With a transaction fee market and without a block size limit in Bitcoin network; there exists a Nash equilibrium point of the mining game

Moustapha Ba

With a transaction fee market and without a block size limit in Bitcoin network; there exists a Nash equilibrium point of the mining game

Dr. Moustapha BA[a,*]

[a]*MODAL'X: the Mathematics and Computer Sciences laboratory of Université Paris Nanterre (Paris X), ministerial label EA 3454. 200 av. de la République, 92000 Nanterre, FRANCE.*

Abstract

We are interested in mining incentives in the Bitcoin protocols. The blockchain Bitcoin. The mining process is used to confirm and secure all transactions in the network. This process is organized as a speed game between individuals or groups, referred to as "miners" or "pools of miners", respectively. Miners or pools of miners use different computational powers to solve a mathematical problem, obtain a proof-of-work, spread their solution, and this solution is verified by the community before the block is added in the only public blockchain replicated over all nodes. First, we define and specify this game in the case with n players, $n \geq 2$, under the assumptions denoted by *(H)* below. Next, we analytically find its Nash equilibrium points. In other words, we generalize the idea of [1] by taking into account the hypotheses of Peter Rizun's paper [2], through cumbersome computations. Our purpose here is to show some intuitions about the model rather than derive applicable results.

Keywords: Blockchain, Bitcoin, mining process, game, Nash equilibrium point

1. Introduction

Bitcoin was invented in 2008 by Satoshi Nakamoto [3]. By 2013, Bitcoin had left its circle of strict early adopters and had become very popular. Bitcoin is usually described by laymen as a form of electronic or internet money. However, this definition is much criticized by the computer science community, which considers Bitcoin to be a disruptive and revolutionary protocol. As a protocol, Bitcoin is still in its early stages of development, and its specifications are still being modified. To reach the implementation stage, a proposed modification must go through a whole process of validation. Questions remain regarding some specifications of the Bitcoin protocol, including queries about the value and structure of the rewards earned by miners. In this paper, we analyze this aspect of the Bitcoin protocol. Our work was inspired by the qualitative intuitions of the Bitcoin protocol given in 2014 by Nicolas Houy [1] who, in turn, was

☆This research was supported by MODAL'X, the Mathematics and Computer Sciences public Laboratory of Université Paris X, FRANCE. *Dr. Moustapha BA is a Ph D in applied mathematics of Aix-Marseille universite in 2014. His topics focus on stochastic calculus, stochastic analysis, stochastic network model, computer sciences and new technologies. He is qualified lecturer in applied mathematics and pure mathematics by the Universities National Council of France in 2017 and affiliated with the random modeling laboratory (MODAL'X), department of Mathematics and cumputers sciences, of Universite Paris Nanterre. Passionate about new technologies and the financial industry, Dr. BA advises and supports banks, fund management compagnies, financial institutions in the design and development of blockchain applications and cryptocurrency.*

*Corresponding author

Email address: ba.moustapha@parisnanterre.fr (Dr. Moustapha BA)

inspired by G. Andressen [4]. An extended work of P. Rizun in [2] will be also token into account in Section 2. To analyze the mining aspect, we need to describe, at least superficially, how Bitcoin actually work. When an individual sends bitcoins to another individual, this transaction is broadcast to the peer-to-peer Bitcoin network. For this transaction to be confirmed and secured, it needs to be included with other transactions as a block, in the blockchain, by miner in the network. The blockchain is a public ledger that contains the full history of all transactions ever processed in Bitcoin. Miners do work of confirming and securing transactions. This security aspect of the mining activity is often forgotten or not known by Bitcoin critics. Briefly, this mining process consists of two principle steps. The first step is to solve a mathematical problem (equation 1), called find a proof of work (in this paper, we consider there are no difference between expressions "solve a mathematical problem", "find a block" or "find a proof-of-work"). The second step of the mining process is the diffusion of the solution to the network for it to reach consensus. Each node, as soon as it receives a new solution, verifies that the solution is exact and added the new block to its local blockchain abandon the block that it is working on and start trying to build a new block. The description of this process is recalled in many papers (see [3], [5], [6]) but a work about the game that it implies is never been developed, unless in [1] where author studies the mining incentives in the case of two players. Thus, the complete game theoretical analysis that we propose here, is very important motivation.

We are interested in the protocol of securing transactions, called mining, in the Bitcoin blockchain. The Bitcoin mining process of confirming and securing transactions involves regrouping a finite number of transactions into a block, looking for a proof-of-work based on the idea of [7] and broadcast its solution in the network. Others miners working on the same blockchain, verify that this solution is valid and added this block to its local blockchain. If 50% of total computational powers existing in the network work with a new released hash, the miner who has broadcast this one, get a fixed reward and variables reward coming from the transactions fees in the bloc. To resume, we say that after selecting a finite number of transactions from the Mempool's node (Short for Memory Pool), each miner looks for solution n_i of the equation:

$$s_i = \text{SHA256}(h_i + n_i + s_{i-1})) \leq d, \tag{1}$$

where the function SHA256(.) is a crypto-graphic hash function belonging to the set of Secure Hash Algorithm (SHA) functions, $h_i = \text{SHA256}(B_i)$, B_i is a character string representing the set of transactions, $+$ is the concatenation operator of strings and n_i the value of the nonce, s_{i-1} is the previous hash of its local blockchain, and d the current mining difficulty which periodically calculated by the network. The nonce is a value to be sought randomly or systematically to change the result of the hash function and to have a result that satisfies the equation 1. After having found a result satisfying the equation 1, miner M_i added bloc B_i in its version of blockchain, and automatically diffuses its solution (B_i, n_i, h_i, s_i) to all members of the peer-to-peer network. When another miner M_j, who is also working on the blockchain C, receives the communication, it will compute:

$$s^{'} = \text{SHA256}(n_i + h_i + s_{j-1}). \tag{2}$$

If $s^{'} = s_i$, then miner M_j will add block B_i to its blockchain C, abandon the block B_j that it is working on and start trying to add a block to the chain CB_i. Any transactions in B_j that are not in B_i will be incorporated into in this new block. Importantly, miners M_i and M_j now, have identical versions of the blockchain. The first mined block who is added by the majority of miners (in terms of computational power) gets automatically a reward. We consider in this paper that all miners are honest and follow the standard protocol implemented in Bitcoin as it is explained in [3], even if in others papers like in [8] and in [9] for example, authors consider that colluding miners in the network can deviate from the protocol and following some strategies other than that who is implemented in Bitcoin protocol. Example: the strategy of block withholding called also Selfish mining strategy (see [8], [9]. There may exist others dishonest mining strategies in the network, but in this paper we consider that all miners are honest and follow the protocol as it is implemented in Bitcoin.

Our first objective is to show that, at the time a honest miner starts creating a block with the last public hash, means, after having already verified equation (2) and added the new block, he is in competition with others miners who has received the same hash.

The Bitcoin protocol requires that a block newly found will be added in the public blockchain as soon as more than 50% of the total computational power has accepted the solution (see [3]) (work with the solution s_i from equation (1)). The first miner who completes these two steps first, has its block included in the blockchain and earns a reward in BITCOIN (BTC). In the current implementation of Bitcoin Core, this reward comes from both an ex-nihilo creation of new bitcoins and as fees that Bitcoin users can add to their transactions. To control the monetary base, mining is made more complex than it could be. A first approximation, the probability that a miner solve a mining problem depends on their computational power; therefore, the mining complexity is dependent on the total computational power of all miners. The complexity is dynamically adjusted so that a block is solved and bitcoins (BTC) are created every 10 minutes in average. Once a block is inserted in the public blockchain, the mathematical problem faced by all miners are modified and we can consider that a fresh new speed game starts between miners.

This article tackles the issue of the incentives offered to miners as a function of the reward structure and values. Currently, the fixed reward is 12.5 bitcoins (BTC) per block. The fixed reward was 50 BTC in the first days of Bitcoin in 2009; this amount was halved every 210,000 blocks. The number of bitcoins issued is programmed to reach a maximum of 21,000,000 asymptotically. At the time that this article was written, there were about 16,000,000 BTC in circulation. The variable reward is 0.0001 BTC / KB of transaction.

When mining a block, a miner is free to choose which of the transactions in the Mempool's node they wish to include in block. In a very good first approximation, computing the mathematical problem (equation (1)) by including more transactions is not more expensive in terms of CPU power, disk space, or bandwidth. However, the larger a block is, the longer it will take to be propagated and verify by other miners. Thus, including more transactions in a block can have the adverse effect of lowering the probability that a miner will earn any reward. When a miner finds a block but is outraced by another miner, the block becomes orphaned. As we will show, this trade-off depends on how many

transactions other miners include in their blocks. The number of transactions included in the blocks is the outcome of a game : namely, the Bitcoin mining game that we propose to study in this article.

It is also of importance in the current context of hot debates about the block's 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, P. Rizun constructs this offer function in a decision theory framework considering the costs and benefits mentioned above and atomistic miners.

