Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks

Zehui Xiong, *Student Member, IEEE*, Shaohan Feng, *Student Member, IEEE*, Wenbo Wang, *Member, IEEE*, Dusit Niyato, *Fellow, IEEE*, Ping Wang, *Senior Member, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*—Public blockchain networks using proof of work (PoW)-based consensus protocols are considered as a promising platform for decentralized resource management with financial incentive mechanisms. In order to maintain a secured, universal state of the blockchain, PoW-based consensus protocols financially incentivize the nodes in the network to compete for the privilege of block generation through cryptographic puzzle solving. For rational consensus nodes, i.e., miners with limited local computational resources, offloading the computation load for PoW to the cloud/fog providers (CFPs) becomes a viable option. In this paper, we study the interaction between the CFPs and the miners in a PoW-based blockchain network using a game theoretic approach. In particular, we propose a lightweight infrastructure of the PoW-based blockchains, where the computation-intensive part of the consensus process is offloaded to the cloud/fog. We formulate the computation resource management in the blockchain consensus process as a two-stage Stackelberg game, where the profit of the CFP and the utilities of the individual miners are jointly optimized. In the first stage of the game, the CFP sets the price of offered computing resource. In the second stage, the miners decide on the amount of service to purchase accordingly. We apply backward induction to analyze the subgame perfect equilibria in each stage for both uniform and discriminatory pricing schemes. For uniform pricing where the same price applies to all miners, the uniqueness of the Stackelberg equilibrium is validated by identifying the best response strategies of the miners. For discriminatory pricing where the different prices are applied, the uniqueness of the Stackelberg equilibrium is proved by capitalizing on the variational inequality theory. Further, the real experimental results are employed to justify our proposed model.**

***Index Terms*—Blockchain, computation offloading, game theory, pricing, proof-of-work, variational inequalities (VIs).**

Manuscript received May 28, 2018; revised August 29, 2018; accepted September 17, 2018. Date of publication September 24, 2018; date of current version June 19, 2019. This work was supported in part by WASP/NTU under Grant M4082187 (4080), in part by the Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17 and MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15 and Grant NRF2015-NRF-ISF001-2277, in part by EMA Energy Resilience under Grant NRF2017EWT-EP003-041, in part by the U.S. MURI, and in part by the NSF under Grant CNS-1717454, Grant CNS-1731424, Grant CNS-1702850, Grant CNS-1646607, and Grant ECCS-1547201. An earlier version of this paper was accepted by IEEE ICC in [1]. *(Corresponding author: Ping Wang.)*

Z. Xiong, S. Feng, W. Wang, and D. Niyato are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore.

P. Wang is with the Department of Electrical Engineering and Computer Science, York University, Toronto, ON M3J 1P3, Canada (e-mail: pingw@yorku.ca).

Z. Han is with Electrical and Computer Engineering Department and the Computer Science Department, University of Houston, Houston, TX 77204 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 130-701, South Korea.

Digital Object Identifier 10.1109/JIOT.2018.2871706

I. Introduction

BLOCKCHAIN networks were first designed to be the backbone of a distributed, permissionless/public database for recording the transactional data of cryptocurrencies in a tamper-proof and totally ordered manner [2], [3]. The blockchain network is essentially organized as a virtual overlay peer-to-peer (P2P) network, where the database state is maintained in a purely decentralized manner and any node in the network is allowed to join the state maintenance process without the need of identity authentication. As indicated by the name "blockchain," the records of transactions between nodes in the network are organized in a data structure known as the "block." A series of blocks are arranged in a strictly increasing-time order by a linked-list-like data structure known as the chain of blocks (i.e., blockchain). The blockchain is maintained as the appending-only local replicas by the nodes participating in the replicated consensus process. Unlike the traditional distributed ledger systems using the practical Byzantine fault-tolerant [4] or Paxos [5] protocols, a permissionless blockchain network no longer needs any centralized authorities (e.g., authenticating/authorizing servers) and is able to accommodate a much larger number of consensus nodes in the network [6]. Such an objective is achieved by blockchain networks with the Nakamoto consensus protocol [2] (or protocols alike). Per the Nakamoto protocol, financial incentive is introduced into the consensus process to ensure that the best strategies of the pseudonymous consensus nodes is to follow the given rules of blockchain maintenance/extension. Otherwise they will suffer from monetary loss.

