Resource Allocation for Edge Computing-based Blockchain: A Game Theoretic Approach

Wenlong Guo†, Zheng Chang*, Xijuan Guo†, Dushnatha Nalin K. Jayakody‡ and Tapani Ristaniemi*
†College of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China
*University of Jyvaskyla, Faculty of Information Technology, P. O. Box 35, FI-40014 Jyvaskyla, Finland
‡School of Computer Science and Robotics, National Research Tomsk Polytechnic University, Tomsk, Russia

***Abstract*—Blockchain has been progressively applied to various Internet of Things (IoT) platforms. As the efficiency of the blockchain depends on its computing capability, how to make sure the acquisition of the computational resources and participation of the devices would be the driving force. In this work, an edge computing-based blockchain network is considered, where the edge service provider (ESP) offers computational resources for the miners. The focus is to investigate an efficient incentive mechanism for the miners to purchase the computational resources. Accordingly, a two-stage Stackelberg game is formulated between the miners and ESP. By exploring the Stackelberg equilibrium of the optimal mining strategy under two different mining schemes. The aim is to find the optimal incentive for the ESP and miners to choose auto-fit strategies. Through theoretical analysis and numerical simulation, we demonstrate the effectiveness of the proposed scheme on encouraging devices to participate the Blockchain.**

I. Introduction

The emergence of the Internet of Things (IoT) will be the driving forces of the development of the future information and communication technology (ICT). Meanwhile, the blockchain has evolved from the original digital currency to extensive IoT applications due to its distributed, tamper-resistant, retrospective and transparent features [1]. It has a great potential to provide a secure and efficient decentralized IoT paradigm. In blockchain, a block contains specific data about cryptographic transactions. In peer-to-peer (P2P) network, blockchain technology allows to operate applications in a distributed manner without a trusted third party as intermediate media, which would enable individual to interact with others in a verifiable way. In general, the generation of blockchain involves two processes: computing and releasing. Computing refers to the process of solving the Proof of Work (PoW) by computing to obtain a settlement or an unverified block and releasing means that when miners successfully solve the PoW problem and then report the result to blockchain network for verification. When the verification is correct, the blockchain will reach consensus and then obtain rewards. The users/nodes who participant in the computing are also named as miners while the computing for consensus is called mining.

To further realize the blockchain in the IoT, edge computing can play a significant role. The miners with insufficient hash power recent the computational resources from Edge Service Provider (ESP). As we know, the computing capability is the key to the security and efficiency of blockchain, how to incentivize the miners to participate the blockchain process and obtain the computational resources is of profound significance. In [2], the authors present an action game architecture to study the optimal profits of ESP and miners based on deep learning. The authors of [3] design a novel approximation algorithm and study how to maximize the social welfare of blockchain network. There are also several works utilizing the game theory on designing the incentive schemes [4]- [5]. The authors of [4] propose to investigate the optimal profits of ESPs and miners under different pricing strategies via game theoretic approaches. The authors of [5] suggest a two-miner model to find the strategy of hash power utilization and find the Nash Equilibrium (NE) in the blockchain. Motivated by the aforementioned observations, in this paper, we aim at proposing a novel incentive mechanism for an edge computing-based blockchain, in order to find the optimal purchase and pricing strategies for the ESP and miners. The main contribution can be summarized as follows.

In the considered system, to encourage the users to participate the mining process and the ESP to provide the computational resources, we aim to explore the relations and interactions between two parties. The optimal incentive mechanism is presented based on the game theoretic approach, i.e. Stackelberg game, where ESP is the leader and user is the follower. Two mining schemes are particularly investigated. The first one is that after after successfully computing, the miner will report immediately, and the other one is to report strategically after successfully computing. Then we have proved the existence and uniqueness of Nash equilibrium, and apply backward induction to find the global optimal solution. The proposed mechanisms can help both parties to obtain the best benefits and essentially stimulate the development of blockchain system. Numerical results demonstrate the effectiveness of the proposed incentive mechanism.

