Cluster Computing (2020) 23:2035–2046
https://doi.org/10.1007/s10586-020-03046-w

S.I. : BLOCKCHAIN FOR IOT

A game theoretic analysis of resource mining in blockchain

Rajani Singh[1] · Ashutosh Dhar Dwivedi[1,2] · Gautam Srivastava[3,4] · Agnieszka Wiszniewska-Matyszkiel[5] · Xiaochun Cheng[6]

Received: 27 July 2019 / Revised: 20 September 2019 / Accepted: 19 October 2019 / Published online: 24 January 2020

Abstract

Blockchain and cryptocurrency are a hot topic in today's digital world. In this paper, we create a game theoretic model in continuous time. We consider a dynamic game model of the bitcoin market, where miners or players use mining systems to mine bitcoin by investing electricity into the mining system. Although this work is motivated by BTC, the work presented can be applicable to other mining systems similar to BTC. We propose three concepts of dynamic game theoretic solutions to the model: *Social optimum*, *Nash equilibrium* and *myopic Nash equilibrium*. Using the model that a player represents a single "miner" or a "mining pool", we develop novel and interesting results for the cryptocurrency world.

Keywords Blockchain · Bitcoin mining · Dynamic game theory · Differential game · Hamilton–Jacobi–Bellman equation · Social optimum · Nash equilibrium · Myopic Nash equilibrium · Pigovian tax

1 Introduction

A bitcoin is created by miners, using complex mathematical "proof of work" procedures by computing hashes [8]. For each successful attempt, miners get rewards in terms of bitcoin and transaction fees. Miners participate in mining voluntarily in exchange for rewards as income. Electricity plays an essential role in the bitcoin mining process since created blocks and solving computationally hard problems uses large amounts of electricity. We can consider electricity as a semi-renewable resource—depending on the source of resources used for its production. The electricity consumed by the mining systems is directly proportional to the computational power of the system being used. The fact is that at each new block creation only one miner will be rewarded (the one who will win the mining game by first creating and updating the blockchain). 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 effecting bitcoin mining.

Bitcoin [19] was introduced in 2009. Its security is based on a concept known as `Proof of Work` (POA), and a transaction is only considered valid once the system obtains proof that a sufficient amount of computational work has been exerted by an actively mining node. The miners (responsible for creating blocks) constantly try to solve cryptographic puzzles in the form of hash computations. The process of adding a new block to the blockchain is called *mining* and these blocks contain a set of transactions that have been authenticated (confirmed). The average time to create a new block in the blockchain is 10 minutes. Two types of agents participate in the Bitcoin network: *miners*, who validate transactions and *clients*, who trade in BTC [4]. The blockchain is a shared data structure responsible for storing all transactional history to

✉ Agnieszka Wiszniewska-Matyszkiel
agnese@mimuw.edu.pl

Gautam Srivastava
SRIVASTAVAG@BrandonU.CA

[1] Department of Electrical and Computer Engineering, Faculty of Engineering, University of Waterloo, Waterloo, Canada

[2] DTU Compute, Technical University of Denmark, Kongens Lyngby, Denmark

[3] Department of Mathematics & Computer Science, Brandon University, Brandon R7A6A9, Canada

[4] Research Center for Interneural Computing, China Medical University, Taichung 40402, Taiwan, ROC

[5] Faculty of Mathematics, Informatics, and Mechanics, University of Warsaw, Warsaw, Poland

[6] Department of Computing Science, Middlesex University, London, UK

date. 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 given in Table 1.

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 one new block. The creator of the block is rewarded with BTC. In this work, we assume that miners are honest and follow the protocol as described thus far.

Electricity, one of the necessities of today's society, can be considered as renewable if it is generated from renewable resources. For example, solar energy, hydro-power, and windmill power are renewable versions of electricity. There are also non-renewable types if it is produced from thermal power plants that use coal—a non-renewable resource. So, depending on if renewable non-renewable resources, it is considered semi-renewable.

Exploitation of a shared resource is a significant problem [5]. Since electricity can be considered a semi-renewable resource, we have seen an unexpected growth of electricity (or computational power) consumption resulting from BTC mining [21, 22]. This has brought many miners to despair because the reward of mining a bitcoin decreases every 4 years by 50%. Therefore, miners need to mine BTC strategically to make BTC mining a long lasting activity that remains prosperous. However, there are still transaction fees that can keep the BTC market profitable for many years to come. In this paper, we use the tools of dynamic game theory to solve a novel dynamic game model. Our game model can be stated as follows: a miner's objective is to use more powerful (computationally) mining systems that consume more electricity, in order to maximize the net profit gain from producing or mining BTC. They can then sell the gained BTC to the prevailing market at the current market value.

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 BTC market price as profit so, they jointly maximize their profit and the profit is equally shared among them—and *non-cooperative*—each miner behaves selfishly and individually wants to maximize the profit gained from BTC mining.

Table 1 Structure of the blockchain [19]

Field	Size
Block header	80 bytes
Block size	4 bytes
Transaction counter	1 to 9 bytes
Transaction	Depends on the transaction size

Although this work is motivated by BTC, it is more heavily influenced by the future of Blockchain. The work and game theoretic model presented here can be applicable to other mining systems that utilize a similar mining system to BTC, therefore well versed in many different potential Blockchain applications [3, 16, 30]. Furthermore, the work presented here can be easily adapted to other mining schemes in the future making this a pivotal model and work on game theory and its relation to the mining process for Blockchain.

The rest of the paper is organized as follows. We survey some of the closest related works next in Sect. 2. We follow this with the formulation of our mode in Sect. 3. We then give our main results in Sect. 4 with solutions to the concepts presented in Section 3. We based our results with some discussion on how to enforce social optimality in Sect. 5. Finally, we conclude this paper with some remarks in Sect. 6.

2 Related work

Since the early days of BTC, blockchain technology and cryptocurrencies have caught the attention of both researchers and investors alike. The original paper on BTC was improved in [23], mostly focussing on security analysis. Showing an attack in which large pools can gain more than their fair share, Eyal et al. showed that BTC mining protocol is not incentive compatible [10], which was a significant work.

The linear quadratic differential game is the best-researched class of dynamic games (see Engwerda [9]). Dynamic games with linear quadratic structure and with linear state dependent constraints were studied by Singh and Wiszniewska-Matyszkiel in [26, 27] but in the discrete time horizon.

