Mean Field Game for Equilibrium Analysis of Mining Computational Power in Blockchains

Amirheckmat Taghizadeh, Hamed Kebriaei, *Senior Member, IEEE*, and Dusit Niyato, *Fellow, IEEE*

***Abstract*—In a blockchain network, to mine new blocks like in cryptocurrencies or secure IoT networks, each node or player specifies the amount of computational power as its strategy by compromising between the cost and expected utility. Since the strategies of all players affect the expected utility of others through the probability of success, in this article, we first formulate the mining competition among the players in a blockchain network as a noncooperative game. The existence and uniqueness of the Nash equilibrium (NE) point of the game are proven. We consider a gradient learning strategy for the players while preserving their private information as a bounded rational learning model. Furthermore, the convergence of this learning strategy to the ϵ-NE point of the game is studied analytically using the concept of the mean field (MF) game theory. While conventional analytical tools face problems in dealing with a large number of participants, which is a key feature in many IoT networks, deploying the MF game theory facilitates analyzing the behavior of a large population of players by encapsulating the network behavior in an MF term. As the number of players becomes larger, the accuracy of the MF method becomes greater. Moreover, in the MF approach, no information exchange among the agents is needed for optimal decision making and the privacy of the players is preserved. The minimal information exchange is also a proper motivation for using the MF approach in the IoT networks.**

***Index Terms*—ϵ-Nash equilibrium, blockchain, computational game theory, convergence analysis, mean field game, proof of work.**

I. Introduction

In RECENT years, blockchain technologies have gained much attention due to their promising features as a secure distributed data-keeping platform. As a main application, cryptocurrencies, such as Bitcoin, have been implemented using blockchain as a distributed ledgers [1]. Nevertheless, the blockchain technology can be used for other applications [2], such as Internet of Things [3]–[5], edge and cloud computing [6]–[8], smart power grids [9], content delivery networks [10], and crowdsourcing [11]. Blockchain is especially of interest in IoT networks since it can create a secure robust network, where services are distributed among different nodes and the network [12]. The data in blockchain are stored in blocks that are chained together through Hash pointers to form a tamper proof and temporally ordered data structure. Participants in the blockchain network check the validity of transactions registered in each block. In order to motivate participants to take part, the network protocol provides incentives to those who successfully generate a new block. The process of creating new blocks on the blockchain is called mining. The most prevalent form of mining is through Proof of Work (PoW), which involves solving a mathematically complex problem, generally, a hash puzzle [13]. Alternative proof concepts have been introduced as well, such as Proof of Stake (PoS) [14], [15]. In PoS schemes, each player commits a certain asset as stake (usually the network tokens), and the probability of winning the mining game is proportional to the amount of assets committed as stake. Since PoW is more widely used and has been utilized in many research and commercial services, including in the IoT systems, the focus of this article is on PoW networks. For example, [7], [16], and [17], all use PoW as the basis of their IoT blockchain network. As for the commercial system, IOTA, which is the backbone of many commercial IoT blockchain services, uses PoW as well.

Due to the exponential growth of computational power of network participants, an individual miner with limited hash power compared to the whole network hash power has a negligible chance of winning the mining game in each iteration. In order to achieve more stable income, i.e., lower variance, in real-world blockchain networks, individual miners usually form mining pools [1]. A mining pool is a coalition of individual miners who act as a single miner in which, aggregating their computational power increases the chance of winning in each round. The acquired profit from a mined block is then distributed among the miners of pool. Joining a mining pool could greatly lower the variance of profit, although it has a small effect on a player's expected payoff. Pool management

Manuscript received October 29, 2019; revised February 14, 2020 and March 19, 2020; accepted April 7, 2020. Date of publication April 16, 2020; date of current version August 12, 2020. This work was supported in part by the Institute for Research in Fundamental Sciences under Grant CS 1398-4-256, in part by the National Research Foundation (NRF), Singapore, through Singapore Energy Market Authority, Energy Resilience under Grant NRF2017EWT-EP003-041, in part by Singapore NRF under Grant NRF2015-NRF-ISF001-2277, in part by the Singapore NRF National Satellite of Excellence, Design Science and Technology for Secure Critical Infrastructure under Grant NSoE DeST-SCI2019-0007, in part by the A*STAR-NTU-SUTD Joint Research Grant Call on Artificial Intelligence for the Future of Manufacturing under Grant RGANS1906 and Grant WASP/NTU M4082187 (4080), in part by Singapore MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15, and in part by Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17. *(Corresponding author: Hamed Kebriaei.)*

Amirheckmat Taghizadeh is with the School of ECE, College of Engineering, University of Tehran, Tehran 1439957131, Iran (e-mail: taghizadeh.amirheckmat@gmail.com).

Hamed Kebriaei is with the School of ECE, College of Engineering, University of Tehran, Tehran 1439957131, Iran, and also with the School of Computer Science, Institute for Research in Fundamental Sciences, Tehran 19395-5746, Iran (e-mail: kebriaei@ut.ac.ir).

Dusit Niyato is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore (e-mail: dniyato@ntu.edu.sg).

Digital Object Identifier 10.1109/JIOT.2020.2988304

usually takes a small percentage of the pool's profit as management costs. Hence, although joining a mining pool may slightly reduce the expected profit of a miner since it reduces the profit risk, miners are willing to forgo a small portion of their income to have more persistent income. For example, more than 80% of bitcoin network power are focused on different mining pools [18]. Since each node in the IoT network has limited storage and computational power, forming mining pools to cooperate in solving the network puzzle is reasonable.

In this article, the competition of players in mining pools in a blockchain network is modeled as a game in which, the mining computational power is the strategy of each pool that needs to be determined. The payoff function of each pool is considered to be the difference between the expected utility gained from mining and the computational cost. The existence and uniqueness of the Nash equilibrium (NE) point of the game are proven. Furthermore, we analyze the learning behavior of pools under incomplete information, and bounded rational decision making of the players is studied using the gradient learning method and the concept of the mean field (MF) game theory. In addition, the convergence of learning strategies to the ϵ-NE point of the game is investigated. The proposed MF approach can be used in lightweighted and bandwidth-limited blockchain networks, e.g., mobile and IoT-based blockchain networks, where limited bandwidth impedes full information exchange and only limited information about the network is available to the agents [7], [19], [20]. Also, the use of the gradient-based decision mechanism ensures that low-cost computations for decision making is achieved.

The main contributions of this article are as follows.

1) We exploit the MF theory for equilibrium analysis of the mining game in a blockchain network.
2) We provide the conditions for the existence and uniqueness of the NE point of the game.
3) We analyze both the rational and bounded rational decision-making dynamics by using the MF game.
4) We prove the convergence of the learning strategies of players to the ϵ-NE point of the game.

The remainder of this article is structured as follows. In Section II, the related works in the literature are reviewed. In Section III, the mining game is introduced and formulated. In Section IV, the NE of the game is represented and its existence and uniqueness are proved. Section V discusses the MF game and gradient-based decision dynamics. The update algorithm is represented and its convergence is proved. Moreover, the concept of MF ϵ-NE and its relationship with the exact NE point is also introduced. Section VI includes computational simulations to show the convergence of different algorithms under different conditions. Section VII concludes this article.

II. Related Works

Different tools and approaches have been used for analyzing blockchain networks, including performance analysis [19], [21]–[25], security analysis [26]–[28], or even economical analysis [29]. Taking into account the competitive/cooperative behavior of mining individuals/pools, the game theory is a well-suited tool for analyzing the blockchain network. In [30], an extensive literature on the game theoretical analysis of blockchain is provided.

