An Incentive Mechanism for Building a Secure Blockchain-Based Internet of Things

Xingjian Ding, Jianxiong Guo, Deying Li, and Weili Wu, *Senior Member, IEEE*

***Abstract*—The world-changing blockchain technique provides a novel method to establish a secure, trusted, and decentralized system for solving the security and personal privacy problems in the Internet of Things (IoT) applications. As the mining process in blockchain requires high computational power, the lightweight IoT devices need to purchase computational resources from edge servers and thus can offload their computational tasks. The amount of computational resource purchased by IoT devices depends on how many profits they can get in the mining process, and will directly affect the security of the blockchain network. The security of the blockchain is closely related to the profits of the blockchain platform. Actually, there is a trade-off between blockchain security and the profits of the blockchain platform. In this paper, we investigate the incentive mechanism for the blockchain platform to attract IoT devices to purchase more computational power from edge servers to participate in the mining process, thereby building a secure blockchain network while guaranteeing the profits of the blockchain platform. We model the interaction between the blockchain platform and IoT devices as a two-stage Stackelberg game, where the blockchain platform act as the leader, and IoT devices act as followers. We analyze the existence and uniqueness of the Stackelberg equilibrium, and propose an efficient algorithm to compute the Stackelberg equilibrium point. Furthermore, we evaluate the performance of our algorithm through extensive simulations, and analyze the strategies of the blockchain platform and IoT devices under different situations.**

***Index Terms*—Internet of things, blockchain, cloud mining, incentive mechanism, Stackelberg game.**

I. Introduction

CURRENTLY, Internet of Things (IoT) has attracted more and more attention in many areas, such as smart cities, agriculture, health care, industry, etc. Especially in the smart factory area [1], IoT provides interconnection to smart factories by connecting different types of industrial machines and devices, which helps to realize intelligent manufacturing. To deal with the huge number of IoT devices, a traditional centralized architecture is applied to provide services for IoT devices, where IoT devices are connected to a cloud server through the internet. With the rapid growth of the number of IoT devices and the performance requirement of the IoT applications, however, the traditional centralized IoT architecture faces many challenges, such as security, personal privacy, bandwidth constraint, and service delay [2]. To avoid these issues, some works introduce decentralized peer-to-peer (P2P) architectures for IoT applications [3]–[5], where each device can exchange information or trade directly with other devices without a third-party organization. However, these P2P architectures are still faced with security and personal privacy issues.

In the past few years, the world-changing technology, blockchain, provides an effective way to solve the above issues, due to its inherent security and privacy protection properties, and has been widely used in IoT applications [6]–[9]. There are many types of blockchains based on different consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Directed Acyclic Graph (DAG). In this paper, we consider that the PoW consensus mechanism is adopted when constructing an IoT blockchain. The reason is that PoW is by far the most mature consensus mechanism, which has been verified on the Bitcoin system [10] for years. While PoS is affected by the Matthew effect, where the rich get richer phenomenon will happen [11]; PBFT has poor scalability and high latency [12]; DAG-based blockchain is vulnerable to double-spending attacks [13], and facing the threat of spam attacks and denial of service attacks [14]. Under the PoW consensus mechanism, participants (miners) of the blockchain need to compete with each other to solve a hash puzzle, which is very costly to get the right answer but easy to be validated. The winner has the right to generate a new block and will get a reward from the blockchain platform (the process is called *mining*). However, PoW consumes too much computing resources, which prevents IoT devices from directly joining the construction of the blockchain. Fortunately, the edge computing architecture makes it possible for IoT applications to establish a blockchain network, where IoT devices can offload the computational tasks to edge servers [15]–[18]. Specifically, incentivized by the reward from the platform for packeting a new block, each IoT device will purchase a certain amount of computational resources (such as CPU and GPU) from edge servers to participate in the mining process for maximizing its own profit.

Manuscript received July 21, 2020; revised August 31, 2020 and September 28, 2020 and October 23, 2020; accepted November 22, 2020. Date of publication November 25, 2020; date of current version March 17, 2021. This work was supported by the National Natural Science Foundation of China (Grants 12071478, 11671400), and partially by National Science Foundation 1907472. Recommended for acceptance by Dr. Di Wu. *(Corresponding author: Deying Li.)*

Xingjian Ding and Deying Li are with the School of Information, Renmin University of China, Beijing 100872, China (e-mail: dxj@ruc.edu.cn; deyingli@ruc.edu.cn).

Jianxiong Guo and Weili Wu are with the Department of Computer Science, Erik Jonsson School of Engineering and Computer Science, University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: jianxiong.guo@utdallas.edu; weiliwu@utdallas.edu).

Digital Object Identifier 10.1109/TNSE.2020.3040446

For the blockchain platform, one of the most important property is security. A more secure blockchain network will attract more IoT devices to join in, thereby generating more transactions. The blockchain platform charges a certain transaction fee for each transaction. Therefore, the security of the blockchain network is closely related to its benefits. The better the security, the more the benefits got by the platform. For the blockchain with the PoW consensus mechanism, its security mainly depends on the total computational power of the entire network. An attacker who wants to tamper with the context in a block of the blockchain needs to solve the hash puzzle faster than the current whole network. Thus, it's much harder for attackers to modify the blocks if all miners provide more computational power for the blockchain network. The blockchain platform will give a reward to those who generate a new block, so as to attract IoT devices (miners) to purchase more computational resources from edge servers. If the reward is too small, it will not attract miners to purchase enough computational resources, which will make the blockchain not sufficiently secure. If the reward is too large, the cost of the platform will increase, and the platform will get fewer profits or even make a loss. Thus, there exists a trade-off between blockchain security and profits of the platform.

In this paper, therefore, we study the incentive mechanism of the blockchain platform to motivate IoT devices to purchase more computational resources to participate in the mining process, so that a secure blockchain network can be established while the profits of the blockchain platform can be guaranteed. The main contributions of this paper are listed as follows.

- By considering the trade-off between blockchain security and profits of the platform, we design an incentive mechanism for the IoT blockchain platform to attract IoT devices to purchase more computational power from edge servers. Thereby building a secure blockchain network while guaranteeing the profits of the blockchain platform.
- We analyze the relationship between the security of the blockchain network and the total computational power of the entire network, and give the probability that an attacker can successfully tamper with the blockchain.
- We formulate the interaction between blockchain platform and miners as a two-stage Stackelberg game. We analyze the existence and uniqueness of the Stackelberg equilibrium, then propose an efficient algorithm to compute the Stackelberg equilibrium point.
- We conduct extensive simulations to evaluate the performance of our proposed algorithm, and we analyze the strategies of platform and miners in different situations. Our work is helpful for the IoT blockchain platform to set a reasonable reward pricing strategy to maximize its utility, which is closely related to the security of the blockchain network.

The remainder of this paper is structured as follows. In Section II, we introduce the related works of this paper. In Section III, we describe the system model and analyze the blockchain security that motivated our problem, and then we formulate our problem as a two-stage Stackelberg game. In Section IV, we analyze the existence and uniqueness of the Stackelberg equilibrium, and give the best strategies for miners and blockchain platform. We conduct extensive performance evaluations in Section V. And finally, we conclude this paper in Section VI.

II. Related Works

Recently, there are numerous works that concentrate on IoT blockchain networks. Hassan *et al.* [19] discuss the integration of blockchain in a smart energy system, their work is helpful in developing flexible blockchain platforms for the smart energy system. Mollah *et al.* [20] investigate the application of blockchain technology in the Internet of Vehicles (IoV), they point out several key challenges in applying blockchain in IoV, and introduce some related works for solving these challenges. Xu *et al.* [21] propose a blockchain-based fair nonrepudiation network computing service provisioning scheme for IoT, in which the blockchain is used as a service publication proxy and an evidence recorder. The massive data of IoT applications can be stored on remote servers with network storage technology, and it is a critical challenge to ensure the security and integrity of the data. Some studies deal with the challenge with blockchain technology. Xu *et al.* [22] propose a blockchain-based decentralized arbitrable remote data auditing scheme for network storage service, in which they use the smart contact to solve the data possession disputes. The authors in [23] propose a deduplicatable data auditing mechanism for network storage services based on blockchain technology. Their design could meet the security requirements of network storage services and meanwhile improve the scalability of the system.

