-h_M \beta (B_H - \overline{B})/T - h_L \beta (B_H - B_L)/T}\right] \quad (15)$$

$$P_H = (R + \alpha B_H) h_H e^{-h_M \beta (B_H - \overline{B})/T - h_L \beta (B_H - B_L)/T}.$$

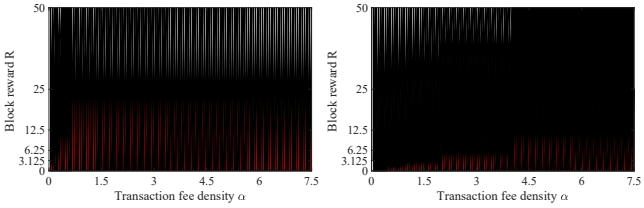
We can calculate B_L^* and B_H^* by solving the equations $\partial P_L / \partial B_L = 0$ and $\partial P_H / \partial B_H = 0$ if R, α, and β are all given. Again, we use numerical analysis here and the corresponding results are present in Fig. 7 and Fig. 8.

In Fig. 7, we fix R while vary α and β and the red shaded areas are peaceful equilibria given different values of α and β. Comparing Fig. 7 with Fig. 5, we find the peaceful equilibria are reduced. This is because more misbehaved miners leads to



(a) $R = 12.5$ (b) $R = 0$

Fig. 7: Existence of the peaceful equilibrium when R is fixed.



(a) $\beta = 8.2$ (b) $\beta = 82$

Fig. 8: Existence of the peaceful equilibrium when β is fixed.

a more unstable and unpredictable mining environment. When $R = 12.5$, Fig. 7(a) shows that a peaceful equilibrium appears if α is high and β is low. That is, if transaction fee density is high enough and network delay is within a low range, both B_L^* and B_H^* are over 1 MB, thereby they have to choose the default block size to obtain a maximized payoff in expectation. In Fig. 7(b), we assume the block reward runs dry, *i.e.*, $R = 0$, we find that a peaceful equilibrium comes as long as the network delay β falls into a reasonable range since transaction fees are the only income source. In Fig. 8, we fix β while vary R and α. These figures show that, if R is low and α is high, then a peaceful equilibrium is possible; however, if either of these parameters is deviant, then there can be no peace. Thus, when transaction fees dominate, L and H with any mining power have the motivation to choose larger block sizes. Fig. 8 also shows the red shaded area obviously shrinks as the number of misbehaved players increases. Thus, the more misbehaved players, the less stable Bitcoin mining will be.

B. One-Sided Misbehaviors

We also want to know when only L is deviant from the default block size, which means $B_L^* < \overline{B}$ and $B_H^* \geq \overline{B}$. Below are the payoff functions under the assumption $B_L < \overline{B}$ and $B_H = \overline{B}$. The equation given below is the corresponding payoff functions when only L misbehaves.

$$\begin{aligned} P_L &= (R + \alpha B_L) \times \\ &\left[1 - \frac{h_M}{h_L + h_M} e^{-h_L \beta (\overline{B} - B_L)/T} - \frac{h_L h_H}{h_M + h_L} e^{-h_L \beta (\overline{B} - B_L)/T}\right] \\ &= (R + \alpha B_L) \left[1 - (1 - H_L) e^{-h_L \beta (\overline{B} - B_L)/T}\right] \\ P_H &= (R + \alpha \overline{B}) h_H e^{-h_L \beta (\overline{B} - B_L)/T}. \end{aligned} \tag{16}$$

Again, we conduct numerical analysis to find Nash equilibrium and see how parameters affect the achieved equilibria. The red shade in Fig. 10 shows all possible equilibria when L's mining power varies given some fixed parameter(s). We can see with a low transaction rate and a high network delay, a miner with lower mining power cannot achieve more payoff even by choosing a smaller block size than the default block size. Thus, we can conclude that, the manipulation on the block size doesn't work here. In practice, however, the transaction rate is high and the network delay is usually controlled at a reasonable level. In those cases, we find that there exists an upper bound for L's mining power. See the example in Fig. 10(a) given the parameters: $R = 12.5, \alpha = 6, \beta = 8.2$, the upper bound is around 8%. Once exceeding this bound, there is no existence of equilibria, which means, if L holds more than 8% mining power, then his optimal block size is definitely smaller than $\overline{B}$. As a misbehaved player, L could choose a B_L^* instead of $\overline{B}$. Thus, the current default block size 1 MB can never ensure any player would behave well, since a misbehaved player with over 8% mining power can manipulate his block size by setting it smaller than the default to gain more than his fair reward share.

