LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

RESEARCH ARTICLE

The Bitcoin Mining Game

Nicolas Houy*†

Abstract. This article deals with the mining incentives in the Bitcoin protocol. The mining process is used to confirm and secure transactions. This process is organized as a speed game between individuals or firms – the *miners* – with different computational powers to solve a mathematical problem, bring a proof of work, spread their solution and reach consensus among the Bitcoin network nodes with it. First, we define and specify this game. Second, we analytically find its Nash equilibria in the two-player case. We analyze the parameters for which the miners would face the proper incentives to fulfill their function of transaction processors in the current situation. Finally, we study the block space market offer.

1. Introduction

Bitcoin is a network protocol that enables individuals to transfer property rights on account units called "bitcoins", created in limited quantity. When an individual sends some bitcoins to another individual, this information is broadcast to the peer-to-peer Bitcoin network. However, for technical purposes we won't address here, this transaction needs to be included – together with other transactions forming a *block* – in the *blockchain* in order to be confirmed and secured. As a consequence, the blockchain is a public ledger that contains the whole history of all the transactions of bitcoins ever processed and all Bitcoin users can trust this decentralized, distributed ledger.

It is the role of *miners* to do this work of confirming and securing transactions through insertion in the blockchain. Practically and slightly simplifying, for any miner, this work consists in considering a set of transactions that are present in the network, solving a mathematical problem that depends on this set and spreading the result to the Bitcoin network for this solution to be checked and for it to reach consensus. Once all these steps are done successfully, the set of transactions considered by the miner forms a block that is added on top of the blockchain. The first miner to succeed in this process is rewarded in bitcoins for his useful work.

In the current implementation of Bitcoin, this reward comes from both an *ex-nihilo* creation of some new bitcoins and some fees Bitcoin users can add to their transactions. Since some bitcoins are created in the mining process and in order to control the monetary base, mining is made more complex than it could be. And, since in a first approximation, the probability for each miner to solve a mining problem depends on his computational power, the complexity of mining is made proportional to the total computational power of all miners. More precisely, the complexity is

*

†N. Houy (houy@gate.cnrs.fr) is an economics researcher at the Groupe d'Analyse et de Théorie Economique (GATE) at the University of Lyon, France.
*1PcPoNQ1YMihqumZzTzQirkGudZJB7EZ3E

dynamically adjusted so that a block solving – and hence a creation of bitcoins – occurs every ten minutes in expectation. Once a block is inserted in the blockchain, the mathematical problem faced by all miners are modified and we can consider that a fresh new speed game starts between miners. Hence, the whole building of the blockchain can be considered as independent block insertions from the miners' point of view.

In this article, we tackle the question of the incentives faced by the miners as a function of the reward scheme and values. First, let us see the possible gains for a miner. As it is today, the fixed reward is 25 bitcoins (BTC) per block. The variable reward is typically 10^{-4} BTC per transaction today but it can also be considered as the price on the market for space in blocks.[1] Second, let us see the cost structure. When mining a block, a miner is free to choose which of the transactions in the network he wishes to include in the block he is trying to solve. In a very good first approximation, computing the mining mathematical problem with more transactions included in it is not more expensive in terms of CPU, disk or bandwidth use. However, it should be considered that the larger a block, the longer it takes for it to be spread in the Bitcoin network and reach consensus. Then, including transactions in a block can have the adverse effect of lowering the probability of a miner to earn any reward. When a block is mined but is outraced by another one, it becomes *orphaned* and all associated rewards are lost for its finder. Then, there exists a tradeoff problem that sets the number of transactions miners should include in their blocks. However, as we will show, the solution to this tradeoff depends on how many transactions other miners include in the block they are trying to mine. Then, the number of transactions included in blocks is the outcome of a game: the Bitcoin mining game that we propose to study in this article. Notice that our study is inspired by the qualitative intuitions given by Andresen.[19] It is also of importance in the current context of hot debates about the block size limit that should be imposed in the Bitcoin protocol. Indeed, this debate is much about the transaction space offer function of miners. For instance, Rizun constructs this offer function in a decision theory framework considering the costs and benefits mentioned above and atomistic miners.[29] In this article, we show that the game theory framework is more adapted to tackle this question.

In Section 2, we describe the Bitcoin mining game. In Section 3, we analytically study the Nash equilibria of this game in the case of two miners. In Section 4, we study the current situation of the Bitcoin mining environment. We show that Bitcoin miners are currently not playing strategies of a Nash equilibrium for the typical fee.[2] Indeed, a unilateral deviation by any miner could increase his benefit by about 1%. We also show that with the current incentives, all miners should simply play the strategy of including no transaction in their blocks. Finally, we will show that, *ceteris paribus*, the equilibrium where no miner includes a transaction in a block will stop being one in about 5 years or today if the transaction fee is increased by a factor greater than 3. In Section 5, we study implications in terms of block space market offer. Section 6 concludes.

2. Model

Let us consider a set $N = \{1,...,N\}$ of miners in the Bitcoin network with $N \geq 2$.[3] Each miner $i \in N$ has a relative computational power $h_i > 0$ such that $\sum_{j \in N} h_j = 1$. Miners play against each other in a race to find the solution of a mathematical problem. This mathematical problem is

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

solved by a try and guess strategy and the occurrence of solving the problem can be modeled as a random variable following a Poisson process. As explained in the introduction, the complexity of finding a block is dynamically adjusted so that this operation takes $T = 600$ seconds in expectation. Then, the mining Poisson process has a fixed parameter T^{-1} for the whole network of miners.

The set of transactions included in a block to be solved is chosen by each miner. This set has no effect on the cost to solve it in a first approximation. However, once a miner has found a block with a given set of transactions in it, he needs to broadcast his solution to the Bitcoin network and his solution must reach consensus. The time needed for a block to reach consensus is dependent on its size and hence on the set of transactions in it. Let $\tau(Q)$ be the time needed for a block with size Q to reach consensus. We will make the assumption that this time function is linear, $\tau(Q) = z.Q$ with $z > 0$.[4] The first miner to find a block that reaches consensus earns (in bitcoins) a fixed reward, $R \geq 0$, and a variable one, $\rho.Q$, with $\rho \geq 0$ the fee density.

