Bitcoin Mining: A Game Theoretic Analysis

Rajani Singh[1,2], Ashutosh Dhar Dwivedi[1,4], Gautam Srivastava[3,4]

[1] Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland
[2] Faculty of Mathematics, Informatics, and Mechanics, University of Warsaw, Warsaw, Poland
[3] Research Center for Interneural Computing, China Medical University, Taichung, Taiwan, China
[4] Department of Mathematics and Computer Science, Brandon University, Brandon, Manitoba, Canada

Keywords: Bitcoin Mining, Dynamic Game Theory, Hamilton-Jacobi-Bellman Equation, Social optimum, Nash equilibrium, Pigovian Tax

Abstract

Bitcoin is a decentralized cryptocurrency payment system, working without a single administrator or a third party bank. A bitcoin is created by miners, using complex mathematical "proof of work" procedure by computing hashes. For each successful attempt, miners get rewards in terms of bitcoin and transaction fees. Miners participate in mining to get this reward as income. Mining of cryptocurrency such as bitcoin becomes a common interest among the miners as the bitcoin market value is very high. As a side effect of this mining process, a lot of electricity is used in it.

Electricity is a semi-renewable resource — depending on the type of resource used for its production. Nevertheless, electricity plays an essential role in the bitcoin mining process since the whole mining process is based on it. The electricity consumed by the mining system is directly proportional to the computational power of that system. Moreover, powerful computers that specially designed for bitcoin mining process, consumes much more electricity than the regular computers. From the fact that at each time only one miner will be rewarded (the one who will win the mining game by first creating and updating the blocks), while the remaining miners' effort, as well as electricity used for mining at that time, will be wasted. Therefore, optimizing the consumption of electricity is one of the essential and most challenging problems nowadays.

One of the possible solutions to the problem mentioned above is to mine strategically rather than mining unreasonably. The strategy could be a plan of action designed to achieve a long-term goal, either *Cooperative*— where miners can benefit by cooperating and binding agreements or *Non-Cooperative*– where miners do not make binding agreements and compete against each other. In this paper, we create a game theoretic model in continuous time. We consider a dynamic game model of bitcoin market, where miners or players use mining systems to mine or producing the bitcoin by investing the electricity to the mining system. They sell their product — mined bitcoin in common market where the price of bitcoin is fixed and decide by the linear demand function— price of a product is linear in market demand of product (in economics it is called the linear inverse demand function). The game is played an infinite number of times.

We propose two different types of game theory solutions to the game model: **Social optimum:** (*Cooperative*) when the miners altogether maximize their total profit and **Nash equilibrium:** (*Non-Cooperative*) when each miner behaves selfishly and individually wants to maximize his/her total profit. Note that in our game theory model, a player represents a single "miner" or a "mining pool" who is responsible for creating a block in the blockchain. Our work here found that the electricity depleted very fast for the **Nash equilibrium** even if it is sustainable for the **Social optimum**. Our result is quite intuitive to the common

belief that mining in cooperation will give the higher payoff or profit to each miner than mining individually. Finally, to make the electricity consumption at equilibrium, we also propose a linear tax system which is of Pigovian type in order to enforce social optimality and refrain from over-consumption of electricity in our dynamic game model.

1 Introduction

Bitcoin [12] is a digital currency which was introduced in 2009. Its security is based on a *proof of work*, and a transaction is only considered valid once the system obtains proof that a sufficient amount of computational work has been exerted by authorizing nodes. The miners (responsible for creating blocks) constantly try to solve cryptographic puzzles in the form of a hash computation. The process of adding a new block to the blockchain is called *mining* and these blocks contain a set of transactions. The average time to create a new block in blockchain is ten minutes. Two types of agents participate in the Bitcoin network: *miners*, who validate transactions and *clients*, who trade in currency. The blockchain is a shared data structure responsible for storing all transaction history. The blocks are connected with each other in the form of a chain. The first block of the chain is known as **Genesis**. Each block consists of a Block Header, Transaction Counter and Transaction. The structure of blockchain is as follows:

Table 1. Structure of the Blockchain

Field	Size
Block Header	80 bytes
Block Size	4 bytes
Transaction Counter	1 to 9 bytes
Transaction	Depends on the transaction size

Each block in the chain is identified by a hash in the header. The hash is unique and generated by the Secure Hash Algorithm (SHA-256). SHA takes any size plaintext and calculates a fixed size 256-bit cryptographic hash. Each header contains the address of the previous block in the chain. The process of adding blocks in the blockchain is called "mining of blocks". If miners mine a valid block, it publishes the block in the blockchain and extends the blockchain by a new block. The creator of the block is rewarded with the bitcoin. We assume that miners are honest and follow the protocol.