Game theory has been also used to analyze mining strategies and behavior of players in the blockchain network. In the existing works, the strategy of players consists of whether they release or withhold their mining block, which is called selfish mining, and also which block to mine on [31], [32]. In addition, "computational power allocation" was studied in [33] and [34]. In [33], a complete information game was considered and the NE point is achieved only for two-player games. In [34], the strategy of players is considered to be the time in which they turn on each of their mining rigs. However, because of the complexity of the model, theoretical analysis was not provided and only the sensitivity of model parameters is shown by simulations. Mining pool coalition formation was studied in [35]. Liu *et al.* [35] analyzed the dynamics of pool formation using the evolutionary game theory. In their work, it is assumed that each mining pool requires its participants to provide a minimum computational power. Different equilibrium points for the case of two mining pools were calculated and the evolutionary stability of those equilibrium points was studied. In this article, the authors assumed that all miners in a mining pool participate with the same computational power, which is dictated by the pool management.

However, when the number of players becomes larger and they do not have information exchange due to their selfishness and privacy, classical game theoretical models cannot be effective due to lack of information or computational complexities. To face such problems, the MF game has been developed as a promising tool [36]. The MF game theory uses the same principle as the MF theory in physics [36]. The idea is that, when the number of agents is high, in many cases, the effect of all agents could be encapsulated in a term which is called the MF term. Each agent only needs to know the value of "MF term" while making decisions, which is the mass effect of players' strategies on its payoff function, rather than an individual strategy of rivals [37]. In this way, information exchange among the players is avoided and the privacy of the players is preserved. The reason is that the information of the MF term is usually publicly available or measurable for all players. In other words, the MF term is macroscopic information about the system [36]. This feature makes the MF game an appropriate tool to analyze the games of incomplete information with no information exchange among the players. MF game can be seen as an approximation of the original game. The accuracy of this approximation increases by increasing the number of players since the effect of decision making of a single player on the whole population becomes negligible.

The MF game approach has been utilized in many practical applications, such as smart grids and electric vehicles [38]–[40], or wireless networks [41]–[43]. However, to the best of our knowledge, it has not been applied to analyze the behavior of players in blockchain networks.

III. System Model and Problem Formulation

In this article, we consider a blockchain network using the PoW protocol. In the PoW concept, in order for a player to mine a new block and receive the monetary incentives provided by the network protocol, she should successfully guess a correct "nonce" so that the hash of the block would be less than a target value defined by the network. The hash puzzle difficulty, which is controlled by the difficulty parameter of the network, is maintained in such a way that the expected time of mining blocks would be fixed. Since hash functions that are used as the PoW problem show random-like properties, players have no option but to randomly try different nonce values to reach the aforementioned condition. Due to the random property of the hash function, the chance of winning the mining game for a player in each round is equal to the ratio of its computational power to the whole network computational power [32], [44]

$$P_i^{\text{win}} = \frac{x_i}{\sum_{j\in\mathcal{N}} x_j} \tag{1}$$

where $\mathcal{N} = \{1, 2, \ldots, N\}$ is the set of all players, P_i^{win} is the probability of winning for a player i, and x_i is the player i's computational power, in terms of hash rate. We assume $x_i \in X_i$, where $X_i = [x_i^{\min}, x_i^{\max}]$, and $0 \le x_i^{\min} \le x_i^{\max} < \infty$.

Equation (1) shows the winning probability of an individual miner. The expected portion that a miner inside a mining pool receives from each block could be represented in the same way. This is due to the fact that miners who are part of a mining pool receive a share of the reward from the pool-mined blocks proportional to the ratio of their computational power to the pool's computational power. Distribution schemes in mining pools often consist of a flat rate for the pool manager and the rest is distributed proportionally to the computational power of miners in the pool. Therefore, the expected utility of the player i can be modeled as follows:

$$A_i \frac{x_i}{\sum_{k\in\mathcal{N}_i} x_k} \times \frac{\sum_{k\in\mathcal{N}_i} x_k}{\sum_{j\in\mathcal{N}} x_j} \tag{2}$$

where $\mathcal{N}_i$ is the set of players in the same pool as the player i. Since an individual miner could be seen as a pool with only one miner, we assume players as mining pools. A_i represents the expected reward from a successfully mined block for the player i, which incorporates the pool management share reduction and distribution scheme, which is known to all pool members, as well as other influencing factors. Also, different participants in the network may value the network tokens differently. This can be due to different levels of the changeability of network tokens in different countries, or different privacy and anonymity preferences among participants. Also, different participants face different network propagation delays and use different styles of filling the blocks. All of these factors are encapsulated in A_i.

By taking into account the cost of computational power, the payoff function of the player i can be expressed as follows:

$$J_i(x) = \begin{cases} A_i \frac{x_i}{\sum_{j\in\mathcal{N}} x_j} - p_i x_i, & \sum_{j\in\mathcal{N}} x_j > 0 \\ 0, & \sum_{j\in\mathcal{N}} x_j = 0 \end{cases} \tag{3}$$

where $x = (x_1, \ldots, x_N)$ and p_i is the unit price of computational power (usually electricity consumption price and other maintaining fees) for the player i. As seen in (3), a player's payoff is dependent to all other players' computational power. Therefore, the competition of players could be formalized as the following "Mining Game" by introducing the set of players, strategies, and payoff functions, respectively

$$\mathcal{G} = \left(\mathcal{N}, \{X_i\}_{i\in\mathcal{N}}, \{J_i\}_{i\in\mathcal{N}}\right). \tag{4}$$

From (3), the coupling term among the players' payoff function is the aggregative term $\sum_{j\in\mathcal{N}} x_j$, which is the total computational power (hash rate) of the network. Although it is not reasonable to assume that a player has information of all other players' hash powers, a player can estimate the aggregative term by knowing the expected number of required hash function calculations (which is determined by difficulty parameter of the network) [44]–[46]. To be more specific, we consider that players use a naive estimation from the expected total hash rate. This type of estimation is known also as "myopic" estimation in the literature and is well suited to model the human behavior [47], [48]. In this way, the expected value of the overall hash power in the next round is approximated by the expected current hash power. The expected current hash power of the network could be approximated by knowing the network's difficulty, based on the expected number of hash completions required to mine a block, and the actual time taken for the last block to be mined. Dividing these two can provide an appropriate estimate of the expected value of the current network hash power. In the theory of the MF game, the estimation of the agents from the aggregative term is known as the MF term. The main feature of the MF game is that by knowing the MF term, each player can decide on its strategy based on (3), independent to other players. The player updates its strategy depending also on different humanoid factors, including the level of adaptation, computational capability, and the level of foresightedness. After each decision making, the strategy of players is fed into the network and based on the network's parameters, the MF term is updated for the next round. Hence, in an iterative procedure, each player updates its estimate and decision until the convergence is achieved. Fig. 1 shows this procedure. In the subsequent sections, first, we analyze the NE point of $\mathcal{G}$. Then, by considering the gradient update rule of players as the learning method, the convergence of the strategy update to the Nash/ϵ-NE point of the mining game is studied using the MF game theory.

IV. Nash Equilibrium

The NE of $\mathcal{G}$ is studied in this section. An NE is a state of the game where no player can increase its payoff if other players do not change their strategies. The NE of $\mathcal{G}$ can be obtained by intersecting the best response (BR) function of players.

Assumption 1: We assume that there are at least two active miners in the game which means that there are at least two players with positive strategies.

To obtain the BR solution, we take the derivative to find the optimal solution. The first derivative should be equal to zero at the optimal point.