II. System Model

We consider a scenario where there is one ESP and N miners. The set of miners is denoted as $\mathcal{N}$. We assume that price of computational resource for miner i is q_i and the purchase strategy of miner i is s_i. The set of price of computational resource for miners is $\mathcal{Q} = \{q_1, q_2...q_n, ..., q_N\}$ and the set of purchase strategy (purchased amount) is $S = \{s_1, s_2..., s_n, ..., s_N\}$ and $s_i \in [s_{\min}, s_{\max}]$ where $s_{\min}$ and $s_{\max}$ is the minimum and maximum computational resource purchased by miner i, respectively. Meanwhile, we assume

978-1-7281-7440-2/20/$31.00 ©2020 IEEE

the hash power proportion of miner i in the whole blockchain network is α_i, which can be expressed by $\alpha_i = s_i / \sum_{j \in \mathcal{N}} s_j$.

During the computing process, we assume that the probability that miner i successfully solves the PoW problem is μ_i. Considering the miner's solution to the PoW problem follows the Poisson distribution with a compliance parameter λ [5], we can obtain $\mu_i = \alpha_i e^{-\lambda t_i}$ where the computing delay t_i is related to the block size π_b of each block b and the computing capability ς_i. We can consider $t_i = \varsigma_i \pi_b$. Similarly, we assume that the probability that the miner successfully announces the solutions of the PoW problem from verification is ν_i. Also we consider the miner's solution to the PoW problem follows the Poisson distribution with a compliance parameter γ, then we have $\nu_i = \alpha_i e^{-\gamma \tau_i}$, where τ_i is the delay, which is also related to the block size and computing capability. Also we assume $\tau_i = \xi_i \pi_b$. For simplicity, we assume for each block, the size is equal, which means $\pi_b = \pi$. Meanwhile, the process of verification would consume less computational resources and shorter processing time than computing the PoW.

When there are new tasks and transactions, they are firstly being verified. After successful verification, the task will be published to the blockchain. If it is successfully solved through general consensus algorithm, a new block will be generated on a certain chain. We assume that the new block would be generated at the beginning of the pseudo-genesis block. For single rational miner i, there are generally two effectively mining schemes of obtaining rewards. One is that the miner can obtain the reward from single block generation and the other one is from a chain of blocks or branched chain. However, miner i may face the risk that the others can release their results after computing before him. Thus, there are two mining and reporting schemes: immediate reporting after successfully computing (IR) and strategically reporting after successfully computing (SR).

III. Problem Formulation

A. Rewards

In the process of block generation, there are three types of rewards for the miners: fixed reward, performance reward and participant reward. The fixed reward R_f is the constant reward for computing the newly generated block. For example, for Bitcoin, a new block would be generated approximately every 10 minutes and the bonus generated by the Bitcoin has been halved every four years. Therefore, the fixed reward of blockchain can be regarded as an attenuation function which the half-life is T. That is $R_f = R_f^{\max} \left(\frac{1}{2}\right)^{\frac{t}{T}}$, where $R_f^{\max}$ is the constant reward from genesis block.

The performance reward R_p is related to the volume of transactions contained within the generated block, e.g., the size of each block. We denote it as $R_p = r\pi$, where r is an evaluation factor and π is the size of block.

The participant reward $R_{\varepsilon,i}$ depends on the degree of participation in the computing process while the new block is generated, i.e. $R_{\varepsilon,i} = \varepsilon \alpha_i$, where ε is an evaluation factor.

B. Stackelberg Game

In this paper, we investigate the profits for miners and ESP by introducing a two-stage Stackelberg game. We define the ESP as the "leader" and the miner as the "follower" in this game model. In the formulated game, the utility functions of ESP and miners in each stage can be described in the following.

1) In the first stage, the ESP sets the pricing strategy $\mathcal{Q} = \{q_1, q_2 ...\}$ and the utility/profit function is:

$$U_{ESP}(\mathcal{S}, \mathcal{Q}) = \sum_{i}^{N} s_i \left(q_i - c\right), \tag{1}$$

where c is the cost of providing resources of the ESP which is related to power consumption and hardware loss, etc.

2) In the second stage, the purchase strategy of miner i is s_i and the utility/profit function of i is:

$$U_i(\mathcal{S}, \mathcal{Q}) = \mu_i \nu_i \alpha_i^2 \left(R_f + R_p\right) + R_{\varepsilon,i} - q_i s_i - c_i, \tag{2}$$

where c_i is the cost of miner i.

Accordingly, at each stage, the problem can be formulated n in the following.