Moreover, there are a series of works study the blockchain from the aspect of auction or game theory. Sun *et al.* [24] consider a multi-task cross-server resource allocation scenario in blockchain-based mobile edge computing, they model the interaction between edge servers and mobile devices as a double auction, and propose two double auction mechanisms. Yao *et al.* [25] model the resource management and pricing problem as a Stackelberg game, and they design a multiagent reinforcement learning algorithm to search the near-optimal policy. Jiao *et al.* [26] propose an auction-based market model for the trading between the cloud computing service provider and miners. Their purpose is to efficiently allocate computing resources to maximize the social welfare. Wang *et al.* [27] propose a blockchain and double auction mechanism-based decentralized electricity transaction mode for microgrids, to achieve secure and quick electricity transactions. Xiong *et al.* [28] formulate the interaction between the cloud providers and miners as a Stackelberg game, and apply backward induction to analyze the equilibria in each sub-game. Chang *et al.* [29] formulate a two-stage Stackelberg game between the edge service provider and miners, and they aim to find the Stackelberg equilibrium under two different mining schemes. However, most of the above works only consider the interaction between the cloud servers and miners, and none of them consider the profits brought by blockchain security from the

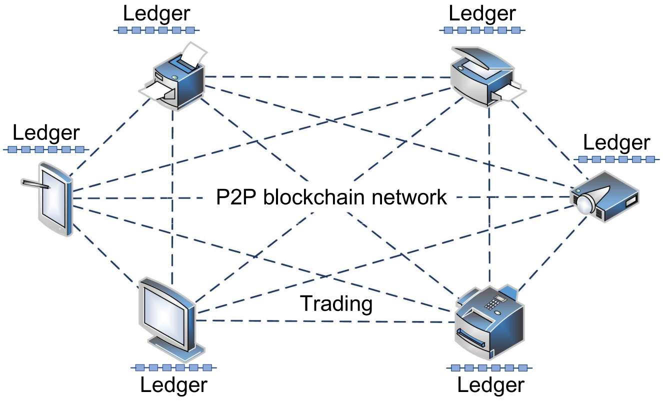

Fig. 1. The P2P blockchain network structure [30].

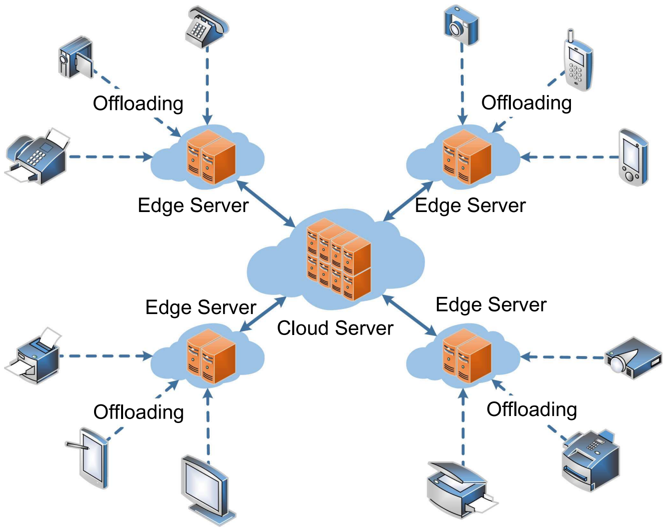

Fig. 2. The architecture of edge computing [31].

perspective of the blockchain platform, which is fundamentally different from our work.

III. System Model and Problem Formulation

In this section, we first introduce the edge computing system of the IoT blockchain network. We then analyze the security of the blockchain network. Finally, we formulate the incentive problem between the blockchain platform and miners.

A. System Model

In the blockchain network, the core problem is to achieve a distributed consensus. Satoshi Nakamoto proposed the PoW consensus protocol in 2008 which is used for Bitcoin [10]. In the PoW consensus, the users who want to generate a new block need to solve a hash puzzle, which is very costly to be addressed but easy for others to verify. This process is called mining, and these users are termed as miners. These miners compete with each other to solve a hash puzzle, the one who first solve the hash puzzle has the right to generate a new block and will get a reward from the blockchain platform.

For the IoT blockchain network, the lightweight IoT devices cannot directly participate in the mining process due to the limited computational capability. Incentivized by the reward from the blockchain platform, IoT devices will purchase computation resources from edge servers, each edge server offers its own unit price for computational resources. As shown in Fig. 1, the blockchain network is maintained by all of the IoT devices. As for the mining process, each miner will offload its computational task to the edge server to compete with others, as shown in Fig. 2. The probability of each miner winning the competition depends on the amount of computational resource it purchased. All the miners purchase computational resources with the goal of maximizing their own profits.

B. Blockchain Security

Blockchain is a list of blocks that are linked by block hash value, and each block record a set of transactions. More specifically, a block contains two parts: block content and block header. The block content is the details of transactions information, which records all the inputs and outputs of each transaction. The block header consists of the previous block hash value, which is used as a cryptographic link that creates the chain, a version number that used for tracking for software or protocol updates, a timestamp that records the time at which the block is generated, a Merkle tree root of all the transactions, a hash threshold value that records the current mining difficulty, and a nonce, which is used for solving the PoW puzzle.

The blockchain starts with a genesis block which is given by the blockchain platform, and all subsequent blocks will put some previously generated block's hash value into their block header. Miners compete with each other to solve a hash puzzle, the one who first solve the puzzle has the right to generate a new block, and new blocks will be added behind the genesis block. Forks may happen when multiple miners solve the hash puzzle at the same time, thus each user maintains the blocks in the form of a block tree [32]. According to the longest chain principle [10], each user will choose the longest branch in the block tree as the current blockchain, as shown in the left part of Fig. 3.

For a blockchain miner, to get the right to generate a new block, it needs to solve a hash function (PoW puzzle), that is, it needs to find a nonce and record it in the block header such that the hash value of the block header is less than the hash threshold. As the hash function has no back door, the only way to find such a nonce is to run many hash operations. The difficulty of the PoW puzzle is determined by the given hash threshold value, which is a 256-bit binary number that starts with a certain number of consecutive zeros (difficulty). For example, if the hash threshold starts with 60 consecutive zeros, the probability of finding the correct nonce by performing a hash operation is 2^{-60}, which means that it takes an average of 2^{60} hash operations to solve the PoW puzzle. To stabilize the growth rate of the blockchain, the platform will dynamically adjust the difficulty of the PoW puzzle based on the total computational power of the whole blockchain network. Take the bitcoin blockchain as an example, the difficulty of the PoW puzzle will

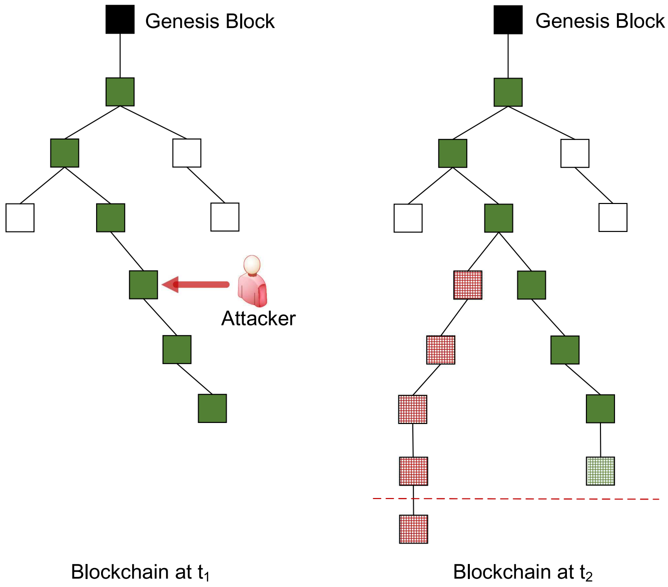

Fig. 3. Attackers tamper with the blockchain by winning the block mining race.

be updated every 2 weeks to ensure that it takes 10 minutes (on average) for the blockchain to generate a new block[33].