2.1. Mining payoffs—Let us first compute the mining benefit earned by miners. We assume that all miners start trying to find a new block at the same time, $t = 0$. Each miner $i \in N$ tries to mine a block with size $Q_i \geq 0$, with, for the sake of simplicity, $Q_i \in \mathbb{R}^+$. Let $\overrightarrow{Q} = (Q_1, ..., Q_N)$ be the sequence of sizes for the next block to be found, one for each miner. Obviously, using standard Poisson process results, the probability for i to find a block between t and $t + dt$ and that this block will be the first to reach consensus is:[6]

$$\left[\prod_{j \in N, t+\tau(Q_i)-\tau(Q_j) \geq 0} \exp(-h_j T^{-1}(t + \tau(Q_i) - \tau(Q_j))) \right] h_i T^{-1} dt. \tag{1}$$

After simple calculation, for any miner $i \in N$, the probability $P_i(\overrightarrow{Q})$ to find a block and that this block will be the first to reach consensus is the integral of Equation 1 between $t = 0$ and $t = \infty$. It can be rewritten as

$$P_i(\overrightarrow{Q}) = h_i T^{-1} \int_{t=0}^{\infty} \exp\left(-T^{-1} \left((1 - B_i(\overrightarrow{Q}, t))(t + \tau(Q_i)) + A_i(\overrightarrow{Q}, t) - \overline{\tau}(\overrightarrow{Q}) \right) \right) dt,$$

where

$$\overline{\tau}(\overrightarrow{Q}) = \sum_{j \in N} h_j \tau(Q_j),$$

and $\forall i \in N, \forall t > 0$,[6]

$$B_i(\overrightarrow{Q}, t) = \sum_{j \in N} h_j \mathbb{1}_{(\tau(Q_j) > t + \tau(Q_i))},$$

$$A_i(\overrightarrow{Q}, t) = \sum_{j \in N} h_j \tau(Q_j) \mathbb{1}_{(\tau(Q_j) > t + \tau(Q_i))}.$$

The expected reward $\Pi_i(\overrightarrow{Q})$ is equal to the probability to find the first block to reach consensus times the reward if this is the case.

$$\Pi_i(\overrightarrow{Q}) = (R + \rho.Q_i) P_i(\overrightarrow{Q}). \tag{2}$$

The following proposition is straightforward from Equations 1 and 2.[7]

Proposition 1. *Let $i \in N$ and $\overrightarrow{Q} \in (\mathbb{R}^+)^N$.*

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

(1) $[] \forall j \in N \setminus \{i\}, \dfrac{\partial \Pi_i(\overrightarrow{Q})}{\partial Q_j} \geq 0$,

(2) $[] \forall j \in N \setminus \{i\}, \dfrac{\partial \Pi_i(\overrightarrow{Q})}{\partial Q_j} > 0$ *whenever* $(R + \rho.Q_i) > 0$,

(3) $[] \dfrac{\partial \Pi_i(\overrightarrow{Q})}{\partial Q_i} < 0$ *whenever* $\rho = 0$ *and* $R > 0$,

(4) $[] \dfrac{\partial \Pi_i(\overrightarrow{Q})}{\partial Q_i} = 0$ *whenever* $\rho = 0$ *and* $R = 0$.

Proposition 1 ((1)-(2)) shows that considering larger blocks by a miner has positive externalities on other miners. Indeed, when a miner $i \in N$ tries to solve a larger block, he makes the time needed to spread his block longer, in turn allowing more time for other miners to find the next block, spread it to the network and reach consensus with it. Then, the expected profit of a miner increases with the size of blocks other miners consider. However, notice that this does not imply that the expected reward Π_i is necessarily a decreasing function of Q_i. Indeed, because the set of transactions in a block is not constant, the mining race is not a constant-sum game. More precisely, it is true that trying to solve a larger block decreases i's probability to find it and reach consensus with it first (Proposition 1 ((3)-(4))). But it also increases the reward he earns in case he is actually the first one to find and spread the next block to consensus. Notice also that, in general, considering a larger block by a miner modifies the marginal – with respect to their own block size decisions – probability of other miners to be rewarded. This implies that the decisions regarding the sizes of their blocks by miners should be treated in a game theoretical framework rather than in a decision theoretical framework.

Proposition 2 shows that the sum of the expected rewards for all miners has no maximum since it increases with the size of blocks and we considered for now that this value has no upper limit.[8]

Proposition 2. *Let* $\rho > 0$ *and let* $\overrightarrow{Q}, \overrightarrow{Q'} \in (R^+)^N$. *If* $\overrightarrow{Q} > \overrightarrow{Q'}$, *then* $\sum_{i \in N} \Pi_i(\overrightarrow{Q}) > \sum_{i \in N} \Pi_i(\overrightarrow{Q'})$.

Notice that, obviously, when $\rho = 0$, the sum of the expected rewards equals R regardless of $\overrightarrow{Q}$ and Proposition 2 does not apply.

Finally, we will need the following lemma in the remainder of our article. Assume that all miners consider blocks with the same size, formally, $\forall i \in N, Q_i = Q$. Then, for each miner $i \in N$, the probability to earn the reward associated with a block solving is just the probability to solve the mining mathematical problem first and hence is directly proportional to the relative computational power h_i. Formally, in this case, $\forall i \in N, \forall t \geq 0, A_i(\overrightarrow{Q}, t) = B_i(\overrightarrow{Q}, t) = 0$ and Lemma 2.1 is proved with simple calculation.

Lemma 2.1. *Let* $\overrightarrow{Q} \in (\mathbb{R}^+)^N$ *be such that* $\forall i \in N, Q_i = Q$. *Then, for all* $i \in N$, $P_i(\overrightarrow{Q}) = h_i$ *and* $\Pi_i(\overrightarrow{Q}) = (R + \rho.Q)h_i$.

2.2. The Bitcoin mining game—We call the Bitcoin mining game, the game $\mathcal{G} = (N, (S_i)_{i \in N}, (\Pi_i)_{i \in N})$ where N is the set of players, $(S_i)_{i \in N}$ with $\forall i \in N, S_i = \mathbb{R}^+$ is the set of strategies and $(\Pi_i)_{i \in N}$ as described in Equation 2 is the set of payoff functions.

For each miner $i \in N$, the correspondence of best response for the size of the block to mine,

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

$\mathcal{B}_i$, is given by solving the following maximization program.

$$\mathcal{B}_i(\overrightarrow{Q}_{-i}) = \arg\max_{Q_i \in \mathbb{R}^+} \Pi_i(\overrightarrow{Q}). \tag{3}$$

with the usual meaning for the notation $\overrightarrow{Q}_{-i} = (Q_1, ..., Q_{i-1}, Q_{i+1}, ..., Q_N)$.

Let $\mathcal{E} \subseteq (\mathbb{R}^+)^N$ be the set of Nash equilibria of the Bitcoin mining game. Formally, $\forall \overrightarrow{Q^*} = (Q_1^*, ..., Q_N^*) \in (\mathbb{R}^+)^N$, $\overrightarrow{Q^*} \in \mathcal{E}$ if and only if $\forall i \in N, Q_i^* \in \mathcal{B}_i(\overrightarrow{Q^*}_{-i})$.

