Bitcoin Mining: A Game Theoretic Analysis

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

[1] Faculty of Mathematics, Informatics, and Mechanics, University of Warsaw, Warsaw, Poland
[2] Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland
[3] 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. Bitcoin is a non-renewable resource, since the reward of mining a bitcoin decreases over time, obvious questions that arise are what will be the incentive for miners in bitcoin mining over time? Moreover, how will balance be maintained in the bitcoin mining market as time goes on ? From the fact that at any time only one miner will be rewarded (the one who will win the mining game by first creating and updating the blocks and the remaining miners effort will be wasted at that time), it is better for them to mine strategically. However, this 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 where we consider bitcoin mining as a continuous time dynamic game which is played an infinite number of times. We propose two different types of game theory solutions: **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 single "mining pool" who is responsible to create a block in the blockchain. Our work here found that the bitcoin is never sustainable and 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 retain the bitcoin market at equilibrium we also propose a linear tax system which is of Pigovian type in order to enforce social optimality in our bitcoin dynamic game model.

1 Introduction

Bitcoin [25] 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. 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:

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

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

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 extend 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.

Exploitation of a common resource is one of the biggest problems in society especially if the resource is non-renewable because then the problem is even more complex as it will lead to a fast depletion of the resource. Since bitcoin is a non-renewable resource, we have seen an unexpected growth of mining bitcoin. 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 bitcoin mining model where every miner's objective is to maximize the net profit gain from mining a bitcoin. We propose two ways to maximize the profit of miners: *cooperative*– all miners cooperate and jointly maximize their profit and the reward is equally shared among them and *non-cooperative*— each miner behaves selfishly and individually mines bitcoin.

Here in the cooperative approach we are not taking a *mining pool* as a group of miners but we assume a mining pool as a single miner (A mining pool is a way of sharing processing power or resources over a network by miners. Miners share the reward equally according to the work they contributed to create a block in a pool.) .

2 Related Work

Since the early days of bitcoin in 2009 given in [25], blockchain technology and cryptocurrencies have caught the attention of both researchers and investors alike. The original paper on bitcoin was improved in [31], mostly focussing on the security analysis. In [3], the authors examined a common scenario in which only participants that are aware of the information can compete for some reward focussing on incentive issues within Bitcoin. 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 [19], which was a very important work.

Ron and Shamir [30] analyzed transaction graphs, and made attempts to identify which accounts belong to the same entity. Zohar at el. [21] 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 in a stable way: some participants are always incentivized to switch between pools. Furtheremore, Lewenberg et al. [22] also suggested a modifcation 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 [26], 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.

Cooperation among agents has been widely studied in the ever growing artificial intelligence literature. In some relatively early work like the paper by Sandholm and Lesser [32], the authors analyzed coalitions among self-interested agents that need to solve combinatorial optimization problems to operate effciently in the world. Further to this, Shehory and Kraus [35] considered task allocations via agent coalition formation. We propose a cooperative game model for analyzing Bitcoin mining pools here. Cooperative game models have been used for many real world applications, including

1. network analysis [11, 9, 24, 29]
2. voting [12, 7, 16, 17, 37, 38, 34]
3. team formation [10, 8, 35, 2]
4. negotiation [5]
5. pricing cloud services [14]
6. auctions [4]

We have also seen the computational aspects of cooperative games being the focus of other works, most notably the work of Elkind et al. [16] who showed that many stability-related solution concepts in weighted voting games are hard to compute. Moreover, in the work of Aziz and De Keijzer [2] where an algorithm for finding an optimal coalition structure for games with few player types was proposed.

Cooperative games with coalition structures were introduced by Aumann and Dreze [1] quite early. In the common practice of cooperative games with coalition structures, also known as characteristic function games, the value of each coalition is independent of nonmembers' actions [6, 15, 23, 27, 33]. Our model shows similarities to one proposed by Ray and Vohra in [28], in which the value of a coalition depends on the coalition structure.