1) In the first stage, the game of the ESP aims at addressing problem (P1).

$$\begin{aligned} \textbf{P1}: \quad & \max_{\mathcal{Q}} U_i(\mathcal{S}, \mathcal{Q}), \\ \text{s.t.} \quad & q_i \in \left[q_{\min}, q_{\max}\right]. \end{aligned}$$

2) In the second stage, to maximize the profit of the miners, the optimization problem at miner i is formulated as

$$\begin{aligned} \textbf{P2}: \quad & \max_{\mathcal{S}} U_i(\mathcal{S}, \mathcal{Q}), \\ \text{s.t.} \quad & s_i \in \left[s_{\min}, s_{\max}\right]. \end{aligned}$$

C. Stackelberg Equilibrium

Based on our presented Stackelberg game model, we can bring the definition of the Stackelberg equilibrium (SE) as follows.

Definition 1. *Let $\mathcal{Q}^*$ be a solution for P1 and $\mathcal{S}^*$ denote a solution for P2, Then, the point $(\mathcal{S}^*, \mathcal{Q}^*)$ is a Stackelberg equilibrium for the game if for any $(\mathcal{S}, \mathcal{Q})$ the following conditions are fulfilled:*

$$\begin{aligned} U_{ESP}\left(\mathcal{S}^*, \mathcal{Q}^*\right) &\geq U_{ESP}\left(\mathcal{S}, \mathcal{Q}\right), \\ U_i\left(\mathcal{S}^*, \mathcal{Q}^*\right) &\geq U_i\left(\mathcal{S}, \mathcal{Q}\right). \end{aligned}$$

We can see that from the definition, a two-stage iterative algorithm is required to reach a SE. In the first stage, the ESP sets a price of the resources. Then, the miners can compete in a non-cooperative fashion in the second stage. After the NE is reached, the ESP will reset the price based on the purchase strategies of the miners. This two-stage update will iterate until the conditions in Definition 1 are satisfied. In this paper, we will apply the backward induction to find the SE of the formulated game [9].

IV. Incentive Mechanism for Mining

A. IR Scheme

1) Game of Miners in IR: At first, we study the existence of NE and then to provide the uniqueness. In the IR scheme, we assume the miners can successfully announce the solution after computing, which means $\nu_i = 1$. To simplify the calculation, in the follow, we use $u_{esp} = U_{ESP}(\mathcal{S}, \mathcal{Q})$, and $u_i = U_i(\mathcal{S}, \mathcal{Q})$, and we assume

$$R_c = R_f + R_p. \tag{3}$$

First, we will provide the proof of existence for NE under the considered game model. After some calculations, we can see that u_i is strictly convex with respect to s_i. Accordingly, we can arrive the following lemmas and theorems.

Lemma 1. *The strategy set $\mathcal{A}$ of this game is a non-empty convex and compact set, and the utility function is a continuous function.*

Proof. There are N pricing strategies of ESP in the first stage and there are N purchase strategies of miners in the second stage. Then the domain of all elements of this Stackelberg game is $A^{N\times N}$. As there is least one strategy, the solution set is a non-empty set. In addition, as we have proved, the utility function is a strictly convex function. We can also see the sets are convex sets. The domain of the set has its upper bound, which means it is a compact set. Moreover, we can easily observe that the function is continuous. □

Lemma 2. *The considered game is finite, i.e. the number of miners and ESP is denumerable, and the strategy set is limited.*

Proof. Due to the limited rewards in the generation of new block, there would be a finite number of game participants: ESP and miners. Although the demand sets of miners $\mathcal{S} = \{s_1, s_2...\}$ and the strategy set of ESP $\mathcal{Q} = \{q_1, q_2...\}$ may have infinite number of elements,as we have shown in the proof of Lemma 1, both of them are bounded closed sets. □

Theorem 1. *If the complete information static game is finite, i.e. the number of miners and ESP is denumerable, and the pure strategy involved is limited, then there must be at least one NE $(\mathcal{S}^*, \mathcal{Q}^*)$, where the profits of ESP and miners can reach optimum.*

Proof. Similar proof can be found in [7], due to limitation of the space, we omit here. □

We have shown the existence of the NE and next we can derive the uniqueness of the NE.

Theorem 2. *The defined utility functions have the fixed points.*

Proof. From Lemma 1, the strategy set $\mathcal{A}$ of this game is a non-empty convex and compact set, and the utility functions are continuous. Therefore, the defined utility functions must have the fixed points [6]. Due to the limitation of the space, detailed proof can be found in [6], so we omit here. □

Theorem 3. *The NE that obtains the optimal profits for miners and ESP must be the fixed point of the utility function [9].*

Proof. Similar proof can be found in [8], due to limitation of the space, we omit here. □

Next, we demonstrate the uniqueness of NE upon the method of Standard function [9]. First, we present the definition of Standard function.