Electricity, one of the necessities of the human beings, can be considered as both renewables if it generates from the renewable resource for example solar energy or hydropower or water plants and non-renewable if it produced from the thermal power plant that uses the coal— a non-renewable resource. So, depending on renewable or non-renewable resources, chosen for production of electricity, it can also be considered as semi-renewable which means that it has a combined fraction of both means of electricity production.

Exploitation of a shared resource is one of the most significant problems in society especially if the resource is semi-renewable because then the problem is even more complicated as it will lead to fast depletion of the resource. Since electricity can be considered as a semi-renewable resource, we have seen an unexpected growth of electricity (or computational power) consumption resulted from the bitcoin mining process. This has brought many miners to despair because the reward of mining a bitcoin decreases every four years by half. Therefore, miners need to mine bitcoin strategically to make bitcoin mining long lasting. In this paper, we use tools of dynamic game theory to solve our dynamic game model where every miner's objective is to use more powerful mining systems that consumes more elec-

tricity, in order to maximize the net profit gain from producing or mining the bitcoin and then selling it to the prevailing market.

We propose two ways to maximize the profit of miners: *cooperative*– all miners cooperate and decide to consume some fixed amount of electricity and in return, they get the bitcoin market price as profit so, they jointly maximize their profit and the profit is equally shared among them. *Non-cooperative*— each miner behaves selfishly and individually wants to maximize the profit gained from bitcoin mining.

2 Related Work

Since the early days of bitcoin in 2009 given in [12], blockchain technology and cryptocurrencies have caught the attention of both researchers and investors alike. The original paper on bitcoin was improved in [14], mostly focussing on the security analysis. Showing an attack in which large pools can gain more than their fair share, Eyal et al. showed Bitcoin mining protocol is not incentive compatible [3], which was significant work.

The linear quadratic differential game is the best-researched class of dynamic games (see Engwerda [2]). Dynamic games with linear quadratic structure and with linear state dependent constraint were studied by Singh and Wiszniewska-Matyszkiel [17, 16] but in discrete time horizon.

Zohar at el. [10] examined dynamics of pooled mining and the rewards that pools manage to collect, and use cooperative game theoretic tools to analyze how pool members may share these rewards. They showed that for some network parameters, especially under high transaction loads, it is difficult or even impossible to distribute rewards stably: some participants are always incentivized to switch between pools. Furthermore, Lewenberg et al. [11] also suggested a modification to Bitcoin's data structure, in the form of directed acyclic graphs know as DAGs, and have analyzed the game-theoretic aspects quite well of their proposal. In our opinion, one of the closest connected works to this paper is the work of Niyato, Vasilakos and Kun [13], which shows how to model blockchain technology as a cooperative game, in which cloud providers can cooperate. They show a novel solution of the core issues can be found using linear programming.

Kiayias [8] considered the Blockchain Mining Game with incomplete information as a stochastic dynamic game in discrete time. They considered the two type of strategies: when miners release every mined block immediately and when a block is mined it is announced immediately, but it may not be released so that other miners cannot continue mining from it. However, miners are always strategic on choosing of which blocks to mine. As a result, they found that the best response of the miners with less computational power matches to the expected behavior of the bitcoin designer, while for the miner with sizeable computational power, he/ she deviates from the expected behavior, and other Nash equilibria arise.

Salimitari [15] discussed the mining profitability of a new miner or pool by calculating the expected value of profit. In their model, they assume the cost of mining was linear to the price of electricity consumed in the mining process. Hayes [6] study the model to check the marginal cost of production, proposed to set the market value of the digital bitcoin currency. They show that the marginal cost of production of bitcoin plays an essential role in explaining bitcoin prices.

Houy [7] considered the bitcoin mining game where they studied the mining incentives as a decision regarding how many transactions they should include in the block they are mining in order to win the game and update the block first. Harvey et al. [4] considered the model of miners' profitability from the mining cost analysis of the electrical energy invested in bitcoin mining production. They also show that how the profit model changes as mining scales from the individual to the industrial level.

Laszka et al. [9] considered a game-theoretic model that allows capturing short term as well as long-term impacts of attacks against mining pools. Using this model, we study the

conditions under which the mining pools have no incentives to cheat against each other and the conditions under which one mining pool is marginalized by cheating.