Eyal also presented a paper [18] which explored a block withholding attack among Bitcoin mining pools — an attack that is possible in any similar system that rewards for proof of work. Such systems are gaining popularity, running most digital currencies and related services. He observe that no-pool-attacks is not a Nash equilibrium: If none of the other pools attack, a pool can increase its revenue by attacking the others.

2.1 Formulation of the model

We consider a continuous time dynamic game model of exploitation of a non-renewable resource — bitcoin. 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 individual mining pools.
2. The state of resource x is the number of bitcoin available to mine at that time. Since one cannot mine a negative number of bitcoin, we assume that $x \in (0, +\infty)$ with initial state $X(0) = x_0$ representing the number of bitcoin available at the beginning of mining game.
3. At each time instant miner i mines s_i number of bitcoin. 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 and $s_{\sim i}$ is the decision of the remaining miners. $S_i(X(t))$ 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 feedback strategies $S_i : (0, +\infty) \to \mathbb{R}$. It means that the number of bitcoin a miner decides to mine (decision of miner) at every time will depend on how much bitcoin is left to mine 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 mining rate. So, for every miner i, mining strategy $s_i \in (0, Mx]$. This represents a real situation where a miner cannot mine more than the available bitcoin for mining, or a negative number of bitcoin. We denote the set of decision profiles by $\mathcal{U}^n$.
6. The current or instantaneous payoff g_i of miner i is the net revenue which equals the reward R earned by him/her for successfully mining the bitcoin minus the quadratic cost of mining. We assume that the cost of mining is identical for each miner. In our infinite time horizon dynamic game model, the profit does not directly depend on time t. Therefore, the current payoff is given by
   $$g_i(x, s_i) = \left(Rs_i - \frac{Cs_i^2}{2}\right), \tag{1}$$
   for positive constants R regarded as reward of bitcoin mining and C being the cost of bitcoin mining with $R >> C$.
7. A function $X : (0, +\infty) \to \mathbb{R}_+$ is called a trajectory of the state of the system and it is defined as
   $$\dot{X}(t) = \psi\left(X(t), S(X(t))\right), \text{ with the initial condition } X(0) = x_0, \tag{2}$$

for a function ψ describing the behaviour of the system dynamics given by

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

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

$$J_i\left(x_0, [S_i, S_{\sim i}]\right) = \int_{t=0}^{\infty} e^{-rt} g_i(X(t), S_i(X(t)))dt \text{ for } i = 1, 2, \cdots n. \tag{4}$$

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 with each other. 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 $\sum\limits_{i=1}^{n} J_i(x_0, s)$.*

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 with each other. 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 are interested in calculating the social optimum mining profile — a solution of the cooperative mining game.

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

$$\max_{S \in [0, Mx]^n} J\left(x_0, S\right), \text{ for } X \text{ given by} \tag{5a}$$

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

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

Theorem 1. *a) The optimal solution in the case of cooperation of all miners is*

$$S^{\mathrm{SO}}(x) := \begin{cases} \frac{(2-r)Cx + nR(r-1)}{nC} & x < \hat{x}, \\ \frac{R}{C} & x \geq \hat{x}. \end{cases} \tag{6}$$

for the constant $\hat{x} = \frac{R}{MC}$ We called this optimal solution "a social optimum mining profile".

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

$$V^{\mathrm{SO}}(x) := \begin{cases} \frac{(r-2)(Cx-nR)^2}{2nC} + \frac{nR^2}{2rC}, & x < \hat{x}, \\ \frac{nR^2}{2rC} & x \geq \hat{x}. \end{cases} \tag{7}$$

while the total payoff or payoff of an individual miner i is

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

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 [20], Başar and Olsder [13], Zabczyk [36]) for any function $V(x)$ can be written as

$$rV(x) = \sup_{s_i \in [0,Mx]^n} \sum_{i=1}^{n} \left[\left(R - \frac{Cs_i}{2}\right) s_i\right] + \left(x - \sum_{i=1}^{n} s_i\right) \frac{\partial V(x)}{\partial x}. \tag{9}$$