Definition 2. *A general function $f(x)$ can be seen as a Standard function when it satisfy the conditions as follows:*

- *Positivity*

$$\forall x \in \mathrm{X}, f(x) > 0. \tag{4}$$

- *Monotonicity*

$$\forall x_1, x_2 \in \mathrm{X}, x_1 \le x_2, f(x_1) \le f(x_2). \tag{5}$$

- *Scalability*

$$\forall \rho > 1, x \in \mathrm{X}, f(\rho x) \le \rho . f(x). \tag{6}$$

Accordingly, in the following, we will prove that the strategy function is a Standard function. As we have shown in **Theorem 2** and **Theorem 3**, there are at least one NE and it is the fixed point. Then we have

$$(\mathbf{s}^*) = (f(s_1^*), f(s_2^*) ... f(s_N^*)). \tag{7}$$

For miner i, $f(s_i)$ is the purchase strategy. Then we set $\frac{\partial u_i}{\partial s_i} = 0$ and obtain

$$\sum_{j\in N} s_j = \sqrt{\frac{(\mu R_c + \varepsilon)\cdot \sum\limits_{j\neq i} s_j}{q}}. \tag{8}$$

As we know

$$s_i = \sum_{j\in N} s_j - \sum_{i\neq j} s_j, \tag{9}$$

and we can substitute (8) into (9) and get

$$s_i^* = f(s_i) = \sqrt{\frac{(\mu_i R_c + \varepsilon)\cdot \sum\limits_{i\neq j} s_j}{q_i}} - \sum_{i\neq j} s_j. \tag{10}$$

Then we can arrive the following lemma and theorem.

Lemma 3. *The strategy function of miner i is Standard function.*

Proof. We will prove the lemma according to the definition of Standard Function. As s_i is the purchase strategy of miner i and we have given the expression of $f(s_i)$ in (10), so we can obtain that:

$$\forall s_i \in \mathcal{S}, f(s_i) > 0. \tag{11}$$

Next, we assume that $s_1, s_2\,(s_1 \in \mathcal{S}, s_2 \in \mathcal{S})$ and $s_1 < s_2$, and after substituting it into (10), we can obtain that:

$$f(s_1) - f(s_2) = -\left(\sqrt{\sum_{j\neq 1} s_j} - \sqrt{\sum_{j\neq 2} s_j}\right)\sqrt{\frac{(\mu_i R_c + \varepsilon)}{q}} - \left(\sqrt{\sum_{j\neq 1} s_j} - \sqrt{\sum_{j\neq 2} s_j}\right)\left(\sum_{j\neq 2} s_j + \sum_{j\neq 1} s_j\right). \tag{12}$$

As $s_1 < s_2$, we can see $\sqrt{\sum_{j\neq 1} s_j} - \sqrt{\sum_{j\neq 2} s_j} > 0$, which means $f(s_1) - f(s_2) \leq 0$. Considering $\forall \rho > 1$, we have

$$\rho f(s_i) - f(\rho s_i) = (\rho - \sqrt{\rho})\sqrt{\frac{(\mu_i R_c + \varepsilon)\cdot \sum_{i\neq j} s_j}{q_i}} > 0. \tag{13}$$

Then, all the conditions of Standard function have been satisfied. □

Theorem 4. *If the strategy function of miner i is Standard function, and there must exist only one NE in the space of strategy set [9].*

We have proved the existence and uniqueness of NE of the second stage of the game. The existence and uniqueness of NE of the first stage can also be provided using similar approach. Then we can obtain the optimal strategy of miners by applying Karush-Kuhn-Tucker (KKT) conditions and Lagrangian method in the following steps.