2.1 Formulation of the model

We consider a continuous time dynamic game model of exploitation of a semi-renewable resource—electricity. Our dynamic game $\hat{\mathcal{G}}$ consists of:

1. The set of finite players: $\mathbb{I} = \{1, 2, \cdots, n\}$. Players can be either individual miners or mining pools.
2. The state of resource x is the amount of available computational power, proportional to the electric power consumption. Since no one uses a negative amount of computational power so, we assume that $x \in (0, +\infty)$ with initial state $X(0) = x_0$ representing the initial amount of computational power.
3. At each time instant miner i decided to consume s_i amount of electricity, which we called strategy of miner i. These s_i in common constitute a profile of strategies and is defined as $s = (s_1, \cdots, s_n)$.
   Notational convention: For simplicity, we introduce the notion for a profile of decisions $s = [s_i, s_{\sim i}]$ where, s_i is the decision of miner i (amount of electricity he decided to consume) and $s_{\sim i}$ is the decision of the remaining miners (amount of electricity decided by the remaining players to consume).
   $S_i(X(t))$ is any function defined by $S_i(X(t)) = s_i$, and $X(t)$ is any function defined as $X(t) = x$.
4. We are interested in calculating the feedback strategies $S_i : (0, +\infty) \to \mathbb{R}$. It means that the amount of electricity that he decides to use at every time instant t will depend on the fact that how much electricity available at that time.
5. We denote the set of available decisions of miner i by $\mathcal{U} = (0, Mx]$ for some positive constant M representing the maximum fraction of the electricity. So, for every miner i, mining strategy $s_i \in (0, Mx]$. This represents a real situation where a miner cannot consume more than the available electricity, or a negative number of electricity. We denote the set of decision profiles by $\mathcal{U}^n$.
6. We consider the economic scenario where a bitcoin miner i invests some amount of electricity to the mining system in order to solve "proof of work." As a result of successfully mining a block into the blockchain, he produces some bitcoin. He sells their bitcoin into the common-market for a fixed market price of bitcoin. This market price of bitcoin is decided by the linear demand which is also known as the inverse demand function. So, in this economic model net profit of miner is given by the net revenue minus the mining cost of bitcoin. In the model, the cost of mining is linearly proportional to the price of electricity consumed.
   In our infinite time horizon dynamic game model, the profit does not directly depend on time t. So, the current or instantaneous payoff or profit g_i of miner i is given by

$$g_i(x, s_i) = \left(P - \sum_{j=1}^{n} s_j \right) s_i - C s_i, \tag{1}$$

   where P is the fixed market price of bitcoin in dollars given by the inverse demand function and C is the fixed price of electricity in dollars.
   In economics generally, P is substantially higher than C.
7. A function $X : (0, +\infty) \to \mathbb{R}_+$ is called a trajectory of the state of the system and given by

$$\dot{X}(t) = \psi\left(X(t), S(X(t))\right), \text{ with the initial condition } X(0) = x_0, \tag{2}$$

for the state transition function ψ, describing the behaviour of the system dynamics:

$$\psi(x,s) = \left(\xi x - \sum_{j=1}^{n} s_j\right), \tag{3}$$

where r is called the regeneration rate of the electricity.

8. The total payoffs or total profits of the miner i in the game are discounted by a discount factor $r \in (0,1)$. It means that after each time interval the payoff or profit of the miner in bitcoin mining decreases by a factor r which we call the discount rate.
9. The total payoff function or total profit of the miner after the termination of the game is

$$J_i\left(x_0, [S_i, S_{\sim i}]\right) = \int_{t=0}^{\infty} e^{-rt} g_i(X(t), S_i(X(t)))dt, \tag{4}$$

for $i = 1, 2, \cdots n$ and for X given by Eq. (2).
Analogously, we can define $J_i\left(\bar{x}, [S_i, S_{\sim i}]\right)$ for arbitrary initial $\bar{x} \geq 0$.

3 Solution concept of bitcoin mining model

Here we discuss the definitions of solution types for our bitcoin mining game.

Social Optimum mining profile: A social optimum mining profile is a solution of our mining game where all miners cooperate. In other words, it is a profile at which all miners jointly maximize their current payoffs or profits. Social optimum mining profile can be the result of decision making by a single miner regarded as a social planner or just full cooperation of all miners.

Definition 1. *A mining profile $\bar{s}$ is called a* social optimum *mining profile in our n miner bitcoin mining game iff $\bar{s}$ maximizes $\sum_{i=1}^{n} J_i(x_0, s)$.*

Nash equilibrium mining profile: A Nash equilibrium mining profile is a solution of our mining game where all miners behave selfishly and do not cooperate. A mining profile $\bar{s}$ is called in *Nash equilibrium* if no miner can benefit from unilateral deviation from it. Formally it can be defined as follows,

Definition 2. *A mining profile $\bar{s}$ is called a* ***Nash equilibrium*** *iff for every miner $i \in \mathbb{I}$ and for every mining strategy s_i of miner i,*

$$J_i\left([s_i, \bar{s}_{\sim i}]\right) \leq J_i\left([\bar{s}_i, \bar{s}_{\sim i}]\right).$$

3.1 Calculation of social optimum

First, we calculate the social optimum strategy profile — solution of the cooperative game and the value function — the total profit of a cooperative miner.