Assume that an attacker wants to tamper with the context of a block, the change of the context will change the hash value of the block, so the attacker needs to find a new nonce to solve the PoW puzzle of this block. Moreover, as each block contains the hash value of the previous block, the change of a block context will change all the subsequent blocks, so the attacker should find the nonce for every subsequent block. In fact, the attacker needs to fork a new branch, and start a block mining race against other miners of the network. The attacker successfully tamper with the blockchain once the attacker wins the race, as the new branch forked by the attacker becomes the longest one in the block tree. As shown in Fig. 3.

Now we analyze the probability of success of an attacker. Assume that the total computational power of the blockchain network is H by the hash rate, and the attacker's computation power is h. Then the probability an honest miner finds the next block can be denoted by $p = \frac{H-h}{H}$, and the probability that the attacker finds the next block is $q = \frac{h}{H}$. According to [34], the probability that the attacker will ever win the race from z blocks behind can be calculated by

$$P(z) = \begin{cases} 1, & \text{if } q \geq \frac{1}{2}, \\ I_{4pq}(z, \frac{1}{2}), & \text{otherwise}, \end{cases} \tag{1}$$

where $I_x(u, v)$ is the regularized incomplete beta function:

$$I_x(u, v) = \frac{\Gamma(u+v)}{\Gamma(u)\Gamma(v)} \int_0^x t^{u-1}(1-t)^{v-1}\, dt, \tag{2}$$

and $\Gamma(\cdot)$ is the gamma function.

Consider that an attacker's computational power is $h = 1\ TH/s$, and he wants to tamper with the context of the 4th block from the blockchain tip. Fig. 4 shows the probability of the success of the attacker against the total computational power of the network. It can be seen that as the total computational power of the network increases, the probability that the attacker successfully tamper with the blockchain significantly decreases. Specifically, when $H = 10\ TH/s$, $P(4) = 0.387\%$; when $H = 20\ TH/s$, $P(4) = 0.033\%$. The probability of the success of the attacker is reduced by more than 10 times if we double the computational power of the entire network. The result suggests that the larger the computational power of the whole blockchain network, the harder it is for the attacker to tamper with the blockchain, and thus the more secure the blockchain network will be.

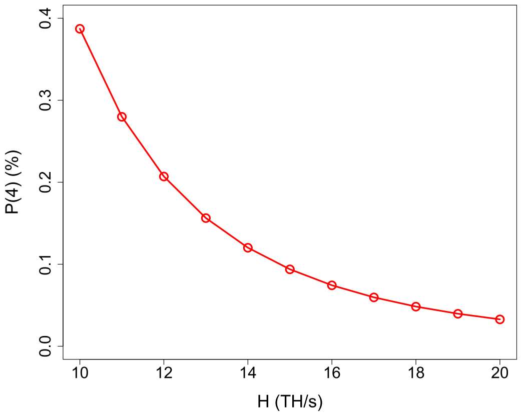

Fig. 4. The probability that an attacker will ever win the race from 4 blocks behind.

C. Problem Description

We first show the notations that used in our problem description in Table I.

As described before, the blockchain platform provides certain rewards to incentivize miners to participate in the mining process, and each miner purchase computational resources from its nearby edge server for getting more profits.

For the blockchain platform, the revenue is mainly derived from the transaction fees. We assume that the average transaction fees in a block is B. The platform will give a reward R to the miner who packaging a new block. Note that the reward R should be no larger than B, otherwise the blockchain cannot maintain perpetual operation. As discussed in Section III-B, the total computational power will significantly affect the blockchain security, so the blockchain platform will get benefit from the huge computational power provided by the miners. As shown in Fig .4, the decrease speed of the probability that an attacker successfully tamper with the blockchain slows down as the total computational power of the entire network increases. Moreover, the blockchain security cannot bring unlimited profits, and with the improvement of blockchain security, the increase in profits will become smaller. Therefore, we use the *sigmoid function* to describe the profits brought by the total computational power of the entire network. Then we define a utility function U to make a trade-off between blockchain security and profits of the blockchain platform.

$$U = \alpha \cdot \left[\sigma\left(\beta \cdot \sum_{s_i \in S} \mu_i\right) - \frac{1}{2}\right] - R, \tag{3}$$

TABLE I
NOTATIONS FOR PROBLEM DESCRIPTION

Notation	Description
S	The set of IoT devices (miners), $S = \{s_1, s_2, \ldots, s_n\}$
U	The utility of the blockchain platform
μ_i	The amount of computational power purchased by device s_i
$\sigma(\cdot)$	The *sigmoid function* that defined as $\sigma(x) = \frac{1}{1+e^{-x}}$
R	The amount of reward given by blockchain platform
B	The average transaction fee of a block
N	The number of new blocks generated per day
p_i	The probability that s_i winning the competition among all miners in solving the PoW puzzle
P_i	Expected profit of miner s_i in one day
λ_i	Unit price of the computational power purchased by s_i
$\boldsymbol{\mu}$	Strategies of all miners, $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_n\}$
$\boldsymbol{\mu_{-i}}$	Strategies of all miners except s_i, $\boldsymbol{\mu_{-i}} = \{\mu_1, \mu_2, \ldots, \mu_{i-1}, \mu_{i+1}, \ldots, \mu_n\}$

where S is the miners set, μ_i is the computational power provided by the $i\text{-}th$ miner, $\sigma(\cdot)$ is the *sigmoid function* that defined as $\sigma(x) = \frac{1}{1+e^{-x}}$, $\alpha > 1$ is a constant parameter that controls the importance of the total computational power, and $0 < \beta < 1$ is a constant parameter that controls the convergence rate of the sigmoid function.

For the miners, consider there are a set S of IoT devices that are interested in participating in the mining process, where $S = \{s_1, s_2, , s_n\}$. Each miner $s_i \in S$ will purchase μ_i computational power from edge servers to compete with others in pursuit of a maximum financial profit. According to the principle of the PoW consensus protocol, the speed of a miner for solving the hash puzzle depends on the number of hash operations it can perform per unit of time, that is, its computational power. Therefore, the miner who purchases the most computational power is most likely to solve the PoW puzzle first. We use p_i to denote the probability that miner s_i winning the competition among all miners in solving the PoW puzzle, p_i can be defined as

$$p_i = \frac{\mu_i}{\sum_{s_j \in S} \mu_j}. \tag{4}$$

The unit price of the computational power purchased by miners may be different, as they purchase computational power from different edge servers. Assume that the unit price of the computational power purchased by s_i is λ_i per day. We also assume that the blockchain will generate an average of N new blocks per day. Then the expected reward that miner s_i can get in a day is $p_i RN$, and its cost is $\lambda_i \mu_i$. We use P_i to represent the expected profit got by miner s_i in one day, then P_i can be calculated as follows,

$$P_i = p_i RN - \lambda_i \mu_i. \tag{5}$$

Both the blockchain platform and miners will dynamically adjust their strategies to get the maximum profit. We model the interaction between the blockchain platform and miners as a two-stage Stackelberg game. In the upper stage, the blockchain platform sets the reward to incentivize miners to participate in the mining process. In the lower stage, miners decide the optimal amount of computational power they purchase. We formulate the optimization problems for the blockchain platform and miners as follows.