Zohar et al. [18] examined dynamics of pooled mining and the rewards that pools manage to collect. They 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 given incentives to switch between pools. The work of Niyato et al. [20] 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 considered the Blockchain Mining Game with incomplete information as a stochastic dynamic game in discrete time [15]. They considered two types of strategies. First they considered when miners release every mined block immediately and secondly when a block is mined and announced immediately but not released. The latter causes other miners to continue mining transactions that will soon be committed. Miners are always strategic in choosing which blocks to mine. As a result of their research, they found that the best response of a miners with low computational power matches the expected behaviour of BTC designers while for the miner with sizeable computational power, he/she deviates from the expected behaviour, and other Nash equilibria arise.

Salimitari discussed the mining profitability of a new miner or pool by calculating the expected value of profit [24]. In their model, they assume the cost of mining was linear to the price of electricity consumed in the mining process. Hayes studied the model to check the marginal cost of production and proposed to set the market value of the digital BTC currency [13]. They show that the marginal cost of production of BTC plays an essential role in explaining BTC prices.

Houy considered the BTC 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 [14]. Harvey et al. considered the model of miners' profitability from the mining cost analysis of the electrical energy invested in bitcoin mining production [11]. They also show that how the profit model changes as mining scales from the individual to the industrial level.

Laszka et al. consider a game-theoretic model that allows capturing short term as well as long-term impacts of attacks against mining pools [17]. Using this model, they studied 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.

Our model is not a one shot game model or static game model. It is a dynamic game meaning that players make a decision at each time instant that is based on amount of resource—electricity available at that time instant. To the best of author's knowledge, such dynamic games have never appeared before.

3 Formulation of the model

We consider a continuous time dynamic game model of exploitation of a semi-renewable resource—electricity. Since electricity is produced from renewable resource or partly from renewable and partly from non-renewable resource in constant proportion and for simplicity by "electricity", we mean the *stock of this resource*.

The game $\hat{\mathcal{G}}$ consists of the following parts:

GP1. The set of players: $\mathbb{I} = \{1, 2, \ldots, n\}$. Players can be either individual miners or mining pools.

GP2. The *state of resource* x is the stock of resource used for electric energy production which may be used for mining—proportional to the amount of available computational power and to the maximal available electricity consumption for mining. Since there is nothing like negative amounts of computational power and it is not zero, we assume that $x \in (0, +\infty)$ with the initial state $X(0) = x_0$ representing the initial amount of resource (we use notation X for trajectories, i.e., state as a function of time, and x for state, so we can write $X(t) = x$).

GP3. At each time instant t, miner i decides to consume s_i amount of electricity, which we call strategy of miner i. These s_i in common constitute a profile of strategies and is defined as $s = (s_1, \ldots, s_n)$. Denote a function by S_i and defined as $S_i(X(t)) = s_i$. Therefore, at time instant t, seeing that $X(t)$ amount of power is available, miner i will use strategy $S_i(X(t))$.

GP4. The set of decisions of each miner is $U_i = \mathbb{R}_+$, representing intensity of electricity use. However, there are state dependent constraints on decisions.

GP5. Given state x, the set of available decisions is $\mathcal{U}_i(x) = [0, Mx]$ (the closed interval), for some constant $M > 1$. 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 intensity of electricity consumption available to him/her, or a negative amount of electricity. We denote the set of decision profiles by $\mathcal{U}_i^n$.

GP6. We consider the economic scenario where a BTC miner i invests some amount of electricity to the mining system in order to solve a "Proof of Work" problem. As a result of successfully mining a block into the blockchain, he produces BTC. He/she sells BTC into the common-market for a fixed market price of BTC—in order to concentrate on problems related to energy consumption, we skip the exogenous randomness of BTC price. Mining, however, may end up with a failure. *Efficiency* (measured in expected value of the reward in dollars) in this process of a unit of energy consumption by a miner is a decreasing function of joint energy consumption by all miners. (This efficiency plays a role similar to *price* in economic models of oligopolies defined by the so called *inverse demand function*).

We consider a simple approximation.

$$Efficiency(s) = P - \sum_{j=1}^{n} s_j \tag{3.1}$$

for some positive constant P.

GP7. The *cost* of mining for miner i in dollars, is linearly proportional to the price of electricity consumed i.e. s_i.

$$Cost(s_i) = C \cdot s_i$$

for some positive C. We assume that the cost of mining is identical for each miner.

GP8. So, in this economic model, the *net profit* of each miner is given by the expected net revenue minus the mining cost. So, the *current* or *instantaneous payoff* or *profit* g_i of miner i is given by

$$\begin{aligned} g_i(x, s_i, s_{\sim i}) &= Efficiency(s) \cdot s_i - Cost(s_i) \\ &= \left(P - \sum_{j=1}^{n} s_j\right) s_i - Cs_i, \end{aligned} \tag{3.2}$$

where $s_{\sim i}$ is a way in which we denote the vector of consumptions of the other miners. Whenever we consider profiles in which decisions of the others are identical, by a slight abuse of notation, we write this single decision only, not the whole vector.

In economics generally, P is substantially higher than C.

GP9. A function $X : (0, +\infty) \to \mathbb{R}_+$ is called a trajectory of the state of the system and given by

$$\begin{aligned} &\dot{X}(t) = \psi(X(t), S(X(t))), \\ &\quad \text{with the initial condition } X(0) = x_0, \end{aligned} \tag{3.3}$$

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

$$\psi(x, s) = \xi x - \sum_{j=1}^{n} s_j, \tag{3.4}$$

where $0 < \xi < 1$ is called the regeneration rate of electricity, which is semi-renewable.

GP10. We are interested in calculating the *feedback strategies* $S_i : (0, +\infty) \to \mathbb{R}_+$ such that the constraint is fulfilled and Eq. (3.3) has a unique solution. It means that the intensity of electricity consumption that s/he decides to use at every time instant t depends on $X(t)$. The set of such strategies is denoted by $\mathbb{S}_i$.

GP11. The payoffs of miners in the game are discounted and the interest rate used for discounting is $r \in (0, 1)$. This is typical for economic problems. If we look at discrete time and yearly interest rate, then for 1 dollar at the bank account we will get $1 + r$ after a year. So, the present value of a dollar which we are going to obtain after a year is $\frac{1}{1+r}$, while the present value of a dollar which we are going to obtain after t years is $\frac{1}{(1+r)^t}$. If the bank pays the interest more and more often, then it uses a continuous time limit of this process e^{-rt} instead of $\frac{1}{(1+r)^t}$, and this works also for t that is an arbitrary real number. We assume that $\frac{\xi}{2} \leq r \leq \xi << (P - C)$.