Consider the total profit $J(x,S) = \sum_{i=1}^{n} J_i\left(x, [S_i, S_{\sim i}]\right)$, then the dynamic optimization problem of finding social optimum mining profile is defined by

$$\sup_{S \in [0, Mx]^n} J(x_0, S), \tag{5a}$$

$$\dot{X}(t) = \xi X(t) - \sum_{i=1}^{n} S_i(X(t)), \tag{5b}$$

$$X(0) = x_0. \tag{5c}$$

Theorem 1. *The optimal solution in the case of cooperation of all miners is given by*

$$S_i^{\mathrm{SO}}(x) := \begin{cases} \frac{(2\xi-r)2\xi x+(P-C)(r-\xi)}{2n\xi} & x < \hat{x}, \\ \frac{P-C}{2n} & x \geq \hat{x}. \end{cases} \tag{6}$$

for the constant $\hat{x} = \frac{P-C}{2\xi}$.
We called this optimal solution "a social optimum profile".

The combined total profit of all miners for this social optimum mining profile is given by

$$V^{\mathrm{SO}}(x) := \begin{cases} \frac{Hx^2}{2} + Gx + K \\ \frac{(P-C)^2}{4r} & x \geq \hat{x}. \end{cases} \tag{7}$$

for constants $H = 2(r-2\xi),\ G = \frac{-(P-C)(r-2\xi)}{\xi}$ *and* $K = \frac{(P-C)(r-\xi)^2}{4r\xi^2}$.

The total payoff or profit of an individual miner i *is given by*

$$V_i^{\mathrm{SO}}(x) := \frac{V^{\mathrm{SO}}(x)}{n}. \tag{8}$$

This total payoff is called a "value function" of miner i *at social optimum profile.*

Proof. The Hamiltonian-Jacobi-Bellman equation (see e.g., Haurie, Krawczyk and Zaccour [5], Başar and Olsder [1], Zabczyk [19], Stokey Lucas [18]) for any function $V(x)$ can be written as

$$rV(x) = \sup_{s_i \in [0,Mx]^n} \sum_{i=1}^{n} \left[\left(P - C - \sum_{i=1}^{n} s_i \right) s_i \right] + \left(\xi x - \sum_{i=1}^{n} s_i \right) \frac{\partial V(x)}{\partial x}. \tag{9}$$

To calculate the optimal strategy s_i, differentiate the right hand side of Eq. (9) with respect to s_i and equate to 0, we get the optimal value $\bar{s}_i$ as

$$2\bar{s}_i = P - C - \sum_{j=1, j\neq i}^{n} s_j - \frac{\partial V(x)}{\partial x},\ i = 1, 2 \cdots n. \tag{10}$$

Note that the right hand side of Eq. (10) is identical for all i, so, the optimal value $\bar{s}_i$ will be the same for all n miners.

If we take the value of parameter M as sufficiently large, then the optimal value $\bar{s}_i$ will always be less than or equal to Mx.

Now, the social optimum can be found by solving the following differential equation for given optimal $\bar{s}_i$ and a function $V(x)$,

$$rV(x) = n\left(P - C - n\bar{s}_i\right)\bar{s}_i + \frac{\partial V(x)}{\partial x}\left(\xi x - n\bar{s}_i\right). \tag{11}$$

The quadratic structure of the social optimum problem suggests that the value function is of quadratic form. Therefore, we assume that the value function has the form

$$V(x) = K + Gx + \frac{Hx^2}{2}, \tag{12}$$

for some constants H, G and K. Since this equation has to hold for all x, the coefficients of x^2, x and the constant term on the left-hand side and the right-hand side have to be equal in order to calculate the values of the constants.

So, we have the two set of values of the constants:

$$(i)\ H = 0,\ G = 0\ K = \frac{(P-C)^2}{4r},$$

then $\bar{s}_i = \frac{P-C}{2n}$ will be the optimal solution only if $\frac{P-C}{2n} \leq Mx$.

$$(ii)\ H = 2(r-2\xi),\ G = \frac{-(P-C)(r-2\xi)}{\xi},\ K = \frac{(P-C)(r-\xi)^2}{4r\xi^2},$$

then the optimal solution will be $\bar{s}_i = \frac{(2-r)Cx+nR(r-1)}{nC}$, only if $0 \leq \bar{s}_i < Mx$.