3. The two-miner case

For the sake of simplicity, we now concentrate on the case with $N = 2$ even though most of our results can be generalized to the $N > 2$ case with no logical difficulty but at the price of cumbersome calculation.[9]

Let us consider the Bitcoin mining game $\mathcal{G}$ with $N = \{1,2\}$. For any miner $i \in N$, if $Q_i \geq Q_{3-i}$,[10] then $\forall t > 0$, $A_i((Q_1,Q_2),t) = B_i((Q_1,Q_2),t) = 0$. Then, the expected reward earned by miner i is

$$\Pi_i(Q_1,Q_2) = (R + \rho.Q_i)h_i \exp\left(-(1-h_i)T^{-1}(\tau(Q_i) - \tau(Q_{3-i}))\right).$$

Following, assume $Q_i < Q_{3-i}$, the expected reward earned by miner i is

$$\Pi_i(Q_1,Q_2) = (R + \rho.Q_i)\left(1 - (1-h_i)\exp\left(-h_i T^{-1}(\tau(Q_{3-i}) - \tau(Q_i))\right)\right).$$

Our first result is rather trivial and follows directly from Proposition 1((3)). When $\rho = 0$ and $R > 0$,[11] considering a larger block has the only consequence to make longer the period needed for a miner's block to reach consensus. The marginal reward associated with this inclusion is 0. Hence, there are only negative incentives for miners to include transactions in blocks.

Proposition 3. *Let $\rho = 0$ and $R > 0$. The Bitcoin mining game has a unique Nash equilibrium $(Q_1^*, Q_2^*) \in (\mathbb{R}^+)^2$ with $Q_1^* = Q_2^* = 0$. Moreover, $\Pi_1(Q_1^*, Q_2^*) = h_1 R$ and $\Pi_2(Q_1^*, Q_2^*) = h_2 R$.*

For non trivial cases with $\rho > 0$, let us first concentrate on the game with symmetric computational power, $h_1 = h_2 = 1/2$. In this case, there exists a unique Nash Equilibrium and it is symmetric.

Proposition 4. *Let $\rho > 0$. Assume $h_1 = h_2 = 1/2$. The Bitcoin mining game has a unique Nash equilibrium $(Q_1^*, Q_2^*) \in (\mathbb{R}^+)^2$ with $Q_1^* = Q_2^* = \max\left\{0, \frac{2T}{z} - \frac{R}{\rho}\right\}$. Moreover, $\Pi_1(Q_1^*, Q_2^*) = \Pi_2(Q_1^*, Q_2^*) = \max\left\{R/2, \frac{\rho.T}{z}\right\}$.*

Now, let us study the asymmetric case. With no loss of generality, let us assume $h_1 > h_2$.

Proposition 5. *Let $\rho > 0$. Assume $h_1 > h_2$. The Bitcoin mining game has a unique Nash equilibrium $(Q_1^*, Q_2^*) \in (\mathbb{R}^+)^2$ with*

- *if $\frac{T}{z(1-h_1)} - \frac{R}{\rho} \leq 0$, $Q_1^* = Q_2^* = 0$.*
- *if $\frac{T}{z(1-h_1)} - \frac{R}{\rho} > 0$, $Q_1^* = \frac{T}{z(1-h_1)} - \frac{R}{\rho} > Q_2^* \geq 0$.*

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

Then, in the asymmetric case, we can notice that in all cases, the size of the block looked for by the miner with the greatest computational power is larger than the size of the block looked for by the miner with the lowest computational power. Moreover, there is a set of parameters for which considering the smallest block possible for both miners is the only Nash equilibrium of the Bitcoin mining game. Now, the question is to know whether this set of parameters is relevant to Bitcoin. One way to check this is to study the Bitcoin environment as it is today.

4. The current case

In this Section, we study the current behavior of the miners in the Bitcoin network. In fact, miners can be mining pools but, for the sake of simplicity,[12] we will make no difference as we will consider that the best strategy for a miner is the same whether it is a pool or a single miner, benefits being redistributed among the participants of a mining pool, proportionally to the computational power they bring along to their pool. All the data we need for this study is public in the Bitcoin blockchain and protocol or relies on the simplifying assumption that, today, all miners include all the transactions present in the network when trying to find a block.[13] We will also work with a typical fee of 10^{-4} BTC per 0.6kB transaction. Unless otherwise stated, the values for our computations are displayed in Table 1.

Table 1. Data values.

Data	Value	Dimension	Description and Source
T	600	second	Bitcoin protocol parameter.
s	0.6	kB	Average transaction size, statistics from the blockchain.
z	0.017	second.kB^{-1}	Marginal time needed to reach consensus per kB.[29,31,32]
z_s	0.0102	second.tx^{-1}	Marginal time needed to reach consensus per transaction (tx), $z \times s$.
c	10^{-4}	BTC	Typical fee for a low priority 0.6 kB transaction.
R	25	BTC	Bitcoin protocol current implementation parameter.

Let us start our analysis of the current situation as displayed in Table 2. In reality, transactions can have different sizes and require different levels of fees to be computed. The size of a transaction depends on many parameters (number of inputs and outputs mainly) but not directly on the amount paid in the transaction. Throughout this section, we will make the simplifying assumption that all transactions have the same size. 884 is the average number of transactions in the blocks inserted in the blockchain between blocks 377,261 and 378,260. The average size of a transaction over the same period is 600 bytes.

We will also consider that the Bitcoin network computational power is distributed as shown in Table 2 (column B). We inferred these relative computational powers of miners from an analysis of

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

the blocks found. Indeed, we make, as already noted, the assumption that all miners include all the transactions in the network in their blocks. Formally, with our notation, $\forall i \in N, Q_i = 884 \times 0.6kB$. Then, by Lemma 2.1, the probability to solve a block for any miner is exactly equal to his relative computational power. Further, we make the assumption that the frequency of blocks found by a miner, that we can observe, is the best estimation of the probability that he solves a block and, hence, the best estimation of his relative computational power.

We can now consider each miner and compute his best response to the other miners' current strategy. This optimal number of 0.6kB transactions to include in the current computed block is 0 for all miners (column D). This shows that the current situation is not a Nash Equilibrium and *all* miners have a profitable deviation. If unilaterally mining blocks with no transaction, a miner would increase his probability to earn the fixed 25 BTC reward (as displayed in column E) at the cost of the $884 \times 10^{-4} = 0.0884$ BTC variable reward in case of successful mining. In the current case, this deviation would lead to a higher expected benefit (columns F,G).

Table 2. A: miner's name, B: relative computational power, C: expected reward when $\forall i \in N, Q_i = 884 \times 0.6kB$, D: optimal number of transaction included by miner i in the current block when $\forall j \in N \setminus \{i\}, Q_j = 884 \times 0.6kB$ (solution to Equation 3), E: probability to be the first miner to find a block reaching consensus when $\forall j \in N \setminus \{i\}, Q_j = \times 0.6kB$ and Q_i given in D, F: expected reward when $\forall j \in N \setminus \{i\}, Q_j = 884 \times 0.6kB$ and Q_i given in D, G: F-C difference in %. H: expected reward of miners in BTC when $\forall i \in N, Q_i = 0$.