GP12. The *total payoff* function or *total profit* of a miner given the initial state x_0, a strategy of player i S_i and strategies of the remaining players $S_{\sim i}$ is

$$\begin{aligned} &J_i(x_0, [S_i, S_{\sim i}]) \\ &\quad = \int_{t=0}^{\infty} e^{-rt} g_i(X(t), S_i(X(t)), S_{\sim i}(X(t)))dt, \end{aligned} \tag{3.5}$$

for $i = 1, 2, \ldots n$ and for X given by Eq. (3.3). The notation $[S_i, S_{\sim i}]$ is a convenient way of writing a strategy profile S emphasizing the special role of player i in it.

Analogously, we can define $J_i(\bar{x}, [S_i, S_{\sim i}])$ for arbitrary initial $\bar{x} \geq 0$. If it does lead to confusion, we will also use shorter form $J_i(\bar{x}, S)$.

4 Solution for BTC mining model

Here we discuss the solution types for our BTC mining game.

Social Optimum mining profile A social optimum mining profile is defined as a solution to our mining game where all miners cooperate. In other words, it is a profile where all miners jointly maximize their current payoffs or profits. A social optimum mining profile can be the result of decision making by a single miner, known 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 the n miner BTC mining game if and only if $\bar{S}$ maximizes $\sum_{i=1}^{n} J_i(x_0, S)$.

Nash equilibrium mining profile A Nash equilibrium mining profile is defined as a solution of our mining game where all miners behave selfishly and do not cooperate with each other. A mining profile $\bar{S}$ is a *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** if and only if for every miner $i \in \mathbb{I}$ and for every mining strategy S_i of miner i,

$$J_i(x,[S_i,\bar{S}_{\sim i}]) \le J_i(x,[\bar{S}_i,\bar{S}_{\sim i}]) \text{ for all } x. \tag{4.1}$$

We will also use another solution concept—a myopic Nash equilibrium—a profile of strategies in which each of the players maximizes his/her current payoff. Such profiles often appear in dynamic games with many players, in which players treat their influence of the state variable as negligible.

Definition 3 A mining profile $\bar{S}$ is called a **greedy** or **myopic Nash equilibrium** if and only if for every miner $i \in \mathbb{I}$ and for every x and every mining decision $s_i \in [0, Mx]$ of miner i,

$$g_i(x,s_i,\bar{S}_{\sim i}(x)) \le g_i(x,\bar{S}_i(x),\bar{S}_{\sim i}(x)) \text{ for all } x. \tag{4.2}$$

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

$$\sup_{S \in \mathbb{S}^n} J(x_0,S), \tag{4.3a}$$

$$\dot{X}(t) = \xi X(t) - \sum_{i=1}^{n} S_i(X(t)), \tag{4.3b}$$

$$X(0) = x_0. \tag{4.3c}$$

Theorem 1 *The optimal solution for cooperation of all miners is given by*

$$llS_i^{\mathrm{SO}}(x) := \begin{cases} 0 & 0 \le x < \hat{x}_0, \\ \dfrac{(2\xi - r)2\xi x + (P-C)(r-\xi)}{2n\xi} & \hat{x}_0 \le x < \hat{x}_1, \\ \dfrac{P-C}{2n} & x \ge \hat{x}_1. \end{cases} \tag{4.4}$$

for the constant $\hat{x}_0 = \frac{(P-C)(r-\xi)}{2\xi(r-2\xi)}$, $\hat{x}_1 = \frac{P-C}{2\xi}$.

We call this optimal solution "a social optimum profile".

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

$$V^{\mathrm{SO}}(x) := \begin{cases} \left(\dfrac{x}{\hat{x}_0}\right)^{\frac{r}{\xi}} \left(\dfrac{H\hat{x}_0^{\,2}}{2} + G\hat{x}_0 + K\right) & 0 \le x < \hat{x}_0, \\ \dfrac{Hx^2}{2} + Gx + K & \hat{x}_0 \le x < \hat{x}_1, \\ \dfrac{(P-C)^2}{4r} & x \ge \hat{x}_1. \end{cases} \tag{4.5}$$

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

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

$$V_i^{\mathrm{SO}}(x) := \frac{V^{\mathrm{SO}}(x)}{n}. \tag{4.6}$$

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

One of the methods to find the optimal control is by solving the *Bellman* or *Hamilton–Jacobi–Bellman* (*HJB*) equation—a partial differential equation which is central to optimal control theory (see Haurie, Krawczyk and Zaccour [12], Başar and Olsder [6], Zabczyk [32], Stokey Lucas [29]). The HJB equation is assumed to return the value function V as a function of state, with $V(x)$ being the maximal payoff if the system starts from x as the initial condition. In the infinite horizon problem with discounting with the rate r, the HJB equation is of the form $rV(x) = \max_s\{$ current payoff $(s) + \frac{\partial V(x)}{\partial x} \cdot$ state transition $(x,s)\}$ for each x, where s is the control parameter. If a regular solution V of the HJB equation exists, an optimal control can be found as the maximizer of the right hand side of the HJB equation with the actual value function V. In the infinite horizon, a sufficient condition for a *continuously differentiable* function V to be the value function and a feedback control s to be optimal is that V fulfils the HJB equation, s maximizes its right hand side and V fulfils the *terminal condition* $\limsup_{t\to\infty} V(X(t))e^{-rt} = 0$ for every admissible trajectory of the state. Since in our problem, the state is one dimensional, the HJB equation becomes an ordinary differential equation.

Proof The Hamilton–Jacobi–Bellman equation for any function $V(x)$ can be written as

$$rV(x) = \sup_{s_i \in [0,Mx]^n} \sum_{i=1}^{n} \left[\left(P - C - \sum_{j=1}^{n} s_j \right) s_i \right] + \left(\xi x - \sum_{j=1}^{n} s_j \right) \frac{\partial V(x)}{\partial x}. \tag{4.7}$$

To calculate the optimal strategy S_i, differentiate the right hand side of Eq. (4.7) with respect to s_i and equate to 0. We get the optimal value $\bar{s}_i$ as

$$2\bar{s}_i = P - C - \sum_{j=1, j \neq i}^{n} s_j - \frac{\partial V(x)}{\partial x}, \quad i = 1, 2 \ldots n. \tag{4.8}$$

Note that the right hand side of Eq. (4.8) with $\bar{s}_i$ subtracted from both sides is identical for all i. So, the optimal value $\bar{s}_i$ is the same for all n miners.