Therefore, the social optimum strategy profile is given by Eq. (6) while the total profit of a miner is given by Eq. (8). □

3.2 Calculation of Nash equilibrium

Next, we calculate the Nash equilibrium strategy profile — solution of the non-cooperative game and the value function — total profit of a non-cooperative or selfish miner.

Given strategies of the remaining miners $S_{\sim i}$, optimization problem of miner i is defined by

$$\sup_{S_i \in [0,Mx]} J_i\left(x_0, [S_i, S_{\sim i}]\right) \tag{13a}$$

$$\dot{X}(t) = \xi X(t) - S_i(X(t)) - \sum_{j=1, j\neq i}^{n} S_j(X(t)), \tag{13b}$$

$$X(0) = x_0. \tag{13c}$$

Theorem 2. *The optimal solution in the case of non-cooperation of the miners is*

$$S_i^{\mathrm{NE}}(x) = \begin{cases} \frac{(n+1)(2\xi-r)x}{2n^2} + \frac{(P-C)(n^2r+r-2\xi)}{2n^2\xi(n+1)} & x < \tilde{x} \\ \frac{P-C}{n+1} & x \geq \tilde{x}. \end{cases} \tag{14}$$

for $\tilde{x} = \frac{(n^2+1)(P-C)}{\xi(n+1)^2}$. *We call this optimal solution a "Nash equilibrium strategy profile".*

The total payoff or profit of miner i at this Nash equilibrium strategy profile is given by

$$V_i^{\mathrm{NE}}(x) = \begin{cases} \frac{\bar{H}x^2}{2} + \bar{G}x + \bar{K} & x < \tilde{x} \\ \frac{(P-C)^2}{r(n+1)^2} & x \geq \tilde{x}. \end{cases} \tag{15}$$

for constants $H = \frac{(n+1)^2(r-2\xi)}{2n^2}$, $G = \frac{-(n^2+1)(P-C)(r-2\xi)}{2n^2\xi}$ *and* $K = \frac{(rn^2+r-2\xi)(rn^2+r-2n^2\xi)(P-C)^2}{4\xi^2n^2(n+1)^2r}$.

Proof. The Hamiltonian-Jacobi-Bellman equation for any function $V_i(x)$ can be written as

$$rV(x) = \sup_{s_i \in [0,Mx]} \left(P - C - \sum_{i=1}^{n} s_i\right) s_i + \left(\xi x - s_i - \sum_{j=1, j\neq i}^{n} s_i\right) \frac{\partial V(x)}{\partial x}. \tag{16}$$

To calculate the optimal mining strategy s_i, differentiate the right hand side of Eq. (16) with respect to s_i and equate to 0, we get the optimal value $\bar{s}_i$ as

$$2\bar{s}_i = P - C - \sum_{j=1, j\neq i}^{n} s_j - \frac{\partial V(x)}{\partial x},\ i = 1, 2 \cdots n. \tag{17}$$

Note that the right hand side of Eq. (17) is identical for all i. Therefore, the optimal value $\bar{s}_i$ will be same for each miner. Moreover, since the mining strategy of all miners is symmetric, so, we substitute $s_j = s_i$ in Eq. (17).

If we take the value of parameter M as sufficiently large, then the optimal value $\bar{s}_i$ will always be less than or equal to Mx.

Now, the Nash equilibrium can be found by solving the following differential equation for given optimal $\bar{s}_i$ and a function $V_i(x)$,

$$rV(x) = (P - C - n\bar{s}_i)\,\bar{s}_i + \frac{\partial V(x)}{\partial x}\,(\xi x - n\bar{s}_i)\,. \tag{18}$$

The quadratic structure of the problem suggests that the value function is of quadratic form. Therefore, we assume that the value function has the form

$$V_i(x) = K_i + G_i x + \frac{H_i x^2}{2}, \tag{19}$$

Since we have a symmetric optimal mining strategy which implies that also H_i, G_i and K_i are equal for all $i = 1, \cdots, n$. So, we substitute $H_i = \bar{H}$, $G_i = \bar{G}$ and $K_i = \bar{K}$.

Since the Eq. (18) has to hold for all x, the coefficients of x^2, x and the constant term on the left-hand side and the right-hand side have to be equal.