In this article, we show that the game theory framework is more adapted to tackle theirs questions. In Section 2, we describe the Bitcoin mining game and all hypotheses that we will use in this paper. We analytically study the Nash equilibrium points of the game in the case of n miners ($2 \leq n < \infty$). When remuneration is fixed for all miners, the Nash equilibrium is reached at the beginning of the process when no transaction is included by the miners. All miners have a profitable deviation. We also study the case where the remuneration depends on the number of included transactions, as well as the influence of minor powers on decision strategies. We provide the model, assumptions, and main results in Section 2, Proofs of the main results of this paper, summarized in Theorem 6 , are given in Section 3. Conclusions are provided in Section 4. A discussion of the findings and related work are provided in Section 5.

2. Model, statements and main results

Consider a set $\mathcal{M} = \{M_1, M_2, ..., M_n\}$ of miners on the Bitcoin's network working on the public blockchain called C, and we call by $\mathbf{M} = \{1, 2, ..., n\}$ with $2 < n < \infty$, the indexing set. Each miner $M_i \in \mathcal{M}$ has a relative hash power $\alpha_i > 0$, proportional to the probability of solving the mathematical problem. Then, without loss of generality, we can assume that:

$$\sum_{i=1}^{n} \alpha_i = 1.$$

The mathematical problem of equation (1) is solved by a try-and-guess strategy, such that the occurrence of a problem solution can be modeled as a random variable following a Poisson process. The complexity of finding a block is dynamically adjusted so that the operation is expected to take 600 seconds to complete. Thus, the mining process is a Poisson process with intensity $\lambda = 1/600 > 0$ for the whole network. The first observation is that the number of transactions included in a block will have no effect on the complexity of solving the mathematical problem or on CPU cost. The problem of block's size in Bitcoin Core was opened by Satoshi in [3] as a possibility to improve the Bitcoin protocol. Satoshi said that the block's size limit (1 MB) could be raised in the future when the need arrived. This is one of the main feartures of Bitcoin Unlimited. In a recent paper ([2]), P. Rizun shows how a rational Bitcoin miner should select transactions from his node's mempool, when creating a new block, in order to maximize his profit in the absence of a block's size limit. P. Rizun introduces two novel concepts: the *block space supply curve* and *mempool demand curve*. In this paper, as in [1], we consider also that there is no limit for the block's size, and the marginal cost to add a transaction in block is zero. We associate each block's size by the number of transactions included inside the

block, and we deal with this number instead of block's size. We denote here by x_i the number of transactions included in the block in preparation by miner M_i, $x_i \in \mathbb{R}^+$.

Once a miner has found a block (i.e, get a proof-of-work by solving the mathematical problem) containing a given number of transactions, the protocol requires that the miner broadcast automatically the solution to the Bitcoin network. We assume that all miners are honest and there is no code changes to delay the transmission like the selfish mine strategy in [8]. By taking into account the fact that the block's size is the dominant factor of the transmission of information in the network, then more a block is larger more it takes time to be propagated and verified in the network (see [10]). So, we assume that the time needed for a block to be propagated in the network and verified by the community before it will be added to the public blockchain depends linearly on the block's size and, thus, depends linearly on the number of transactions included in the block. Let $k(x_i)$ be the time needed for a block of x_i transactions to be propagated and verified by the majority of miners in the network.

$$k(x_i) = k.x_i \qquad k > 0. \tag{3}$$

where $k.x_i$ is the scalar product in $\mathbb{R}$ between k and x_i. This assumption is in perfect line with those suposed by P. Rizun in [2] (see equation (9) of [2]). In paper [2] P. Rizun assumes that the block's propagation delay is approximately equal to the size of the block produced, divided by the coding gain with which the block solution can be transmitted, and divided by the effective capacity of the communication channel. These two constants are denoted in [2] by C (block solution coding gain) and Υ (channel capacity) respectively. In this model the constant k in equation (3) is equivalent to $\frac{1}{\mathsf{C}\Upsilon}$.

The first miner to solve the mathematical problem (i.e., to find a block) and to have the block verified at first by the majority, earns a fixed reward $R > 0$ (in BTC) and variable reward amount transactions fees. In Bitcoin Core, the sender of transaction choose to do a transaction with fees or without fees. Since miners are rationals, we consider that they selectionne only transactions with fees in the Mempool's node and it is well known that transactions without fees can probably never be effective. We then assume, in this paper, as in [2] that all transactions in Bitcoin require fees. In Bitcoin Core, the fees are calculated relative to the size of transaction message and the remuneration is equal to 10^{-4} for each KB (kilobyte) of transaction. In view of [4], the average Bitcoin transaction is about 250 bytes. Thus, for all x_i transactions (in average $x_i.250.10^{-3}KB$) included in one block, the variable reward from transactions fees depends linearly on the number of transactions. If miner M_i is the first to be added in the public blockchain, i.e, if he finds a solution of mathematical problem and the solution is the first to be approved by the majority of miners; the reward earned is:

$$R(x_i) = R + c.x_i \qquad c \geq 0, R > 0. \tag{4}$$

The proof of work can be achieved by choosing values for nonce randomly or systematically until equation (1) is satisfied. Let t_i be the random variable representing the time required for a miner to find a proof-of-work. This time is exponentially distributed with parameter $\lambda.\alpha_i$, where λ is the intensity of mining process and α_i is the computational

power of miner M_i.

Consider that the blockchain C of miner M_i, in section Introduction, is the public blockchain, means the longest chain, that which contains more blocks starting from the *genesis* (see [3]). At the time $t = 0$ when miner M_i add the last public bloc B_i, broadcast its solution and start looking for a new block, he is in competition with all other miners who will added the last public bloc B_i, until another solution appears. We assume that miners can not detect the creation of block by their opponents and thus, have not the ability to mine on top of such blocks before they receive them (not spy mining for example). This means the competition is between $\{M_j\}_{j\in\mathbf{M}}$ who have verified that the solution $s^{'} = s_i$ before a new public block is announced to them. However, note that miners working on the same blockchain do not receive the hash at the same moment but progressively because of the propagation delay of information in the network, as we have precised in the preceding paragraph.

Technical assumptions for simplified calculations. Between the date when n miners $\mathcal{M} = \{M_1, M_2, ..., M_n\}$ have already received the last public block header hash and start looking for a new block and the date when a new block will be added in the public blockchain, each miner M_j has a finite number of transactions, $x_j > 0$ to include in its block and a computational power α_j to solve its mathematical problem. these numbers can be equals or not equals but by re-indexing the set of miners, we call by x_1 the smallest number of transactions included, and miner M_1 is the miner who has included x_1 transactions, $x_2 \geq x_1$ for miner M_2 and so on. Let x_n be the largest number of transactions included and we call this miner by M_n. Let $\overrightarrow{x} = (x_1, x_2, ..., x_n)$ be the sequence of numbers of transactions included for a bloc to be found, one for each miner. Thus, we have:

$$x_n \geq x_{n-1} \geq ... \geq x_1. \tag{5}$$

By this assumption, we define without lost of generality, the set of profile strategic in which we will find the Nash equilibrium points:

$$\Xi = \{x = (x_1, x_2, ..., x_n) \in (\mathbb{R}^+)^n |\, x_n \geq x_{n-1} \geq ... \geq x_1\}. \tag{6}$$

This technical assumption will allow us to give a simplified expression of the probability in equation (7) and facilitate all following calculations.

2.1. Mining benefit

Let us compute the mining benefit earned by miners. We evaluate at first the probability of the event:
$\{$ *the block of miner* M_i *is the first to be added on the public blockchain*$\}$. This even is equivalent to:

$$\{t_i + k.x_i < t_j + k.x_j, \forall j \in \mathbf{M} \setminus i\}.$$

Then the probability that miner M_i will solve the mathematical problem associated to its block between t and $t+dt$ and that block will be the first to be added in the public blockchain, is equal to:

$$\begin{aligned}\mathbb{P}\left\{t_j + k.x_j > t + k.x_i, t \leq t_i \leq t + dt\right\} =& \lambda\alpha_i e^{-\lambda\alpha_i t}dt \prod_{j\in\mathbf{M}\setminus\{i\}, t+k.x_i-k.x_j\geq 0} e^{-\lambda\alpha_j(t+k.x_i-k.x_j)} \\ =& \lambda\alpha_i dt \prod_{j\in\mathbf{M}, t+k.x_i-k.x_j\geq 0} e^{-\lambda\alpha_j(t+k.x_i-k.x_j)}.\end{aligned}$$

By integrating this quantity between $t=0$ and $t=+\infty$, we obtain the probability $P_i(\overrightarrow{x})$ that miner M_i will find a block and that its block will be the first to be added to the public blockchain by the majority (in terms of computational power).

$$P_i(\overrightarrow{x}) = \lambda\alpha_i \int_0^{+\infty} \left(\prod_{j\in\mathbf{M}, t+k.x_i-k.x_j\geq 0} e^{-\lambda\alpha_j(t+k.x_i-k.x_j)} \right) dt. \tag{7}$$

$\forall i \in \mathbf{M}, \forall t > 0$, we define:

$$\mathcal{Q}_i(x,t) = \sum_{j\in\mathbf{M}} \alpha_j 1_{\{k.x_j \geq t+k.x_i\}}, \quad \mathcal{A}_i(x,t) = \sum_{j\in\mathbf{M}} \alpha_j k.x_j 1_{\{k.x_j \geq t+k.x_i\}}$$

$$\bar{k}(x,t) = \sum_{j\in\mathbf{M}} \alpha_j k.x_j.$$

Taking all of these definitions together, we can prove easily that equation (7) is equivalent to

$$P_i(\overrightarrow{x}) = \lambda\alpha_i \int_0^{+\infty} e^{-\lambda\left((1-\mathcal{Q}_i(x,t))(t+k.x_i)+\mathcal{A}_i(x,t)-\bar{k}\right)}dt. \tag{8}$$

The following remark gives a simple expression of $P_n(\overrightarrow{x})$, the probability that miner M_n earns the reward, derived from equation (8).