C. Two-Sided Misbehaviors

We now analyze when both sides want to misbehave, which means $B_L^* < \overline{B}$ and $B_H^* < \overline{B}$. Given these assumptions, we start our analysis on the two-sided-misbehavior scenario by expressing the utilities of both parties.

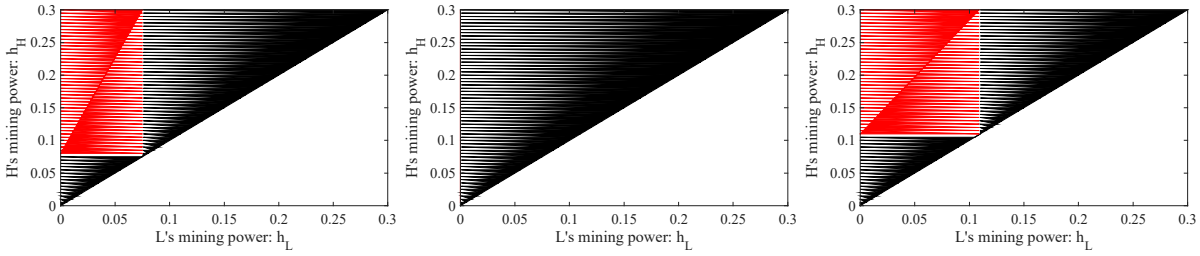
According to our previous analysis, we know that the player with higher mining power always performs better if its block size is bigger than that of a miner with lower mining power, *i.e.*, $B_H \geq B_L$ given $h_H \geq h_L$. Below are the payoff functions under the assumption $B_L \leq B_H < \overline{B}$:

$$\begin{aligned} P_L =& (R + \alpha B_L) \left[1 - \frac{h_H}{h_L + h_H} e^{-h_L \beta (B_H - B_L)/T} \right. \\ & \left. - \frac{h_L h_M}{h_L + h_H} e^{-h_L \beta (\overline{B} - B_L/T) - h_H \beta (\overline{B} - B_H)/T}\right] \\ P_H =& (R + \alpha B_H) \left[\frac{h_H}{h_L + h_H} e^{-h_L \beta (B_H - B_L)/T} \right. \\ & \left. - \frac{h_H h_M}{h_L + h_H} e^{-h_L \beta (\overline{B} - B_L)/T - h_H \beta (\overline{B} - B_H)/T}\right]. \end{aligned} \tag{17}$$

According to the numerical analysis, we found the anticipated equilibrium is hardly to be found in the current Bitcoin network. This means, even in such a simplified scenario, the default block size 1 MB cannot refrain players from manipulating block sizes to gain more. Thus, we need to reconsider how the Bitcoin network designs the default block size $\overline{B}$. An important design protocol is that, $\overline{B}$ should be smaller the optimal block size of every player with any mining power. In the next part, we will use the current information of the Bitcoin network to recommend a suitable default block size according to the previously-mentioned design protocol.

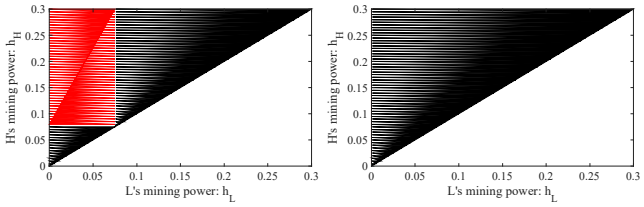
D. Extension on Real Bitcion Mining Network

We now make an educated estimation on the real Bitcion network. In Bitcoin today, there are 7 mining pools [11] controlling about 85% of the mining power, while the rest is divided among many smaller mining pools. Although they



(a) $\beta = 8.2$ (b) $\beta = 82$ (c) $\beta = 82$

Fig. 9: Existence of the peaceful equilibrium when β is fixed. Red shaded areas represent parameter combinations where the peaceful equilibrium exists.