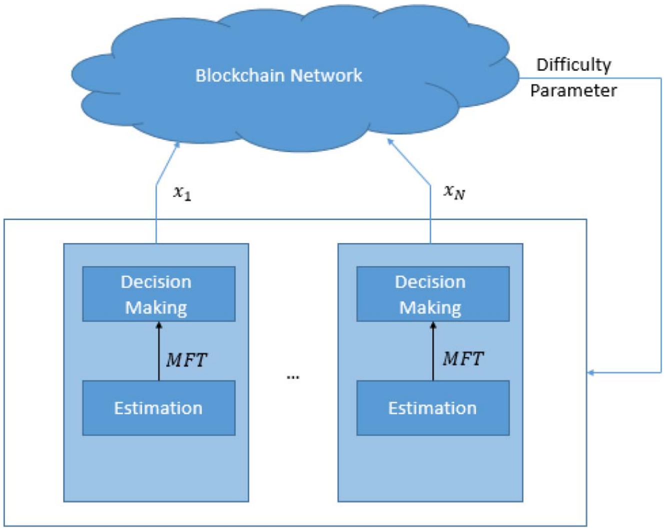


Fig. 1. Estimation of MF term by each agent, and subsequent decision making based on MF term.

Applying the derivative operator to (3) and solving it for x_i leads to

$$\tilde{x}_i(x_{-i}) = \sqrt{A_i \frac{\left(\sum_{j\in\mathcal{N}, j\neq i} x_j\right)}{p_i}} - \sum_{j\in\mathcal{N}, j\neq i} x_j \quad (5)$$

where $x_{-i} = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_N)$.

Taking the second derivative from (3), we get

$$\frac{\partial^2 J_i(x)}{\partial x_i^2} = -2A_i \frac{\sum_{j\in\mathcal{N}, j\neq i} x_j}{\left(\sum_{j\in\mathcal{N}} x_j\right)^3}. \quad (6)$$

Since it is always negative, the solution in (5) is the maximum of the payoff function.

Applying the constraint $x_i \in X_i$, the solution should be projected into X_i, and finally, the BR of the player i is obtained as follows:

$$x_i^*(x_{-i}) = \begin{cases} x_i^{\max}, & x_i^{\max} \leq \tilde{x}_i \\ \tilde{x}_i, & x_i^{\min} \leq \tilde{x}_i \leq x_i^{\max} \\ x_i^{\min}, & \tilde{x}_i \leq x_i^{\min}. \end{cases} \quad (7)$$

The next two sections prove the existence and uniqueness of the NE point in the mining game.

A. Existence of NE

Definition 1 (Concave Game): A game is concave if $\forall x_i \in X_i$, $x \in C$, where C is a compact convex set and the payoff function $J_i(x)$ is continuous with respect to x and concave with respect to x_i $\forall x \in C$.

Lemma 1: $\mathcal{G}$ is a concave game.

Proof: Since $x_i \in [x_i^{\min}, x_i^{\max}]$, C is closed, bounded, and convex. According to (6), $J_i(x)$ is concave with respect to x_i. As a result, $\mathcal{G}$ is a concave game. ■

Reference [49, Th. 1] proves that for every concave N-person game, an NE point exists and therefore, there exist an NE point for $\mathcal{G}$ as well.

B. Uniqueness of NE

Definition 2 (Diagonally Strictly Concave Function) [49]: The function $f(x, r) = \sum_{i=1}^N r_i J_i(x)$ is called diagonally strictly concave for $x \in X = X_1 \times X_2 \times \cdots \times X_N$ and fixed $r = (r_1, r_2, \ldots, r_N) > 0$, if for every $u, v \in X$, we have

$$(u - v)^T g(v, r) + (v - u)^T g(u, r) > 0 \quad (8)$$

where g is a pseudogradient of f which is defined as

$$g(x, r) = \left[r_1 \frac{\partial J_1(x)}{\partial x_1}, \ldots, r_n \frac{\partial J_n(x)}{\partial x_n} \right]^\top. \quad (9)$$

To prove the uniqueness of the NE point, we employ [49, Th. 2]. This theorem says that the NE point of an N-player concave game with a diagonally strictly concave function $f(x, r)$ is unique.

Theorem 1: $\mathcal{G}$ admits a unique NE point.

Proof: Taking the first derivatives from (3) and substituting in (9) yields

$$g(x, r) = \begin{bmatrix} r_1 A_1 \frac{\sum_{j\in\mathcal{N}} x_j - x_1}{\left(\sum_{j\in\mathcal{N}} x_j\right)^2} - p_1 \\ \vdots \\ r_n A_n \frac{\sum_{j\in\mathcal{N}} x_j - x_n}{\left(\sum_{j\in\mathcal{N}} x_j\right)^2} - p_n \end{bmatrix}. \quad (10)$$

According to [49, Th. 6], a sufficient condition for $f(x, r)$ to be diagonally strictly concave is

$$G(x, r) + G^T(x, r) < 0 \quad (11)$$

where $G(x, r)$ is the Jacobian matrix of $g(x, r)$ with respect to x. Choosing $r_i = 1/A_i$ and taking the derivative of (9) with respect to x, and constructing $G + G^T$ results in

$$[G + G^T]_{ii} = -4 \frac{\sum_{j\in\mathcal{N}} x_j - x_i}{\left(\sum_{j\in\mathcal{N}} x_j\right)^3} \quad (12)$$

$$[G + G^T]_{ik} = -2 \frac{\sum_{j\in\mathcal{N}} x_j - x_i - x_k}{\left(\sum_{j\in\mathcal{N}} x_j\right)^3}. \quad (13)$$

To simplify the notation, define the auxiliary variables: $S \triangleq \sum_{j\in\mathcal{N}} x_j > 0$, $S_i \triangleq \sum_{j\in\mathcal{N}} x_j - x_i > 0$, $S_{il} \triangleq \sum_{j\in\mathcal{N}} x_j - x_i - x_l \geq 0$. Hence, we have

$$G + G^T = -2\frac{1}{S^3} \begin{bmatrix} 2S_1 & S_{12} & S_{13} & \ldots & S_{1N} \\ S_{12} & 2S_2 & S_{13} & \ldots & S_{1N} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ S_{1N} & S_{2N} & S_{3N} & \ldots & 2S_N \end{bmatrix}. \quad (14)$$

Since $S > 0$, the criterion is changed to proving the matrix part is positive definite. To this end, we prove that all of its leading principal minors are positive.

By defining $S_i^k = \sum_{j=1}^k x_j - x_i$, $S_{il}^k = \sum_{j=1}^k x_j - x_i - x_l$, and $\bar{S}^k = \sum_{j=k+1}^N x_j$, we can write the kth leading principal minor as follows:

$$\det\left(\overbrace{\begin{bmatrix} S_1^k & S_{12}^k & S_{13}^k & \cdots & S_{1k}^k \\ S_{12}^k & S_2^k & S_{13}^k & \cdots & S_{1k}^k \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ S_{1k}^k & S_{2k}^k & S_{3k}^k & \cdots & S_k^k \end{bmatrix}}^{F^k} + \underbrace{\begin{bmatrix} \bar{S}^k & \bar{S}^k & \bar{S}^k & \cdots & \bar{S}^k \\ \bar{S}^k & \bar{S}^k & \bar{S}^k & \cdots & \bar{S}^k \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \bar{S}^k & \bar{S}^k & \bar{S}^k & \cdots & \bar{S}^k \end{bmatrix}}_{G^k} + \underbrace{\begin{bmatrix} S_1 & 0 & 0 & \cdots & 0 \\ 0 & S_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & S_k \end{bmatrix}}_{H^k}\right). \tag{15}$$

According to the Minkowski determinant theorem [50], if A, B, and C are positive semidefinite matrices, we have

$$\det(A + B + C) \geq \det(A) + \det(B) + \det(C) \geq 0. \tag{16}$$

Thus, we can analyze the three terms separately. Since $S_i > 0$, H^k in (15) is positive definite and its determinant is strictly positive. G^k is also positive semidefinite since it can be written as $G^k = {N^k}^\top N^k$ where $N^k = \sqrt{\bar{S}^k}\vec{\mathbf{1}}_{1\times k}$. Therefore, if the Matrix F^k in (15) is positive semidefinite, then the theorem is proved. To show that F^k is positive semidefinite, we study its leading principal minors.