We first introduce the lower stage of the game. Given the reward R of the blockchain platform and other miners' strategies $\boldsymbol{\mu_{-i}}$, where $\boldsymbol{\mu_{-i}} = \{\mu_1, \mu_2, , \mu_{i-1}, \mu_{i+1}, , \mu_n\}$. The miner s_i decides the amount of computational power μ_i it purchased to maximize its own profit. This sub-game problem can be written as follows.

Problem 1: miners' sub-game.

$$\begin{aligned} \max_{\mu_i} \quad & P_i(\mu_i | \boldsymbol{\mu_{-i}}, R) \\ s.t. \quad & \mu_i \geq 0 \end{aligned}$$

For the upper stage of the game, the blockchain platform will dynamically adjust the reward R to maximize its utility. As defined in equation (3), the utility of the blockchain platform is directly related to the strategies $\boldsymbol{\mu}$ of miners, where $\boldsymbol{\mu} = \{\mu_1, \mu_2, , \mu_n\}$, and the reward R. This sub-game can be formulated as follows.

Problem 2: blockchain platform's sub-game.

$$\begin{aligned} \max_{R} \quad & U(R, \boldsymbol{\mu}) \\ s.t. \quad & 0 \leq R \leq B \end{aligned}$$

Problem 1 and Problem 2 together form a Stackelberg game. The object of the game is to find a *Stackelberg equilibrium* point where neither the leader (blockchain platform) nor the followers (miners) want to change their strategies. In this paper, the Stackelberg equilibrium can be defined as follows.

Definition 1: Let $\boldsymbol{\mu}^*$ and R^* be the optimal strategies of miners and blockchain platform, respectively, where $\boldsymbol{\mu}^* = \{\mu_1^*, \mu_2^*, , \mu_n^*\}$. Then, the point $(\boldsymbol{\mu}^*,\ R^*)$ is the Stackelberg equilibrium point if it satisfies the following two conditions,

$$U(R^*, \boldsymbol{\mu}^*) \geq U(R, \boldsymbol{\mu}^*), \forall\ 0 \leq R \leq B, \tag{6}$$

and

$$P_i(\mu_i^* | \boldsymbol{\mu_{-i}^*}, R^*) \geq P_i(\mu_i | \boldsymbol{\mu_{-i}^*}, R^*), \forall i, \forall \mu_i \geq 0, \tag{7}$$

where $\boldsymbol{\mu_{-i}^*} = \boldsymbol{\mu}^* \backslash \{\mu_i^*\}$.

IV. GAME ANALYSIS FOR THE INCENTIVE MECHANISM

In this section, we analyze the existence and the uniqueness of the Stackelberg equilibrium of our proposed Stackelberg game. We first analyze the lower stage of the game, in which we aim to find the *Nash equilibrium* for the miners' sub-game. Based on the analysis of the lower stage, we then analyze the utility maximization of the blockchain platform's sub-game in the upper stage.

A. Analysis of the Miners' Sub-Game

After the blockchain platform set the reward R for miners, all of the miner will dynamically adjust their strategies to get the maximum profits until reach a Nash equilibrium. In the following, we will prove that the Nash equilibrium point exists in the miners' sub-game through a theorem.

Theorem 1: The Nash equilibrium point exists in the miners' sub-game.

Proof: For the miners' sub-game, the object function $P_i(\cdot)$ is defined in $[0, \infty)$. From equation (5), we can know that $\mu_i \leq \frac{RN}{\lambda_i}$, otherwise, the profit of miner s_i will be negative. Thus μ_i is continuously chosen in $[0, \frac{RN}{\lambda_i}]$, which is a nonempty, convex and compact subset of the Euclidean space. Next, we calculate the first order and second order derivatives of function $P_i(\cdot)$.

$$\frac{\partial P_i}{\partial \mu_i} = RN \frac{\sum_{s_j \in S} \mu_j - \mu_i}{\left(\sum_{s_j \in S} \mu_j\right)^2} - \lambda_i, \tag{8}$$

$$\frac{\partial^2 P_i}{\partial \mu_i^2} = \frac{\partial(\frac{\partial P_i}{\partial \mu_i})}{\partial \mu_i} = -2RN \frac{\sum_{s_j \in S} \mu_j - \mu_i}{\left(\sum_{s_j \in S} \mu_j\right)^3} \leq 0. \tag{9}$$

Therefore, $P_i(\cdot)$ is a strictly concave function, and we then conclude that the Nash equilibrium point exists in the miners' sub-game. ■

As $P_i(\cdot)$ is a strictly concave function with μ_i, given the reward R of the blockchain platform and other miners' strategies $\boldsymbol{\mu_{-i}}$, miner s_i has a unique best strategy u_i, and it can be achieved when the first order derivative of $P_i(\cdot)$ equals to 0, i.e.,

$$\frac{\partial P_i}{\partial \mu_i} = RN \frac{\sum_{s_j \in S} \mu_j - \mu_i}{\left(\sum_{s_j \in S} \mu_j\right)^2} - \lambda_i = 0. \tag{10}$$

Solving equation (10), we have $\mu_i = \sqrt{\frac{RN \sum_{s_j \in S \setminus \{s_i\}} \mu_j}{\lambda_i}} - \sum_{s_j \in S \setminus \{s_i\}} \mu_j$. As each strategy μ_i for s_i is an nonnegative number, the best strategy μ_i^* for s_i is given as follows.

$$\mu_i^* = \begin{cases} 0, & \text{if } \frac{RN}{\sum_{s_j \in S \setminus \{s_i\}} \mu_j} \leq \lambda_i, \\ \sqrt{\frac{RN \cdot \sum_{s_j \in S \setminus \{s_i\}} \mu_j}{\lambda_i}} - \sum_{s_j \in S \setminus \{s_i\}} \mu_j, & \text{otherwise} \end{cases} \tag{11}$$

Corollary 1: Given the optimal strategies of miners $\boldsymbol{\mu}^* = \{\mu_1^*, \mu_2^*, , \mu_n^*\}$, for any $\mu_i^*, \mu_j^* \in \boldsymbol{\mu}^*$, if $\lambda_i \leq \lambda_j$, then $\mu_i^* \geq \mu_j^*$.

Proof: We prove this corollary by contradiction. Suppose that there exist two miners' strategies $\mu_i^*, \mu_j^* \in \boldsymbol{\mu}^*$, where $\lambda_i \leq \lambda_j$ and $\mu_j^* > \mu_i^* \geq 0$. As $\mu_j^* > 0$, according to equations (10) and (11), we can easily know that $\frac{\partial P_j}{\partial \mu_j}(\mu_j^* | \boldsymbol{\mu_{-j}^*}) = 0$.

Similarly, If $\mu_i^* > 0$, we have $\frac{\partial P_i}{\partial \mu_i}(\mu_i^* | \boldsymbol{\mu_{-i}^*}) = 0$. If $\mu_i^* = 0$, according to equation (11), we have $\frac{RN}{\sum_{s_j \in S \setminus \{s_i\}} \mu_j} \leq \lambda_i$, substituting it in to equation (10), we have $\frac{\partial P_i}{\partial \mu_i}(\mu_i^* | \boldsymbol{\mu_{-i}^*}) \leq 0$. In summary, we know that $\frac{\partial P_i}{\partial \mu_i}(\mu_i^* | \boldsymbol{\mu_{-i}^*}) \leq 0$.