Since M is sufficiently large, the optimal value $\bar{s}_i$ is always less than or equal to Mx.

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

$$rV(x) = n(P - C - n\bar{s}_i)\bar{s}_i + \frac{\partial V(x)}{\partial x}(\xi x - n\bar{s}_i). \tag{4.9}$$

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

$$V(x) = K + Gx + \frac{Hx^2}{2}, \tag{4.10}$$

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. This yields two sets of values of the constants:

$$(i)\ H = 2(r - 2\xi), G = \frac{-(P-C)(r-2\xi)}{\xi}, \\ K = \frac{(P-C)^2(r-\xi)^2}{4r\xi^2}, \tag{4.11}$$

$$(ii)\ \hat{H} = 0,\ \hat{G} = 0,\ \hat{K} = \frac{(P-C)^2}{4r}, \tag{4.12}$$

Case 1 If the constants are as in (i), then the optimal solution is $\bar{s}_i = \frac{(2-r)Cx + nR(r-1)}{nC}$, only if $0 \leq \bar{s}_i < Mx$.

(a) For $0 \leq x < \hat{x}_0$, the zero-derivative $\bar{s}_i \leq 0$ so, for this interval of x, the optimal strategy will be $\bar{s}_i = 0$. Thus, player i will wait with the waiting time $\bar{t}(x)$, without any energy consumption for $X(t)$ to grow from x at 0 to $\hat{x}_0$ at $\bar{t}(x)$. The dynamics of the electricity becomes: $\frac{dX(t)}{dt} = \xi X(t); X(0) = x$. Solving the differential equation for X gives $X(t) = xe^{\xi t}$. So, $xe^{\xi t} = \hat{x}_0$. Solving this for $t = \bar{t}(x)$ we have the waiting time as $\bar{t}(x) = \frac{\ln(\hat{x}_0) - \ln(x)}{\xi}$. The value function for this interval of x is given by $e^{-r\bar{t}(x)}\left(\frac{H\hat{x}_0{}^2}{2} + G\hat{x}_0 + K\right)$, which simplifies to $\left(\frac{x}{\hat{x}_0}\right)^{\frac{r}{\xi}}\left(\frac{H\hat{x}_0{}^2}{2} + G\hat{x}_0 + K\right)$.

(b) For $\hat{x}_0 \leq x < \hat{x}_1$, the optimal decision is $\bar{s}_i = \frac{(2-r)Cx + nR(r-1)}{nC}$ and the value function is $\frac{Hx^2}{2} + Gx + K$.

Case 2 If the constants are as in (ii), then the optimal solution is $\bar{s}_i = \frac{P-C}{2n}$ only if $0 \leq \bar{s}_i < Mx$ and the value function is $\hat{K} = \frac{(P-C)^2}{4r}$.

The function V^{SO} defined by Eq. (4.6), composed from Case 1 and Case 2, is continuous and continuously differentiable, it fulfils the HJB equation and the profile S^{SO} defined by Eq. (4.4) maximizes the rhs. of the HJB equation with V^{SO}. The terminal condition is trivially fulfilled since V^{SO} is bounded.

Therefore, the social optimum strategy profile is given by Eq. (4.4) while the total profit of a miner is given by Eq. (4.6). □

4.2 Calculation of Nash equilibrium

Next, we illustrate the process of calculation of a Nash equilibrium strategy profile and we derive the unique greedy/myopic Nash equilibrium—solution of the non-cooperative game and the total profit of a selfish miner corresponding to it.

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

$$\sup_{S_i \in [0, Mx]} J_i(x_0, [S_i, S_{\sim i}]) \tag{4.13a}$$

$$\dot{X}(t) = \xi X(t) - S_i(X(t)) - \sum_{j=1, j \neq i}^{n} S_j(X(t)), \tag{4.13b}$$

$$X(0) = x_0. \tag{4.13c}$$

However, a feedback Nash equilibrium, besides solving n dynamic optimization problems, requires finding a fixed point of the resulting best response correspondence (in the space of feedback profiles). Presence of constraints on energy consumption dependent on x makes the problem so compound that it is not solvable in a way analogous to that used in the proof Theorem 1, i.e. using the undetermined coefficient method assuming quadratic value function for the model without constraints, then replacing the solution at points of violation of constraints pointwise by the violated constraint and proposing the total payoff for the resulting solution as the candidate for the value function and checking the sufficient condition.

Theorem 2

(a) The problem cannot be solved in a way analogous to the proof of Theorem 1.

(b) A profile defined by

$$S_i^{\mathrm{NE}}(x) = \begin{cases} Mx & x < \tilde{x}_0 \\ \dfrac{P-C}{n+1} & x \geq \tilde{x}_0. \end{cases} \tag{4.14}$$

for $\tilde{x}_0 = \frac{P-C}{M(n+1)}$ is a myopic Nash equilibrium strategy profile.

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

$$V_i^{\mathrm{NE}}(x) = \begin{cases} \dfrac{\bar{H}x^2}{2} + \bar{G}x + \bar{K} & x < \tilde{x}_0 \\ V_I(x) + e^{-r\tilde{t}(x)}\left(\dfrac{\bar{H}\tilde{x}_0^2}{2} + \bar{G}\tilde{x}_0 + \bar{K}\right) & \tilde{x}_0 \leq x < \tilde{x}_1 \\ \dfrac{(P-C)^2}{r(n+1)^2} & x \geq \tilde{x}_1. \end{cases} \tag{4.15}$$

for constants $\bar{H} = \frac{2M^2n}{2\xi - r - 2nM}$, $\bar{G} = \frac{M(P-C)}{r+nM-\xi}$, $\bar{K} = 0$. $\tilde{x}_1 = \frac{n(P-C)}{(n+1)\xi}$, $\tilde{t}(x) = \ln\left(\frac{(nM-\xi)(-P+C)}{((\xi x - P + C)n + \xi x)M}\right)\xi^{-1}$ and $V_I(x) = -(P-C)^2\left(\left(\frac{(nM-\xi)(-P+C)}{((\xi x - P + C)n + \xi x)M}\right)^{-\frac{r}{\xi}} - 1\right) r^{-1}(n+1)^{-2}$.

Proof (a) We start the proof similarly to the proof of Theorem 1, by an attempt to derive a preliminary candidate, we modify it to encompass constraints and check a sufficient condition.