We have to prove that the determinant of the tth leading principal minors of F^k is nonnegative. Let us denote

$$F_t^k \triangleq \begin{bmatrix} S_1^k & S_{12}^k & S_{13}^k & \cdots & S_{1t}^k \\ S_{12}^k & S_2^k & S_{13}^k & \cdots & S_{1t}^k \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ S_{1t}^k & S_{2t}^k & S_{3t}^k & \cdots & S_t^k \end{bmatrix}. \tag{17}$$

We break F_t^k down into two matrices

$$\left|F_t^k\right| = \det\left(\overbrace{\begin{bmatrix} S_1^t & S_{12}^t & S_{13}^t & \cdots & S_{1t}^t \\ S_{12}^t & S_2^t & S_{13}^t & \cdots & S_{1t}^t \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ S_{1t}^t & S_{2t}^t & S_{3t}^t & \cdots & S_t^t \end{bmatrix}}^{L^t} + \underbrace{\begin{bmatrix} \sum_{j=t+1}^{k} x_j & \sum_{j=t+1}^{k} x_j & \cdots & \sum_{j=t+1}^{k} x_j \\ \sum_{j=t+1}^{k} x_j & \sum_{j=t+1}^{k} x_j & \cdots & \sum_{j=t+1}^{k} x_j \\ \vdots & \ddots & \ddots & \vdots \\ \sum_{j=t+1}^{k} x_j & \sum_{j=t+1}^{k} x_j & \cdots & \sum_{j=t+1}^{k} x_j \end{bmatrix}}_{M_t^k}\right). \tag{18}$$

Again, we apply the Minkowski determinant theorem. Matrix M_t^k is positive semidefinite, because it has the same structure as G^k. Therefore, sufficient condition for $F_t^k \geq 0$ is $L^t \geq 0$. Comparing L^t with F^k in (15) shows their similar structure. Since the theorem holds for the base case, i.e., $F^1 = 0$, the proof is completed by induction. ■

V. Mean Field Game With Gradient Learning Dynamics

Finding the NE point of the game by intersecting the BR functions of the players in (7) is not practical nor computationally tractable for large populations. Because, first, one needs to know the objective function of all the agents which is not reasonable, and second, to obtain the NE point, we need to intersect too many saturating functions in (7) which is not computationally feasible. Therefore, we employ the MF approach to avoid such problems. From the other side, in the real world, usually, players do not act "fully rational." That could be due to the tendency of humans to decide myopic with gradual decision update and limited computation. This feature of decision making is known as "bounded rationality." It has been shown that naive expectation and myopic adjustment can well represent the human behavior in decision making without anticipation of the future [49], [51]–[53]. Due to this point, the gradient-based method as a prevalent model of bounded rationality is used for the decision making of players.

In gradient-based learning (GD), players use the following strategy:

$$x_i[k+1] = x_i[k] + \gamma_i \frac{\partial J_i(x)}{\partial x_i} \tag{19}$$

where k is the game iteration and γ_i is the learning rate of the player i. However, to compute the derivation of the payoff function in (19), each player needs to know the strategy of other players. A possible solution for this problem is the use of the MF game theory.

By looking at (3), it can be realized that the payoff function of the player i is affected by the strategies of all other agents by an aggregative term. We can consider this aggregative term as the MF term and estimate its value using the naive estimation as follows:

$$Z[k] = \sum_{j=1}^{N} x_j[k] \tag{20}$$

where $Z[k]$ is the MF term at iteration k.

Algorithm 1: MF Gradient Learning

```
Initialization: $k = 1$ and $Z[0] = Z_0$
while $\epsilon > \epsilon_0$ do
    Players choose their strategy according to
    Equation (22)
    Update MF term by (23).
    $\epsilon = |Z[k+1] - Z[k]|$
    $k = k + 1$
end
```

A fundamental assumption behind the MF game is that the number of players is large enough in which, the change in a single player's strategy would not significantly change the MF term. This assumption is valid in our case which is a blockchain network. Therefore, each player estimates the total computational power of the network at each iteration (i.e., $Z[k]$).

The payoff for player i is rewritten as

$$J_i^{\mathrm{MF}}[k] = A_i \frac{x_i[k]}{Z[k]} - p_i x_i[k]. \tag{21}$$

Applying (21) to (19), we will get

$$x_j[k+1] = x_j[k] + \gamma_j\left(\frac{A_j}{Z[k]} - p_j\right). \tag{22}$$

As we see, the updated strategy of each player is obtained as a function of the MF term. Therefore, the update equation for the MF term in (20) can be rewritten as the following fixed-point iteration:

$$Z[k+1] = \Omega(Z[k]) = Z[k] + \sum_{j\in\mathcal{N}} \gamma_j\left(\frac{A_j}{Z[k]} - p_j\right). \tag{23}$$

Finally, the game overlying algorithm is given in Algorithm 1 which shows alternating update of the MF term and the strategies of players.

A. Convergence

In what follows, the convergence of the proposed MF gradient learning algorithm is studied.

Theorem 2: A Sufficient condition for the convergence of Algorithm 1 is

$$\sum_{j\in\mathcal{N}} \gamma_j A_j < 2\underline{S}^2 \tag{24}$$

where $\underline{S} = \sum_{i\in\mathcal{N}} x_i^{\min}$.

Proof: According to the Banach fixed-point theorem [54], the iteration provided in (23) converges if the mapping $\Omega(.)$ is contractive, which is

$$\|\Omega(w) - \Omega(v)\| < \|w - v\| \tag{25}$$

where $\Omega(w)$ is obtained from (23), and w and v are any possible values for $Z[k]$.

Simplifying the left-hand side of (25)

$$\begin{aligned}\|\Omega(w) - \Omega(v)\| &= \left\| w - v + \sum_{j\in\mathcal{N}} \gamma_j A_j \left(\frac{1}{w} - \frac{1}{v}\right)\right\| \\ &= \|w - v\|.\left\| 1 - \frac{1}{wv}\sum_{j\in\mathcal{N}} \gamma_j A_j\right\|. \end{aligned} \tag{26}$$

From Assumption 1, we consider $\underline{S} = \sum_{j\in\mathcal{N}} x_j^{\min} > 0$. Hence, $w, v \geq \underline{S} > 0$. Applying these inequalities, we obtain

$$\frac{\|\Omega(w) - \Omega(v)\|}{\|w - v\|} \leq \left\| 1 - \frac{\sum_{j\in\mathcal{N}} \gamma_j A_j}{\underline{S}^2}\right\|. \tag{27}$$

In order to satisfy the contractive mapping condition, we should choose γ_j such that

$$\sum_{j\in\mathcal{N}} \gamma_j A_j < 2\underline{S}^2. \tag{28}$$

■

In the special case where $\gamma_j = \gamma$, this condition could be simplified as

$$\gamma < \frac{2\underline{S}^2}{\sum_{j\in\mathcal{N}} A_j}. \tag{29}$$

Note that the above condition is the conservative lowest bound of γ. γ_j could be chosen a much bigger value and the MF term will still converge to its final value.