A	B	C	D	E	F	G	H
F2Pool	18.900%	4.74171	0	19.130%	4.78251	0.860%	4.725
AntPool	18.200%	4.56609	0	18.423%	4.60586	0.871%	4.550
Bitfury	14.400%	3.61273	0	14.585%	3.64626	0.928%	3.600
BTCC	13.100%	3.28658	0	13.271%	3.31773	0.948%	3.275
KNCMiner	8.100%	2.03216	0	8.212%	2.05295	1.023%	2.025
BW Pool	7.200%	1.80636	0	7.300%	1.82509	1.037%	1.800
Slush	6.900%	1.73110	0	6.996%	1.74912	1.041%	1.725
21 Inc.	3.900%	0.97845	0	3.956%	0.98908	1.086%	0.975
Eligius	3.500%	0.87809	0	3.551%	0.88769	1.092%	0.875
GHash.IO	1.900%	0.47668	0	1.928%	0.48200	1.116%	0.475
Telco 214	1.600%	0.40141	0	1.624%	0.40591	1.121%	0.400
BitMinter	0.700%	0.17562	0	0.710%	0.17761	1.135%	0.175
Other	0.500%	0.12544	0	0.507%	0.12687	1.138%	0.125
EclipseMC	0.400%	0.10035	0	0.406%	0.10150	1.139%	0.100
Kano CKPool	0.300%	0.07527	0	0.304%	0.07612	1.141%	0.075
Solo CKPool	0.200%	0.05018	0	0.203%	0.05075	1.142%	0.050
BitClub Network	0.100%	0.02509	0	0.102%	0.02538	1.144%	0.025
P2Pool.org	0.100%	0.02509	0	0.102%	0.02538	1.144%	0.025

We can also check that all miners including no transaction in the block they are mining

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

$(\forall i \in N, Q_i = 0)$ is a Nash Equilibrium with the current parameters given in Table 1. The expected reward for miner i, in this case where $\forall j \in N, Q_j = 0$ is $h_i R$ by Lemma 2.1. The actual values are given in Table 2, column H.

Now, we study the conditions under which the situation where all miners include no transaction in their blocks is a Nash equilibrium. From Equation 2, it is straightforward to see that $\Pi_i(\overrightarrow{Q}) = (R + \rho Q_i) h_i \exp\left(-T^{-1}(1-h_i)\tau(Q_i)\right)$ whenever $\overrightarrow{Q}$ is such that $\forall j \in N \setminus \{i\}, Q_j = 0$. Then, since $\rho > 0$, the best response number of transactions to include in a block by $i \in N$ is[13] $\arg\max_{x_i > 0} \Pi_i(\overrightarrow{Q}) = \{\max\{0, \frac{T}{(1-h_i)z} - \frac{R}{\rho}\}\}$. Then, the situation where all miners include no transaction in their blocks stops being a Nash equilibrium when $\exists i \in N, \frac{cT}{(1-h_i)z_s} > R$. The highest value of R for which this occurs is $R \approx 7.25$ BTC below which F2Pool will have an incentive to include some transactions in the blocks it mines. The fixed reward was 50 BTC in 2009, in the first days of Bitcoin. This amount is halved every 210,000 blocks (about 4 years). Then, the situation with $R \leq 7.25$ BTC will occur in about 5 years when $R = 6.25$ BTC.[15] Obviously, this 5 years projection should be seen as an illustration rather than a prediction. Indeed, it would certainly be unsound to state that, during the next 5 years, the mining environment will remain unchanged, especially regarding the computational power distribution among miners and z that highly depends on bandwidth. Moreover, the equality between the time needed to mine 210,000 blocks and 4 years is inaccurate if, as it is the case today, the actual computational power of the Bitcoin network is continuously and significantly increasing and hence above the predicted computational power at each difficulty adjustment.

Equivalently, the lowest value of c for which the situation where all miners include no transaction in their blocks is not a Nash equilibrium is $c \approx 3.4 \times 10^{-4}$ BTC. This corresponds to an increase from the current value of the transaction fee of a factor approx. 3.5. At the time this article is written, 3.4×10^{-4} BTC can be bought for about \$0.15. With $R = 25$ BTC and $c = 10^{-4}$ BTC, we can estimate the maximal value of z for which all miners mining empty blocks is not a Nash equilibrium of the Bitcoin mining game with the current computational powers. After simple calculation, this value is $z \approx 0.0049$ s.kB^{-1}.

5. Block space offer

In this section, we study the relationship between Rizun[29] and our study. In particular, we look at the implications in terms of block space offer. Rizun (Equation 10[29]) finds the following expression for the block space offer on the market as a function of ρ,

$$Q = \max\{0, \frac{T}{z} \ln\left(\frac{\rho T}{zR}\right)\}, \tag{4}$$

where, with our notation, $Q = \sum_{i \in N} \Pi_i(\overrightarrow{Q}) Q_i$. In order to obtain this result, Rizun[29] makes two implicit assumptions: a) there is an infinite number of symmetric atomistic miners, and b) miners consider that others mine empty blocks, which implies the orphaning probability (Rizun's Equation 4[29]) as suggested by Andresen.[19] In order to be in the same framework, we will also make the assumption of an infinite number of symmetric atomistic miners. In this case, we find[16]

$$Q = \max\{0, \frac{T}{z} - \frac{R}{\rho}\}, \tag{5}$$

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

In Fig. 1, we display Q as a function of ρ as obtained in Equations 4 and 5 for parameter as given in Table 1.

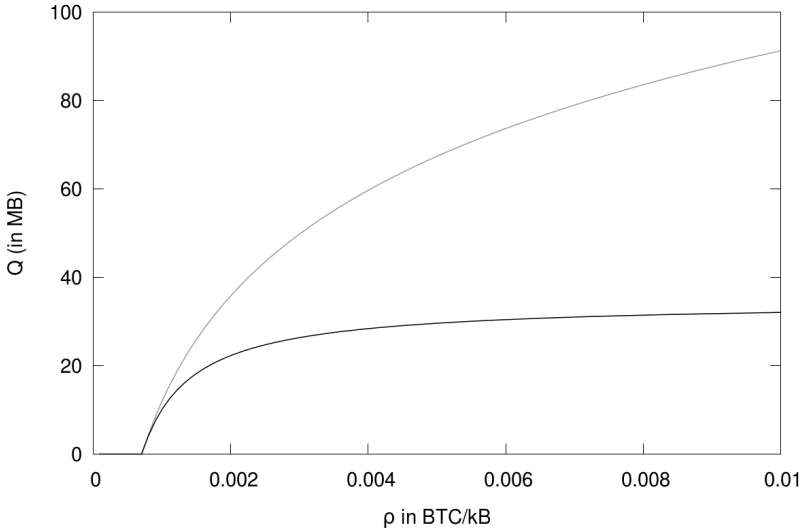

Fig. 1. Q as a function of ρ as obtained in Equations 4 (light grey) and 5 (black).