From (8), we can obtain that:

$$\frac{q_i}{(\mu_i R_c + \varepsilon)} = \frac{\sum_{i\neq j} s_j}{\left(\sum_{j\in\mathcal{N}} s_j\right)^2}, \tag{14}$$

which equals to:

$$\sum_{j\in\mathcal{N}}\left(\frac{q_i}{\mu_i R_c + \varepsilon}\right) = (N-1)\frac{\sum_{j\in\mathcal{N}} s_j}{\left(\sum_{j\in N} s_j\right)^2}. \tag{15}$$

After some calculation, we have

$$\sum_{j\in\mathcal{N}} s_j = \frac{N-1}{\sum_{j\in\mathcal{N}} \frac{q_i}{\mu_i R_c + \varepsilon}}. \tag{16}$$

Then we substitute (8) into (16), and obtain

$$\sqrt{\frac{(\mu_i R_c + \varepsilon)\sum_{i\neq j} s_j}{q_i}} = \frac{N-1}{\sum_{j\in\mathcal{N}} \frac{q_i}{\mu_i R_c + \varepsilon}}. \tag{17}$$

Correspondingly, we can obtain the optimal strategy as follows,

$$s_i{}^* = \frac{N-1}{\sum_{j\in N} \frac{q_i}{\mu R_c + \varepsilon}} - \left(\frac{N-1}{\sum_{j\in N} \frac{q_i}{\mu R_c + \varepsilon}}\right)^2 \cdot \frac{q_i}{\mu R_c + \varepsilon}. \tag{18}$$

2) Game of ESP in IR: In the first stage, the pricing strategy of ESP depends on the service demand s_i. When we get the NE of the second stage, then we can try to find the best pricing strategy for ESP to obtain the optimal profits. After substituting (18) into (1), one can arrive

$$u_{esp} = (q_i - c_1)\frac{(N-1)\sum_{j\in\mathcal{N}}\left(e^{-\lambda t_i} R_c + \varepsilon\right)}{q_i} - (q_i - c_1)\frac{(N-1)^2\left(\sum_{j\in\mathcal{N}}\left(e^{-\lambda t_i} R_c + \varepsilon\right)\right)^2}{q_i\left(e^{-\lambda t_i} R_c + \varepsilon\right)}. \tag{19}$$

Then, with some calculations, we can see that the u_{esp} is also a convex function with respect to the q_i. Accordingly, there must be a $\mathcal{Q}^*$ which enables ESP to obtain the optimal profits. The proof of existence and uniqueness are similar to the ones in the second stage. With the optimal purchase strategy s_i^* of miner i, we will obtain the optimal pricing strategy q_i^*. In other words, under the combination of the strategy $(\mathcal{S}^*, \mathcal{Q}^*)$, both the miners and the ESP can achieve the optimal profit, which is essentially the SE of the game. We could then apply the KKT conditions and Lagrangian method to solve the P1 to find the optimal q_i^*.

In the IR scheme, the existence and uniqueness of NE of each stage of the formulated game model can be proved according to the presented theorems. The backward induction method is used to solve the SE of the two-stage Stackelberg game to obtain the global optimal solution. First, the optimal purchase strategy of the miners in the second stage is solved. Then we can obtain the pricing strategy of the ESP in the first stage.

B. SR Scheme

When miners decide to participate in mining, some of the miners may choose to temporarily hide their solutions of complex transactions due to the their stronger hash power. We assume rational miners who are with stronger hash power, i.e, a certain level of hash power, would tend to utilize the SR mining scheme instead of IR to get a better reward. However, the miner who would like to choose SR will suffer a higher risk as the other miners may report their solutions before it. In this work, we do not consider the situation of "orphan"-like to avoid the folk game with different branches. That is, although the miner i can obtain a better reward when choosing SR, it will suffer more risk to generate a chain of abandoned blocks.

Similar to the solution of the IR, we advocate the backward induction and first study the second stage.

1) Game of Miners in SR: After successfully mining block m, miner i who select the SR has the utility function that:

$$U_{i,m}{}^{SR}(\mathcal{S}, \mathcal{Q}) = \mu_i \nu_i m R_1 + \varepsilon\alpha_i - q_i s_i - c_i + \sum_{n=0}^{m-1} u_{i,n}^{SR}. \tag{20}$$