Remark 1.

$$\forall x \in \Xi, \quad P_n(\overrightarrow{x}) = \alpha_n e^{-\lambda\left((1-\alpha_n)kx_n - \sum_{j=1}^{n-1}\alpha_j k.x_j\right)}, \tag{9}$$

and the expected reward of miner M_n is:

$$\Pi_n(\overrightarrow{x}) = P_n(\overrightarrow{x})R = R\alpha_n e^{-\lambda\left((1-\alpha_n)kx_n - \sum_{j\in\mathbf{M}\setminus n}\alpha_j k.x_j\right)}.$$

Proof. For all $x \in \Xi$, because $x_n \geq x_j$ for all $j \in \mathbf{M}\setminus n$,

$$\begin{cases} \mathcal{Q}_n(x,t) = 0 \\ \mathcal{A}_n(x,t) = 0 \end{cases},$$

From equation (8), we get the result by computing the integral. □

More generally:

Proposition 2. *For all $x \in \Xi$, for all $i \in \mathbf{M}$ we have:*

$$P_i(\overrightarrow{x}) = \frac{\alpha_i \, \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)}}{\sum_{j=1}^{i} \alpha_j} - \alpha_i \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)},$$

by assuming that:

$$\sum_{l=n+1}^{n} \left[\frac{1}{\sum_{j=1}^{l} \alpha_j} - \frac{1}{\sum_{j=1}^{l-1} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)} = 0 (\textit{case} i = n).$$

Proof. The proof is very easy. It uses equation (7) and some techniques of integral's calculations. But authors are ready to provide a complete text of the proof. We can also verify easily that for all fixed $\overrightarrow{x} \in \Xi$, $\sum_{i=}^{n} P_i(\overrightarrow{x}) = 1$.

□

The expected reward $\Theta_i(\overrightarrow{x})$ associated to miner M_i, is then equal to the probability $P_i(\overrightarrow{x})$ time the reward defined (4):

$$\Theta_i(\overrightarrow{x}) = (R + c.x_i) P_i(\overrightarrow{x}). \tag{10}$$

2.2. The Bitcoin mining game:

The Bitcoin mining game is the given $\left(\mathcal{M}, (S_i)_{i\in\mathbf{M}}, (\Theta_i)_{i\in\mathbf{M}}\right)$, where $\mathcal{M}$ is the set of players, $S_i = \mathbb{R}^+$ the set of strategies of miner M_i, and Θ_i described in equation (10) is the payoff function of miner M_i. To justify our theoretical approach of the Bitcoin mining game, we prove the following proposition.

Proposition 3. *Let $c > 0$, $R > 0$. Let $\overrightarrow{x} = (x_1, x_2, ..., x_n)$ be the profile strategy in Ξ. For all miner $M_i \in \mathcal{M}$ and for all $r \in \mathbf{M} \setminus \{i\}$, the function $x_r \mapsto \Theta_i(\overrightarrow{x}) = \Theta_i(x_1, x_2, ..., x_{r-1}, x_r, x_{r+1}, ..., x_n)$ is derivable on $]x_{r-1}, x_{r+1}[$ and*

$$\frac{\partial \Theta_i}{\partial x_r}(\overrightarrow{x}) > 0. \tag{11}$$

This proposition shows that introducing transactions in blocks by a miner M_r has positive externalities on other miner M_i for all $i \in \mathbf{M}$. Hence, our game theoretical approach is justified.

Indeed, when a miner $M_r \in \mathcal{M}$ introduces more transactions in his block, he makes longer the time needed to spread his block in the network, in turn allowing more time for other miners to find the next block, spread it to the network and will be verified by the majority of miners. However, this does not imply that the expected reward decreases for miner r. Indeed, it is true that introducing more transactions in the block, the miner is looking for decreases its probability to find and spread it first. But it also increases the reward he earns in case he is actually the first one to find and spread the next block. Of course, for this reasoning to be valid, we need to have $c > 0$ or else the marginal benefit to include transactions in blocks vanishes.

In the trivial case where $c = 0$ and $R = 0$, the benefits of mining is obviously 0 anyway: there is nothing to earn whatever the strategy profile $\overrightarrow{x}$.

Proof. We use the following remark to prove Proposition 3. This remark will also be used in Section 3 and Subsection 3.4.

Remark 4. $\forall \overrightarrow{x} \in \Xi$, $\forall i \in M, \forall l \in [i, n]$,

$$\mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)} \leq \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)}.$$

Proof. The proof is easy and does not use any Proposition or Remark in the preceding. Only the technical assumption (5). Authors are ready to provide a complete text of the proof of this remark.

□

Let us prove Proposition 3. For $\overrightarrow{x} = (x_1, \ldots, x_n) \in \Xi$, we calculate $\frac{\partial \Theta_i}{\partial x_r}(\overrightarrow{x})$.
In view of definition of $\Theta_i(\overrightarrow{x})$ we have for $r \neq i$:

$$\frac{\partial \Theta_i}{\partial x_r}(\overrightarrow{x}) = (R + c.x_i)\frac{\partial P_i}{\partial x_r}(\overrightarrow{x})$$

By the expression of $P_i(\overrightarrow{x})$ in Proposition 2, we get:
if $r < i$,

$$\frac{\partial P_i}{\partial x_r}(\overrightarrow{x}) = \lambda k \alpha_r \left(\frac{\alpha_i \, \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)}}{\sum_{j=1}^{i} \alpha_j} - \alpha_i \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)} \right).$$

By Remark 4, for $i < l \leq n$,

$$\mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)} \leq \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)}. \tag{12}$$

Then,

$$\begin{aligned}
\frac{\partial P_i}{\partial x_r}(\overrightarrow{x}) &\geq \left(\frac{\alpha_i}{\sum_{j=1}^{i} \alpha_j} - \alpha_i \left[\frac{1}{\sum_{j=1}^{i} \alpha_j} - \frac{1}{\sum_{j=1}^{n} \alpha_j} \right] \right) \lambda k \alpha_r \alpha_i \, \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)} \\
&\geq \alpha_i \lambda k \alpha_r \alpha_i \, \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)} > 0.
\end{aligned}$$

If $r > i$,

$$\begin{aligned}
\frac{\partial P_i}{\partial x_r}(\overrightarrow{x}) = &- \left(\sum_{j=1}^{r-1} \alpha_j \right) (-\lambda k \alpha_i) \left[\frac{1}{\sum_{j=1}^{r-1} \alpha_j} - \frac{1}{\sum_{j=1}^{r} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{r-1} -\lambda\alpha_j(k.x_r - k.x_j)} \\
&- \lambda k \alpha_r \alpha_i \sum_{l=r+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)} \\
&\geq \lambda k \alpha_i \alpha_r \, \mathrm{e}^{\sum_{j=1}^{r-1} -\lambda\alpha_j(k.x_r - k.x_j)} > 0.
\end{aligned}$$

□

Because miners are considered to be rational, they will try to find the strategy that maximizes their expected reward. To determine the optimal number of transactions to include in a block, each miner $M_i \in \mathcal{M}$ will solve the following maximization problem:

$$\max_{x_i \in \mathbb{R}^+} \Theta_i(\overrightarrow{x}). \tag{13}$$

Using the technical assumptions (5), the maximization problem of each miner becomes:

$$\max_{x_i\in\mathbb{R}^+ | x_1\leq x_2\leq ...\leq x_{i-1}\leq x_i\leq x_{i+1}\leq ...\leq x_n} \Theta_i(\overrightarrow{x}). \tag{14}$$

Before announcing and proving our main result, we recall some notation, definition and the well-known Nash theorem, for reader's convenience.

We denote by $\overrightarrow{x_{-i}} = (x_1, x_2, ..., x_{i-1}, x_{i+1}, ..., x_n)$ and $(x_i, \overrightarrow{x_{-i}}) = (x_1, x_2, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) = \overrightarrow{x}$.

Definition 5. *A point $\overrightarrow{x^*} = (x_1^*, x_2^*, ..., x_n^*)$ is called a Nash Equilibrium point if and only if:*

$$\forall i \in \mathbf{M}, \quad x_i^* = \arg\max_{x_i\in\mathbb{R}^+} \Theta_i(x_i, \overrightarrow{x_{-i}^*}).$$

In others words, for all $i \in \mathbf{M}$, if we fix any $n-1$ elements $x_1^*, x_2^*, ..., x_{i-1}^*, x_{i+1}^*, ..., x_n^*$, the function $x_i \longmapsto \Theta_i(x_1^*, x_2^*, ..., x_{i-1}^*, x_i, x_{i+1}^*, ..., x_n^*)$ is maximized in x_i^*.

We recall the well-known theorem of Nash which ensures the existence of Nash equilibrium points in our game model. But we recall for readers that our goal is to give explicitly these points.

Nash Theorem (1950) 1. *All finite mixed-strategy form game admits at least a Nash equilibrium point.*

For a best understanding about Nash equilibrium point in game theory, we suggest reader to learn [11].