The core component of the Nakamoto consensus protocol is a computation-intensive process known as proof of work (PoW). For the consensus nodes that propose their local blockchain view to be the new state of the blockchain database, PoW requires them to solve a cryptographic puzzle, i.e., to find a partial preimage satisfying certain conditions of a hash mapping based on the proposed blockchain state. According to [7], a typical PoW process is executed in the following steps. First, with an input contribution function, a consensus node validates and bundles a subset of unconfirmed transactions into a new block. Then, the consensus node computes the PoW solution to the cryptographic puzzle, which is formed based on the value of the new block. Immediately after the puzzle solution is obtained, the consensus node broadcasts the new block to the entire network as its own proposal of the new blockchain head. On the other hand, the rest of nodes in the network run a

chain validation-comparison function to determine whether to accept such a proposal or not. In the blockchain network, an honest consensus node follows "the-longest-chain" rule and adopts the longest one among the received blockchain proposals to update its local view of the blockchain state. In such a process, the nodes that devote their computational resources to the generation of new blocks (i.e., PoW solutions) are also known as the block "miners." This is mainly because according to the Nakamoto protocol, a certain amount of blockchain tokens will be awarded to the node that has its proposed blockchain state accepted by the majority of the network. The theoretic proof and analysis for secure and private communication with the Nakamoto protocol can be found in [7].

With the blossom of various cryptocurrencies, permissionless blockchains are considered to be especially appropriate for constructing the decentralized autonomous resource management framework in (wireless) communication networks. Specifically, when the resource management relies on the design of incentive mechanisms (e.g., resource access control [8] and proactive edge caching [9]), permissionless blockchains are able to provide fast implementation of the self-organized trading platform with small investment in the operational infrastructure. Furthermore, with the PoW-based Nakamoto consensus protocol, the users of a decentralized application (DApp) are incentivized to turn themselves from the free riders of the blockchain network into consensus nodes (i.e., block miners) for more profit. However, due to the required computation contribution by the PoW, the computationally lightweight nodes such as the Internet of Things (IoT) devices may be prevented from directly participating in the consensus process. To alleviate such limitation, "cloud mining" becomes a viable option where the mobile devices offload their storage load and/or computation tasks in PoW to the cloud/fog providers (CFPs) or even other edge devices [10], [11]. In the case of computation offloading, the lightweight devices may employ the existing cloud-mining protocols such as Stratum [12] without causing any significant transmission overhead. From the perspective of the blockchain-based DApp's designer, the benefit of encouraging cloud-based mining is multifold. First, by incorporating more consensus nodes, the robustness of the blockchain network is naturally improved [7]. Second, the user devices may improve their valuation of the DApps, thanks to the additional reward obtained in the consensus process. Also, the high level of user activities may attract more users and in return further improve the robustness of the underlying blockchain network.

In this paper, we study the interaction between the computationally lightweight devices and a CFP, where the lightweight devices (i.e., block miners) purchase the computing power from the CFP to participate in the consensus process of a PoW-based blockchain for block-mining revenues. Game theory can be leveraged as a promising mathematical tool to analyze the interactions among the CFP and block miners. For example, Zhang *et al.* [13] formulated a Stackelberg game to solve the resource management in fog computing networks, where the game theoretic study of the market and pricing strategies are presented. Zhang *et al.* [14] studied the spectrum resource allocation in order to mitigate the interference management among multiple cellular operators in the unlicensed system. A multileader multifollower Stackelberg game is proposed to model the interactions among the operators and users in unlicensed spectrum. Similarly, we also model the resource offloading market as a two-stage Stackelberg game. In the first stage, the CFP sets the unit price for computation offloading. In the second stage, the miners decide on the amount of services to purchase from the CFP. In particular, we analyze two pricing schemes [15], i.e., uniform pricing where a uniform unit price is applied to all the miners and discriminatory pricing where different unit prices are assigned to different miners. The uniform pricing leads to a straightforward implementation as the CFP does not need to keep track of information of every miner, and charging the same prices is fair to all miners. However, from the perspective of the CFP, discriminatory pricing yields a higher profit by allowing price adjustment for different miners [16]. The main contributions of this paper are summarized as follows.