As $\lambda_i \leq \lambda_j$ and $\mu_j^* > \mu_i^* \geq 0$, we have

$$\begin{aligned} \frac{\partial P_j}{\partial \mu_j}(\mu_j^* | \boldsymbol{\mu_{-j}^*}) &= RN \frac{\sum_{s_k \in S} \mu_k^* - \mu_j^*}{\left(\sum_{s_k \in S} \mu_k^*\right)^2} - \lambda_j \\ &< RN \frac{\sum_{s_k \in S} \mu_k^* - \mu_i^*}{\left(\sum_{s_k \in S} \mu_k^*\right)^2} - \lambda_i \\ &= \frac{\partial P_i}{\partial \mu_i}(\mu_i^* | \boldsymbol{\mu_{-i}^*}) \leq 0, \end{aligned} \tag{12}$$

which contradicts $\frac{\partial P_j}{\partial \mu_j}(\mu_j^* | \boldsymbol{\mu_{-i}^*}) = 0$. Therefore, the corollary holds. ■

Sort the miners in ascending order of λ_i, for clarity, miners are renumbered and still denoted by $S = \{s_1, s_2, \cdots, s_n\}$. According to Corollary 1, we have $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n \geq 0$.

We assume that the the first q miners have a non-zero strategy, i.e., $\mu_q > 0$, $\mu_{q+1} = 0$. We let $S_q = \{s_1, s_2, , s_q\}$. It's obvious that $\sum_{s_j \in S} \mu_j = \sum_{s_j \in S_q} \mu_j$, and we have the following corollary.

Corollary 2: Let q be the number of miners that have a non-zero strategy in a Nash equilibrium, then we have $q \geq 2$.

Proof: Firstly, it's clear that $q > 0$, otherwise, according to equation (5), any miner s_i who purchase computational power with the amount in $(0, \frac{RN}{\lambda_i})$ can get more profit. Then we consider the case that $q = 1$. Let s_1 be the miner who has a positive strategy, and its current best strategy is to purchase μ_1 amount of computational power. According to equation (5), s_1's current profit is $RN - \lambda_1 \mu_1$. However, s_1 can increase its profit by continuously reducing μ_1 to 0, which indicates that miners didn't reach a Nash equilibrium point. Therefore, the corollary holds. ■

Summing up equation (10) with $i = 1, 2, , q$, we have

$$\frac{RN(q-1)}{\sum_{s_j \in S_q} \mu_j} - \sum_{s_i \in S_q} \lambda_i = 0. \tag{13}$$

Thus we have

$$\sum_{s_j \in S_q} \mu_j = \frac{RN(q-1)}{\sum_{s_i \in S_q} \lambda_i}. \tag{14}$$

Substituting equation (14) into equation (10), we obtain

$$\mu_i = \frac{RN(q-1)}{\sum_{s_j \in S_q} \lambda_j} \left(1 - \frac{(q-1)\lambda_i}{\sum_{s_j \in S_q} \lambda_j}\right). \tag{15}$$

As $\mu_q > 0$, and we have proven that $q \geq 2$, we then have $1 - \frac{(q-1)\lambda_q}{\sum_{s_j \in S_q} \lambda_j} > 0$, i.e., $\lambda_q < \frac{\sum_{s_j \in S_{q-1}} \lambda_j}{q-2}$.

Based on the above analysis, we design the following algorithm to find the Nash equilibrium point for the miners' sub-game.

In the following, we first prove the strategies produced by Algorithm 1 is a Nash equilibrium for the miners' sub-game, then we prove that the Nash equilibrium is unique.

Algorithm 1: Calculate Nash equilibrium for miners.

```
Sort miners in ascending order of $\lambda_i$ and renumber miners, i.e., $\lambda_1 \leq \lambda_2 \leq\leq \lambda_n$.
$S' = \{s_1, s_2\}$, q = 2
while $q < n$ and $\lambda_{q+1} < \frac{\sum_{s_i \in S'} \lambda_i}{|S'|-1}$ do
    $S' \leftarrow S' \cup \{s_{q+1}\}$ ;
    $q \leftarrow q + 1$;
end while
for $i = 1; i \leq n; i++$ do
    if $s_i \in S'$ then
        $\mu_i^* = \frac{RN(q-1)}{\sum_{s_j \in S'} \lambda_j}(1 - \frac{(q-1)\lambda_i}{\sum_{s_j \in S'} \lambda_j})$;
    else
        $\mu_i^* = 0$;
    end if
end for
return$\boldsymbol{\mu}^* = \{\mu_1^*, \mu_2^*, , \mu_n^*\}$
```

Theorem 2: The strategies produced by Algorithm 1 is a Nash equilibrium for the miners' sub-game.

Proof: For miners in S', their strategies are calculated by equation (15), it's clear that these miners get the current best strategies as the first order of $P_i(\cdot)$ equals to 0 for $s_i \in S'$. To prove the theorem, we only need to prove that for any miner $s_j \in S \backslash S'$, its current best strategy is 0. According to the description of Algorithm 1, we have

$$\lambda_j \geq \frac{\sum_{s_i \in S'} \lambda_i}{|S'| - 1}, \forall s_j \in S \backslash S'. \tag{16}$$

From equation (14), we know that $\sum_{s_i \in S'} \lambda_i = \frac{RN(|S'|-1)}{\sum_{s_i \in S'} \mu_i}$, substituting it into equation (16), we obtain that $\frac{RN}{\sum_{s_i \in S'} \mu_i} \leq \lambda_j$ for any $s_j \in S \backslash S'$. As $s_j \notin S'$, we have $\sum_{s_i \in S'} \mu_i = \sum_{s_i \in S \backslash \{s_j\}} \mu_i$. Therefore, $\frac{RN}{\sum_{s_i \in S \backslash \{s_j\}} \mu_i} \leq \lambda_j$ for any $s_j \in S \backslash S'$. According to equation (11), we know that the current best strategy for any miner $s_j \in S \backslash S'$ is 0. Thus the theorem holds. ■

The following corollary helps us to prove the uniqueness of the Nash equilibrium for the miners' sub-game.

Corollary 3: Given any Nash equilibrium $\boldsymbol{\mu}^{\boldsymbol{ne}} = \{\mu_1^{ne}, \mu_2^{ne}, , \mu_n^{ne}\}$ for the miners' sub-game, let S_h be the set of miners with a non-zero strategy, then we have $S_h = S'$, where S' is got by Algorithm 1, and $|S'| = p$.

Proof: Assume that miners have been sorted in ascending order of λ_i. According to Corollary 1, we know that $\mu_1^{ne} \geq \mu_2^{ne} \geq\geq \mu_n^{ne} \geq 0$. Suppose that $S_h = \{s_1, s_2, , s_h\}$, i.e. $|S_h| = h$. To prove $S_h = S'$, we only need to prove that $h = p$. If $h > p$, then $s_{p+1} \in S_h$, from description of Algorithm 1, we have $\lambda_{p+1} \geq \frac{\sum_{s_i \in S'} \lambda_i}{|S'|-1} \geq \frac{\sum_{s_i \in S_h} \lambda_i}{|S_h|-1}$, substituting this into equation (15), we obtain that $\mu_{p+1}^{ne} \leq 0$, which contradicts $s_{p+1} \in S_h$. If $h < p$, then we have $\mu_{h+1}^{ne} = 0$ and $\lambda_{h+1} < \frac{\sum_{s_i \in S_h} \lambda_i}{|S_h|-1}$, according to equation (10), the first order derivative of $P_{h+1}(\cdot)$ with respect to μ_{h+1} when $\mu_{h+1} = \mu_{h+1}^{ne} = 0$ is

$$\begin{aligned} \frac{\partial P_{h+1}}{\partial \mu_{h+1}}(0|\boldsymbol{\mu}_{\boldsymbol{-(h+1)}}^{\boldsymbol{ne}}) &= RN\frac{\sum_{s_j \in S} \mu_j - 0}{(\sum_{s_j \in S} \mu_j^{ne})^2} - \lambda_{h+1} \\ &= \frac{RN}{\sum_{s_j \in S} \mu_j^{ne}} - \lambda_{h+1} = \frac{RN}{\sum_{s_j \in S_h} \mu_j^{ne}} - \lambda_{h+1}, \end{aligned} \tag{17}$$

where $\boldsymbol{\mu}_{\boldsymbol{-(h+1)}}^{\boldsymbol{ne}} = \boldsymbol{\mu}^{\boldsymbol{ne}} \backslash \{\mu_{h+1}^{ne}\}$.