Our main theorem give Nash equilibrium points of this model and our approach to prove the Nash's equilibrium points of this game is to use optimization techniques by doing cumbersome calculations. First, we summarize here the main hypotheses used in this model before announcing the main theorem associated to it. We consider in this paper the following assumptions:

$$(H)\begin{cases} \text{The block's size is not limited ([2]).} \\ \text{All transactions have fees.} \\ \text{Miners can not detect the creation of blocks by their opponents (no spy mining).} \\ \text{There is no protocole changes to delay the transmission of block like in [8] (i.e there is no selfish-mine attack} \\ \text{in the network, all miners are honest and follow the protocole)} \end{cases},$$

The following theorem provide the main results of this paper.

Theorem 6. *Consider the mining game described in Section 2, in the context of Bitcoin blockchain. Then, we have the following results:*

1) If $c = 0$, then the mining game has a unique Nash equilibrium point $x^* = (x_1^*, x_2^*, ..., x_n^*) \in (\mathbb{R}^+)^n$ with $x_1^* = x_2^* = ... = x_n^* = 0$. Moreover, $\forall i \in \mathbf{M}$, $\Theta_i(x^*) = \alpha_i R$.

2) If $c > 0$ and $\alpha_1 = \alpha_2 = ... = \alpha_n = \frac{1}{n}$, then the mining game has a unique Nash equilibrium point $\overrightarrow{x^*}$. More clearly, if $\frac{1}{\lambda k(1-\alpha_n)} > 0, \overrightarrow{x^*} = \left(\frac{1}{\lambda k(1-\alpha_n)}, \frac{1}{\lambda k(1-\alpha_n)}, ..., \frac{1}{\lambda k(1-\alpha_n)}\right)$ else $\overrightarrow{x^*} = \overrightarrow{0}$.

3) If $c > 0$, then the mining game has a Nash equilibrium point $x^* = (x_i^*)_{i=1,...,n} \in (\mathbb{R}^+)^n$. Values of $(x_i^*)_{i=1,...,n}$ are not explicitly given in this paper. However we will give, for all miner M_i, for all fixed profile strategic $\overrightarrow{x_{-i}}$, an interval in which the point x_i^0 which maximizes its reward function, is located.

This theorem is proved in Section 3.

Our first result is trivial. It signifies that including transactions in a block has the only consequence of extending the period needed for a miner's block to reach consensus. The marginal reward associated with this inclusion is null. Hence, there are only negative incentives for miners to include transactions in blocks. The second result means that the Nash equilibrium points are symmetric. This situation is in line with the idea that when including transactions in blocks, a miner has positive externalities on other miners.

In the third case, there is a large set of parameters for which the only Nash equilibrium of the Bitcoin mining game occurs when no miners include any transactions in their blocks. It is crucial to check for the plausibility of such a set of parameters because when all miners do not include transactions in their blocks, Bitcoin cannot be used for its intended purpose as a payment system. This rationale is one motivation for studying the mining environment.

3. Proof of main results

The proof of 1) and 2) of Theorem 6 are very simple. The proof of 3) is very technical and requires a little more of attention. Let us characterize, in the following subsection, the main functions of this paper: P_i and Θ_i. Readers do not forget we are in maximization's problem.

3.1. Characterization of the probability function and the expected reward function

In this part, we characterize the probability $P_i(\overrightarrow{x})$ calculated in Proposition 2 and the expected reward function of miner M_i denoted by $\Theta_i(\overrightarrow{x})$ for all $\overrightarrow{x} = (x_1, x_2, ..., x_n) \in \Xi$ where $\overrightarrow{x}$ is the profile strategic.

Let us define the following set:

$$D_{-i} = \{\overrightarrow{x_{-i}} = (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in \mathbb{R}^{n-1} \mid x_1 \leq \cdots \leq x_{i-1} \leq x_{i+1} \cdots \leq x_n\}. \tag{15}$$

We define also, $\forall\ \overrightarrow{x_{-i}}$ fixed in D_{-i}, the real function:

$$x_i \longmapsto \tilde{P}_i(x_i, \overrightarrow{x_{-i}}) \text{ and } x_i \longmapsto \Pi_i(x_i, \overrightarrow{x_{-i}}) \tag{16}$$

by:

$$\tilde{P}_i(x_i, \overrightarrow{x_{-i}}) = P_i(\overrightarrow{x})|_{\Xi} = \frac{\alpha_i\, \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)}}{\sum_{j=1}^{i} \alpha_j} - \alpha_i \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j}\right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)}.$$

and

$$\Pi_i(x_i, \overrightarrow{x_{-i}}) = \Theta_i(\overrightarrow{x})_{|_{\Xi}} = (R + c.x_i)\tilde{P}_i(x_i, \overrightarrow{x_{-i}})).$$

In all the following, we denote by $\overrightarrow{x} = (x_1, x_2, ..., x_n)$, $\frac{\partial \Pi_i}{\partial x_i}(\overrightarrow{x})$ the derivative of Π_i with respect to the variable x_i at the vector $\overrightarrow{x}$ and, by $\frac{\partial \Pi_i}{\partial x_i}(\overrightarrow{x})|_{x_i=y}$ the derivative of Π_i with respect to the variable x_i at the vector $(x_1, x_2, ..., x_i = y, x_{i+1}, ...x_n)$.

Since the main problem for each miner is to maximize the function Θ_i in Ξ in view of the assumption (5) above, our

approach for the proof of Theorem 6 is to maximize $x_i \longmapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}^+$ with $\overrightarrow{x_{-i}} \in D_{-i}$ fixed, and taking only solutions $x_i \in [x_{i-1}, x_{i+1}]$. More clearly, we deal for all i, the following maximization problem:

$$\overrightarrow{x_{-i}} \in D_{-i}, \quad \max_{x_i \in [x_{i-1}, x_{i+1}]} \Pi_i(x_i, \overrightarrow{x_{-i}}). \tag{17}$$

For all i, if the solution of the problem (17) is unique and does not depend on $\overrightarrow{x_{-i}}$, we will regroup all the solutions $(x_1^0, x_2^0, ..., x_n^0)$ which constitute the unique Nash equilibrium point (case of 1) and 2) of Theorem 6). For the proof of 3) of Theorem 6, the solution is unique but depends on $\overrightarrow{x_{-i}}$. For reader's convenience, we take into account in this paper the fact that in all the following of this paper,

$$\sum_{j=1}^{0} f_j = 0 \text{ for all reals } f_j, \text{ and more general } \sum_{l=n+1}^{n} [\frac{1}{\sum_{j=1}^{l} \alpha_j} - \frac{1}{\sum_{j=1}^{l-1} \alpha_j}] \, \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)} = 0. \tag{18}$$

Characterization of the first derivatives of the reward function:

Proposition 7. *Let $i \in \mathbf{M}$ and let $\overrightarrow{x_{-i}} \in D_{-i}$. The two functions $x_i \longmapsto \tilde{P}_i(x_i, \overrightarrow{x_{-i}})$ and $x_i \longmapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ are derivable on $\mathbb{R}$. Moreover,*

$$\frac{\partial \tilde{P}_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) = \lambda\alpha_i k \left(\tilde{P}_i(x_i, \overrightarrow{x_{-i}}) - e^{\sum_{j=1}^{i} -\lambda\alpha_j(k.x_i - k.x_j)} \right) \tag{19}$$

and

$$\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}})) = (c + (R + c.x_i)\lambda k\alpha_i)\tilde{P}_i(x_i, \overrightarrow{x_{-i}})) - (R + c.x_i)\lambda k\alpha_i \, \mathrm{e}^{\sum_{j=1}^{i} -\lambda\alpha_j(k.x_i - k.x_j)}. \tag{20}$$

Proof. In view of Proposition 2 we have by deriving:

$$\begin{aligned} \frac{\partial \tilde{P}_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) = \alpha_i \frac{\sum_{j=1}^{i-1} -\lambda\alpha_j k}{\sum_{j=1}^{i} \alpha_j} \, \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)} \\ + \alpha_i \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l} \alpha_j} - \frac{1}{\sum_{j=1}^{l-1} \alpha_j} \right] \lambda\alpha_i k \, \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)}. \end{aligned} \tag{21}$$

By rewriting this expression, we get:

$$\begin{aligned} \frac{\partial \tilde{P}_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) &= \alpha_i \frac{\sum_{j=1}^{i-1} -\lambda\alpha_j k - \lambda\alpha_i k}{\sum_{j=1}^{i} \alpha_j} \, \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)} + \alpha_i \frac{\lambda\alpha_i k}{\sum_{j=1}^{i} \alpha_j} \, \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)} \\ &+ \alpha_i \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l} \alpha_j} - \frac{1}{\sum_{j=1}^{l-1} \alpha_j} \right] \lambda\alpha_i k \, \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)} \\ &= \lambda\alpha_i k \left(\tilde{P}_i(x_i, \overrightarrow{x_{-i}}) - \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)} \right). \end{aligned}$$

Let us prove the second equality of preceding Proposition. In view of definition (10),

$$\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) = c\tilde{P}_i(x_i, \overrightarrow{x_{-i}}) + (R + cx_i)\frac{\partial \tilde{P}_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}). \tag{22}$$