So, we have two sets of values of the constants:

$$(i)\ \bar{H} = 0,\ \bar{G} = 0,\ \bar{K} = \frac{(P-C)^2}{r(n+1)^2},$$

then $\bar{s}_i = \frac{P-C}{n+1}$ will be the optimal solution only if $\frac{P-C}{n+1} \leq Mx$.

$$(ii)\ \bar{H} = \frac{(n+1)^2(r-2\xi)}{2n^2}, \bar{G} = \frac{-(n^2+1)(P-C)(r-2\xi)}{2n^2\xi}, \bar{K} = \frac{(rn^2+r-2\xi)(rn^2+r-2n^2\xi)(P-C)^2}{4\xi^2 n^2(n+1)^2 r},$$

then the optimal solution will be $\bar{s}_i = \frac{(2-r)Cx + R(nr-1)}{(2n-1)C}$, only if $0 \leq \bar{s}_i < Mx$.

Therefore, the Nash equilibrium strategy profile is given by Eq. (14) while the total profit of a miner is given by Eq. (15). □

Figure 1–2 are drawn for the values of constants: $P = 11511 \cdot 10^3\$, C = 5327\$, n = 1800, \xi = 0.03, r = 0.02$. Figure 1 shows the total profit earned by miner in USD by consuming the electricity strategically, depending on the optimal strategy (see Fig. 2): cooperative or non-cooperative he/she chooses. For $x \geq \tilde{x}$, miner will get the same profit since the optimal strategy is constant in both cooperative and non-cooperative cases for such values of x.

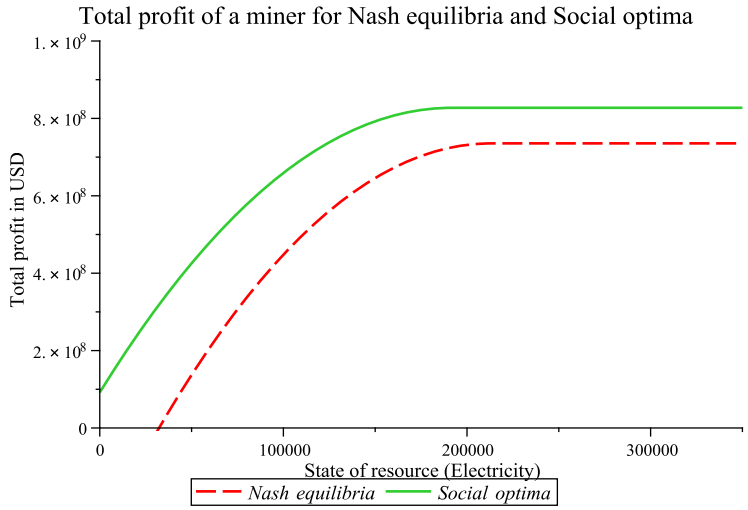

Fig. 1. Total profit of a miner at a Nash equilibrium and the social optimum

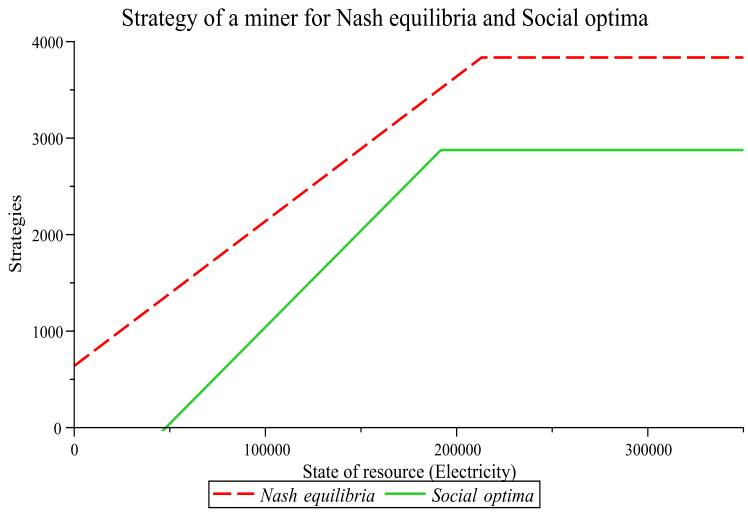

Fig. 2. Optimal strategy of a miner at a Nash equilibrium and the social optimum

4 Enforcing social optimality by a tax-subsidy system

In this section, we consider a tax system or penalty system which can be implemented by an external authority such as government, administration. Therefore, in this case, if the miners' consume the electricity more than the social optimum or social welfare level, then they would have to pay some extra amount to the external authority for the extra amount of electricity consumption. This introduction of a tax system is essential in order to maintain the equilibrium in the society and to make electricity sustainable. If we will not be able

to control electricity consumption, then it would lead to the serious electricity crises in the future.