Fix any i and consider the optimization problem of player i given strategies of the others $\bar{S}_j$ symmetric. The Hamilton–Jacobi–Bellman equation for any function $V_i(x)$ can be written as

$$rV_i(x) = \sup_{s_i \in [0, Mx]} \left(P - C - \sum_{j=1, j \neq i}^{n} \bar{S}_j(x) - s_i\right) s_i + \left(\xi x - s_i - \sum_{j=1, j \neq i}^{n} \bar{S}_j(x)\right) \frac{\partial V_i(x)}{\partial x}. \tag{4.16}$$

To calculate the optimal mining strategy s_i, differentiate the right hand side of Eq. (4.16) with respect to s_i and equate to 0. We get the zero-derivative point $\bar{s}_i$ as

$$2\bar{s}_i = P - C - \sum_{j=1, j \neq i}^{n} \bar{S}_j(x) - \frac{\partial V_i(x)}{\partial x}, \quad i = 1, 2 \ldots n. \tag{4.17}$$

Since the problem is symmetric and the current payoff strictly concave, we look for symmetric solutions i.e. such that $\bar{S}_j(x) = \bar{s}_i$, and, consequently, $V_i = V_j$.

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

$$rV_i(x) = (P - C - n\bar{s}_i)\bar{s}_i + \frac{\partial V_i(x)}{\partial x}(\xi x - n\bar{s}_i). \tag{4.18}$$

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

$$V_i(x) = K + Gx + \frac{Hx^2}{2}, \tag{4.19}$$

We substitute it to Eq. (4.18), and write equations for the coefficients. We get two sets of values of the constants: (i) $H = \frac{(n+1)^2(r-2\xi)}{2n^2}$, $G = \frac{-(n^2+1)(P-C)(r-2\xi)}{2n^2\xi}$ and $K = \frac{(rn^2+r-2\xi)(rn^2+r-2n^2\xi)(P-C)^2}{4\xi^2n^2(n+1)^2r}$ and (ii) $\bar{H} = 0$, $\bar{G} = 0$, $\bar{K} = \frac{(P-C)^2}{r(n+1)^2}$.

We substitute $S_i(x) = \bar{s}_i$ from Eq. (4.17) to each of them and we get that in case (i), $\bar{S}_i(x) > Mx$ for small x and for all $x \leq \tilde{x}_0$ the trajectory originating from such an x is strictly decreasing (so it eventually end in the region of x in which $\bar{S}_i(x) > Mx$), while for (ii), $\bar{S}_i(x) \leq Mx$ for $x \geq \tilde{x}_0$. So, as a natural candidate for the Nash equilibrium strategy, we take S_i^{NE}. We calculate $J_i(x, S^{\mathrm{NE}})$ and we get V_i^{NE} as follows.

(1) For $0 \leq x < \tilde{x}_0$, the candidate for Nash equilibrium strategy is Mx and if the initial condition is in this area, $X(t)$ remains in it. So, we get a quadratic function with the coefficients of x^2, x and constant $\bar{H} = \frac{2M^2n}{2\xi - r - 2nM}$, $\bar{G} = \frac{M(P-C)}{r+nM-\xi}$, $\bar{K} = 0$. Therefore, the candidate for the value function in this case is given by $\frac{2M^2n}{2(2\xi - r - 2Mn)}\frac{x^2}{2} + \frac{M(P-C)}{r+Mn-\xi}x$.

(2) If $x \geq \tilde{x}_1$, then not only $\frac{P-C}{n+1} \leq Mx$, but $\tilde{x}_1$ is a steady state of dynamics with strategies $\frac{P-C}{n+1}$, since $\xi x - \frac{n(P-C)}{n+1} = 0$ and each trajectory originating from this set is nondecreasing. So, if the initial condition is in this set, it remains in it. The payoff for $x \geq \tilde{x}_1$ and S^{NE} is given by $J_i(x, S^{\mathrm{NE}}) = \frac{(P-C)^2}{r(n+1)^2}$.

(3) For the initial condition $\tilde{x}_0 \leq x < \tilde{x}_1$, the trajectory X corresponding to $\frac{P-C}{n+1}$ decreases over time. So, after time $\tilde{t}(x)$ it will reach the set in which the strategy is Mx. It is given by $X(\tilde{t}(x)) = \tilde{x}_0$, with the dynamics of the electricity $\frac{dX(t)}{dt} = \xi X(t) - \frac{n(P-C)}{(n+1)}; X(0) = x$. Solving this differential equation and inverting gives $\tilde{t}(x) = \ln\left(\frac{(nM-\xi)(-P+C)}{((\xi x - P + C)n + \xi x)M}\right)\xi^{-1}$.

The payoff for x in this interval is given by $J_i(x, S^{\mathrm{NE}}) = e^{-r\tilde{t}(x)}\left(\frac{H\tilde{x}_0{}^2}{2} + G\tilde{x}_0 + K\right) + \int\limits_0^{\tilde{t}(x)} e^{-rt} g_i\left(x, \frac{P-C}{n+1}, \frac{P-C}{n+1}\right) dt.$

Although the Bellman equation is fulfilled in (1) and (2) and S_i^{NE} maximizes its right hand side in those sets, for $\tilde{x}_0 \le x < \tilde{x}_1$, S_i^{NE} does not maximize the right hand side of the Bellman equation with V_i^{NE}. Moreover, the function V_i^{NE} is not only non-differentiable at $\tilde{x}_1$, but its derivative tends to $+\infty$ as x tends to $\tilde{x}_1$ from below. So, standard tools do not work. The latest results for solving such irregular problems with infinite horizon by Baumeister et al. [7] cannot be applied either since our model does not fulfil the strong assumptions of [7].

b) It is easy to check that the profile S^{NE}, which was derived in the proof of a), maximizes $g_i(x, s_i, S^{\mathrm{NE}}_{\sim i})$. Therefore, a greedy Nash equilibrium strategy profile is given by Eq. (4.14), while the total profit of a miner at this profile is given by Eq. (4.15).

To show that S^{NE} is the unique greedy Nash equilibrium, we first look for the zero-derivative point of optimization of player i. We get the unique solution

$$2\bar{s}_i = P - C - \sum_{j=1, j \neq i}^{n} \bar{S}_j(x), \; i = 1, 2 \ldots n. \tag{4.20}$$

Subtracting $\bar{s}_i$ from both sides yields identical rhs for all i, so, all $\bar{s}_i$ are identical. The maximized function is strictly concave, so maxima are $\bar{s}_i = \frac{P-C}{n+1}$, if it does not exceed Mx, while otherwise all of them are Mx. □

Next, we graphically show the total profit and mining strategy for both: the social optimum and the unique greedy/myopic Nash equilibrium case. Figures 1 and 2 are drawn for the values of constants: $M = 2$, $P = 11511$, $C = 5.327$, $n = 10$, $\xi = 0.03$, $r = 0.02$.