To calculate the optimal mining 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

$$\bar{s}_i = \frac{1}{C}\left(R - \frac{\partial V(x)}{\partial x}\right), i = 1, 2 \cdots n. \tag{10}$$

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 be always 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 $V(x)$,

$$rV(x) = n\left(R - \frac{\bar{s}_i}{2}\right)\bar{s}_i + \left(x - \frac{n\bar{s}_i}{C}\right) \cdot \frac{\partial V(x)}{\partial x}. \tag{11}$$

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 the 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: First set of values are $H = 0$, $G = 0$ and $K = \frac{nR^2}{2rC}$, then the optimal solution will be $\frac{R}{C}$ only if $\frac{R}{C} \leq Mx$.

Second set of values of the constants are

$$H = \frac{C(r-2)}{n},\ G = R(2-r),\ K = \frac{nR^2(r-1)^2}{2rC},$$

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

Therefore, the social optimum mining 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 mining profile — a solution of the non-cooperative mining game.

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

$$\max_{S_i \in \mathcal{U}} J_i\left(x_0, [S_i, S_{\sim i}]\right) \text{ for } X \text{ given by} \tag{13a}$$

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

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

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

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

for $\hat{x} = \frac{R}{MC}$. We call this optimal solution "a Nash equilibrium mining profile".

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

$$V_i^{\mathrm{NE}}(x) = \begin{cases} \frac{(r-2)(Cx-nR)^2}{2(2n-1)C} + \frac{R^2}{2rC} & x < \hat{x} \\ \frac{R^2}{2rC} & x \geq \hat{x}. \end{cases} \tag{15}$$

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

$$rV_i(x) = \sup_{s_i \in [0, Mx]} \left(R - \frac{Cs_i}{2} \right) s_i + \left(x - s_i - \sum_{j \neq i}^{n} s_j \right) \frac{\partial V_i(x)}{\partial x}. \tag{16}$$

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

$$\bar{s}_i = \frac{1}{C} \left(R - \frac{\partial V_i(x)}{\partial x} \right), i = 1, 2 \cdots n. \tag{17}$$

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, 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 be always 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 $V_i(x)$,

$$rV_i(x) = \left(R - \frac{\bar{s}_i}{2} \right) \bar{s}_i + (x - n\bar{s}_i) \frac{\partial V_i(x)}{\partial x}. \tag{18}$$

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 $i = 1, \cdots, n$.

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: First set of values are $H_i = 0$, $G_i = 0$ and $K_i = \frac{R^2}{2rC}$, then the optimal solution will be $\frac{R}{C}$ only if $\frac{R}{C} \leq Mx$. Second set of values of the constants are

$$H_i = \frac{C(r-2)}{2n-1}, \; G_i = \frac{nR(2-r)}{2n-1}, \; K_i = \frac{R^2(nr-1)(nr-2n+1)}{2(2n-1)rC},$$