Finally, we have:

$$\begin{aligned}\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) &= c\tilde{P}_i(x_i, \overrightarrow{x_{-i}}) + (R + c.x_i)\lambda\alpha_i k \left(\tilde{P}_i(x_i, \overrightarrow{x_{-i}}) - \mathrm{e}^{\sum_{j=1}^{i} -\lambda\alpha_j(k.x_i - k.x_j)}\right) \\ &= (c + (R + c.x_i)\lambda k\alpha_i)\tilde{P}_i(x_i, \overrightarrow{x_{-i}}) - (R + c.x_i)\lambda k\alpha_i \, \mathrm{e}^{\sum_{j=1}^{i} -\lambda\alpha_j(k.x_i - k.x_j)}. \end{aligned} \tag{23}$$

The proof of the proposition is ended. □

More explicit we have:

Proposition 8. *$\forall\, i \in \mathbf{M}$, $\forall\, \overrightarrow{x_{-i}} \in D_{-i}$:*

$$\begin{aligned}\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) = \alpha_i &\left(\frac{c - (R + cx_i)\lambda k \sum_{j=1}^{i-1} \alpha_j}{\sum_{j=1}^{i} \alpha_j}\right) \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)} \\ &- (c + (R + cx_i)\lambda\alpha_i k)\alpha_i \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j}\right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)}. \end{aligned}$$

Proof. We develop the expression (23) replacing $\tilde{P}_i(x_i, \overrightarrow{x_{-i}})$ by it expression in Proposition 2. □

Remark 9. *$\forall\, i \in \mathbf{M}$, $\forall\, \overrightarrow{x_{-i}} \in D_{-i}$:*

$$\frac{\partial \tilde{P}_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) < 0.$$

Proof. This Remark holds from the formula (21).

$$\begin{aligned}\frac{\partial \tilde{P}_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) = &-\lambda k\alpha_i \frac{\sum_{j=1}^{i-1} \alpha_j}{\sum_{j=1}^{i} \alpha_j} \mathrm{e}^{\sum_{j=1}^{i} -\lambda\alpha_j(k.x_i - k.x_j)} \\ &- \lambda k(\alpha_i)^2 \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j}\right] \mathrm{e}^{\sum_{j=1}^{l} -\lambda\alpha_j(k.x_l - k.x_j)} < 0. \end{aligned}$$

□

Remark 10. *$\forall\, i \in \mathbf{M} \setminus \{1\}$, $\forall \overrightarrow{x_{-i}} \in D_{-i}$, $\forall y > \frac{1}{\lambda k(1 - \sum_{j=1}^{i-1} \alpha_j)} - \frac{R}{c}$ then*

$$\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}})|_{x_i = y} < 0.$$

Proof. See expression of Π_i in Proposition 8. Indeed, we have a sum of one negative or null term and $\eta(x_i) = \alpha_i \left(\frac{c - (R + cx_i)\lambda k \sum_{j=1}^{i-1} \alpha_j}{\sum_{j=1}^{i} \alpha_j}\right) \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda\alpha_j(k.x_i - k.x_j)}$. Since $\eta(x_i)$ is strictly negative if and only if $x_i > \frac{1}{\lambda k(\sum_{j=1}^{i-1} \alpha_j)} - \frac{R}{C} = \frac{1}{\lambda k(1 - \sum_{j=i}^{n} \alpha_j)} - \frac{R}{c}$. The remark is proved. □

Characterization of the second derivatives of reward function:

Proposition 11. $\forall\, i \in \mathbf{M}, \forall\, \overrightarrow{x_{-i}} \in D_{-i}$:

$$\frac{\partial^2 \Pi_i}{\partial x_i^2}(x_i, \overrightarrow{x_{-i}}) = -\alpha_i \lambda k \left(\sum_{j=1}^{i-1} \alpha_j \right) \left(\frac{2c - (R + cx_i)\lambda k \sum_{j=1}^{i-1} \alpha_j}{\sum_{j=1}^{i} \alpha_j} \right) \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda \alpha_j (k.x_i - k.x_j)}$$
$$- (2c + (R + cx_i)\lambda \alpha_i k)\lambda k \alpha_i^2 \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda \alpha_j (k.x_l - k.x_j)}.$$

Proof. It suffices to derive again with respect to x_i $\left(\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) \right)$ using Proposition 8. □

Remark 12. *If* $i = 1, \forall\, \overrightarrow{x_{-1}} \in D_{-1}$, *we have:* $\frac{\partial^2 \Pi_1}{\partial x_1^2}(x_1, \overrightarrow{x_{-1}}) < 0$.

$\forall\, i \in \mathbf{M} \setminus \{1\}, \forall\, \overrightarrow{x_{-i}} \in D_{-i}$, *if* $y < \frac{2}{\lambda k (1 - \sum_{j=i}^{n} \alpha_j)} - \frac{R}{c}$, *then* $\frac{\partial^2 \Pi_i}{\partial x_i^2}(x_i, \overrightarrow{x_{-i}})|_{x_i = y} < 0$.

Proof. It follows from Proposition 11.

Indeed: if $i = 1$, the result follows from $\sum_{j=1}^{0} \alpha_j = 0$,

If $i \neq 1$, expression in Proposition (11) is a sum of negative or null term and

$\Lambda(x_i) = -\alpha_i \lambda k \left(\sum_{j=1}^{i-1} \alpha_j \right) \left(\frac{2c - (R + cx_i)\lambda k \sum_{j=1}^{i-1} \alpha_j}{\sum_{j=1}^{i} \alpha_j} \right) \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda \alpha_j (k.x_i - k.x_j)}$. Since $\Lambda(x_i)$ is strictly negative if and only if $x_i < \frac{2}{\lambda k (\sum_{j=1}^{i-1} \alpha_j)} - \frac{R}{c} = \frac{2}{\lambda k (1 - \sum_{j=i}^{n} \alpha_j)} - \frac{R}{c}$. The remark is proved. □

We combine now all the preceding propositions and Remarks to show Theorem 6.

3.2. Proof of 1) of Theorem 6

Let's prove the point 1-) of Theorem 6.

By Proposition 8, $\forall\, i \in M, \forall\, \overrightarrow{x_{-i}} \in D_{-i}$, if $c = 0$,

$$\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) = \alpha_i \left(\frac{-R\lambda k \sum_{j=1}^{i-1} \alpha_j}{\sum_{j=1}^{i} \alpha_j} \right) \mathrm{e}^{\sum_{j=1}^{i-1} -\lambda \alpha_j (k.x_i - k.x_j)}$$
$$- R\lambda \alpha_i k \alpha_i \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda \alpha_j (k.x_l - k.x_j)} < 0.$$

Then 0 is the unique point who maximizes $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}^+ = [0, +\infty[$, for all $i \in M$.

So the point $\overrightarrow{0} = (0, \ldots, 0)$ is the unique Nash Equilibrium point.

3.3. Proof of 2) of Theorem 6

Let us prove the point 2-) of Theorem 6. In Proposition 8, we take $i = n$. By the fact that

$$\sum_{j=1}^{0} \alpha_j = 0$$

and

$$\sum_{l=n+1}^{n} \left[\frac{1}{\sum_{j=1} l - 1} - \frac{1}{\sum_{j=1} l} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda \alpha_j (k.x_l - k.x_j)} = 0,$$

we have: $\forall \overrightarrow{x_{-n}} \in D_{-n}$,

$$\frac{\partial \Pi_n}{\partial x_n}(x_n, \overrightarrow{x_{-n}}) = \alpha_n(c - (R + cx_n)\lambda k(1-\alpha_n))\, \mathrm{e}^{\sum_{j=1}^{n} -\lambda\alpha_j(kx_n - kx_j)}\,.$$

$\frac{\partial \Pi_n}{\partial x_n}(x_i, \overrightarrow{x_{-n}}) = 0 \Longleftrightarrow (c - (R + cx_n)\lambda k(1-\alpha_n)) = 0 \Longleftrightarrow x_n = \frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c}$.

Then $x_n^0 = \frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c}$ maximizes $x_n \mapsto \Pi_n(x_n, \overrightarrow{x_{-n}})$ on $\mathbb{R}$ for all $\overrightarrow{x_{-n}} \in D_{-n}$ and it is unique.

• if $x_n^0 = \frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c} < 0$, $\left(\frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c} \notin \mathbb{R}^+\right)$, 0 is the unique $\arg\max$ of $\Pi_i(., \overrightarrow{x_{-n}})$ and by assumption (5) $x_j^* = 0,\ \forall j \in \mathbf{M} \setminus n$. Conclusion, $\overrightarrow{0}$ is a unique Nash Equilibrium point.

• if $x_n^0 = \frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c} \geq 0$, then we pose $x_n^* = \frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c}$. For $i < n$, we fix $\overrightarrow{x_{-i}^*} = (x_n^*, \ldots, x_n^*) \in D_{-i}$ and we study the function $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}^*})$.