In the following, we also assume $u_{i,m}^{SR} = U_{i,m}^{SR}(\mathcal{S}, \mathcal{Q})$. First, we take the first order and second order derivatives of (20) with respect to s_i, and we can obtain

$$\frac{\partial {u_{i,m}}^{SR}}{\partial s_i} = 2e^{-\lambda t_i - \gamma\tau_i} mR_1 \alpha_i \frac{\sum\limits_{s\neq j} s_j}{\left(\sum\limits_{j\in\mathcal{N}} s_j\right)^2} + \varepsilon \frac{\sum\limits_{j\neq i} s_j}{\left(\sum\limits_{j\in\mathcal{N}} s_j\right)^2} - q_i, \tag{21}$$

$$\begin{aligned}\frac{\partial^2 {u_{i,m}}^{SR}}{\partial {s_i}^2} &= 2e^{-\lambda t_i - \gamma\tau_i} mR_1 \left(\frac{\partial \alpha_i}{\partial s_i}\right)^2 \\ &+ \left(2e^{-\lambda t_i - \gamma\tau_i} mR_1 \alpha + \varepsilon\right) \frac{\partial^2 \alpha_i}{\partial s_i^2}\end{aligned} \tag{22}$$

We assume a content-specified function, and can arrive

$$\begin{aligned}\frac{\partial^2 {u_{i,m}}^{SR}}{\partial {s_i}^2} &< 2e^{-\lambda t_i - \gamma\tau_i} mR_1 \left(\frac{\partial \alpha_i}{\partial s_i}\right)^2 + 2e^{-\lambda t_i - \gamma\tau_i} mR_1 \frac{\partial^2 \alpha_i}{\partial s_i^2} \\ &< 2e^{-\lambda t_i - \gamma\tau_i} mR_1 \left(\left(\frac{\partial \alpha_i}{\partial s_i}\right)^2 + 2\frac{\partial^2 \alpha_i}{\partial s_i^2}\right) = \omega\end{aligned} \tag{23}$$

which equals to

$$\omega = 2e^{-\lambda t_i - \gamma\tau_i} mR_1 \frac{\sum\limits_{j\neq i} s_j \left(\sum\limits_{j\neq i} s_j - 4\sum\limits_{j\in\mathcal{N}} s_j\right)}{\left(\sum\limits_{j\in\mathcal{N}} s_j\right)^4} < 0. \tag{24}$$

Then, we can conclude that $\frac{\partial^2 u_2}{\partial {s_i}^2} < 0$, which means the utility function is convex. When we set $\frac{\partial u_2}{\partial s_i} = 0$ and obtain that:

$$2e^{-\lambda t_i - \gamma\tau_i} mR_1 \alpha_i \frac{\sum\limits_{j\neq i} s_j}{\left(\sum\limits_{j\in\mathcal{N}} s_j\right)^2} + \varepsilon \frac{\sum\limits_{j\neq i} s_j}{\left(\sum\limits_{j\in\mathcal{N}} s_j\right)^2} - q_i = 0. \tag{25}$$

By substituting (9) into (25), we can obtain

$$\begin{aligned}&2e^{-\lambda t_i - \gamma\tau_i} mR_1 s_i^2 + \left(\varepsilon\left(\sum_{j\in\mathcal{N}} s_j\right) - 2e^{-\lambda t_i - \gamma\tau_i} mR_1\right) s_i \\ &- \left(\varepsilon\left(\sum_{j\in\mathcal{N}} s_j\right)^2 - q\left(\sum_{j\in\mathcal{N}} s_j\right)^3\right) = 0.\end{aligned} \tag{26}$$

Then we assume a content-specified function $l(s)$, set the equation $\theta = \sum\limits_{j\in N} s_j$, and we can obtain that $\sum\limits_{j\neq i} s_j = \theta - s_i$, and

$$\begin{aligned}l(s_i) &= 2mR_1 e^{-\lambda t_i - \gamma\tau_i} s_i^2 + \left(\varepsilon\theta - 2mR_1 e^{-\lambda t_i - \gamma\tau_i}\theta\right) s_i \\ &- \left(\varepsilon\theta^2 - q\theta^3\right).\end{aligned} \tag{27}$$

When we set the equation $l(s_i) = 0$, and we can see that the discriminant is

$$\begin{aligned}\Delta &= \left(\varepsilon\theta - 2mR_1 e^{-\lambda t_i - \gamma\tau_i}\theta\right)^2 + 8mR_1 e^{-\lambda t_i - \gamma\tau_i}\left(\varepsilon\theta^2 - q\theta^3\right) \\ &> \theta\left(4mR_1 e^{-\lambda t_i - \gamma\tau_i}\left(mR_1 e^{-\lambda t_i - \gamma\tau_i} + \varepsilon - 2q\theta\right)\right).\end{aligned} \tag{28}$$