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

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

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

$$\tau(x) = \frac{(r-2)(n-1)(Cx-Rn)}{n^2} \tag{20}$$

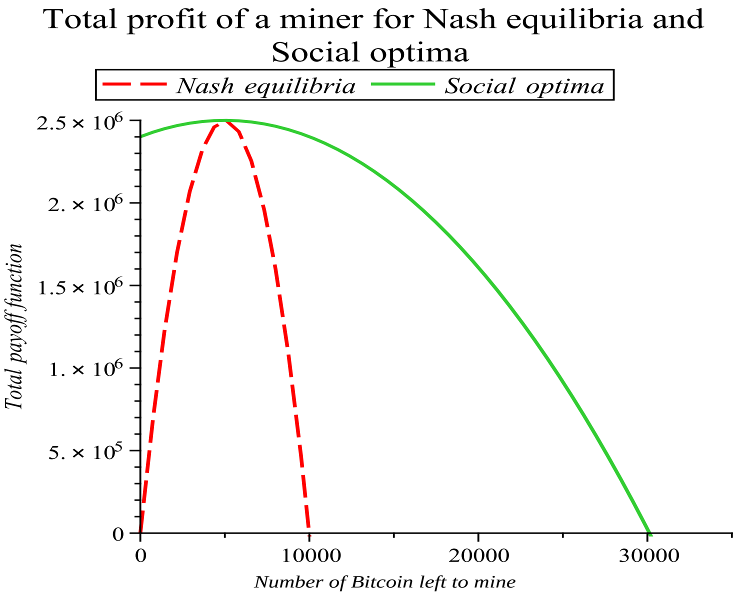

Fig. 1. Total profit of a miner at Nash equilibrium and at social optimum for the values of the parameters are $n = 20$ and $r = 0.02$

Figure 1 shows the total profit gained by miner for $x < \tilde{x}$ by mining a bitcoin strategically depending on which mining strategy: cooperative or non-cooperative he/she chooses. For $x \geq \tilde{x}$, miner will get the same profit since the optimal mining strategy is constant in both cooperative and non-cooperative cases for such x.

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 or bitcoin market owner to name a few. Therefore, in this case if the miner mines bitcoin more than the social optimum or social welfare level then he/she would have to pay some extra amount to the external authority. This introduction of a tax system is very important in order to maintain the equilibrium in the bitcoin mining market. If not, we may see that mining will no longer be interesting from the point of view of the miners.

We are interested in making sure 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., $\text{tax}(s_i, x) = \tau(x)s_i$. 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 $Rs_i - \frac{Cs_i^2}{2} - \text{tax}(s_i, x)$.

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 social optimum level he/she will have to pay an extra amount as a penalty for over-mining the bitcoin.

$$\text{tax}(s_i, x) = \tau(x)\left(s_i - \frac{(2-r)Cx + nR(r-1)}{nC}\right). \tag{21}$$

So, the total payoff function in the mining game becomes

$$J_i^{\tau}(x,[S_i,S_{\sim i}])=\int\limits_{t=0}^{\infty}e^{-rt}\left(Rs_i-\frac{Cs_i^2}{2}\right)-\tau(x)\left(s_i-\frac{(2-r)Cx+nR(r-1)}{nC}\right)dt. \tag{22}$$

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.* (22)*.*

Theorem 4. *The rate of linear tax enforcing the socially optimal behaviour of the miners is given by*

$$\tau(x)=\frac{(r-2)(n-1)(Cx-Rn)}{n^2} \tag{23}$$

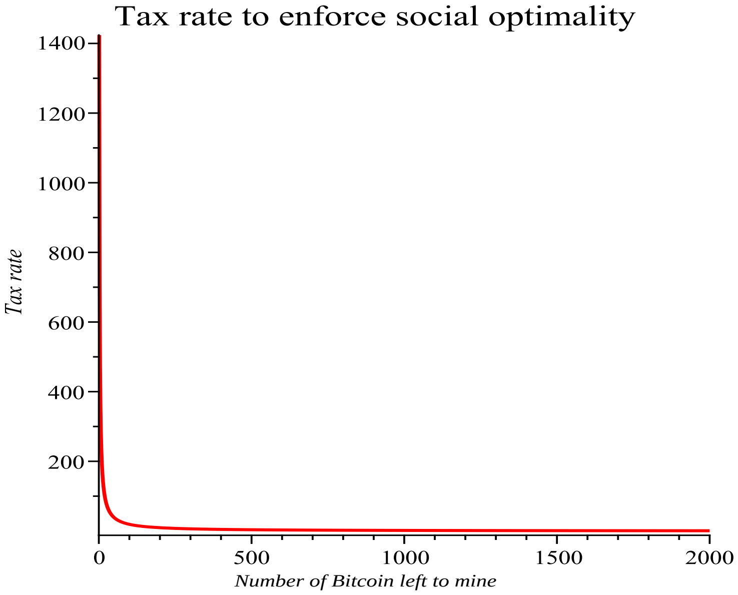

Fig. 2. Tax rate $\tau(x)$ enforcing the socially optimal profile for the values of the parameters are $n = 20$ and $r = 0.02$

Figure 2 presents the tax rate of the linear tax enforcing the socially optimal profile. We can see when fewer bitcoin which remain to be mined, larger tax rates are required.