By simple computation, we have for all fixed $\overrightarrow{x_{-i}^*} \in D_{-i}$,

$$\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}^*})|_{x_i = x_n^*} = 0. x_n^* \text{ is candidate.} \tag{24}$$

Indeed, we fix $\overrightarrow{x_{-i}^*} \in D_{-i}$, by Proposition 8, we have:

$$\begin{aligned}\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}^*})|_{x_i = x_n^*} = \alpha_i \left(\frac{c - (R + cx_n^*)\lambda k \sum_{j=1}^{i-1} \alpha_j}{\sum_{j=1}^{i} \alpha_j}\right) \mathrm{e}^0 \\ - (c + (R + cx_n^*)\lambda\alpha_i k)\alpha_i \sum_{l=i+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1}\alpha_j} - \frac{1}{\sum_{j=1}^{l}\alpha_j}\right] \mathrm{e}^0\,.\end{aligned}$$

By using the assumption $\alpha_i = \alpha_n \quad \forall i \in \mathbf{M} \setminus i$, the equation (24) holds.

Now, let us study $\frac{\partial^2 \Pi_i}{\partial x_i^2}(x_i, \overrightarrow{x_{-i}^*})$. By Remark 12,

$*$ For $i = 1$, $\frac{\partial^2 \Pi_1}{\partial x_1^2}(x_1, \overrightarrow{x_{-1}^*}) < 0$ on $\mathbb{R}^+$, so $\Pi_1(x_1, \overrightarrow{x_{-1}^*})$ is concave on $\mathbb{R}^+$, and then $x_1 = x_n^*$ is the unique point on $\mathbb{R}^+$ which maximizes the function :

$x_1 \mapsto \Pi_1(x_1, \overrightarrow{x_{-1}^*})$.

$*$ For $i \in \mathbf{M} \setminus \{1\}$, if $y < \frac{2}{\lambda k(1-\sum_{j=i}^{n}\alpha_j)} - \frac{R}{c}$ then

$$\frac{\partial^2 \Pi_i}{\partial x_i^2}(x_i, \overrightarrow{x_{-i}^*})|_{x_i = y} < 0.$$

So $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}^*})$ is concave on $[0, \frac{2}{\lambda k(1-\sum_{j=i}^{n}\alpha_j)} - \frac{R}{c}]$ and then $x_i = x_n^*$ is the unique maximum of $x_i \longmapsto \Pi_i(x_i, \overrightarrow{x_{-i}^*})$ on $[0, \frac{2}{\lambda k(1-\sum_{j=i}^{n}\alpha_j)} - \frac{R}{c}]$.

By Remark 10, for all $y \geq \frac{2}{\lambda k(1-\sum_{j=i}^{n}\alpha_j)} - \frac{R}{c} > \frac{1}{\lambda k(1-\sum_{j=i}^{n}\alpha_j)} - \frac{R}{c}$

$$\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}^*})_{x_i = y} < 0.$$

So x_n^* maximizes also $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}^*})$ on $\mathbb{R}^+*$. In the other words,

$$\frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c} = \arg\max_{x_i \in \mathbb{R}^+} \Pi_i(x_i, \overrightarrow{x_{-i}^*}). \quad \forall i \in \mathbf{M}.$$

The point

$$(x_1^*, x_2^*, ..., x_n^*) = \left(\frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c}, \frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c}, \ldots, \frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c} \right) \tag{25}$$

is a unique Nash equilibrium point in Ξ.

Replacing α_n by $1 - \frac{1}{n}$, the 2) of Theorem 6 is proved.

3.4. Proof of 3) of Theorem 6

To prove this part, we use the following Proposition.

Proposition 13. *If $c > 0$, for all $i = 1, \ldots, n$, for all fixed $\overrightarrow{x_{-i}} \in D_{-i}$, there exists an unique point $x_i^0 \in \mathbb{R}$ which maximizes $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}$ with*

$$x_i^0 \in \begin{cases} H[\overrightarrow{x_{-1}}] = \left[\min\left\{ \frac{1}{\lambda k(1-\alpha_1)} - \frac{R}{c}, x_2 \right\}, \max\left\{ \frac{1}{\lambda k \alpha_2} - \frac{R}{c}, x_2 \right\} \right] & \text{if } i = 1 \\ H[\overrightarrow{x_{-i}}] = \left[\min\left\{ x_{i+1}, \frac{1}{\lambda k(1-\alpha_i)} - \frac{R}{c} \right\}, \frac{1}{\lambda k(1-\sum_{j=i}^n \alpha_j)} - \frac{R}{c} \right] & \text{if } i = 2, \ldots, n. \end{cases}$$

Proof. The proof of this proposition is divided in two cases. The case where $i = 1$ and the case where $i > 1$ separately.

3.4.1. For $i = 1$

To prove the case $i = 1$, we prove the following proposition.

Proposition 14. *For all fixed $\overrightarrow{x_{-1}} \in D_{-1}$ we have:*

$$\begin{cases} \dfrac{\partial \Pi_1}{\partial x_1}(x_1, \overrightarrow{x_{-1}}) \leq 0 & \text{if } x_1 \geq \max\left\{ \dfrac{1}{\lambda k \alpha_2} - \dfrac{R}{c}, x_2 \right\} \\ \dfrac{\partial \Pi_1}{\partial x_1}(x_1, \overrightarrow{x_{-1}}) \geq 0 & \text{if } x_1 \leq \min\left\{ \dfrac{1}{\lambda k(1-\alpha_1)} - \dfrac{R}{c}, x_2 \right\} \end{cases}$$

then, there exists an unique $x_1^0 \in H[\overrightarrow{x_{-1}}] = \left[\min\left\{ \frac{1}{\lambda k(1-\alpha_1)} - \frac{R}{c}, x_2 \right\}, \max\left\{ \frac{1}{\lambda k \alpha_2} - \frac{R}{c}, x_2 \right\} \right]$ which maximizes $x_1 \mapsto \Pi_1(x_1, \overrightarrow{x_{-1}})$ on $\mathbb{R}$.

Proof. We give here a sketch of the proof. Before, we recall that

$$\text{for all reals } f_j, \sum_{j=1}^{0} f_j = 0 \text{ and more general } \sum_{l=n+1}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda \alpha_j (k.x_l - k.x_j)} = 0.$$

By Proposition 8, we have:

$$\begin{aligned} \frac{\partial \Pi_1}{\partial x_1}(x_1, \overrightarrow{x_{-1}}) = c &- (c + (R + cx_1)\lambda \alpha_1 k)\, \alpha_1 \frac{\alpha_2}{\alpha_1(\alpha_1 + \alpha_2)} \mathrm{e}^{-\lambda \alpha_1 (k.x_2 - k.x_1)} \\ &- (c + (R + cx_1)\lambda \alpha_1 k)\, \alpha_1 \sum_{l=3}^{n} \left[\frac{1}{\sum_{j=1}^{l-1} \alpha_j} - \frac{1}{\sum_{j=1}^{l} \alpha_j} \right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda \alpha_j (k.x_l - k.x_j)}. \end{aligned}$$

Since $\overrightarrow{x_{-1}}$ is fixed in D_{-1}, we have: If $x_1 \geq x_2$ then $\mathrm{e}^{-\lambda\alpha_1(k.x_2-k.x_1)} \geq 1$. so,

$$\frac{\partial \Pi_1}{\partial x_1}(x_1, \overrightarrow{x_{-1}}) \leq c - (c + (R + cx_1)\lambda\alpha_1 k)\,\alpha_1 \frac{\alpha_2}{\alpha_1(\alpha_1+\alpha_2)} - (c + (R + cx_1)\lambda\alpha_1 k)\,\alpha_1 \sum_{l=3}^{n} \left[\frac{1}{\sum_{j=1}^{l-1}\alpha_j} - \frac{1}{\sum_{j=1}^{l}\alpha_j}\right] \mathrm{e}^{\sum_{j=1}^{l-1} -\lambda\alpha_j(k.x_l - k.x_j)}.$$

$\frac{\partial \Pi_1}{\partial x_1}(x_1, \overrightarrow{x_{-1}})$ is negative if and only the first term is negative. In other word if and only $x_1 \geq \frac{1}{\lambda k \alpha_2} - \frac{R}{c}$.
In summary, if $x_1 \geq \max\left\{x_2, \frac{1}{\lambda k \alpha_2} - \frac{R}{c}\right\}$ then $\frac{\partial \Pi_1}{\partial x_1}(x_1, \overrightarrow{x_{-1}}) < 0$. By the same reasoning, if $x_1 \leq \min\left\{x_2, \frac{1}{\lambda k(1-\alpha_1)} - \frac{R}{c}\right\}$ then $\frac{\partial \Pi_1}{\partial x_1}(x_1, \overrightarrow{x_{-1}}) \geq 0$. The existence of one point between $\max\left\{x_2, \frac{1}{\lambda k \alpha_2} - \frac{R}{c}\right\}$ and $\min\left\{x_2, \frac{1}{\lambda k(1-\alpha_1)} - \frac{R}{c}\right\}$ maximizing the function $x_1 \longmapsto \Pi_1(x_1, \overrightarrow{x_{-1}})$, say $H[\overrightarrow{x_{-1}}]$, is proved. To prove the uniqueness, we use the second derivative in Proposition 11 and show that the function $x_1 \mapsto \Pi_1(x_1, \overrightarrow{x_{-1}})$ is concave on $H[\overrightarrow{x_{-1}}]$. □

3.4.2. For $i \geq 2$

To prove the case $i \geq 2$, we prove the following proposition.