Since we consider the case with atomistic miners, the only reason why Equations 4 and 5 differ is the following. Rizun[29] considers that decisions are made by miners considering other miners try to mine empty blocks. On the contrary, we consider that, at the Nash equilibrium, miners consider the optimal decision made by other miners. Obviously, close to the point where miners actually mine empty blocks, both assumptions coincide. This is why we can see that Q as obtained in Equations 4 and 5 are strictly positive for the same values of ρ, *i.e.* when $\rho > zR/T$ and are equal for small deviations of ρ above zR/T.

Another important difference between Equations 4 and 5 is that when ρ tends to infinity, Equation 4 has no upper bound whereas Q tends to T/z from below in Equation 5.[17] The reason why Q has an upper bound in our model is as follows: as ρ increases, all miners are willing to include more transactions in their blocks in order to enjoy larger variable rewards. However, as other miners include more transactions in their blocks, this makes the incentive to outrace them by decreasing the size of the block to be found more important. And hence, this limits the trend to always include more transactions. This negative feedback does not exist in Rizun[29] because the changes of behavior by other miners is not considered.

6. Conclusion

In this article, we have introduced and studied the Bitcoin mining game. When miners make a decision regarding how many transactions they should include in the block they are mining, they must study the tradeoff between, on the one side, including more transactions and hence earn more transaction fees if they find the current block first and, on the other side, including less transactions in order to decrease the time they need to spread their block solution and reach consensus with it, hence increase their probability to include their block in the blockchain first. We have studied the two-miner case analytically. We have also showed that, in the current Bitcoin mining environment, miners are not playing strategies of a Nash equilibrium of the Bitcoin

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

mining game as we stated it. Instead, they should all stop including any transaction in their blocks. We showed that this situation where all miners do not include any transaction in their blocks would stop being a Nash Equilibrium if the transaction fee was multiplied or, equivalently, the fixed reward divided by a factor greater than 3. Finally, we studied the difference between our game theoretical approach and the decision theoretical approach displayed in Rizun.[29]

We can see three limitations to our study. The first one is about the sensitivity of our results to the parameters' values. Our result stating that, at the Nash equilibrium, miners should not include transactions in their blocks is strongly dependent on, for instance, the marginal time needed to reach consensus. We took the best estimate for this parameter, $0.017s.kB^{-1}$ but it may be the case that it is smaller in reality and hence, the current case be a Nash Equilibrium. Another assumption of ours is that transactions are all the same in size. In reality, it is not the case and considering this could change some results in a more detailed version of our model.

The second limitation of our study is about the security of the Bitcoin protocol. For Bitcoin to be used as an efficient payment system, it is a minimal necessary requirement that transactions be processed. However, this is not sufficient. Indeed, Bitcoin is vulnerable to what are called 51% attacks.[22,24,26] Such attacks can occur when a miner can solve too many blocks in a row in expectation. It is usually said that this is the case when a miner owns strictly more than 50% of the computational power.[18] In order to make such an attack costly, the total computational power of the Bitcoin network should be as large as possible. Since we did not consider the computational power as an endogenous variable, what matters in our study when an agent makes his decision regarding the number of transactions to be included in his block is the ratio between the fixed and the variable rewards (R/ρ). However, the miners' benefits that will drive the computational power purchase and hence eventually decide on the security of Bitcoin will depend on R and ρ in absolute values. This aspect has already been studied, though in a different context.[25]

The second limitation is about the value of the Bitcoin network. Miners are rewarded in bitcoins. Hence, they have a vested interest in it to function well. Miners know that not processing transactions in their blocks means that Bitcoin loses some if not all of its value. Hence, any reward they may earn from their mining activity has no value either in this case. This suggests that the Bitcoin mining game should include a supplementary public good game on top of it. Other reasons could explain why, even though it may theoretically not be an equilibrium to include transactions in blocks today, miners still do so. The power of default, ideology, fear to appear as a free-rider in the eyes of the Bitcoin community or non-awareness of the theoretical predictions could be such reasons.

Today, there is a debate in the Bitcoin developers community about the variable cost ρ. Should it be encoded and imposed in the protocol as it is partially today or should it be left to the market to decide its value? In the market case, if Bitcoin users want their transactions to be processed, then, they should attach to them a high enough fee. We believe that this paper gives a first result in the study of such a market: if a market was to be organized, with today's parameter, the transaction processing offer would be non null for transactions fees at least 3.4×10^{-4} BTC. For other reasons, we are rather uncertain about the relevance of such a market because of the large externalities induced by the mining activity. It is well-known that markets are not efficient when externalities are at play.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

Acknowledgement

I am grateful to three anonymous referees who helped me significantly improve the quality of this work. Still, all existing errors would remain my full responsibility.

Notes and References

[1] The transaction fee is usually proposed by the user's wallet. It is in fact a function of many parameters we will not consider here for the sake of simplicity. It also is related to the minimum relay fee needed for a transaction to be relayed in the network. We only consider the typical case of a low-priority transaction with size smaller than 1 kilobyte. This proposition is not mandatory, it is depending on the software used to send bitcoins and is not coded as a part of the Bitcoin protocol. See `https://bitcoin.org/en/developer-guide#transaction-fees-and-change` for more information.

[2] Notice that some other works have shown that the "standard" behavior implicitly assumed in the Bitcoin protocol is hardly an equilibrium.[20,22,23,30]

[3] With a slight lack of rigor but with no risk of confusion, N denotes both the set of miners and the cardinality of this set.

[4] This linear approximation is acceptable for the numerical simulations we run in Section 4.[31,32] Also, it would certainly be more appropriate to add a constant term in the τ function definition, see Decker and Wattenhofer.[21] We will only use the τ function in differences so that this constant term would have no effect on our results.

[5] This expression is then the joint probability that a) i finds the block between t and $t+dt$ (this occurs with probability $h_i T^{-1} dt$), and b) no other miner j reaches consensus with a block before i does (i reaches consensus in $t+\tau(Q_i)$ if he finds a block in t), which is equivalent to saying that no other miner j found a block between 0 and $t+\tau(Q_i)-\tau(Q_j)$, which occurs with probability $\exp(-h_j T^{-1}(t+\tau(Q_i)-\tau(Q_j)))$.

[6] For any proposition p, the indicator function $\mathbb{1}_p$ is equal to 1 if p is true, 0 otherwise.

[7] For two sets of miners $I, J \subseteq N$, $I \setminus J$ is the set of miners in I and not in J.

[8] The proof is straightforward and therefore omitted. Notation: $\forall \overrightarrow{Q}, \overrightarrow{Q'} \in (R^+)^N$, we write $\overrightarrow{Q} > \overrightarrow{Q'}$ if $\forall i \in N, Q_i \geq {Q'}_i$ and $\exists i \in N, Q_i > {Q'}_i$.

[9] Obviously, having $N=2$ would be of great concern for the security of the Bitcoin protocol. Our purpose here is only to show some intuitions about the model rather than derive realistic results.

[10] Obviously, if $i=1$ then $3-i=2$ and if $i=2$ then $3-i=1$.