According to equation (14), we have $\sum_{s_j \in S_h} \mu_j^{ne} = \frac{RN(h-1)}{\sum_{s_j \in S_h} \lambda_j}$, substituting it into equation (17), we have that

$$\frac{\partial P_{h+1}}{\partial \mu_{h+1}}(0|\boldsymbol{\mu}_{\boldsymbol{-(h+1)}}^{\boldsymbol{ne}}) = \frac{\sum_{s_j \in S_h} \lambda_j}{h-1} - \lambda_{h+1}. \tag{18}$$

As $\lambda_{h+1} < \frac{\sum_{s_i \in S_h} \lambda_i}{|S_h|-1} = \frac{\sum_{s_i \in S_h} \lambda_i}{h-1}$, we know that $\frac{\partial P_{h+1}}{\partial \mu_{h+1}}(0|\boldsymbol{\mu}_{\boldsymbol{-(h+1)}}^{\boldsymbol{ne}}) > 0$, which implies that miner s_{h+1} can improve its profit by increasing its strategy μ_{h+1}^{ne}. This contradicts that $\boldsymbol{\mu}^{\boldsymbol{ne}}$ is an Nash equilibrium. Therefore, we have $h = p$, and thus the corollary holds. ■

Theorem 3: The miners' sub-game has a unique Nash equilibrium point.

Proof: According to Corollary 3, the miners' sub-game can be seen as a game among miners in S', as for any miner $s_i \in S \backslash S'$ we always have $\mu_i = 0$ in a Nash equilibrium. Therefore, we only need to prove that the sub-game of miners in S' has a unique Nash equilibrium point.

As the strategy of each miner in S' is positive, and the profit $P_i(\cdot)$ for any $s_i \in S'$ is a concave function according to equation (9), each miner will get its best strategy when the first order derivate of $P_i(\cdot)$ equals to 0. As shown in equations (13)-(15), we get unique solutions by solving the set of functions that the first order derivate of $P_i(\cdot)$ equals to 0 for each $s_i \in S'$. Therefore, the miners' sub-game among miners in S' has a unique Nash equilibrium, and thus we can conclude that Theorem 3 holds. ■

B. Analysis of the Blockchain Platform's Sub-Game

According to the analysis in Section IV-A, for any value of reward R given by the blockchain platform, there always exists a unique Nash equilibrium for the miners. Therefore, given any value of R, the blockchain platform has a unique utility, and it can maximize its utility by setting an optimal R. Substituting the result of Algorithm 1 into equation (3) and combining equation (14), we have

$$\begin{aligned} U &= \alpha \cdot \left[\sigma\left(\beta \cdot \sum_{s_i \in S'} \mu_i^*\right) - \frac{1}{2}\right] - R \\ &= \alpha \cdot \left[\sigma\left(\beta \cdot \frac{RN(q-1)}{\sum_{s_i \in S'} \lambda_i}\right) - \frac{1}{2}\right] - R \\ &= \alpha \cdot \left[\sigma(\beta XR) - \frac{1}{2}\right] - R, \end{aligned} \tag{19}$$

where $X = \frac{N(q-1)}{\sum_{s_i \in S'} \lambda_i}$.

Theorem 4: There exists a unique Stackelberg equilibrium $(\boldsymbol{\mu}^*, R^*)$ in our proposed Stackelberg game, where $\boldsymbol{\mu}^*$ and R^* are optimal strategies for miners and blockchain platform.

Proof: As the definition of the blockchain platform's subgame, the utility function $U(\cdot)$ is defined with $R \in [0, B]$. We then calculate the first order and second order derivatives of $U(\cdot)$ with respect to R,

$$\frac{\partial U}{\partial R} = \alpha\beta X\sigma(\beta XR)(1 - \sigma(\beta XR)) - 1, \tag{20}$$

$$\frac{\partial^2 U}{\partial R^2} = \alpha\beta^2 X^2\sigma(\beta XR)(1 - \sigma(\beta XR))(1 - 2\sigma(\beta XR)). \tag{21}$$

As $\beta XR \geq 0$, the range of the sigmoid function $\sigma(\beta XR)$ is $[\frac{1}{2}, 1)$, and then we have $1 - \sigma(\beta XR) > 0$ and $1 - 2\sigma(\beta XR) \leq 0$. Thus $\frac{\partial^2 U}{\partial R^2} \leq 0$ holds. Therefore the utility function $U(\cdot)$ is strictly concave with R for $R \in [0, B]$. It means that a unique R^* can be found to maximize $U(\cdot)$. Combined with Theorem 3, we conclude that there exists a unique Stackelberg equilibrium in our proposed Stackelberg game. ■

The maximization of $U(\cdot)$ is achieved either at the extreme point where the first order derivative of $U(\cdot)$ equals to 0, or at the boundary of domain area (i.e., $R = 0$ *or* B). If $\alpha\beta X < 4$, we have $\frac{\partial U}{\partial R} < 0,\ \forall R \in [0, B]$, then $U(\cdot)$ is a decreasing function in $[0, B]$, and the best strategy of the blockchain platform is $R^* = 0$. If $\alpha\beta X \geq 4$, by solving the equation $\frac{\partial U}{\partial R} = 0$, we have $\sigma(\beta XR) = \sqrt{\frac{1}{4} - \frac{1}{\alpha\beta X}} + \frac{1}{2}$, and thus the best strategy of the blockchain platform is $R^* = \min\{\frac{1}{\beta X}\log(\frac{\frac{1}{2}+\sqrt{\frac{1}{4}-\frac{1}{\alpha\beta X}}}{\frac{1}{2}-\sqrt{\frac{1}{4}-\frac{1}{\alpha\beta X}}}), B\}$. In summary, we have

$$R^* = \begin{cases} 0, & \text{if } \alpha\beta X < 4, \\ \min\left\{\frac{1}{\beta X}\log\left(\frac{\frac{1}{2}+\sqrt{\frac{1}{4}-\frac{1}{\alpha\beta X}}}{\frac{1}{2}-\sqrt{\frac{1}{4}-\frac{1}{\alpha\beta X}}}\right), B\right\}, & \text{otherwise.} \end{cases} \tag{22}$$

V. Performance Evaluation

In this section, we conduct extensive simulations to evaluate the performance of our proposed incentive mechanism for blockchain-based internet of things.

A. Experimental Settings

In our experiments, we set the basic parameters of our problem as follows. We assume there are totally 1000 IoT devices that are interested in participating in the blockchain mining process, i.e., $|S| = 1000$. The unit price λ_i of computational power purchased by each miner s_i from edge servers uniformly ranges from 100 to 105. For the blockchain platform utility model, α is set to be 10000, β is set to be 0.001, and B is set to be 2000. We assume that it takes an average of 10 minutes for the blockchain platform to generate a new block, and thus it will generate an average of 144 new blocks per day, i.e., N is set to be 144. Unless otherwise stated, the above parameters will be set as default settings. Each value in figures in this section is the average of 100 runs.