(a) $\beta = 8.2$ (b) $\beta = 82$

Fig. 10: Existence of the peaceful equilibrium when β is fixed.

vary in size, we approximate that situation by assuming 8 equal-size miners.

Currently, the rewards from minting and fees are 12.5 BTC and about 1 BTC, respectively. We extend from previous analysis and try to find peaceful equilibrium among eight mining pools. With the help of Matlab, we find the default block size, which is suggested to be 4 MB.

IX. Conclusion

We define and analyze the block size game exploring how block sizes form as a function of block subsidy and transaction fees. We show that once fees become significant, then manipulation on the block size appears. However, it does not happen uniformly as previously believed, while it has a significant effect on blockchain security. This means that base rewards are critical for system security, and should be achieved either by subsidies, fee backlogs, or alternative fee schemes [22, 23]. We show that the default block size 4 MB is sufficient to avoid deviant mining behavior of the block sizes in presented scenarios; we expect Bitcoin to drop below this threshold within a decade.

X. Acknowledgment

This research was supported in part by NSF grants CNS 1824440, CNS 1828363, CNS 1757533, CNS 1629746, CNS-1651947, and CNS 1564128.

References

[1] M. Carlsten, H. Kalodner, S. Matthew Weinberg, and A. Narayanan. On the Instability of Bitcoin Without the Block Reward, In CCS, 154167, 2016.

[2] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin:org/bitcoin:pdf, 2008

[3] N. Houy. The Bitcoin Mining Game. In SSRN Electronic Journal, 2014.

[4] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography, 2014.

[5] N. T. Courtois and L. Bahack. On subversive miner strategies and block withholding attack in bitcoin digital currency. arXiv preprint arXiv:1402.1718, 2014.

[6] A. Sapirshtein, Y. Sompolinsky, and A. Zohar. Optimal selfish mining strategies in bitcoin. arXiv preprint arXiv:1507.06183, 2015.

[7] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, Discovering bitcoins public topology and influential nodes. Tech. Rep., [Online]. Available: https://cs.umd.edu/ projects/coinscope/coinscope.pdf, 2015.

[8] A. Biryukov and I. Pustogarov. Bitcoin over Tor isnt a good idea. arXiv preprint arXiv:1410.6079, 2014.

[9] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. Eclipse attacks on bitcoins peer-to-peer network. In USENIX Security, 2015.

[10] I.Eyal. The miners dilemma. arXiv 1411.7099, 2014.

[11] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In AAMAS, 2015.

[12] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. 2013

[13] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa. Electron spectroscopy studies on magneto-optical media and plastic substrate interface. In IEEE Transl. J. Magn. Japan, 1987.

[14] J. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. In TACT, 2015.

[15] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On bitcoin and red balloons. In EC, pages 5673. ACM, 2012.

[16] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In IEEE P2P, pages 110, 2013.

[17] S. L. Reed. Bitcoin Cooperative Proof of Stake. In Computing Research Repository. Tech, 2014.

[18] M. Malte and R. Bhme. Trends, tips, tolls: A longitudinal study of Bitcoin transaction fees. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2015.

[19] I. Tsabary and I. Eyal. The Gap Game. In CCS. ACM, 2018.

[20] G. Juan, A. Kiayias, and N. Leonardos. "The bitcoin backbone protocol: Analysis and applications." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2015.

[21] G. Arthur, G. O. Karame, K. Wst, V. Glykantzis, H. Ritzdorf, and S. Capkun. "On the security and performance of proof of work blockchains." In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security,

[22] L. Ron, O. Sattath, and A, Zohar. "Redesigning Bitcoin's fee market." arXiv preprint arXiv:1709.08881 (2017).

[23] P. Rafael and E. Shi. "Fruitchains: A fair blockchain." In PODC, ACM, 2017.