We want to make sure that the miners behave in a socially optimal manner which is for the welfare of society by a *tax system* or a *tax-subsidy system* which is linear in miner's strategy s_i i.e.,

$$\text{Tax}(x, s_i) = \tau(x)s_i.$$

Formally, *introduction of a tax* or a *tax-subsidy system* is a modification of the original non-cooperative game by changing the payoffs. In our mining game model, the *current payoff function* of miner i changes to $\left(P - C - \sum_{i=1}^{n} s_i\right) s_i - \text{Tax}(x, s_i)$.

We are interested in Pigovian type tax where tax is linear in the surplus over the socially optimum level, so if the miner mines more than the socially optimum level he/she will have to pay an extra amount as a penalty for over-mining the bitcoin.

$$\text{Tax}(x, s_i) = \tau(x)\left(s_i - S_i^{\text{SO}}\right). \tag{20}$$

So, the total payoff function in the mining game becomes

$$J_i^{\tau}\left(x, [S_i, S_{\sim i}]\right) = \int_{t=0}^{\infty} e^{-rt}\left(P - C - \sum_{i=1}^{n} s_i\right) s_i - \tau(x)\left(\frac{(2\xi - r)2\xi x + (P - C)(r - \xi)}{2n\xi}\right) dt. \tag{21}$$

Definition 3. *A tax-subsidy system* enforces *that the mining profile $\bar{C}$ if $\bar{C}$ is a Nash equilibrium mining strategy in the new mining game with the total payoff defined by Eq.* (21).

Theorem 3. *The tax rate, enforcing the socially optimal behaviour of the miners is given by*

$$\tau(x) = \frac{2\xi x(r - 2\xi) + (P - C)(3\xi - r)}{n^2} \tag{22}$$

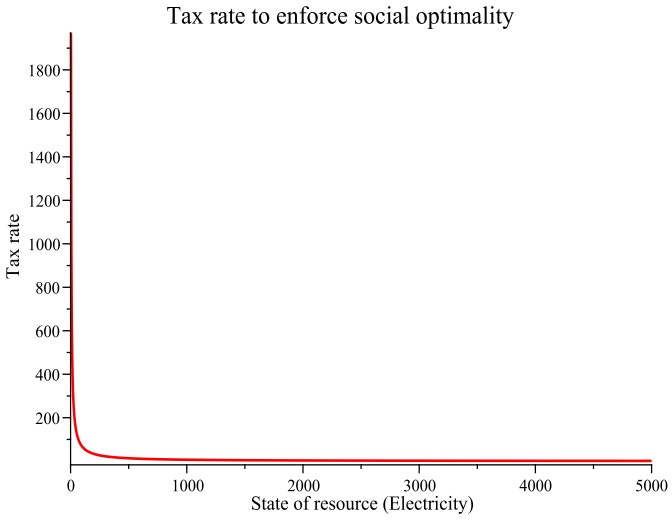

Fig. 3. Tax rate $\tau(x)$ enforcing the socially optimal profile for the values of constants: $P = 1000, C = 10, n = 2, r = 0.01, \xi = 0.02$

Figure 3 presents the tax rate of the linear tax enforcing the socially optimal profile. We can see when fewer bitcoin which remain to be mined, more substantial tax rates are required.

Proof. Consider the game with enforcing the social optimum strategy profile. If a miner mines s_i^{SO} then there is no tax to be paid or subsidy to be obtained. So, if every miner play s_i^{SO}, each of them obtains the total profit $V_i^{\mathrm{SO}}(x)$ and this is the optimal total profit for such an appropriate $\tau(x)$, if it exists. So, the HJB equation for $V_i^{\mathrm{SO}}(x)$ becomes

$$rV_i^{\mathrm{SO}}(x) = \sup_{s_i \in [0, Mx]} \left(P - C - \sum_{i=1}^{n} s_i \right) s_i - \tau(x)(s_i - S^{\mathrm{SO}}(x)) + \left(\xi x - s_i - \sum_{j=1, j \neq i}^{n} s_j \right) \frac{\partial V_i^{\mathrm{SO}}(x)}{\partial x} \tag{23}$$

The first order condition for the above optimization problem is

$$\tilde{s}_i = \frac{4\xi^2 x + ((n-2)(P-C) - 2rx - n\tau)\xi + r(P-C)}{\xi n(n+1)} \tag{24}$$

and the optimal solution should be attained at s_i^{SO}. The condition $\tilde{s}_i = s_i^{\mathrm{SO}}$ yields $\tau(x)$ defined by Eq. (22). Substitute $\tilde{s}_i$ for this $\tau(x)$ into Eq. (23) to see that it is fulfilled. □