B. ϵ-Nash Equilibrium

After convergence analysis of the proposed MF game, a reasonable question that arises is that where does the proposed algorithm converges to. Since in the MF game, each player encapsulates the effect of all players with the MF term and neglects its own effect on the MF game, the MF solution might be slightly different from the BR solution presented in Section IV. Therefore, the concept of MF ϵ-NE is introduced as follows.

Definition 3 (MF ϵ-NE): A strategy profile $(x_1^*, \ldots, x_n^*)$ is an MF ϵ-NE, if there exists $\epsilon > 0$ such that for every player i, the following condition holds:

$$J_i\left(x_i^*, \sum_{j\in\mathcal{N}} x_j^*\right) \geq \max_{y\in X_i} J_i\left(y, \left(y + \sum_{j\neq i} x_j^*\right)\right) - \epsilon. \tag{30}$$

In the MF game, usually, as the number of players grows, ϵ uniformly goes to zero and the MF solution approaches the exact solution [36], [55]. In our case, we show that ϵ uniformly goes to zero as the network computational power increases.

Theorem 3: The difference in the payoff of agents at NE and at the converged point of Algorithm 1 is a decreasing function of the network computational power.

Proof: We are going to calculate the difference between players' exact BR and MF. In the converged point of Algorithm 1, players' strategies satisfy the following condition:

$$x_i^* = \begin{cases} x_i^{\max} & Z^* < \frac{A_i}{p_i} \\ x_i^{\min} & Z^* > \frac{A_i}{p_i} \end{cases} \tag{31}$$

where Z^* is the converged MF term of the algorithm. In general, this condition holds for any decision-making dynamics based on the MF term.

We investigate this difference for three different cases.

1) If $x_i^{\mathrm{BR}} = x_i^{\max}$, then $x_i^{\mathrm{MF}} = x_i^{\max}$. Following the notation introduced in (5) and (7), and considering $S_i \triangleq$

$\sum_{j\in\mathcal{N}} x_j - x_i$, if $x_i^{\max} \le \hat{x}_i$, then $x_i^{\mathrm{BR}} = x_i^{\max}$. Then, we have

$$x_i^{\max} < \sqrt{\frac{A_i}{p_i}S_i} - S_i. \tag{32}$$

Applying $x_i^{\max} \ge x_i^{\min} \ge 0$

$$0 < \sqrt{\frac{A_i}{p_i}S_i} - S_i,\ 0 < S_i < \frac{A_i}{p_i},\ 0 < \sqrt{\frac{A_i}{p_i}S_i} < \frac{A_i}{p_i}. \tag{33}$$

Combining (32) and (33), we have

$$x_i^{\max} + S_i < \frac{A_i}{p_i},\ Z < \frac{A_i}{p_i},\ x^{\mathrm{MF}} = x_i^{\max}. \tag{34}$$

As a result, in this case, the NE and ϵ-NE are exactly the same. $\Delta x = \Delta J = 0$.

2) If $x_i^{\mathrm{MF}} = x_i^{\min}$, then $x_i^{\mathrm{BR}} = x_i^{\min}$. According to (31), we have

$$Z > \frac{A_i}{p_i},\ x_i^{\min} + S_i > \frac{A_i}{p_i},\ \sqrt{S_i} > \sqrt{\frac{A_i}{p_i} - x_i^{\min}}. \tag{35}$$

On the other hand

$$\sqrt{\frac{A_i}{p_i} - x_i^{\min}} > \frac{\sqrt{\frac{A_i}{p_i}} + \sqrt{\frac{A_i}{p_i} - 4x_i^{\min}}}{2}. \tag{36}$$

Combining (35) and (36), we have

$$\sqrt{S_i} > \frac{\sqrt{\frac{A_i}{p_i}} + \sqrt{\frac{A_i}{p_i} - 4x_i^{\min}}}{2},\ x_i^* < x_i^{\min},\ x_i^{\mathrm{BR}} = x_i^{\min}. \tag{37}$$

As a result, in this case, the NE and ϵ-NE are exactly the same. $\Delta x = \Delta J = 0$.

3) If $Z > A_i/p_i$ and $x_i^{\min} < x_i^* < x_i^{\max}$, then $\Delta J = O(1/M)$, where $S_i = Mx_i^{\max}$ and $M >> 1$

$$\begin{aligned} x_i^{\min} &< x_i^* < x_i^{\max}\\ x_i^{\min} &< \sqrt{\frac{A_i}{p_i}S_i} - S_i < x_i^{\max}. \end{aligned} \tag{38}$$

Inequality (38) has two solutions. The first solution

$$\begin{aligned} &\frac{\sqrt{\frac{A_i}{p_i}} - \sqrt{\frac{A_i}{p_i} - 4x_i^{\min}}}{2} < \sqrt{S_i}\\ &< \frac{\sqrt{\frac{A_i}{p_i}} - \sqrt{\frac{A_i}{p_i} - 4x_i^{\max}}}{2}\\ &\frac{A_i}{2p_i} - x_i^{\min} - \frac{1}{2}\sqrt{\frac{A_i}{p_i}}\sqrt{\frac{A_i}{p_i} - 4x_i^{\min}} < S_i\\ &< \frac{A_i}{2p_i} - x_i^{\max} - \frac{1}{2}\sqrt{\frac{A_i}{p_i}}\sqrt{\frac{A_i}{p_i} - 4x_i^{\max}} \end{aligned} \tag{39}$$

and from the assumption of this case, we have

$$Z < \frac{A_i}{p_i},\ S_i + x_i^{\max} < \frac{A_i}{p_i},\ x_i^{\max} << \frac{A_i}{p_i}. \tag{40}$$

As a result

$$\sqrt{\frac{A_i}{p_i} - 4x_i^m} \approx \sqrt{\frac{A_i}{p_i}}\left(1 - \frac{2p_ix_i^m}{A_i}\right) \tag{41}$$

where x_i^m stands for either $x_i^{\min}$ or $x_i^{\max}$. Applying approximation of (41) to inequality for the first solution in (39), we obtain $0 < S_i < 0$, which means this solution is not feasible. The second solution

$$\frac{\sqrt{\frac{A_i}{p_i}} + \sqrt{\frac{A_i}{p_i} - 4x_i^{\max}}}{2} < \sqrt{S_i} < \frac{\sqrt{\frac{A_i}{p_i}} + \sqrt{\frac{A_i}{p_i} - 4x_i^{\min}}}{2} \tag{42}$$

using first term of the Taylor series

$$\begin{aligned} &\frac{A_i}{2p_i} - x_i^{\max} + \frac{1}{2}\sqrt{\frac{A_i}{p_i}}\sqrt{\frac{A_i}{p_i} - 4x_i^{\max}} < S_i\\ &< \frac{A_i}{2p_i} - x_i^{\min} - \frac{1}{2}\sqrt{\frac{A_i}{p_i}}\sqrt{\frac{A_i}{p_i} - 4x_i^{\min}}. \end{aligned} \tag{43}$$

Applying (41)–(43), we have

$$\frac{A_i}{p_i} - 2x_i^{\max} < S_i < \frac{A_i}{p_i} - 2x_i^{\min}. \tag{44}$$

As a result

$$\frac{A_i}{p_i} < (M+2)x_i^{\max}. \tag{45}$$

Now, we form ΔJ

$$\begin{aligned} \Delta J &= J^{\mathrm{BR}} - J^{\mathrm{MF}}\\ &= A_i\frac{x^{\mathrm{BR}}}{x^{\mathrm{BR}} + S_i} - p_ix^{\mathrm{BR}} - A_i\frac{x^{\mathrm{MF}}}{x^{\mathrm{MF}} + S_i} + p_ix^{\mathrm{MF}} \end{aligned} \tag{46}$$

and thus

$$\begin{aligned} \frac{\Delta J}{\Delta x} &= \frac{A_iS_i}{\left(x^{\mathrm{BR}} + S_i\right)\left(x^{\mathrm{MF}} + S_i\right)} - p_i\\ &\le \frac{A_i}{S_i} - p_i = p_i\left[\frac{A_i}{p_iS_i} - 1\right]\\ &\le p_i\left[\frac{(M+2)x_i^{\max}}{Mx_i^{\max}} - 1\right] = p_i\frac{2}{M}. \end{aligned} \tag{47}$$

As a result, in this case, the difference between NE and ϵ-NE decreases as the computational power of the network increases. ■

In summary, as the computational power of the network grows, the MF game becomes a better estimation of the exact game, meaning that MF-ϵ-NE approaches the NE point of the game.