Proof. Consider our mining game with enforcing the social optimum mining 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 mines s_i^{SO}, each of them obtains the total profit $\frac{V^{\mathrm{SO}}(x)}{n}$ and this is the optimal total profit for such an appropriate $\tau(x)$, if it exists. So, the HJB equation for $\frac{V^{\mathrm{SO}}(x)}{n}$ becomes

$$\frac{r}{n}V^{\mathrm{SO}}(x)=\sup_{s_i\in[0,Mx]}(Rs_i-\frac{Cs_i^2}{2})-\tau(x)(s_i-S^{\mathrm{SO}}(x))+(\xi x-s_i-\sum_{j\neq i}^{n}s_j)\frac{\partial V^{\mathrm{SO}}(x)}{n\cdot\partial x} \tag{24}$$

The first order condition for the above optimization problem is

$$\tilde{s}_i=\frac{(R-\tau(x))n^2+(2-r)(Cx-nR)}{n^2C} \tag{25}$$

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. (23). Substitute $\tilde{s}_i$ for this $\tau(x)$ into Eq. (24) to see that it is fulfilled.

5 Conclusion

Bitcoin is a non-renewable resource, so it is very important to mine bitcoin strategically in order to maintain the bitcoin market balance. 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 mining 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 to mine jointly in cooperation with other miners since it will give the miner a higher total profit compared to a miner who mines selfishly. Also, if all the miners choose to mine according to the Nash equilibrium mining strategy, then the bitcoin will deplete much faster than if they choose to mine according to the social optimum mining 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 mining 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 social welfare of the miners.

References

1. Aumann, R.J., Dreze, J.H.: Cooperative games with coalition structures. International Journal of game theory 3(4), 217–237 (1974)
2. Aziz, H., De Keijzer, B.: Complexity of coalition structure generation. In: The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 1. pp. 191–198. International Foundation for Autonomous Agents and Multiagent Systems (2011)
3. Babaioff, M., Dobzinski, S., Oren, S., Zohar, A.: On bitcoin and red balloons. In: Proceedings of the 13th ACM conference on electronic commerce. pp. 56–73. ACM (2012)
4. Bachrach, Y.: Honor among thieves: collusion in multi-unit auctions. In: Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1. pp. 617–624. International Foundation for Autonomous Agents and Multiagent Systems (2010)
5. Bachrach, Y., Kohli, P., Graepel, T.: Rip-off: playing the cooperative negotiation game. In: The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3. pp. 1179–1180. International Foundation for Autonomous Agents and Multiagent Systems (2011)
6. Bachrach, Y., Kohli, P., Kolmogorov, V., Zadimoghaddam, M.: Optimal coalition structure generation in cooperative graph games. In: AAAI (2013)
7. Bachrach, Y., Meir, R., Feldman, M., Tennenholtz, M.: Solving cooperative reliability games. arXiv preprint arXiv:1202.3700 (2012)
8. Bachrach, Y., Meir, R., Jung, K., Kohli, P.: Coalitional structure generation in skill games. In: AAAI. vol. 10, pp. 703–708 (2010)
9. Bachrach, Y., Porat, E., Rosenschein, J.S.: Sharing rewards in cooperative connectivity games. Journal of Artificial Intelligence Research 47, 281–311 (2013)
10. Bachrach, Y., Rosenschein, J.S.: Coalitional skill games. In: Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems-Volume 2. pp. 1023–1030. International Foundation for Autonomous Agents and Multiagent Systems (2008)
11. Bachrach, Y., Rosenschein, J.S.: Power in threshold network flow games. Autonomous Agents and Multi-Agent Systems 18(1), 106 (2009)
12. Bachrach, Y., Shah, N.: Reliability weighted voting games. In: International Symposium on Algorithmic Game Theory. pp. 38–49. Springer (2013)
13. Basar, T., Olsder, G.J.: Dynamic noncooperative game theory, vol. 23. Siam (1999)
14. Blocq, G., Bachrach, Y., Key, P.: The shared assignment game and applications to pricing in cloud computing. In: Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems. pp. 605–612. International Foundation for Autonomous Agents and Multiagent Systems (2014)
15. Elkind, E., Chalkiadakis, G., Jennings, N.R.: Coalition structures in weighted voting games. In: ECAI. vol. 8, pp. 393–397 (2008)
16. Elkind, E., Goldberg, L.A., Goldberg, P., Wooldridge, M.: Computational complexity of weighted threshold games. In: Proceedings of the national conference on artificial intelligence. vol. 22, p. 718. Menlo Park, CA; Cambridge, MA; London; AAAI Press; MIT Press; 1999 (2007)
17. Elkind, E., Goldberg, L.A., Goldberg, P.W., Wooldridge, M.: On the dimensionality of voting games. In: AAAI. pp. 69–74 (2008)