5 Conclusion

Electricity is a semi-renewable resource, so it is essential to exploit or extract it strategically in order to maintain the sustainability of the resource. In this paper, we consider a continuous time dynamic game model of bitcoin mining with infinite time horizon which belongs to the class of differential games. We propose two types of solutions to our model which we call optimal strategies, namely cooperative (social optimum) mining strategy, and non-cooperative (Nash equilibrium) mining strategy. We calculate the total profit of a miner in both cases. We found that it is always beneficial for the miners to consume or use the electricity jointly, in cooperation with the other miners. Cooperation gives the miner a higher total profit compared to a miner who mines selfishly. Moreover, if all the miners choose to mine according to the Nash equilibrium mining strategy, then the Electricity will deplete much faster than if they choose to mine according to the social optimum strategy. Our result fits quite nicely with the common belief that mining in cooperation will be better than mining individually in a non-cooperative game. We also propose a tax system which falls into a Pigovian type. This tax system is linear in the miner's strategy in order to enforce social optimality in our bitcoin dynamic game model. This way, miners will be forced to behave or mine in a way that is best for the social welfare of the miners.

References

1. Basar, T., Olsder, G.J.: Dynamic noncooperative game theory, vol. 23. Siam (1999)
2. Engwerda, J.: LQ dynamic optimization and differential games. John Wiley & Sons (2005)
3. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM 61(7), 95–102 (2018)
4. Harvey-Buschel, J., Kisagun, C.: Bitcoin mining decentralization via cost analysis. CoRR abs/1603.05240 (2016), `http://arxiv.org/abs/1603.05240`
5. Haurie, A., Krawczyk, J.B., Zaccour, G.: Games and dynamic games, vol. 1. World Scientific Publishing Company (2012)
6. Hayes, A.S.: Bitcoin price and its marginal cost of production: support for a fundamental value. Applied Economics Letters pp. 1–7 (2018)

7. Houy, N.: The bitcoin mining game. Ledger 1, 53–68 (2016), https://ledgerjournal.org/ojs/index.php/ledger/article/view/13
8. Kiayias, A., Koutsoupias, E., Kyropoulou, M., Tselekounis, Y.: Blockchain mining games. In: Proceedings of the 2016 ACM Conference on Economics and Computation, EC '16, Maastricht, The Netherlands, July 24-28, 2016. pp. 365–382 (2016), http://doi.acm.org/10.1145/2940716.2940773
9. Laszka, A., Johnson, B., Grossklags, J.: When bitcoin mining pools run dry - A game-theoretic analysis of the long-term impact of attacks between mining pools. In: Financial Cryptography and Data Security - FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers. pp. 63–77 (2015), https://doi.org/10.1007/978-3-662-48051-9_5
10. Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., Rosenschein, J.S.: Bitcoin mining pools: A cooperative game theoretic analysis. In: Weiss, G., Yolum, P., Bordini, R.H., Elkind, E. (eds.) Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, AAMAS 2015, Istanbul, Turkey, May 4-8, 2015. pp. 919–927. ACM (2015), http://dl.acm.org/citation.cfm?id=2773270
11. Lewenberg, Y., Sompolinsky, Y., Zohar, A.: Inclusive block chain protocols. In: International Conference on Financial Cryptography and Data Security. pp. 528–547. Springer (2015)
12. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2009), http://www.bitcoin.org/bitcoin.pdf
13. Niyato, D., Vasilakos, A.V., Kun, Z.: Resource and revenue sharing with coalition formation of cloud providers: Game theoretic approach. In: Cluster Computing and the Grid, IEEE International Symposium on(CCGRID). vol. 00, pp. 215–224 (05 2011), doi.ieeecomputersociety.org/10.1109/CCGrid.2011.30
14. Rosenfeld, M.: Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009 (2014)
15. Salimitari, M., Chatterjee, M., Yuksel, M., Pasiliao, E.: Profit maximization for bitcoin pool mining: A prospect theoretic approach. In: 3rd IEEE International Conference on Collaboration and Internet Computing, CIC 2017, San Jose, CA, USA, October 15-17, 2017. pp. 267–274 (2017), https://doi.org/10.1109/CIC.2017.00043
16. Singh, R., Wiszniewska-Matyszkiel, A.: Discontinuous Nash equilibria in a two stage linear-quadratic dynamic game with linear constraints. IEEE Transactions on Automatic Control 0, 0–0 (2018)
17. Singh, R., Wiszniewska-Matyszkiel, A.: Linear quadratic game of exploitation of common renewable resources with inherent constraints. Topological Methods in Nonlinear Analysis 51, 23–54 (2018)
18. Stokey, N.L., Lucas, R., Prescott, E.: Recursive methods in economic dynamics. Harvard University Press (1989)
19. Zabczyk, J.: Mathematical control theory: an introduction. Springer Science & Business Media (2009)