Figure 1 shows the total profit earned by a miner in *USD* by consuming electricity strategically, depending on the optimal strategy profile (see Fig. 2): both in the cooperative or non-cooperative case. In Fig. 2, an interesting property of optimal strategy profile is that for $x \le \hat{x}_0$, miners refrain from mining in order to let the energy resource to regenerate. For the same x, at a myopic Nash equilibrium, miners use electricity with the maximal available intensity, leading to fast depletion of the resource.

5 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. Some work before on this topic can be seen in [1, 2]. We provide this system only as an example for future cryptocurrencies as this system would be difficult to implement at this stage in BTC.

If the miners consume more electricity than the social optimum or social welfare level, then they pay an extra amount to the external authority for the amount of electricity consumed in excess of the social welfare level as defined by the authority. This introduction of a tax system is essential in order to maintain the equilibrium in a cryptocurrency society and to make electricity sustainable. If we will not be able to control electricity consumption, then, besides contributing to the greenhouse effect, it may lead to a serious electricity crisis in the near future.

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

$$\text{Tax }(x, s_i) = \tau(x) s_i. \tag{5.1}$$

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

$$\left(P - C - \sum_{i=1}^{n} s_i\right) s_i - \text{ Tax }(x, s_i). \tag{5.2}$$

We are interested in Pigovian type tax where tax is linear in surplus over the socially optimal level. For those readers unfamiliar with Pigovian tax, we refer them to more background information in [25, 31]. To summarize here, if a given miner consumes more energy than the social optimum level he/she has to pay an extra amount as a penalty for overuse of energy in mining beyond the socially optimal level. We have seen related work shown in [28].

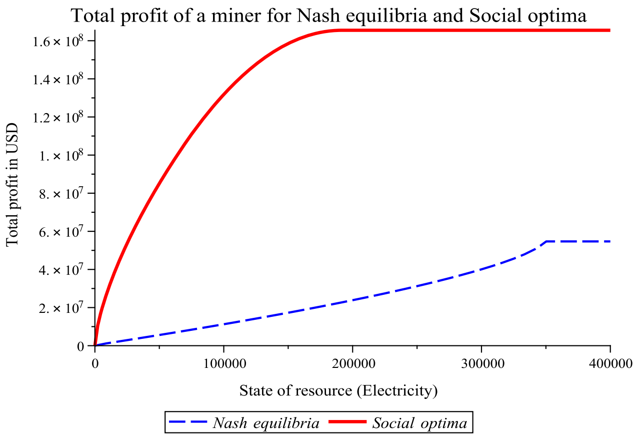

Fig. 1 Total profit of a miner at a greedy Nash equilibrium and the social optimum

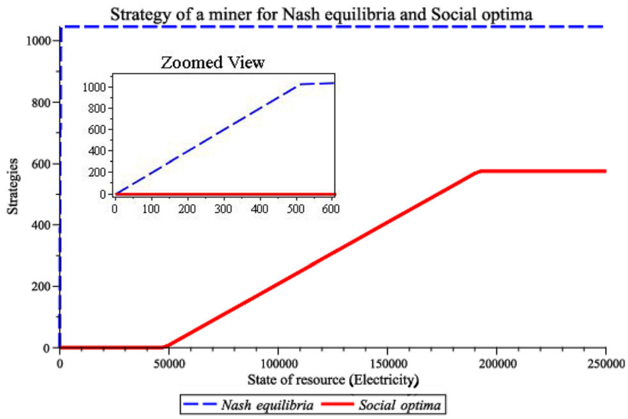

Fig. 2 Optimal strategy of a miner at a greedy Nash equilibrium and the social optimum

$$\text{Tax }(x, s_i) = \tau(x)\left(s_i - S_i^{\text{SO}}(x)\right)^+. \tag{5.3}$$

Therefore, the total payoff function in the mining game becomes

$$J_i^\tau(x, [S_i, S_{\sim i}]) = \int_{t=0}^{\infty} e^{-rt}\left(P - C - \sum_{j=1}^{n} S_j(X(t))\right) S_i(X(t)) - \tau(X(t))(S_i(X(t)) - S_i^{\text{SO}}(X(t)))^+ dt. \tag{5.4}$$

Definition 4 A tax-subsidy system *enforces* the mining profile $\bar{S}$ if $\bar{S}$ is a Nash equilibrium mining strategy in the new mining game with the total payoff defined by Eq. (5.4).

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

$$\tau(x) = \max\left\{\frac{2\xi x(r-2\xi) + (P-C)(3\xi - r)}{n^2}, \frac{(n-1)(P-C)}{2n}\right\}. \tag{5.5}$$

Figure 3 presents the tax rate of a linear tax enforcing strategy in the socially optimal profile. We can see that the less electricity resource is left, the 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 $V_i^{\text{SO}}(x)$ and this is the optimal total profit for such an appropriate $\tau(x)$, if it exists. So, the *HJB* equation for $V_i^{\text{SO}}(x)$ (given the others players play S_j^{SO}) becomes

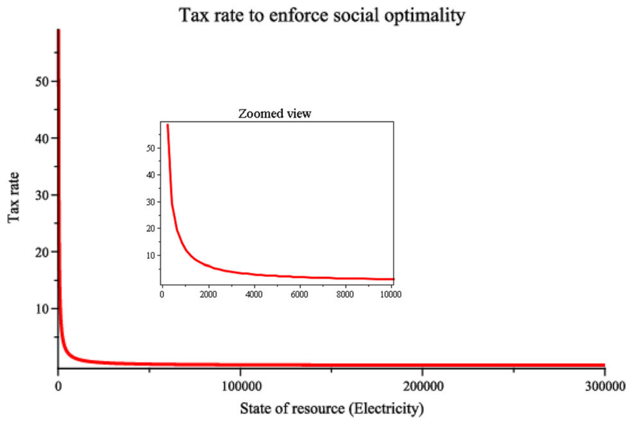

Fig. 3 Tax rate $\tau(x)$ enforcing the socially optimal profile for the values of constants: $M = 2$, $P = 11511$, $C = 5.327$, $n = 10$, $\xi = 0.03$, $r = 0.02$

$$rV_i^{\text{SO}}(x) = \sup_{s_i \in [0, Mx]} \left(P - C - s_i - \sum_{j=1, j\neq i}^{n} S_j^{\text{SO}}(x)\right) s_i - \tau(x)\left(s_i - S_i^{\text{SO}}(x)\right)^+ + \left(\xi x - s_i - \sum_{j=1, j\neq i}^{n} S_j^{\text{SO}}\right)\frac{\partial V_i^{\text{SO}}(x)}{\partial x}. \tag{5.6}$$