[11] Obviously, when both $\rho=0$ and $R=0$, the result is even more trivial since any miner's payoff is 0 whatever the actions by all players, see Proposition 1((4)).

[12] See prior studies about mining pools and the qualitative differences between them and solo miners.[22,23,27]

[13] The data we use from the blockchain come from the 1,000 blocks between blocks 377,261 (mined on Oct. 3, 2015 1:49 PM) and block 378,260 (mined on Oct. 10, 2015 1:27 PM). Data about the protocol can be found in the Bitcoin open-source code; see Nakamoto.[28]

[14] The proof is similar to the proof of Lemma 1.4 given in Appendix and is therefore omitted.

[15] Obviously, this 5 years projection should be seen as an illustration rather than a prediction. Indeed, it would certainly be unsound to state that, during the next 5 years, the mining environment will remain unchanged, especially regarding the computational power distribution among miners and z that highly depends on bandwidth. Moreover, the equality between the time needed to mine 210,000 blocks and 4 years is inaccurate if, as it is the case today, the actual computational power of the Bitcoin network is continuously and significantly increasing and hence above the predicted computational power at each difficulty adjustment.

[16] The proof is similar to the proof of Proposition 4 and therefore, it is omitted.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

[17] This ≈30 MB block size bound has been emphasized by Stone and corresponds to the size of the block that would require $T = 600$ seconds to reach consensus.[31]

[18] Actually, as we showed, at the outcome of the Bitcoin mining game, the probability to solve a block is not necessarily equal to the relative computational power.

[19] Andresen, G. "Back-of-the-envelope calculations for marginal cost of transactions," (2013) (Accessed 3 March 2014) `https://gist.github.com/gavinandresen/5044482`.

[20] Courtois, N.T. and Bahack, L. "On subversive miner strategies and block withholding attack in Bitcoin digital currency," (2014) arXiv: 1402.1718.

[21] Decker, C., Wattenhofer, R. "Information propagation in the Bitcoin network," *13th IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, September 2013* (2013)

[22] Eyal, I. and Sirer, E.G. "Majority is not enough: Bitcoin mining is vulnerable," (2013) arXiv: 1311.0243.

[23] Eyal, I. "The miner's dilemma,"(2014) arXiv: 1411.7099.

[24] Houy, N. "It will cost you nothing to 'kill' a proof-of-stake crypto-currency," *Economics Bulletin* 34.2 1038-1044 (2014).

[25] Houy, N. "The economics of Bitcoin transaction fees," working paper, GATE (2014).

[26] Kroll, J. A., Davey, I. C., Felten, E.W. "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries," *Mimeo* (2013).

[27] Lewenberg, A., Bachrach, Y., Sompolinsky, Y., Zohar, A., Rosenschein, J. S. "Bitcoin mining pools: A co-operative game theoretic analysis," *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems* 919-927 (2015).

[28] Nakamoto, S. "Bitcoin: a peer-to-peer electronic cash system," (2009).

[29] Rizun, P.R. "A transaction fee market exists without a block size limit," (2015). `https://dl.dropboxusercontent.com/u/43331625/feemarket.pdf`.

[30] Sapirshtein, A., Sompolinsky, Y., Zohar, A. "Optimal selfish mining strategies in Bitcoin," (2015) arXiv: 1507.06183.

[31] Stone, A. "An examination of single transaction blocks and their effect on network throughput and block size," (2015) `http://www.bitcoinunlimited.info/1txn/`

[32] No Author. "Bitcoin Network Capacity Analysis – Part 6: Data Propagation," *Tradeblock* (3 June 2013) (accessed 20 December 2015) `https://tradeblock.com/blog/bitcoin-network-capacity-analysis-part-6-data-propagation`

Appendix A:

Most of our analytical results are proved using the following lemmas.

Let us first define the following functions:

$$\Pi^{+}(Q_i, Q_{3-i}) = (R + \rho.Q_i)h_i \exp\left(-(1-h_i)T^{-1}(\tau(Q_i) - \tau(Q_{3-i}))\right),$$

$$\Pi_i^{-}(Q_i, Q_{3-i}) = (R + \rho.Q_i)\left(1 - (1-h_i)\exp\left(-h_i T^{-1}(\tau(Q_{3-i}) - \tau(Q_i))\right)\right).$$

Then, Π^{+} is the expected profit of a miner that would include more transactions than the other miner. Π^{-} is the expected payoff of a miner that would include strictly less transactions than the other miner (these functions are still both defined on $(\mathbb{R}^{+})^2$).

Lemma 1.1 states that $\forall i \in N = \{1,2\}, \Pi_i(Q_1, Q_2)$ is continuous and has a continuous derivative with respect to Q_i at $Q_i = Q_{3-i} > 0$.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

Lemma 1.1. $\Pi^+(Q_i, Q_{3-i}) = \Pi^-(Q_i, Q_{3-i})$ *at* $Q_i = Q_{3-i}$.

Proof. With simple calculation, it is straightforward to show that $\Pi^+(Q_i, Q_{3-i}) = (R+\rho Q_i)h_i = \Pi^-(Q_i, Q_{3-i})$ in $Q_i = Q_{3-i}$.

Lemma 1.2. $\dfrac{\partial \Pi^+(Q_i, Q_{3-i})}{\partial Q_i} = \dfrac{\partial \Pi^-(Q_i, Q_{3-i})}{\partial Q_i}$ *at* $Q_i = Q_{3-i}$.

Proof. It is easy to get $\dfrac{\partial \ln(\Pi^+(Q_i, Q_{3-i}))}{\partial Q_i} = \dfrac{\rho}{R+\rho Q_i} - h_{3-i}T^{-1}z$, and

$$\frac{\partial \ln(\Pi^-(Q_i, Q_{3-i}))}{\partial Q_i} = \frac{\rho}{R+\rho Q_i} - \frac{h_{3-i}h_i z T^{-1}\exp\left(-h_i T^{-1}(\tau(Q_{3-i}) - \tau(Q_i))\right)}{(1 - h_{3-i}\exp\left(-h_i T^{-1}(\tau(Q_{3-i}) - \tau(Q_i))\right))},$$

and it is straightforward to check that both are equal when $Q_{3-i} = Q_i$.

Lemma 1.3. $\dfrac{\partial^2 \Pi^-(Q_i, Q_{3-i})}{\partial Q_i^2} \leq 0.$

Moreover, if $R > 0$ *or* $c > 0$, $\dfrac{\partial^2 \Pi^-(Q_i, Q_{3-i})}{\partial Q_i^2} < 0.$

Proof. Let $P(Q_i, Q_{3-i}) = h_{3-i}\exp\left(-h_i T^{-1}(\tau(Q_{3-i}) - \tau(Q_i))\right)$.