VI. Simulation

In this section, numerical simulations are performed to evaluate the proposed MF method. This section includes two parts. First, the MF approach is compared to the BR method, which is the best theoretical solution, considering complete information on the payoff function of players. Second, the sensitivity analysis of parameters is performed and the convergence of the MF term is investigated also with dynamic settings of a practical network.

TABLE I
PARAMETERS OF SIMULATIONS

Parameter	Value
A_i	uniform(80k, 100k)
p_i	uniform(2, 9)
N	1000
x_{min}	0
x_{max}	100
x_0	uniform(x_{min}, x_{max})

The BR of players is calculated according to (7). For the MF method, players follow Algorithm 1. Unless otherwise mentioned, all simulations use parameters specified in Table I. The parameters are chosen to follow the Bitcoin blockchain network as an example. A_i represents the reward of successfully mining a new block. Currently, each new block contains 12.5 BTC. Each BTC is assumed to worth \$7200, thus, $A = \$90$k. To account for accessibility, ease of spending, and privacy values, this parameter is assumed to be from a uniform distribution in the range of \$80k–\$100k. p_i represents the price of the computational power unit, which is assumed to be the electricity price. The price of electricity varies around the world, but it is mainly between \$0.08 and \$0.33 per kWh. The efficiency and hash rate depend on the type of mining equipment. As an example, Antminer S9 has a hash power of 14 TH/s (Tera Hash per second) and consumes about 1400 W of energy. A simple calculation reveals that this device is capable of 36 000 TH with 1 kWh of energy. Given the price of electricity p_i, which is the price of each hash completion, is calculated to be about \$2–\$9 per EH, hence, it is assumed to be drawn from a uniform distribution on this range.

To analyze the effect of parameter distribution on the evolution of the network, the Monte Carlo simulation is conducted with parameter distributions described in the previous paragraph and summarized in Table I. All simulations are run five times and the average result is depicted. The codes to reproduce the results are available at https://github.com/SmartNetworkLab-UT/Mean-Field-Game-for-Equilibrium-Analysis-of-Mining-Computational-Power-in-Blockchains.

A. Comparison With Best Response

In the following figures, social welfares of the network obtained from the BR and MF gradient-based learning are compared. Social welfare is defined as the sum of all players' payoffs. In all figures, γ is chosen sufficiently small to ensure convergence of the MF term. Social welfare is calculated after the network has converged to the NE point.

Fig. 2 depicts the social welfare for the BR and MF response under gradient-based decision dynamics. Since BR is the theoretical best solution, it always gives higher payoff than that of the MF method. However, the MF solution is very close to the optimal solution by considering incomplete information of the players from the rivals' model. The fluctuations are due to randomness of parameters. As the number of players increases, the network becomes more competitive, and due to competitive action of players, each agents' surplus decreases and the total utility of players, i.e., network's social welfare decreases.

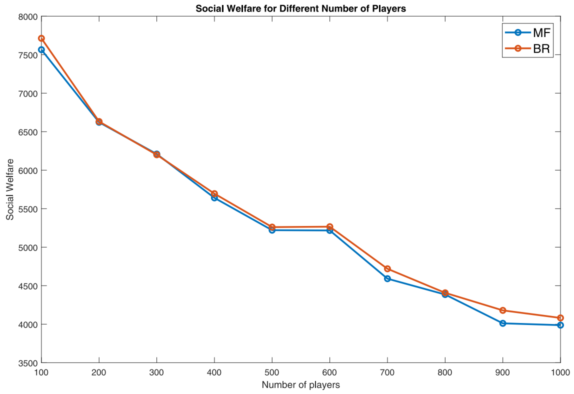


Fig. 2. Social welfare of the network for BR and MF solutions, for different network sizes.

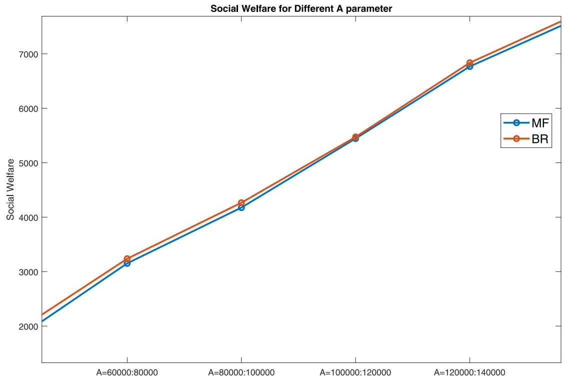


Fig. 3. Social welfare of the network for BR and MF solutions, for different A_i distributions.

In Fig. 3, social welfare for different ranges of A_i is compared. In each case, the A_i of players is uniformly distributed in the given range. As expected, increasing A_i, which represents the expected payoff gained by the agent i for successfully mining a block, results in higher social welfare in the network. Since the relationship between an agent's payoff and its A_i is linear, the social welfare increases almost linearly with A_i.

Finally, Fig. 4 shows the social welfare of the network for BR and MF for different ranges of p_i. In each case, p_i is uniformly distributed in the given range. Since p_i represents the unit price of computational power, it is reasonable to see social welfare decreases as p_i increases. More precisely, since p_i resides in the denominator, the social welfare shows a reciprocal behavior with respect to p_i range.

B. Sensitivity Analysis of Convergence

In this section, the convergence of the MF term is depicted and analyzed. In all simulations, the range of iterations is chosen large enough to show the convergence of the MF term. Fig. 5 shows the MF term evolution for three different values of learning rate, i.e., $\gamma = 0.3$, $\gamma = 0.5$, and $\gamma = 0.7$. The MF term takes about 100 iterations to reach its 5% bound of its settling point. Since on average, every 10 min, a new block is mined in the Bitcoin network, this corresponds to about 17 h. After that, small changes in parameters will quickly

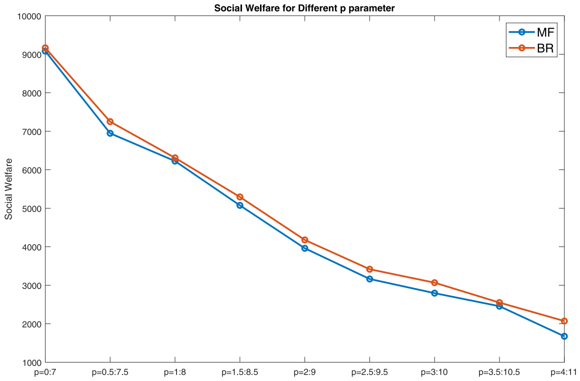


Fig. 4. Social welfare of the network for BR and MF solutions, for different p_i distributions.