Proposition 15. *For $i \geq 2$, for all fixed $\overrightarrow{x_{-i}} \in D_{-i}$ we have:*

$$\begin{cases} \dfrac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) < 0 \text{ if } x_i > \dfrac{1}{\lambda k(1-\sum_{j=i}^{n}\alpha_j)} - \dfrac{R}{c} \\ \dfrac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) > 0 \text{ if } x_i < \min\left\{x_{i+1}, \dfrac{1}{\lambda k(1-\alpha_i)} - \dfrac{R}{c}\right\} \end{cases}$$

then there exists an unique $x_i^0 \in H[\overrightarrow{x_{-i}}] = \left[\min\left\{x_{i+1}, \frac{1}{\lambda k(1-\alpha_i)} - \frac{R}{c}\right\}, \frac{1}{\lambda k(1-\sum_{j=i}^{n}\alpha_j)} - \frac{R}{c}\right]$ which maximizes $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}$.

Proof. Let $i \in \mathbf{M} \setminus \{1\}$. Let $\overrightarrow{x_{-i}} \in D_{-i}$ fixed i.e. $\overrightarrow{x_{-i}} = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ such that $x_1 \leq \cdots \leq x_{i-1} \leq x_{i+1} \leq \cdots \leq x_n$. Let $x_i \in \mathbb{R}$. We set $\overrightarrow{x} = (x_i, \overrightarrow{x_{-i}}) = (x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$. The proof of Proposition 15 is similar to the proof of Proposition 14. We use Proposition 11 and Remark 4.

□

Combining Proposition 14 and Proposition 15, we get Proposition 13. □

Remark 16. *If $i = n$, we have $x_{i+1} = x_{n+1} = +\infty$ and*

$$\frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c} = \frac{1}{\lambda k(1-\sum_{j=n}^{n}\alpha_j)} - \frac{R}{c}$$

So $x_n^0 = \frac{1}{\lambda k(1-\alpha_n)} - \frac{R}{c}$.

Corollary 17. *For all $i = 1, 2, ..., n$ and for all fixed $\overrightarrow{x_{-i}} \in D_{-i}$, by Proposition 13, there $\exists x_i^0 \in H[\overrightarrow{x_{-i}}]$ which maximizes $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}$. If $x_i^0 < 0$, then 0 maximizes $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}_+$.*

Proof. It is the consequence of the definition of the x_i^0. Indeed for all fixed $\overrightarrow{x_{-i}} \in D_{-i}$, since x_i^0 satisfies the maximum then we have:

$$\begin{cases} \dfrac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) \geq 0 \text{ if } \quad x_i \leq x_i^0 \\ \dfrac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) \leq 0 \text{ if } \quad x_i \geq x_i^0. \end{cases}$$

If $x_i^0 < 0$, then for all $x_i \geq 0 > x_i^0$; $\frac{\partial \Pi_i}{\partial x_i}(x_i, \overrightarrow{x_{-i}}) \leq 0$. Therefore, 0 maximizes $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}_+ = [0, +\infty[$ since the function $x_i \longmapsto \Pi(x_i, \overrightarrow{x_{-i}})$ is decreasing in $\mathbb{R}_+$. □

Resume: So far, we have proved for 3) of Theorem 6, the following:

For all $i = 1, 2, ..., n$ and for all fixed $\overrightarrow{x_{-i}} \in D_{-i}$, by Proposition 13, there $\exists x_i^0 \in H[\overrightarrow{x_{-i}}]$ which maximizes $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}$ and If $x_i^0 < 0$, then 0 maximize $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}_+$.

In Proposition 13 and corollary 17, we have proved the existence of the maximizing points, x_i^0 in $\mathbb{R}+$ but they don't ensure the existence of these points in the domain Ξ as we have defined it at the beginning. In the following proposition, we study the relation between the $\arg\max$ points x_i^0 and x_{i+1}^0 for all i. Note that the existence of x_i^0, for all i, depends on the fixed point $\overrightarrow{x_{-i}} \in D_{-i}$. We will show that all relations between the maximizing strategies x_i^0 and x_{i+1}^0 are directly equivalent to relations between the hash powers of miners M_i and M_{i+1} says α_i and α_{i+1}. In others words, more the miner M_i is power, more the optimal number of transaction to included by miner M_i is larger. This allows us to find the Nash equilibrium point in our domain of study Ξ defined in (6) at the beginning.

Proposition 18. *Let $x_i^0 \in \mathbb{R}$ which maximizes $x_i \mapsto \Pi_i(x_i, \overrightarrow{x_{-i}})$ on $\mathbb{R}$ as defined in Proposition 13, let α_i the power of miner M_i and Θ_i is the expected reward of miner M_i. We have the following relation:*

$$\alpha_i = \alpha_{i+1} \Longleftrightarrow x_i^0 = x_{i+1}^0 \tag{26}$$

$$\alpha_i < \alpha_{i+1} \Longleftrightarrow x_i^0 < x_{i+1}^0. \tag{27}$$

In summary, in 3) of Theorem 6, we have shown: for all i, for all fixed $\overrightarrow{x_{-i}} \in D_{-i}$ there exists an unique $(x_i^0) \geq 0$ such that , $x_i^0 = \arg\max_{x_i \in \mathbb{R}^+} \Theta_i(x_i^0, \overrightarrow{x_{-i}})$. And if $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$ we have $x_1^0 \leq \cdots \leq x_n^0$ then $(x_1^0, \cdots, x_n^0) \in \Xi$. Conclusion: we can say that if $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$, there exist one point $\overrightarrow{x^*} = (x_1^*, \ldots, x_n^*)$ which is a Nash equilibrium point in Ξ defined in (6). The proof of 3) of Theorem 6 is ended. The Proof of Theorem 6 is ended. We will show in Remark 20 below that the condition $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$ is always satisfied.
We can retrieve easily the result of 2). See the following remark.

Remark 19. *If $\alpha_1 = \alpha_2 = \cdots = \alpha_n$, then*

$$x_1^* = x_2^* = \cdots = x_n^* = \max\left\{0, \frac{1}{\lambda k(1 - \alpha_n)}\right\}$$

Proof. By Remark 16, $x_n^0 = \frac{1}{\lambda k(1-\alpha_n)}$. The assumption $\alpha_1 = \alpha_2 = \cdots = \alpha_n$ and Proposition 18 give: for $i = 1, \ldots, n$, $x_i^0 = x_n^0 = \frac{1}{\lambda k(1-\alpha_n)}$. Finally, by Corollary 17, $x_1^* = \cdots = x_n^* = \max\left\{0, \frac{1}{\lambda k(1-\alpha_n)}\right\}$ □

In the following remark, we explain more explicit the approach used here to prove 3) of Theorem 6. We will show also that the hypotheses (5) is only technical and allow us to facilitate the calculations.

Remark 20. *Let S_n the set of all permutations on the set $\mathbf{M} = \{1, 2, \ldots, n\}$. For each permutation $\sigma \in S_n$, we define:*

$$\Xi(\sigma) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_{\sigma(1)} \leq x_{\sigma(2)} \leq \cdots \leq x_{\sigma(n)}\}.$$

By definition,

$$\bigcup_{\sigma \in S_n} \Xi(\sigma) = \mathbb{R}^n.$$

Remark that our main assumption (5) in Section 2 corresponds to take the permutation $\sigma = I_d$ ($I_d(i) = i$) and then, Ξ defined in (6) corresponds to $\Xi(I_d)$. So we have showed in 3) of Theorem 6 that:

$$\alpha_{I_d(1)} \leq \alpha_{I_d(2)} \leq \cdots \leq \alpha_{I_d(n)} \Longrightarrow x^0_{I_d(1)} \leq x^0_{I_d(2)} \leq \cdots \leq x^0_{I_d(n)}.$$

In others words,

$$\alpha_{I_d(1)} \leq \alpha_{I_d(2)} \leq \cdots \leq \alpha_{I_d(n)} \Longrightarrow$$

the point $(x^0_{I_d(1)}, x^0_{I_d(2)}, \cdots x^0_{I_d(n)}) \in \Xi_{I_d}$. And then one Nash Equilibrium is given. But this reasoning works also, for any permutation σ in S_n. Indeed, for all permutation σ in $S_n \setminus \{I_d\}$ it suffices to rename $x_{\sigma(i)} = y_i$ for all $i \in \mathbf{M}$, and by copying line by line this paper, replacing x_i by y_i, we have the same results as in Theorem 6.
Indeed, $\forall \sigma \in S_n$, for all $\overrightarrow{x_{\sigma(i)-}} \in D_{\sigma(i)-}$, there exists an unique $x^0_{\sigma(i)} \in H[\overrightarrow{x_{\sigma(i)-}}]$ such that:

$$x^0_{\sigma(i)} = \arg \max_{x_{\sigma(i)} \in \mathbb{R}^+} \tilde{\Theta}_{\sigma(i)}(x_{\sigma(i)}, \overrightarrow{x_{\sigma(i)-}})$$

and if $\alpha_{\sigma(1)} \leq \alpha_{\sigma(2)} \leq \cdots \leq \alpha_{\sigma(n)}$, then $x^0_{\sigma(1)} \leq x^0_{\sigma(2)} \leq \cdots \leq x^0_{\sigma(n)}$, that means $(x^0_{\sigma(1)}, x^0_{\sigma(2)}, ..., x^0_{\sigma(n)}) \in \Xi(\sigma)$. That is sufficient to give the existence of one Nash equilibrium point.
Recall that the miner's powers $(\alpha_i)_{i \in \mathbf{M}}$ are known at the beginning. There exists an unique $\sigma^0 \in S_n$ such that

$$\alpha_{\sigma^0(1)} \leq \alpha_{\sigma^0(2)} \leq \cdots \leq \alpha_{\sigma^0(n)}.$$

If we change our field of study, by taking at the beginning Ξ_{σ^0} instead Ξ, i.e, by changing assumption (6) by:

$$x_{\sigma^0(1)} \leq x_{\sigma^0(2)} \leq \cdots \leq x_{\sigma^0(n)},$$

the maximazing points

$$(x^0_{\sigma^0(1)}, x^0_{\sigma^0(2)}, \cdots, x^0_{\sigma^0(n)}) \in \Xi(\sigma^0).$$

That is sufficient to get on Nash equilibrium point.