Meanwhile, under the condition of the axis of symmetry $s_i = \frac{\varepsilon t_i - 2mR_1 e^{-\lambda t_i - \gamma\tau_i} t}{-4mR_1 e^{-\lambda t_i - \gamma\tau_i}} > 0$, that is the axis of symmetry is the right of the origin. According to Vieta Theorem, it can be known that the relation between the two roots is $s_i^1 s_i^2 = \frac{\varepsilon t^2 - qt^3}{2mR_1 e^{-\lambda t_i - \gamma\tau_i}} < 0$, then we can see that equation $l(s_i) = 0$ has only one positive root. Also, we assume $s_i^2 > s_i^1$ when the domain of strategy is $s_i \in [s_{\min}, s_{\max}]$, there must be only one root

$$s_i^2 = \frac{-\phi_i + \sqrt{\phi_i^2 + 8mR_1 e^{-\lambda t_i - \gamma\tau_i}\left(\varepsilon t^2 - qt^3\right)}}{4mR_1 e^{-\lambda t_i - \gamma\tau_i}} > 0, \tag{29}$$

which makes condition $\frac{\partial u_{i,m}^{SR}}{\partial s_i} = 0$ satisfied, and $\phi_i = \left(\varepsilon t_i - mR_1 e^{-\lambda t_i - \gamma\tau_i} t_i\right)$. Therefore, the optimal purchase strategy for the miner who chooses the SR is found in (30). Under the condition of shared hash power, we can conclude

$$\alpha_i^* \geq \frac{2q_i s_i^*}{mR_1 e^{-\lambda t_i - \gamma\tau_i} + \varepsilon}. \tag{31}$$

Then miner i can obtain optimal profit $u_{i,m}^{SR}$:

$$u_{i,m}^{SR} = e^{-\lambda t_i - \gamma\tau_i} \alpha_i^{*2} mR_1 + \varepsilon\alpha_i^* - q_i s_i^* - c + \sum_{n=0}^{m-1} u_{i,n}^{SR}. \tag{32}$$

Then, we take the first order and second order derivatives of (32) with respect to α_i,

$$\frac{\partial u_{i,m}^{SR}}{\partial \alpha_i} = 2e^{-\lambda t_i - \gamma\tau_i} mR_1 \alpha_i + \varepsilon > 0, \tag{33}$$

$$\frac{\partial^2 u_i^{SR}}{\partial \alpha_i^2} = 2e^{-\lambda t_i - \gamma\tau_i} mR_1 > 0. \tag{34}$$

Thus, for the miner who chooses the strategy to report the solution strategically, higher the proportion of computational resource leads to a higher reward.

2) Game of ESP in SR: In the first stage, we can substitute the optimal strategy (30) into ESP's utility function (1), we can obtain (35). Then, we take the first order and second order derivatives of (35) with respect to q_i, then we would conclude that the utility function u_{esp} of the ESP is strictly convex. Therefore, according to the previous analysis, there is a NE of the game. According to (32), we can obtain the optimal mining strategy $\mathcal{S}^*$ for miner i and we could obtain the optimal pricing strategy $\mathcal{Q}^*$ for ESP by applying the KKT condition. The method of backward induction is used to seek the SE to maximize the profit of participants of the overall game.

$$s_i^* = \frac{-\left(\varepsilon t - mR_1 e^{-\lambda t_i - \gamma\tau_i} t\right) + \sqrt{\left(\varepsilon t - mR_1 e^{-\lambda t_i - \gamma\tau_i} t\right)^2 + 8mR_1 e^{-\lambda t_i - \gamma\tau_i}\left(\varepsilon t^2 - q t^3\right)}}{4mR_1 e^{-\lambda t_i - \gamma\tau_i}}. \tag{30}$$

$$u_{esp} = (q_i - c)\frac{\left(2e^{-\lambda t_i-\gamma\tau_i} mR_1 - \varepsilon\left(\sum_{j\in\mathcal{N}} s_j\right)\right) + \sqrt{\left(\varepsilon\left(\sum_{j\in\mathcal{N}} s_j\right) - 2e^{-\lambda t_i-\gamma\tau_i} mR_1\right)^2 + 8e^{-\lambda t_i-\gamma\tau_i} mR_1\left(\varepsilon\left(\sum_{j\in\mathcal{N}} s_j\right)^2 - q\left(\sum_{j\in\mathcal{N}} s_j\right)^3\right)}}{4e^{-\lambda t_i-\gamma\tau_i} mR_1} \tag{35}$$