1) We explore the possibility of implementing a permissionless, PoW-based blockchain in a network of computationally lightweight devices. By allowing computation offloading to the cloud/fog, we model the interactions between the rational blockchain miners and the CFP as a two-stage Stackelberg game.
2) We study both the uniform pricing scheme and the discriminatory pricing scheme for the CFP. Through backward induction, we provide a series of analytically results with respect to the properties of the Stackelberg equilibrium in different situations.
3) In particular, the existence and uniqueness of Stackelberg equilibrium are validated by identifying the best response strategies of the miners under the uniform pricing scheme. Likewise, the Stackelberg equilibrium is proved to exist and be unique by capitalizing on the variational inequalities (VIs) theory under discriminatory pricing scheme.
4) We conduct extensive numerical simulations to evaluate the performance of the proposed price-based resource management in blockchain networks. The results show that the discriminatory pricing helps the CFP to encourage more service demand from the miners and achieve greater profit. Moreover, under uniform pricing, the CFP has an incentive to set the maximum price for the profit maximization.

The rest of this paper is organized as follows. Section II presents a brief review of the related work. We describe the model of the consensus formation in a permissionless PoW-based blockchain network and formulate the two-stage Stackelberg game between the lightweight nodes and the CFP in Section III. In Section IV, we analyze the optimal service demand of block miners as well as the profit maximization of the CFP using backward induction for both uniform and discriminatory pricing schemes. We present the performance evaluations in Section V. Section VI concludes this paper with summary and future directions.

II. Related Work

A. Public Blockchains, DApps, and Incentive Mechanism

For blockchain networks, the core technological "building blocks" have been recognized as the distributed database (i.e., ledger), the consensus protocol and the executable scripts (i.e., smart contract) based on network consensus [17]. From a data processing point of view, a DApp is essentially a collection of smart contracts and transactional data residing on the blockchain. The realization of a DApp relies on the distributed ledger to identify the state/ownership changes of the tokenized assets. The smart contracts are implemented as transaction (data)-driven procedures to autonomously determine the state transition regarding the asset redistribution among the DApp users [17]. With public blockchains, the implementation of a DApp does not require a centralized infrastructure, namely, dedicated storage and computation provision for the ledger and smart contracts. Instead, the DApp users are allowed to freely enable their functionalities among transaction issuing/validation, information propagation/storage, and consensus participation [17], [18]. More specifically, the token-based incentive mechanisms in public blockchains offload the tasks of resource provision and system maintenance from the DApp providers to the DApp users. Thereby, public blockchain networks are considered to be a suitable platform for implementing the incentive-driven distributed autonomous organization (DAO) systems.

In recent years, a line of work has been dedicated to the study in DAO for wireless networking applications based on public blockchains. In [19], a trading platform for device-to-device (D2D) computation offloading is proposed using a dedicated cryptocurrency network. Therein, resource offloading is executed between neighbor D2D nodes through smart contract-based auctions, and the block mining tasks are offloaded to the cloudlets. In [20], a PoW-based public blockchain is adopted as the backbone of a P2P file storage market, where the privacy of different parties in a transaction is enhanced by the techniques, such as ring signatures and one-time payment addresses. When identity verification is required for market access granting, e.g., in the scenarios of autonomous network slice brokering [21] and P2P electricity trading [22], the public blockchains can be adapted into consortium blockchains by introducing membership authorizing servers with little modification to the consensus protocols and smart contract design.

This paper also relates to the classical literature on incentive mechanisms in crowdsensing [23]–[25]. In crowdsensing, the crowdsensing platform as the service provider offers a reward as the incentive to attract more crowdsensing user participation. In the pioneering work [23], Yang *et al.* considered two system models: 1) the platform-centric model where the provider offers a certain amount of reward that will be shared by the participating users and 2) the user-centric model where the users have their reserve prices for the participation. Chakeri and Jaimes [24] designed the incentive mechanisms for crowdsensing with multiple crowdsourcers, i.e., service providers. The interactions among the service providers are modeled as the noncooperative game. Therein, the authors proposed a discrete time dynamic algorithm utilizing the best response dynamics to compute the Nash equilibrium of the modeled game. Chakeri and Jaimes [25] presented the incentive mechanism in a sealed market where the users have incomplete information on other users' behavior. The convergence to the Nash equilibrium in such a market is then analyzed using the well-known best response dynamics.