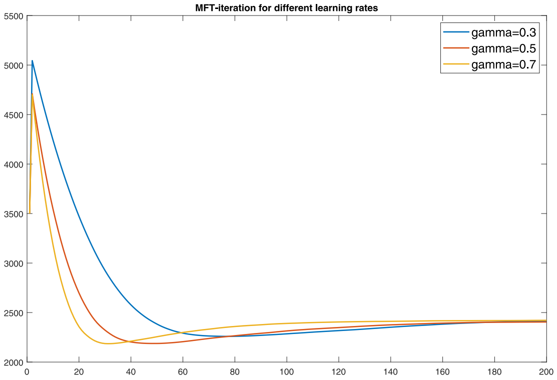


Fig. 5. MF term versus iteration number for $\gamma = 0.3, 0.5, 0.7$.

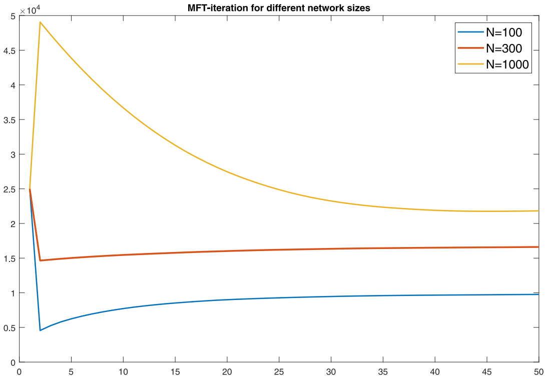


Fig. 6. MF term for different network sizes, versus iteration number.

be traced. We see that as much as the value of the learning rate becomes smaller, the convergence of the MF term becomes slower accordingly. However, a larger learning rate means more fluctuations in the MF term.

Fig. 6 shows the MF term under iterations of Algorithm 1, for different number of agents in the network. As seen in this figure, more agents participating in the network leads to more computational power. Also, converging to the settling point of the system takes more time.

In Fig. 7, the MF term evolution of the network is depicted for a fixed value of $A_i = 80\,000$, while $p_i \sim U(2, 9)$. Three plots represent the average of five simulations and a confidence

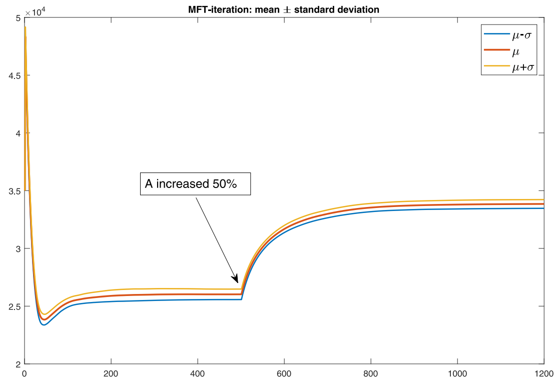


Fig. 7. MF term versus iteration number. A_i of players increase by 50% at the 500th iteration and the MF term converges quickly to the new equilibrium point.

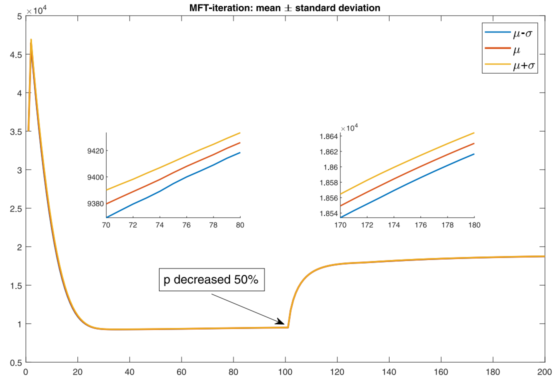


Fig. 8. MF term versus iteration number. p_i of players decreased by 50% at the 100th iteration and the MF term converges quickly to the new equilibrium point.

interval equal to one standard deviation to show the robustness of the proposed MF method. As seen in this figure, the MF term converges after about 200 iterations. To show the behavior of the proposed method under parameter changes, at 500th iteration, A_i increases by 50%. This sudden change in the parameter value causes the system to move to a new equilibrium, which is reached after about 300 iterations. In practice, parameter changes happen more smoothly and the MF term tracks the system more quickly and smoothly.

Finally, Fig. 8 shows the MF term evolution of the network for a fixed value of $p_i = 10$, while $A_i \sim U(80\text{k}, 100\text{k})$. Average over five simulations and a confidence interval of one standard deviation are drawn in this figure. The convergence happens at about 30 iterations. To simulate the dynamic change of parameters in real blockchain networks, p_i is perturbed at 100th iteration by a 50% decrease. The network quickly reaches the new equilibrium point after only 20 iterations. As before, this abrupt change is only meant to show the robustness of the algorithm since, in practice, parameters change gradually.

VII. Conclusion

In this article, the concept of the MF game theory was used to analyze the behavior of mining agents in a PoW network. An MF gradient learning algorithm was introduced and its convergence to ϵ-NE point of the game was analyzed. The difference between BR exact solution and MF solution for each player was calculated and shown that for mining pools with small computational power compared to the rest of network, decision making based on the MF term is not only easier but also as good as the BR method with full information about other players. Furthermore, if A_i increases, i.e., network tokens are more valuable, or p_i decreases, i.e., the unit computational price decreases, e.g., due to technological advancements or lower electricity prices, existing agents would increase their computational power and also new players might enter the network and thus, the total computational power of the network increases, making the MF method even more accurate, and *vice versa*. Namely, decreases in A_i, e.g., due to decrease of the number of network tokens awarded for each mined block, and increases in p_i, e.g., due to rising electricity prices, the total computational power of the network decreases, and thus, the MF method becomes more distant from the BR method and less accurate. On the other hand, the only parameter that each player must choose in the proposed method was the learning rate of the gradient-based algorithm. It was shown that convergence of the MF term is guaranteed for a small enough learning rate. In addition, a smaller learning rate leads to more robustness of the algorithm and a larger learning rate results in faster convergence. Therefore, choosing the value of the learning parameter, one needs to compromise between robustness and learning speed. Extending the analysis provided in this article to other proof concepts, such as PoS, is considered as future works.

References

[1] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[2] M. Swan, *Blockchain: Blueprint for a New Economy*. Beijing, China: O’Reilly Media, 2015.

[3] S. Huh, S. Cho, and S. Kim, “Managing IoT devices using blockchain platform,” in *Proc. IEEE 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 464–467.

[4] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2017, pp. 618–623.

[5] A. Banafa, “IoT and blockchain convergence: Benefits and challenges,” *IEEE Internet Things J.*, early access.

[6] C. Xu *et al.*, “Making big data open in edges: A resource-efficient blockchain-based approach,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 4, pp. 870–882, Apr. 2019.

[7] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When mobile blockchain meets edge computing,” *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[8] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, “Cloud/fog computing resource management and pricing for blockchain networks,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4585–4600, Jun. 2019.

[9] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, “Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[10] N. Herbaut and N. Negru, “A model for collaborative blockchain-based video delivery relying on advanced network services chains,” *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70–76, Sep. 2017.

[11] M. Li *et al.*, “CrowdBC: A blockchain-based decentralized framework for crowdsourcing,” *IEEE Trans. Parallel Distrib. Syst*, vol. 30, no. 6, pp. 1251–1266, Jun. 2019.

[12] T. M. Fernández-Caramés, and P. Fraga-Lamas, “A review on the use of blockchain for the Internet of Things,” *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[13] F. X. Olleros and M. Zhegu, *Research Handbook on Digital Transformations*. Cheltenham, U.K.: Edward Elgar, 2016.