We start from $x < \hat{x}_0$ and we are going to find a tax rate for which another function, $\left(P - C - s_i - \sum_{j=1,j\neq i}^{n} S_j^{\text{SO}}(x)\right) s_i - \tau(x)\left(s_i - S_i^{\text{SO}}(x)\right)^+ + \left(\xi x - s_i - \sum_{j=1,j\neq i}^{n} S_j^{\text{SO}}\right) \frac{\partial V_i^{\text{SO}}(x)}{\partial x}$, is maximized. So, the first order condition for the above optimization problem is

$$\tilde{s}_i = \frac{4\xi^2 x + ((n-2)(P-C) - 2rx - n\tau)\xi + r(P-C)}{\xi n(n+1)}. \tag{5.7}$$

We want the optimal solution to be attained at $\max\{0, \tilde{s}_i\} = S_i^{\text{SO}}$. This holds for $\tau(x) = \frac{2\xi x(r-2\xi)+(P-C)(3\xi-r)}{n^2}$ substitute $\tilde{s}_i$ for this $\tau(x)$ into Eq. (5.6) to see that it is fulfilled.

For $x > \hat{x}_0$, the analogous solution is $\frac{(n-1)(P-C)}{2n}$ and Eq. (5.6) is also fulfilled.

Since the tax rate is multiplied by the nonnegative part of $s_i - S_i^{\text{SO}}$, increasing the tax rate does not spoil the property of enforcing. So, to get a solution that works in all cases, we take maximum of those two. Eq. (5.6) is then fulfilled for all x. □

6 Conclusions

We view electricity as a semi-renewable resource, so it is essential to use it strategically in order to maintain the sustainability of the resource. In this paper, we consider a continuous time dynamic game model of BTC mining in Blockchain with infinite time horizon, which belongs to the class of differential games. Although motivated by BTC, work here is applicable in other resource mining based Blockchain technologies currently and in the future. We propose two types of solutions to our model, namely Cooperative (Social Optimum) mining strategy, and Non-Cooperative (Nash equilibrium and myopic Nash equilibrium) mining strategy. We calculate the total profit of a miner in both cases. We have found that it is always beneficial for the miners to consume or to use electricity jointly, in cooperation with the others. Cooperation gives the miner a higher total profit compared to a situation when all miners mine selfishly. Moreover, if all miners choose to mine according to a greedy Nash equilibrium mining strategy, then the electricity resource will be depleted, while it is sustainable if they choose to mine according to the social optimum strategy. Our result fits 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 the Pigovian tax category, linear in overuse of electricity by the miner, in order to enforce social optimality in our BTC dynamic game model. This way, miners will be forced to behave and to mine in a way that is best for the social welfare of the miners and guarantees sustainability of the resource.

Acknowledgements First and second authors were funded by University of Waterloo, Canada. The research of fourth author was financed by grant 2016/21/B/HS4/00695 of National Science Centre, Poland.

References

1. Ainsworth, R.T., Alwohaibi, M.: Blockchain, bitcoin, and VAT in the GCC: the missing trader example. Boston University School of Law, Law and Economics Research Paper (17-05) (2017)
2. Ainsworth, R.T., Alwohaibi, M.: The first real-time blockchain VAT-GCC solves MTIC fraud. Boston University School of Law, Law and Economics Research Paper (17-23) (2017)
3. Al Ridhawi, I., Aloqaily, M., Kotb, Y., Jararweh, Y., Baker, T.: A profitable and energy-efficient cooperative fog solution for IOT services. IEEE Trans. Ind. Inform. 1–12 (2019). https://doi.org/10.1109/TII.2019.2922699
4. Aloqaily, M., Kantarci, B., Mouftah, H.T.: Multiagent/multiobjective interaction game system for service provisioning in vehicular cloud. IEEE Access **4**, 3153–3168 (2016)
5. Aloqaily, M., Kantarci, B., Mouftah, H.T.: Fairness-aware game theoretic approach for service management in vehicular clouds. In: 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), pp. 1–5. IEEE (2017)
6. Basar, T., Olsder, G.J.: Dynamic Noncooperative Game Theory, vol. 23. SIAM, Philadelphia (1999)
7. Baumeister, J., Leitao, A., Silva, G.N.: On the value function for nonautonomous optimal control problems with infinite horizon. Syst. Control Lett. **56**(3), 188–196 (2007)
8. Butt, T.A., Iqbal, R., Salah, K., Aloqaily, M., Jararweh, Y.: Privacy management in social internet of vehicles: review, challenges and blockchain based solutions. IEEE Access **7**, 79694–79713 (2019)
9. Engwerda, J.: LQ Dynamic Optimization and Differential Games. Wiley, New York (2005)
10. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. Commun. ACM **61**(7), 95–102 (2018)
11. Harvey-Buschel, J., Kisagun, C.: Bitcoin mining decentralization via cost analysis (2016). CoRR arXiv:abs/1603.05240
12. Haurie, A., Krawczyk, J.B., Zaccour, G.: Games and Dynamic Games, vol. 1. World Scientific Publishing Company, Singapore (2012)
13. Hayes, A.S.: Bitcoin price and its marginal cost of production: support for a fundamental value. Appl. Econ. Lett. 1–7 (2018)
14. Houy, N.: The bitcoin mining game. Ledger **1**, 53–68 (2016)
15. 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, pp. 365–382 (2016). https://doi.org/10.1145/2940716.2940773
16. Kotb, Y., Al Ridhawi, I., Aloqaily, M., Baker, T., Jararweh, Y., Tawfik, H.: Cloud-based multi-agent cooperation for iot devices using workflow-nets. J. Grid Comput. 1–26 (2019)
17. 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
18. 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
19. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2009). http://www.bitcoin.org/bitcoin.pdf
20. 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 (2011). https://doi.org/10.1109/CCGrid.2011.30