By definition,

$$\Pi^-(Q_i, Q_{3-i}) = (R+\rho Q_i)(1 - P(Q_i, Q_{3-i})).$$

$$\frac{\partial \Pi^-(Q_i, Q_{3-i})}{\partial Q_i} = \rho(1 - P(Q_i, Q_{3-i})) - (R+\rho Q_i)h_i z T^{-1} P(Q_i, Q_{3-i})$$

$$\frac{\partial^2 \Pi^-(Q_i, Q_{3-i})}{\partial Q_i^2} =$$

$$-\rho h_i T^{-1} z P(Q_i, Q_{3-i}) - \rho h_i T^{-1} z P(Q_i, Q_{3-i}) - (R+\rho Q_i)(h_i T^{-1} z)^2 P(Q_i, Q_{3-i}) \leq 0.$$

Moreover, $\dfrac{\partial^2 \Pi^-(Q_i, Q_{3-i})}{\partial Q_i^2} < 0$ if $R > 0$ or $\rho > 0$.

Lemma 1.4. *Assume* $\rho > 0$.

$\dfrac{\partial^2 \Pi^+(Q_i, Q_{3-i})}{\partial Q_i^2} < 0$ *whenever* $Q_i < \dfrac{2}{h_{3-i}T^{-1}z} - \dfrac{R}{\rho}$.

When $Q_i \geq \dfrac{2}{h_{3-i}T^{-1}z} - \dfrac{R}{\rho}$, $\dfrac{\partial \Pi^+(Q_i, Q_{3-i})}{\partial Q_i} < 0.$

Assume $\rho = 0$ *and* $R > 0$. $\dfrac{\partial \Pi^+(Q_i, Q_{3-i})}{\partial Q_i} < 0.$

Proof. Let $P(Q_i, Q_{3-i}) = h_i\exp\left(-h_{3-i}T^{-1}(\tau(Q_i) - \tau(Q_{3-i}))\right)$.

By definition,

$$\Pi^+(Q_i, Q_{3-i}) = (R+\rho Q_i)P(Q_i, Q_{3-i}).$$

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

I. Assume $\rho > 0$.

$$\frac{\partial \Pi^+(Q_i, Q_{3-i})}{\partial Q_i} = \rho P(Q_i, Q_{3-i}) - (R + \rho Q_i) h_{3-i} T^{-1} z P(Q_i, Q_{3-i}),$$

$$\frac{\partial^2 \Pi^+(Q_i, Q_{3-i})}{\partial Q_i^2} = h_{3-i} T^{-1} z P(Q_i, Q_{3-i})((R + \rho Q_i) h_{3-i} T^{-1} z - 2\rho).$$

Then, obviously, $\frac{\partial^2 \Pi^+(Q_i, Q_{3-i})}{\partial Q_i^2} < 0$ whenever $Q_i < \frac{2T}{h_{3-i} z} - \frac{R}{\rho}$. Also, $\frac{\partial^2 \Pi^+(Q_i, Q_{3-i})}{\partial Q_i^2} \geq 0$ whenever $Q_i \geq \frac{2T}{h_{3-i} z} - \frac{R}{\rho}$.

$$\frac{\partial \Pi^+(Q_i, Q_{3-i})}{\partial Q_i} = -\rho P(Q_i, Q_{3-i}) < 0$$

at $Q_i = \frac{2T}{h_{3-i} z} - \frac{R}{\rho}$. Moreover, it is straightforward to check that $\frac{\partial \Pi^+(Q_i, Q_{3-i})}{\partial Q_i}$ is negative when Q_i is arbitrarily large. Then, necessarily, $\frac{\partial \Pi^+(Q_i, Q_{3-i})}{\partial Q_i} < 0$ whenever $Q_i \geq \frac{2T}{h_{3-i} z} - \frac{R}{\rho}$.

II. Assume $c = 0$.

$$\frac{\partial \Pi^+(Q_i, Q_{3-i})}{\partial Q_i} = -R h_{3-i} T^{-1} z P(Q_i, Q_{3-i}) < 0.$$

Appendix B: Proof of Proposition 3

It is straightforward to check that $\frac{\partial \Pi^+(Q_i, Q^*_{3-i})}{\partial Q_i} < 0$ and $\frac{\partial \Pi^-(Q_i, Q^*_{3-i})}{\partial Q_1} < 0$ on $\mathbb{R}^+$. Hence, by Lemma 1.1, $\mathcal{E} = \{(0,0)\}$.

Appendix C: Proof of Proposition 4

Assume $\mathcal{E} \neq \emptyset$. With no loss of generality, let us assume $Q_1^* \geq Q_2^*$. Then, $\Pi_1(Q_1^*, Q_2^*) = \Pi^+(Q_1^*, Q_2^*) = (R + \rho Q_1^*) h_1 \exp\left(-h_2 T^{-1}(\tau(Q_1^*) - \tau(Q_2^*))\right)$.

$\frac{\partial \Pi_1(Q_1, Q_2^*)}{\partial Q_1} = h_1 \exp\left(-h_2 T^{-1}(\tau(Q_1) - \tau(Q_2^*))\right)(\rho - h_2 T^{-1} z(R + \rho Q_1))$ in $Q_1 = Q_1^*$ which has the sign of $(\rho - h_2 T^{-1} z(R + \rho . Q_1^*))$. Then, by continuity of Π^+ and Lemmas 1.1, 1.2 and 1.4, we necessarily have $Q_1^* = \max\{0, \frac{2T}{z} - \frac{R}{\rho}\}$ or $Q_1^* < Q_2^*$ which contradicts the assumption that $Q_1^* \geq Q_2^*$.

Assume $0 > \frac{2T}{z} - \frac{R}{\rho}$, then $Q_1^* = 0$. By assumption, $Q_2^* = 0$. Then, $\Pi_1(Q_1^*, 0) = \Pi_1^+(Q_1^*, 0)$ and it is straightforward to check that $\frac{\partial \Pi^+(Q_1, 0)}{\partial Q_1} < 0$ at Q_1^*. By Lemma 1.4, $Q_1^* = 0$ is the only maximum of $\Pi^+(Q_1, 0)$. Then, $\mathcal{E} = \{(0,0)\}$.

Assume $0 \leq \frac{2T}{z} - \frac{R}{\rho}$. $Q_1^* = \frac{2T}{z} - \frac{R}{\rho}$. Now, it is straightforward to check that $\frac{\partial \Pi_2(Q_1^*, Q_2)}{\partial Q_2} =$

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

$\frac{\partial \Pi^-(Q_2,Q_1^*)}{\partial Q_2} = 0$ in $Q_2 = Q_1^*$. By Lemmas 1.1, 1.2 and 1.3, $\arg\max_{Q_2\in\mathbb{R}^+} \Pi_2(Q_1^*,Q_2) = \frac{2T}{z} - \frac{R}{\rho}$ and then, $\mathcal{E} = \{(\frac{2T}{z} - \frac{R}{\rho}, \frac{2T}{z} - \frac{R}{\rho})\}$.

Similarly to what has been shown above, it is straightforward to check that $(\frac{2T}{z} - \frac{R}{\rho}, \frac{2T}{z} - \frac{R}{\rho}) \in \mathcal{E}$ and then $\mathcal{E} \neq \emptyset$.