[14] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of activity: Extending bitcoin’s proof of work via proof of stake,” *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.

[15] F. Saleh, “Blockchain without waste: Proof-of-stake,” in *Proc. SSRN*, 2019, Art. no. 3183935.

[16] P. K. Sharma and J. H. Park, “Blockchain based hybrid network architecture for the smart city,” *Future Gener. Comput. Syst.*, vol. 86, pp. 650–655, Sep. 2018.

[17] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, “Hybrid-IoT: Hybrid blockchain architecture for Internet of Things-pow sub-blockchains,” in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2018, pp. 1007–1016.

[18] M. Romiti, A. Judmayer, A. Zamyatin, and B. Haslhofer, “A deep dive into bitcoin mining pools: An empirical analysis of mining shares,” 2019. [Online]. Available: arXiv:1905.05999.

[19] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, “Performance analysis and application of mobile blockchain,” in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (ICNC)*, 2018, pp. 642–646.

[20] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, “Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 695–708, Jan. 2019.

[21] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[22] D. Minoli and B. Occhiogrosso, “Blockchain mechanisms for IoT security,” *Internet Things*, vols. 1–2, pp. 1–13, Sep. 2018.

[23] T. Jiang, H. Fang, and H. Wang, “Blockchain-based Internet of Vehicles: Distributed network architecture and performance analysis,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019.

[24] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, “Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5791–5802, Jun. 2019.

[25] T. Klein, H. P. Thu, and T. Walther, “Bitcoin is not the new gold—A comparison of volatility, correlation, and portfolio performance,” *Int. Rev. Financ. Anal.*, vol. 59, pp. 105–116, Oct. 2018.

[26] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, “Blockchain technologies for the Internet of Things: Research issues and challenges,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[27] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, “Security implications of blockchain cloud with analysis of block withholding attack,” in *Proc. 17th IEEE/ACM Int. Symp. Cluster Cloud Grid Comput.*, 2017, pp. 458–467.

[28] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[29] B. Alvarez-Pereira *et al.*, “Network and conversation analyses of bitcoin,” in *Proc. Complex Syst. Summer School*, 2014. [Online]. Available: https://madeinhaus.s3.amazonaws.com/sfi-com/staging/uploads/ckeditor/2016/11/02/network-and-conversation-analyses-of-bitcoin.pdf

[30] Z. Liu *et al.*, “A survey on applications of game theory in blockchain,” 2019. [Online]. Available: arXiv:1902.10865.

[31] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, “Optimal selfish mining strategies in bitcoin,” in *Proc. Int. Conf. Financ. Cryptography Data Security*, 2016, pp. 515–532.

[32] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, “Blockchain mining games,” in *Proc. ACM Conf. Econ. Comput.*, 2016, pp. 365–382.

[33] N. Dimitri, “Bitcoin mining as a contest,” *Ledger*, vol. 2, pp. 31–37, Sep. 2017.

[34] I. Tsabary and I. Eyal, “The gap game,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2018, pp. 713–728.

[35] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, “Evolutionary game for mining pool selection in blockchain networks,” *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 760–763, Oct. 2018.

[36] J.-M. Lasry and P.-L. Lions, "Mean field games," *Jpn. J. Math.*, vol. 2, no. 1, pp. 229–260, 2007.

[37] O. Guéant, J.-M. Lasry, and P.-L. Lions, "Mean field games and applications," in *Paris–Princeton Lectures on Mathematical Finance 2010*. Berlin, Germany: Springer, 2011, pp. 205–266. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-14660-2_3

[38] F. Bagagiolo and D. Bauso, "Mean-field games and dynamic demand management in power grids," *Dyn. Games Appl.*, vol. 4, no. 2, pp. 155–176, 2014.

[39] R. Couillet, S. M. Perlaza, H. Tembine, and M. Debbah, "Electrical vehicles in the smart grid: A mean field game analysis," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1086–1096, Jul. 2012.

[40] M. Kamgarpour and H. Tembine, "A Bayesian mean field game approach to supply demand analysis of the smart grid," in *Proc. IEEE 1st Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, 2013, pp. 211–215.

[41] F. Mériaux, V. S. Varma, and S. Lasaulce, "Mean field energy games in wireless networks," in *Proc. IEEE Conf. Record 46th Asilomar Conf. Signals Syst. Comput. (ASILOMAR)*, 2012, pp. 671–675.

[42] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1616–1627, Mar. 2014.

[43] H. Tembine, "Energy-constrained mean field games in wireless networks," *Strategic Behav. Environ.*, vol. 4, no. 2, pp. 187–211, 2014.

[44] J. A. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2015, pp. 281–310.

[45] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011. [Online]. Available: arXiv:1112.4980.

[46] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. ISSC*, 2014, pp. 1–6.

[47] M. K. Jensen, "Aggregative games and best-reply potentials," *Econ. Theory*, vol. 43, no. 1, pp. 45–66, 2010.

[48] F. Parise, S. Grammatico, B. Gentile, and J. Lygeros, "Network aggregative games and distributed mean field control via consensus theory," 2015. [Online]. Available: arXiv:1506.07719.

[49] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave *n*-person games," *Econometrica J. Econ. Soc.*, vol. 33, no. 3, pp. 520–534, 1965.

[50] M. Marcus and H. Minc, *A Survey of Matrix Theory and Matrix Inequalities*, vol. 14. Newburyport, MA, USA: Courier Corporat., 1992.

[51] C. Camerer, "Bounded rationality in individual decision making," *Exp. Econ.*, vol. 1, no. 2, pp. 163–183, 1998.

[52] M. Kandori, G. J. Mailath, and R. Rob, "Learning, mutation, and long run equilibria in games," *Econometrica J. Econ. Soc.*, vol. 61, no. 1, pp. 29–56, 1993.

[53] A. Dixit, "Comparative statics for oligopoly," *Int. Econ. Rev.*, vol. 27, no. 1, pp. 107–122, 1986.

[54] A. Granas and J. Dugundji, *Fixed Point Theory*. New York, NY, USA: Springer-Verlag, 2013. [Online]. Available: https://www.springer.com/gp/book/9780387001739

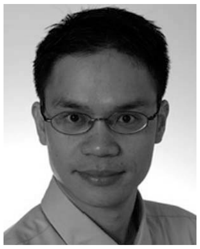
[55] M. Huang, P. E. Caines, and R. P. Malhamé, "Individual and mass behavior in large population stochastic wireless power control problems: Centralized and Nash equilibrium solutions," in *Proc. 42nd IEEE Int. Conf. Decis. Control*, vol. 1, 2003, pp. 98–103.

Amirheckmat Taghizadeh received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Tehran, Tehran, Iran, in 2016 and 2019, respectively.

He is currently a Researcher with the School of Electrical and Computer Engineering, University of Tehran. His research interests include game theory, decentralized control, and smart grids.

Hamed Kebriaei (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Tehran, Tehran, Iran, in 2005, the M.Sc. degree in electrical engineering from Tarbiat Modares University, Tehran, in 2007, and the Ph.D. degree in control systems from the University of Tehran in 2010.

He is currently an Associate Professor with the School of Electrical and Computer Engineering, University of Tehran. His research interests include game theory, and optimization and stochastic control with applications in network systems and smart grids.



Dusit Niyato (Fellow, IEEE) received the B.Eng. degree from the King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Winnipeg, MB, Canada, in 2008.

He is currently a Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests are in the area of energy harvesting for wireless communication, Internet of Things, and sensor networks.