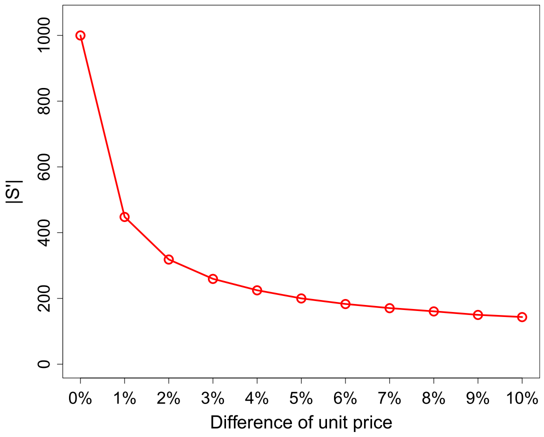

Fig. 5. Impact of the difference of unit price on $|S'|$.

B. Results and Analyses

1) Number of Participating Miners ($|S'|$): As described in Algorithm 1, only the miners in S' will purchase computational power to participate in the mining process, then we study how the unit price of computational power and the total number of IoT devices affect $|S'|$.

In Fig. 5, we set the minimum unit price of computational power to be 100, and set the difference of unit price from 1% to 10%. Here, the difference of unit price represents the range of λ_i for each miner. For example, when the difference of unit price is set to be 2%, then λ_i is randomly chosen in $[100, 102]$ for each miner. From Fig. 5 we can see that $|S'|$ decreases when the difference of unit price of computational power increases. This is because when the difference of unit price is large, λ_i of each miner will become diverse, and thus there will be more miners violate the while condition in Algorithm 1. We can also see that the effect of the difference of the unit price is very significant, even when the difference of unit price is as small as 1%, there are only about 44.8% of miners participate in the blockchain mining process.

In Fig. 6, we fix the difference of unit price of computational power at 5%, and study how the number of IoT devices affect $|S'|$. It can be seen that the growth of $|S'|$ does not have a linear relationship with the number of IoT devices. There are about 28.5% of miners participate in the blockchain mining process when $|S| = 500$, while there are only about 9% of miners participate in the blockchain mining process when $|S|$ increased to 5000.

2) Effect of Unit Price λ_i on Utilities and Strategies: We fix the difference of the unit price of computational power at 5%, and study how λ_i of each miner affect the utilities and strategies of blockchain platform and miners.

As shown in Fig. 7, when the unit price of computation power increases, the blockchain platform needs to improve the reward to achieve maximum utility until the maximum value of the reward is reached. And miners tend to purchase less computational power as it will cost more money. Combining Fig. 7 and Fig. 8, we can observe that the platform utility decreases as the unit price of computational power

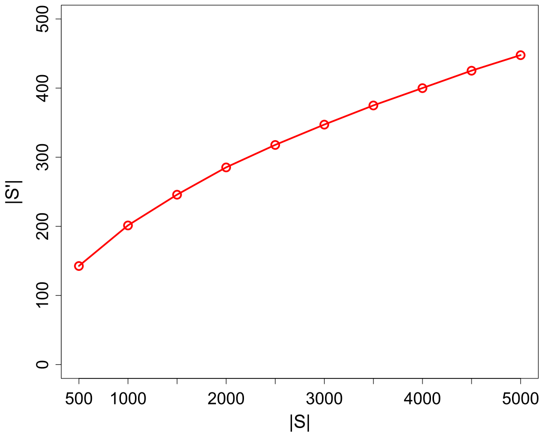

Fig. 6. Impact of number of IoT devices on $|S'|$.

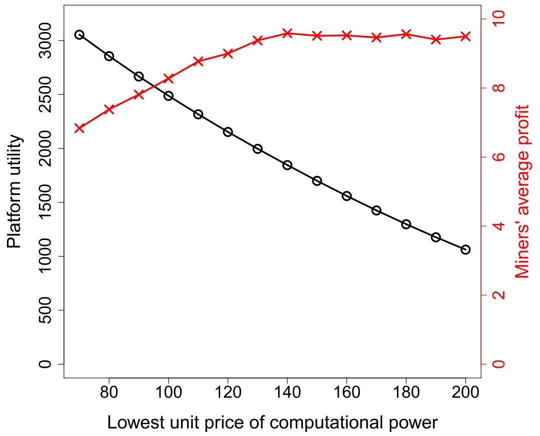

Fig. 8. Impact of λ_i on platform utility and miners profits.

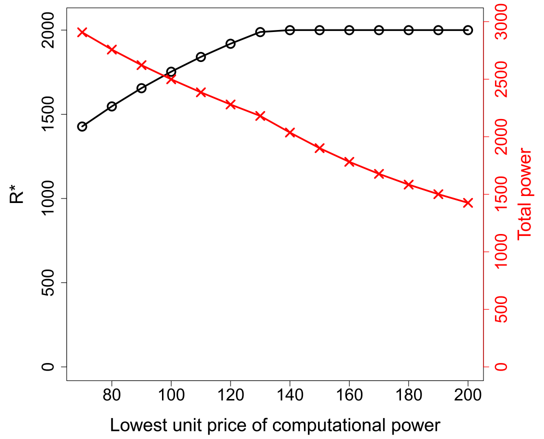

Fig. 7. Impact of the λ_i on strategies.

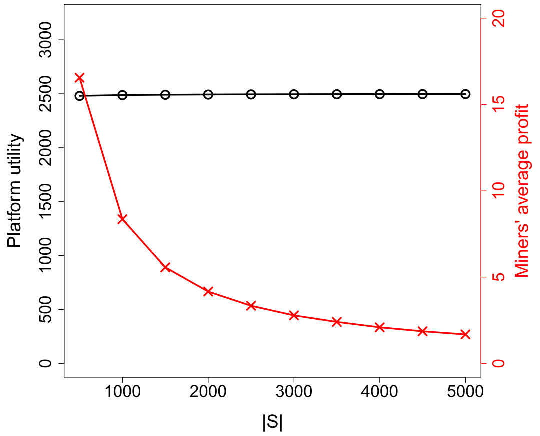

Fig. 9. Impact of $|S|$ on platform utility and miners' profits.

increases, this is because the platform improves the reward but miners provide less computational power. We can also see that the miners' average profit increases even though they have to pay more money to afford unit computational power. The reason is that miners purchase less computational power, while the platform gives more rewards to them.

3) Effect of $|S|$ on Platform Utility and Miners' Profits: We fix the range of the unit price of computational power at $[100, 105]$, and study the effect of $|S|$ on platform utility and miners' profits.

As shown in Fig. 9, the platform always has a stable utility no matter how $|S|$ changes. However, miners' average profit will decrease as $|S|$ increases. This is because there will be more miners participate in the mining process, and thus intensifies the competition.

Fig. 10 shows the profits of miners s_1, s_{50}, and s_{100}. Note that all miners have been sorted and renumbered in the ascending order of λ_i. We can see that the profits of miners s_1 and s_{50} decrease with the increases of $|S|$, the result is similar to that in Fig. 9. However, for miner s_{100}, its profit increases when $|S|$ increases from 500 to 1000, then slowly decreases as $|S|$ increases. The reason is that when $|S|$ increases from 500 to 1000, λ_i of each miner becomes more tight, and then the difference between λ_{100} and any other λ_i $(1 \leq i < 100)$ decreases. So miner s_{100} become more competitive and thus can get more profits. In detail, when $|S| = 500$, $\lambda_1 = 100.011$, $\lambda_{50} = 100.504$ and $\lambda_{100} = 100.992$; when $|S| = 1000$, $\lambda_1 = 100.004$, $\lambda_{50} = 100.247$ and $\lambda_{100} = 100.496$. We can also see that the unit price of computational power will significantly affect the profits of miners, especially when the number of participating miners is small. For example, when $|S| = 500$, λ_{50} and λ_{100} are only 0.49% and 0.98% larger than λ_1, respectively. However, the profit of miner s_1 is 2.5 times that of the miner s_{50} and 10.6 times that of miner s_{100}.