18. Eyal, I.: The miner's dilemma. In: 2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015. pp. 89–103. IEEE Computer Society (2015), https://doi.org/10.1109/SP.2015.13
19. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM 61(7), 95–102 (2018)
20. Haurie, A., Krawczyk, J.B., Zaccour, G.: Games and dynamic games, vol. 1. World Scientific Publishing Company (2012)
21. 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
22. Lewenberg, Y., Sompolinsky, Y., Zohar, A.: Inclusive block chain protocols. In: International Conference on Financial Cryptography and Data Security. pp. 528–547. Springer (2015)
23. Meir, R., Bachrach, Y., Rosenschein, J.S.: Minimal subsidies in expense sharing games. In: International Symposium on Algorithmic Game Theory. pp. 347–358. Springer (2010)
24. Meir, R., Zick, Y., Elkind, E., Rosenschein, J.S.: Bounding the cost of stability in games over interaction networks. In: AAAI. vol. 13, pp. 690–696 (2013)
25. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2009), http://www.bitcoin.org/bitcoin.pdf
26. 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
27. Raiffa, H.: The art and science of negotiation. Harvard University Press (1982)
28. Ray, D., Vohra, R.: A theory of endogenous coalition structures (1998)
29. Resnick, E., Bachrach, Y., Meir, R., Rosenschein, J.S.: The cost of stability in network flow games. In: International Symposium on Mathematical Foundations of Computer Science. pp. 636–650. Springer (2009)
30. Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: International Conference on Financial Cryptography and Data Security. pp. 6–24. Springer (2013)
31. Rosenfeld, M.: Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009 (2014)
32. Sandhlom, T.W., Lesser, V.R.: Coalitions among computationally bounded agents. Artificial intelligence 94(1-2), 99–137 (1997)
33. Sandholm, T., Larson, K., Andersson, M., Shehory, O., Tohmé, F.: Coalition structure generation with worst case guarantees. Artificial Intelligence 111(1-2), 209–238 (1999)
34. See, A., Bachrach, Y., Kohli, P.: The cost of principles: analyzing power in compatibility weighted voting games. In: Proceedings of the 2014 international conference on Autonomous agents and multi-agent systems. pp. 37–44. International Foundation for Autonomous Agents and Multiagent Systems (2014)
35. Shehory, O., Kraus, S.: Methods for task allocation via agent coalition formation. Artificial intelligence 101(1), 165–200 (1998)
36. Zabczyk, J.: Mathematical control theory: an introduction. Springer Science & Business Media (2009)
37. Zick, Y., Skopalik, A., Elkind, E.: The shapley value as a function of the quota in weighted voting games. In: IJCAI. vol. 11, pp. 490–495 (2011)
38. Zuckerman, M., Faliszewski, P., Bachrach, Y., Elkind, E.: Manipulating the quota in weighted voting games. In: AAAI. vol. 8, pp. 215–220 (2008)