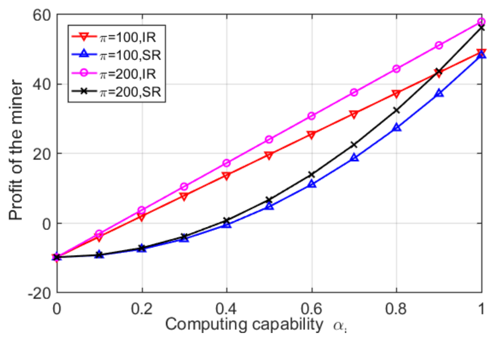

Fig. 1: Computing capability vs. profits

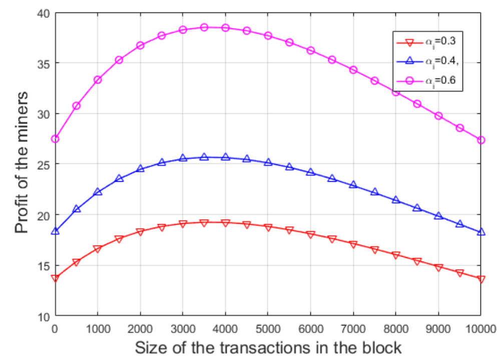

Fig. 2: Size of the transaction block vs. the profits

V. Performance Evaluation

To simplify the evaluation, we assume the miner has no hash power, which means that all the hash power should be purchased from the ESP. Some simulation parameters are from [3]. Fig. 1 presents the relations between the computing capability α_i and the profit of the miner. It can be found that, for the IR scheme, as we consider the probability of successful reporting is 1, it has a better performance than the SR scheme. It is mainly due to the fact that in the SR scheme, the miner has to buy more resources due to the competition, which induce higher cost. It can also be found that the profit increases as the size of block gets bigger.

In Fig. 2, we plot the impact of the size of the transaction in each block on the profit of the miners. In this figure, the performance of IR scheme is presented. As we can see, as the size of the block increases, the profits first become larger, then decrease after reaching the maximum value. When the size of block increases, the time and complexity of computing PoW are incremental. Therefore, after reaching the maximum, the cost dominates the performance of profit no matter what kind of computing capability is considered. Moreover, when computing capability increases, the performance get better.

VI. Conclusion

In this paper, we have investigated the incentive mechanism under edge computing-enabled blockchain. We have formulated a two-stage Stackelberg game model to maximize the profits of both ESP and miners under the two mining schemes. Then, the optimal solutions are presented and backward induction is introduced to find the Stackelberg equilibria. Performance evaluation demonstrate the effectiveness of the proposed inventive mechanism.

VII. Acknowledgment

This work is supported by Academy of Finland (No. 331694, 325692), NSF of Hebei (No. E2017203351) and Key Research and Development Project of Hebei (No. 19252106D).

References

[1] P. K. Sharma, S. Singh, Y. Jeong, and J. H. Park, "Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks," *IEEE Communications Magazine*, vol. 55, pp. 78-85, Sept. 2017.

[2] N. C. Luong, Z. Xiong, P. Wang, and D. Niyato, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," *Proc. IEEE ICC*, Kansas City, May 2018.

[3] Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maximization auction in edge computing resource allocation for mobile blockchain," *Proc. IEEE ICC*, Kansas City, May 2018.

[4] Z. Xiong, et al, "Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4585-4600, June. 2019.

[5] N. Houy, "The Bitcoin Mining Game". *Ledger*, vol. 1, pp. 53-68, 2016.

[6] D. Gale, "The game of hex and the brouwer fixed-point theorem," *American Mathematical Monthly*, vol. 86, no. 10, Dec. 1979.

[7] B. Liu, "Stackelberg-nash equilibrium for multilevel programming with multipe followers using genetic algorithms," *Computers Math*, vol. 36, no. 7, pp. 79-89, Oct. 1998.

[8] K. Etessami and M. Yannakakis, "On the complexity of nash equilibria and other fixed points," *SIAM Journal on Computing*, vol. 39, no. 6, pp.2531-2597, 2010.

[9] Z. Han, D. Niyato, W. Saad, T. Baar, and A. Hjrungnes, Game Theory in Wireless and Communication Networks Theory, Models, and Applications. Cambridge University Press, NY, 2000.