21. O'Dwyer, K.J., Malone, D.: Bitcoin mining and its energy footprint (2014)
22. Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., Kumar, R.: A blockchain framework for securing connected and autonomous vehicles. Sensors **19**(14), 3165 (2019)
23. Rosenfeld, M.: Analysis of hashrate-based double spending (2014). arXiv:1402.2009
24. 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
25. Sandmo, A.: Optimal taxation: an introduction to the literature. J. Public Econom. **6**(1–2), 37–54 (1976)
26. Singh, R., Wiszniewska-Matyszkiel, A.: Discontinuous Nash equilibria in a two stage linear-quadratic dynamic game with linear constraints. IEEE Trans. Autom. Control **0**, 1–10 (2018)
27. Singh, R., Wiszniewska-Matyszkiel, A.: Linear quadratic game of exploitation of common renewable resources with inherent constraints. Topol. Methods Nonlinear Anal. **51**, 23–54 (2018). https://doi.org/10.12775/TMNA.2017.057
28. Somdip, D.: A proof of work: Securing majority-attack in blockchain using machine learning and algorithmic game theory. Ph.D. thesis, Modern Education and Computer Science Press (2018)
29. Stokey, N.L., Lucas, R., Prescott, E.: Recursive Methods in Economic Dynamics. Harvard University Press, Cambridge (1989)
30. Volety, T., Saini, S., McGhin, T., Liu, C.Z., Choo, K.R.: Cracking bitcoin wallets: I want what you have in the wallets. Future Gener. Comput. Syst. **91**, 136–143 (2019). https://doi.org/10.1016/j.future.2018.08.029
31. Wilson, J.D.: A theory of interregional tax competition. J. Urban Econom. **19**(3), 296–315 (1986)
32. Zabczyk, J.: Mathematical Control Theory: An Introduction. Springer, New York (2009)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Rajani Singh is a Postdoctoral Researcher at the Department of Digitalization at the Copenhagen Business School (CBS). She received her B.Sc. degree in mathematics and computer application from the University of Allahabad, India, in 2011 and M.Sc. degree in mathematics from Indian Institute of Technology Delhi, New Delhi, India in 2013. She has completed her Ph.D. in 2019, with the Institute of Applied Mathematics and Mechanics, University of Warsaw, Poland. She has also worked as a full time Visiting Researcher at the University of Waterloo, Ontario, Canada, Research Associate at the Brandon University, Manitoba, Canada and Visiting Research Scholar at the Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland.she has worked as a researcher in Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada. Her research interests include game theory, blockchain technology, dynamic games and their applications to environment, economics and resource extraction, differential games and optimal control problems.

Ashutosh Dhar Dwivedi is a postdoctoral researcher at the DTU Compute, Cyber Security Section, Technical University of Denmark, Denmark, where he focuses on Post Quantum Cryptography. He is having a rich experience of industry and academia of around 7 years. He was with organizations related to software development projects for 2 years in India. In 2015, he moved to Poland and started his PhD in cryptography research at Polish Academy of Sciences. He worked as a Research Associate with the Department of Mathematics and Computer Science, Brandon University, Brandon, Canada, and Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada where he was working on blockchain technology. His primary research interests include symmetric-key cryptography, cryptanalysis of block ciphers, lightweight cryptography, post quantum cryptography and blockchains. From 2018, he has also been serving as a reviewer for many international journals and conferences: IEEE Internet of Things Journal, Energy System, Springer and Mathematics and International Journal of Distributed Sensor Networks, IEEE Access etc. He also worked as a program committee in a few conferences and workshops. Heidelberg Laureate Forum, Germany has selected him among top 100 young researchers all over the world in Computer Science to participate in the HLF-2019 event.

Gautam Srivastava was obtained his B.Sc. degree from Briar Cliff University in U.S.A. in the year 2004, followed by his M.Sc. and Ph.D. degrees from the University of Victoria in Victoria, British Columbia, Canada in the years 2006 and 2011, respectively. He then taught for 3 years at the University of Victoria in the Department of Computer Science, where he was regarded as one of the top undergraduate professors in the Computer Science Course Instruction at the University. From there in the year 2014, he joined a tenure-track position at Brandon University where he currently is active in various professional and scholarly activities. He was promoted to the rank Associate Professor in January 2018. Dr. G, as he is popularly known, is active in research in the field of Deep Learning, Computer Security, Internet of Things and Big Data. In his 8-year academic career, he has published a total of 53 papers in high-impact conferences in many countries and in high-status journals (SCI, SCIE), and has trained 15 HQP to date primarily Brandon University undergraduates. He has also delivered invited guest lectures on Big Data, Cloud Computing, Internet of Things, and Cryptography at many universities worldwide. He has adjunct status at both Lakehead University and China Medical University in Taiwan where he is appointed in the Research Centre for Interneural Computing. He is an Editor of several international scientific research journals including IEEE Access. As of Summer 2019, he is an IEEE Senior Member, the highest grade given to IEEE Members. He was recently awarded a CIRA Research Grant to Cyber Security education platforms for First Nations communities in Manitoba.

Agnieszka Wiszniewska-Matyszkiel was born in Pruszkow, Poland in 1971. He received the M.Sc. degree in mathematics in 1995, the M.Sc. degree in economics in 1997 and the Ph.D. degree in mathematics in 1999 from the University of Warsaw, Poland, and habilitation in Economics in 2013 in Warsaw School of Economics, Poland. Since 1999 she has been working at the Faculty of Mathematics, University of Warsaw, currently as an assistant professor. Her research interests include game theory, optimization and mathematical economics, especially dynamic optimization, dynamic games, games with many players, applications in environmental economics and modelling of markets. She has published more than thirty papers, she has organized international scientific conferences, she have had invited talks in five conferences.

Xiaochun Cheng received the Bachelor degree in Computer Engineering in 1992 and a Ph.D. in Computer Science in 1996 from Jilin University. He has been Computer Science EU Project Coordinator at Middlesex University in London since 2012, a guest professor at Jilin University, Beijing Normal University, ortheast Normal University. He has been a senior member of IEEE since 2004. He is a member of IEEE SMC Technical Committee on Enterprise Information Systems, IEEE SMC Technical Committee on Computational Intelligence, IEEE SMC Technical Committee on Cognitive Computing, IEEE SMC Technical Committee on Intelligent Internet Systems, IEEE Communications Society Communications and Information Security Technical Committee, BCS Information Security Specialist Group, BCS Cybercrime Forensics Specialist Group, and BCS Artificial Intelligence Specialist Group.