VI. Conclusion

In this paper, we first analyze the relationship between the security of the blockchain network and the total computational power of the entire network, and define a utility function to make a trade-off between blockchain security and profits of the blockchain platform. Then we design an incentive mechanism for the IoT blockchain network to motivate IoT devices to purchase more

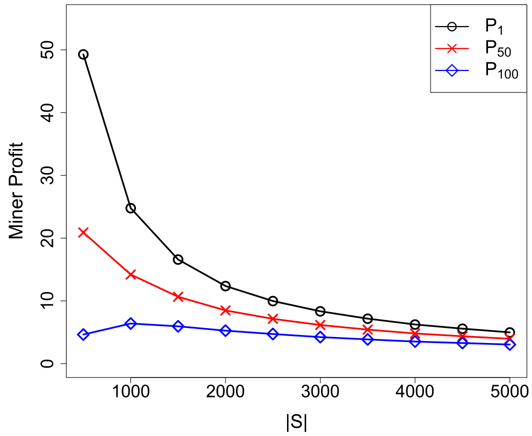

Fig. 10. Impact of $|S|$ on the $1st$, $50th$ and $100th$ miners' profits.

computational resources form edge servers, thus that a secure blockchain network can be established while the profits of the blockchain platform can be guaranteed. We model the interaction between the blockchain platform and IoT devices as a two-stage Stackelberg game. We prove the existence and uniqueness of the Stackelberg equilibrium and design an efficient algorithm to compute the Stackelberg equilibrium point. We also conduct extensive simulations to evaluate the performance of our designs. Our work is helpful for the IoT blockchain platform to set a reasonable reward to build a secure blockchain network.

REFERENCES

[1] F. Shrouf, J. Ordieres, and G. MiraglIoTta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage.*, 2014, pp. 697–701.

[2] M. Rehman, N. Javaid, M. Awais, M. Imran, and N. Naseer, "Cloud based secure service providing for IoTs using blockchain," in *Proc. IEEE Global Commun. Conf.*, 2019, pp. 1–7.

[3] S. Krco, D. Cleary, and D. Parker, "P2P mobile sensor networks," in *Proc. 38th Annu. Hawaii Int. Conf. Syst. Sci.*, 2005, pp. 324c–324c.

[4] R. Mietz *et al.*, "A P2P semantic query framework for the Internet of Things," *PIK-Praxis der Informationsverarbeitung und Kommunikation*, vol. 36, no. 2, pp. 73–79, 2013.

[5] K. Chung and R. C. Park, "P2P cloud network services for IoT based disaster situations information," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 3, pp. 566–577, 2016.

[6] J. Guo, X. Ding, and W. Wu, "A blockchain-enabled ecosystem for distributed electricity trading in smart city," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 2040–2050, Feb. 2021.

[7] P. Koshy, S. Babu, and B. Manoj, "Sliding window blockchain architecture for Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3338–3348, Apr. 2020.

[8] Y. Chen, L. Wang, and S. Wang, "Stochastic blockchain for IoT data integrity," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 373–384, Jan.–Mar. 2020.

[9] M. Baza, N. Lasla, M. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Trans. Netw. Sci. Eng.*, to be published, doi: 10.1109/TNSE.2019.2959230.

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[11] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018.

[12] Y. Wu, P. Song, and F. Wang, "Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in blockchain," *Math. Problems Eng.*, vol. 2020, 2020, Art. no. 7270624, doi: 10.1155/2020/7270624.

[13] P. Ferraro, R. Shorten, and C. King, "On the stability of unverified transactions in a dag-based distributed ledger," *IEEE Trans. Automat. Control*, vol. 65, no. 9, pp. 3772–3783, Sep. 2020.

[14] C. Bai, "State-of-the-art and future trends of blockchain based on dag structure," in *Proc. Int. Workshop Structured Object-Oriented Formal Lang. Method.*, 2018, pp. 183–196.

[15] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.

[16] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11 008–11 021, Nov. 2018.

[17] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Inform.*, vol. 16, no. 3, pp. 1972–1983, Mar. 2020.

[18] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.

[19] N. U. Hassan, C. Yuen, and D. Niyato, "Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions," *IEEE Ind. Electron. Mag.*, vol. 13, no. 4, pp. 106–118, Dec. 2019.

[20] M. B. Mollah *et al.*, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2020.3028368.

[21] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3632–3641, Jun. 2019.

[22] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 289–300, Mar.-Apr. 2020.

[23] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled deduplicatable data auditing mechanism for network storage services," *IEEE Trans. Emerg. Top. Comput.*, to be published, doi: 10.1109/TETC.2020.3005610.

[24] W. Sun, J. Liu, Y. Yue, and P. Wang, "Joint resource allocation and incentive design for blockchain-based mobile edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 9, pp. 6050–6064, Sep. 2020.

[25] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial Internet of Things," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3602–3609, Jun. 2019.

[26] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 9, pp. 1975–1989, Sep. 2019.

[27] J. Wang, Q. Wang, N. Zhou, and Y. Chi, "A novel electricity transaction mode of microgrids based on blockchain and continuous double auction," *Energies*, vol. 10, no. 12, pp. 1–22, 2017.

[28] 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.

[29] Z. Chang, W. Guo, X. Guo, Z. Zhou, and T. Ristaniemi, "Incentive mechanism for edge computing-based blockchain," *IEEE Trans. Ind. Inform.*, vol. 16, no. 11, pp. 7105–7114, Nov. 2020.

[30] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, Jun. 2019.

[31] C. Luo, L. Xu, D. Li, and W. Wu, "Edge computing integrated with blockchain technologies," *Complexity Approx.*, 2020, pp. 268–288, doi: 10.1007/978-3-030-41672-0_17.

[32] A. Hari, M. Kodialam, and T. Lakshman, "Accel: Accelerating the bitcoin blockchain for high-throughput, low-latency applications," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, 2019, pp. 2368–2376.

[33] BitcoinWiki, "Difficulty in mining," Accessed on: Mar. 17, 2020. [Online]. Available: https://en.bitcoinwiki.org/wiki/Difficulty_in_Mining#Difficulty_changes

[34] C. Grunspan and R. Pérez-Marco, "Double spend races," *Int. J. Theor. Appl. Finance*, vol. 21, no. 08, pp. 1–32.

Xingjian Ding received the B.E. degree in electronic information engineering from Sichuan University, Sichuan, China, in 2012, the M.S. degree in software engineering from Beijing Forestry University, Beijing, China, in 2017. He is currently working toward the Ph.D. degree with the School of Information, Renmin University of China, Beijing, China. His research interests include wireless rechargeable sensor networks, algorithm design and analysis, and blockchain.

Jianxiong Guo received the B.S. degree in energy engineering and automation from the South China University of Technology in 2015 and the M.S. degree in chemical engineering from the University of Pittsburgh in 2016. He is the Ph.D. candidate with the Department of Computer Science, the University of Texas, Dallas. His research interests include social networks, data mining, IoT application, blockchain, and combinatorial optimization.

Deying Li received the B.S. and M.S. degrees in mathematics from Huazhong Normal University, China, in 1985 and 1988, respectively. She received the Ph.D. degree in computer science from the City University of Hong Kong in 2004. She is a Professor with the Renmin University of China. Her research interests include wireless networks, ad hoc & sensor networks mobile computing, distributed network system, social networks, and algorithm design etc.

Weili Wu (Senior Member, IEEE) received the M.S. and Ph.D. degrees from the Department of Computer Science, University of Minnesota, Minneapolis, MN, USA, in 1998 and 2002, respectively. She is currently a Full Professor with the Department of Computer Science, The University of Texas, Dallas, Richardson, TX, USA. Her research include the general research area of data communication and data management. Her research focuses on the design and analysis of algorithms for optimization problems that occur in wireless networking environments and various database systems.