Appendix D: Proof of Proposition 5

Let $h_1 > h_2$ and assume that $\mathcal{E} \neq \emptyset$.

I. Assume $Q_1^* \geq Q_2^*$. Then,

$$\Pi_1(Q_1^*,Q_2^*) = \Pi^+(Q_1^*,Q_2^*) = (R+\rho Q_1^*)h_1 \exp\left(-h_2T^{-1}(\tau(Q_1^*) - \tau(Q_2^*))\right).$$

$\frac{\partial \Pi_1(Q_1,Q_2^*)}{\partial Q_1} = h_1 \exp\left(-h_2T^{-1}(\tau(Q_1) - \tau(Q_2^*))\right)(\rho - h_2T^{-1}z(R+\rho Q_1))$ which has the sign of $(\rho - h_2T^{-1}z(R+\rho Q_1))$. Then, by Lemmas 1.1, 1.2 and 1.3, we necessarily have $Q_1^* = \max\{0, \frac{T}{zh_2} - \frac{R}{\rho}\}$ or $Q_1^* < Q_2^*$ which contradicts the assumption that $Q_1^* \geq Q_2^*$.

a) Assume $\frac{T}{zh_2} - \frac{R}{\rho} \geq 0$. Let us compute $\frac{\partial \Pi_2(Q_1^*,Q_2)}{\partial Q_2}$ in $Q_2 = Q_1^*$. After simple calculation, it has the sign of $\rho(1 - \frac{h_1}{h_2})$ and then, it is, since $h_1 > h_2$, strictly negative. By Lemmas 1.1, 1.2 and 1.3, this implies that the best response of miner 2 is unique and strictly below Q_1^* if $Q_1^* > 0$ or equal to Q_1^* if $Q_1 = 0$.

b) Assume $\frac{T}{zh_2} - \frac{R}{\rho} < 0$ and hence $Q_1^* = 0$. $\frac{\partial \Pi_2(Q_1^*,Q_2)}{\partial Q_2}$ in $Q_2 = Q_1^*$ has the sign of $\rho - h_1T^{-1}zR$. $\frac{T}{zh_2} - \frac{R}{\rho} < 0$ and $h_1 > h_2$ imply $\rho - h_1T^{-1}zR < 0$.Then, $Q_1^* = 0$ and $Q_2^* = 0$ is the only Nash Equilibrium by Lemmas 1.1, 1.2 and 1.3.

II. Assume $Q_2^* > Q_1^*$. Then,

$$\Pi_2(Q_1^*,Q_2^*) = \Pi^+(Q_2^*,Q_1^*) = (R+\rho Q_2^*)h_2 \exp\left(-h_1T^{-1}(\tau(Q_2^*) - \tau(Q_1^*))\right).$$

$\frac{\partial \Pi_2(Q_1^*,Q_2)}{\partial Q_2} = h_2 \exp\left(-h_1T^{-1}(\tau(Q_2) - \tau(Q_1^*))\right)(\rho - h_1T^{-1}z(R+\rho Q_2))$ which has the sign of $(\rho - h_1T^{-1}z(R+\rho Q_2^*))$. Then, by Lemmas 1.1, 1.2 and 1.3, we necessarily have $Q_2^* = \max\{0, \frac{T}{zh_1} - \frac{R}{\rho}\}$ or $Q_2^* < Q_1^*$ which contradicts the assumption that $Q_2^* > Q_1^*$. Assume $Q_2^* = 0$, this contradicts the assumption that $Q_2^* > Q_1^*$. Assume $Q_2^* = \frac{T}{zh_1} - \frac{R}{\rho} > 0$. Let us compute $\frac{\partial \Pi_1(Q_1,Q_2^*)}{\partial Q_1}$ in $Q_1 = Q_2^*$. After simple calculation, it has the sign

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13

of $\rho(1-\frac{h_2}{h_1})$ and then is, since

$h_1 > h_2$, strictly positive. By Lemmas 1.1, 1.2 and 1.3, this contradicts the fact that $Q_2^* > Q_1^*$.

Similarly to what has been shown above, it is straightforward to check that $\mathcal{E} \neq \emptyset$.

Appendix E: Alternative parameters' values

Table 3 is equivalent to Table 2 but with a change of k_b parameter value to 0.08 second.kB^{-1} as suggested by Decker and Watenhofer.[21]

Table 3. $k_b = 0.08$. A: miner's name, B: relative computational power, C: expected reward when $\forall i \in N, Q_i = 884 \times 0.6kB$, D: optimal number of transaction included by miner i in the current block when $\forall j \in N \setminus \{i\}, Q_j = 884 \times 0.6kB$ (solution to Equation 3), E: probability to be the first miner to find a block reaching consensus when $\forall j \in N \setminus \{i\}, Q_j = \times 0.6kB$ and Q_i given in D, F: expected reward when $\forall j \in N \setminus \{i\}, Q_j = 884 \times 0.6kB$ and Q_i given in D, G: F-C difference in %. H: expected reward of miners in BTC when $\forall i \in N, Q_i = 0$.

A	B	C	D	E	F	G	H
F2Pool	18.900%	4.74171	0	19.977%	4.99419	5.325%	4.72500
AntPool	18.200%	4.56609	0	19.246%	4.81153	5.375%	4.55000
Bitfury	14.400%	3.61273	0	15.267%	3.81682	5.649%	3.60000
BTCC	13.100%	3.28658	0	13.901%	3.47534	5.743%	3.27500
KNCMiner	8.100%	2.03216	0	8.625%	2.15623	6.105%	2.02500
BW Pool	7.200%	1.80636	0	7.671%	1.91783	6.171%	1.80000
Slush	6.900%	1.73110	0	7.353%	1.83830	6.192%	1.72500
21 Inc.	3.900%	0.97845	0	4.165%	1.04117	6.411%	0.97500
Eligius	3.500%	0.87809	0	3.739%	0.93464	6.440%	0.87500
GHash.IO	1.900%	0.47668	0	2.032%	0.50793	6.556%	0.47500
Telco 214	1.600%	0.40141	0	1.711%	0.42782	6.578%	0.40000
BitMinter	0.700%	0.17562	0	0.749%	0.18729	6.644%	0.17500
Other	0.500%	0.12544	0	0.535%	0.13379	6.658%	0.12500
EclipseMC	0.400%	0.10035	0	0.428%	0.10704	6.666%	0.10000
Kano CKPool	0.300%	0.07527	0	0.321%	0.08029	6.673%	0.07500
Solo CKPool	0.200%	0.05018	0	0.214%	0.05353	6.680%	0.05000
BitClub Network	0.100%	0.02509	0	0.107%	0.02677	6.687%	0.02500
P2Pool.org	0.100%	0.02509	0	0.107%	0.02677	6.687%	0.02500

Articles in this journal are licensed under a Creative Commons Attribution 4.0 License.

Ledger is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2016.13