3.5. Remarks

Remark 21. *A simple case but not obvious, is when all miners include the same number of transactions in their blocks, formally $x_i = y \in \mathbb{R}^+$ for all $i \in \mathbf{M}$. Then, for each miner $M_i \in \mathcal{M}$, the probability that the miner will earn the reward is equal to the probability that they will solve the mining problem first, because all miners take the same time to broadcast their solution to the network to be verified. This probability is directly proportional to the hash's power of miner M_i, called α_i. Then, $\Theta_i(x) = (R + c.x_i)\alpha_i$.*

Remark 22. *If n is large enough, then $\frac{n}{\lambda k(n-1)} - \frac{R}{c} \longrightarrow \frac{1}{\lambda k} - \frac{R}{c}$. In Bitcoin implementation, reward R is halved approximately every 4 years. We observe a geometric sequence with parameter $\frac{1}{2}$. We can easily compute the year when reward R will be less than c and then the year when $\frac{R}{c}$ will be small enough. This computation is easiest if λ, k and c are fixed. Finally, we conclude that if n is large enough and if λ, k and c are constant, then $\frac{n}{\lambda k(n-1)} - \frac{R}{c}$ would be larger than zero.*

4. Conclusion

In this article, we have introduced and studied the mining game in Bitcoin blockchain. We have showed that this process is a competition between some members of the network who choose to mine in the hope of getting a reward, called miners. When miners make a decision regarding how many transactions they should include in the block that they are mining, they must study the trade-off between, rewards and time. If they include more transactions in the block, they will earn more transaction fees if they find the current block first. If they include fewer transactions in the block, they will minimize the time that they need to spread their block solution to the network and will be adopted by the majority, thereby maximizing their probability of including their block in the public blockchain first. We studied the case analytically and found the Nash equilibrium points according to the reward function and the powers of the miners. If the reward is fixed, then the miners will not play a Nash equilibrium. However, the Nash equilibrium is only reached when no transactions are included by the miners. If the reward depends on the number of transactions (i.e, a fixed reward and transactions fees), Nash equilibrium point are symmetric. And there exists a large set of parameters for which not including any transaction in a block for both miners is the only Nash equilibrium situation of the Bitcoin's mining game (second case). In the third case, we have proved the existence of Nash equilibrium points but we have not given explicitly the points. Reader's can remark in the proof of the third case that for each miner M_i, for all strategies $\overrightarrow{x_{-i}}$ token by other miners, there exists one strategy x_i^0 which maximizes its reward function. We have given also an interval in which the values of x_i^0 is located. This remark is limited in reality by the faculty of agents to coordinate. Finding the maximizing strategy for all miner M_i, independently of others strategies could be a good line for future research. Even if our purpose gives some intuitions about the model rather than derive applicable results, we believe that it represents a good starting point for future research about the mining problem in Bitcoin or Ethereum blockchain.

5. Related work and Discussion

In this part, we discuss our model and related works to this one. The security of the Bitcoin network is ensured by the mining protocol. The reward structure provides an incentive for miners to contribute their resources to the system, and is essential to the currency's decentralized nature.

N. Houy in [1] consider the case of two miners and shows that if the marginal cost to a miner to added transactions to a block was zero, then a miner would include all transactions whatever the fee attached. G. Andressen explained in [4], however, that due to the increased chances of orphaning a block, the marginal cost is not zero; a rational miner should include a given transaction if its fee is sufficient to cover the added risk of orphaning. Extending on the work of Houy, P. Rizun in [2], account for Andresen's orphaning factor and show that a rational miner will not in general include all fee-paying transactions, and that a healthy fee market is, in fact, the expected outcome of rational miner behavior, if block size is unconstrained by the protocol. He shows that a transaction fees market should emerge without a block size limit if miners includes transactions in a manner that maximizes the expectation value of their profit.

By considering that miners are rational and they try to maximize their revenues, we account for P. Rizun and G. Andressen, have study the Bitcoin mining process and have proved that it is a speed game between miners and we have given Nash equilibrium points of this game under the assumptions (H). In other words, we have considered Rizun's assumptions in a network without attack, and compute Nash equilibrium points of the Bitcoin mining game, by doing cumbersome calculations. Therefore, as we have announced it in the conclusion, we believe that it will be very interesting to give explicitly in this model, the dominant strategy for each miner M_i, independently of other strategies. We think that this will be a valuable help for mining investors in Bitcoin. Extending our model to Ethereum protocol would be also an interesting work.

The delay hypotheses that we have used in this model and so used in [2] by P. Rizun as a linear function of the block's size can be debated within the scientific community. Some papers working about the mining process consider that the transmission of blocks in the network is intantaneous. This is the case in [8] where I. Eyal and E. G. Sirer assume in [8] that the block propagation is instantaneous and study the reward earned by a colluding pool of miners using the so-called selfish-mining strategy, compared to the reward associated to the honest mining. We believe strongly that is not true in reality and this is proved in many paper. For example in [10] Decker and Wattenhofer measured the difference between the time that a node announced the discovery of a new block or a transaction and the time that it was received by other nodes for a period of operation in the actual Bitcoin network. They observed that the median time until a node receives a block was 6.5 seconds, the mean was 12.6 seconds and the 95th percentile of the distribution was around 40 seconds. Moreover, they showed that an exponential distribution provides a reasonable fit to the propagation delay distribution. In paper [9], J. Gôbel and others extend the selfish-mine model of [8] by assuming that the communication delay between two miners or pool of miners M_i and M_j for all $i \neq j$ in the network, whether collunding pool or honest pool, that lie a distance d_{ij} apart is normally distributed with a mean kd_{ij} proportional to this distance and a constant variance σ^2, independently of other transmission delays. This assumption does not contradict

Decker and Wattenhofer. Thus, the question of delay's hypothesis in Bitcoin network remains debatable. Even if the security of Bitcoin seems infallible in reality thanks to the mining game and the contribution of resources by economic agents (miners), efforts should be made to reduce energy consumption for the mining protocol. Example: K. O'Dwyer and D. Malone show in [10] that the profitable mining process in Bitcoin consume an energy comparable to Ireland's electricity consumption.

Energy efficient is an important topic in the current context of global warming.

Acknowledgements

Author of this article, M. BA, would like to thank the laboratory MODAL'X of Université Paris Nanterre to support this work. He would like to thank the members of the Laboratory MODAL'X for discussions he has with them, suggestions, remarks and lectures made on this paper. He would like also to thank the many thoughtful individuals from the Bitcoin & Ethereum Forum, whose ideas helped us to form the basis of this work, as well as the community of bitcoin for their encouragement and enthusiasm.

Disclosure statement

Conflict of interest : the author states that there is no conflict of interest. The Laboratory MODAL'X in which i am an associate member, is the full owner of this work. He has all rights to this scientific content and the exploitation of this paper belongs to him.

Funding

This research was funded by MODAL'X, the mathematics and computer sciences laboratory of Université Paris Nanterre, FRANCE.

References

[1] N. Houy, the bitcoin mining game, Ledger vol. 1 (2016) pp. 53–68.

[2] P. Rizun, A transaction fee market exists without a block size limit, https://www.bitcoinunlimited.info/resources/feemarket.pdf.

[3] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin.org.
URL `http://www.bitcoin.org/bitcoin.pdf`

[4] G. Andressen, Back-of-the-envelope calculations for marginal cost of transactions (2014, 03).
URL `https://gist.github.com/gavinandresen/5044482#file-marginaltransactioncost-md`

[5] I. D. J. Krool, E. Felten, The economics of bitcoin mining, or bitcoin in the presence of adversaries (2013).

[6] K. Odwyer, D. Malone, Bitcoin mining and its energy footprint, 25th Irish Signals and Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014) (2014) 280–285.

[7] A. Back, Hashcash - a denial of service counter-measure (2002).
URL ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf

[8] I. Eyal, E. G. Sirer, Majority is not enough: Bitcoin mining is vulnerable (2014) 436–454doi:10.1007/978-3-662-45472-5_28.
URL http://dx.doi.org/10.1007/978-3-662-45472-5_28

[9] J. Göbel, H. P. Keeler, A. E. Krzesinski, P. G. Taylor, Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay, Perform. Eval. 104 (2016) 23–41.

[10] C. Decker, R. Wattenhofer, Information Propagation in the Bitcoin Network.

[11] J. V. Neumann, O. Morgenstern, Theory of Games and Economic Behavior, Princeton University Press, 1944.
URL http://jmvidal.cse.sc.edu/library/neumann44a.pdf