B. Consensus and Game Theoretic Mining Models in PoW-Based Blockchains

By the Nakamoto protocol, from a single miner's point of view, the process of solving a PoW puzzle involves an exhaustive query to a collision-resistant hash function (e.g., SHA-256), which aims to find a fixed-length hashcode output with no less than a given number of prefix zeros [2], [7]. For each individual miner, such a process simulates a Poisson process when the required number of prefix zeros is sufficiently large. For a group of miners independently running their own PoW processes at the same time, the first miner to obtain the PoW puzzle solution will have a high probability of getting its block head proposal acknowledged by the entire network. Therefore, block mining under the Nakamoto protocol can also be viewed as a hashing competition, where the probability of a miner winning the competition is roughly proportional to the ratio between its devoted hash power[1] and the total hash power in the network.

According to the theoretical analysis in [7], when the PoW-based blockchain network satisfies the condition of honest majority in terms of computing power, the probability for the blockchain state machine to be compromised is negligible. Therefore, the mainstream research on the PoW-based consensus protocols focus on the protocol's incentive compatibility and thus the search of miners' rational strategy to optimize the reward obtained in the mining process. A plethora of recent studies [26]–[28] model the mining process in PoW-based blockchain networks as a noncooperative game, where rational miners may withhold their newly found blocks with valid PoW solutions to internationally cause the fork of the blockchain. In certain conditions of hash power distribution, it is proved in [26]–[28] that by postponing the newly mined blocks, rational miners may obtain a higher expected payoff than fully abiding by the Nakamoto protocol.

In the literature, the most relevant works to this paper are about the pool-based mining mechanisms. In public blockchains based on outsourceable PoW schemes, a mining pool is essentially a proxy node in the network that only enables its local functionalities of transaction issuing/validation and information propagation/storage. The proxy node offloads the queries to the hash function to the mining workers that subscribe to the pool for mining payment [17], [18]. It is worth noting that most of the existing studies consider the pool-based mining from the perspective of mining workers (i.e., cloud-side resource providers) [29]–[32]. In [29], the process of mining pool formation is modeled as a coalitional game among the mining workers, which is found to have an empty core under the proportional payment scheme. In

[1] We use the hash power and computing power interchangeably throughout this paper.

contrast, the social welfare of miners is considered in [30] and a geometric-payment pooling strategy is found to be able to achieve the optimal steady-state utility for the miners. In [31], the group bargaining solution is adopted by considering the P2P relationship of the miners. In [32], instead of limiting the miner subscription to a single mining pool, a computing power-splitting game is proposed. With the proposed scheme, the miners play a puzzle-solution game by distributing their computing power into different pools in order to maximize the mining reward.

III. System Model and Game Formulation

In this section, we first propose the system model of blockchain under our consideration [33]. Then, we present the Stackelberg game formulation for the price-based computing resource management in blockchain networks assisted by cloud/fog computing.

A. Chain Mining Assisted by Cloud/Fog Computing

We consider a public blockchain network using the PoW-based consensus protocol [1], [34], [35]. The blockchain network dedicatedly works as the backbone of a specific DApp, where most of the nodes are limited in their local computing power (e.g., the IoT devices and smart phones in a typical crowd-sensing market). We assume that the adopted PoW protocol is ASIC-resistant [18], e.g., using the Ethash-based PoW scheme [36] or the schemes alike. Then, to participate in the consensus process, a node only has to solve the PoW puzzle with general-purpose computing devices. In the blockchain network, a set of N nodes denoted as $\mathcal{N} = \{1, \ldots, N\}$, are interested in participating in the consensus process and make extra profit through block mining. In order to achieve this, these block miners purchase the necessary hash power from a public CFP (e.g., Amazon EC2) without hassle of managing the infrastructure such as seeking extra electricity sources [37]. In addition, we consider that the CFP is able to provide the near-to-end computing units such as fog nodes or even edge devices which are closer to the miners[2] [38]. As such, the aforementioned PoW puzzle can be offloaded to the remote cloud or the nearby fog computing unit. The computing resources offered to the miners is priced by the CFP.[3] Fig. 1 shows the system model of the blockchain network under our consideration. Note that we assume that the link between the miners and cloud/fog computing units is sufficiently reliable and secured, which is guaranteed by certain ready-to-use communication protocols (e.g., Stratum [12]).

The CFP, i.e., the seller, sells the computing services, and the miners, i.e., the buyers, access and consume this service from the remote cloud or the nearby fog computing unit.

[2]Note that this fog unit deployment is also more appropriate in hostile environment, where the communications with remote cloud are limited and for the access from personal devices which keep moving, e.g., mobile devices.

[3]Note that the resource may also include communication resource. Specifically, we can consider that the communication cost is part of the price charged by the CFP. In other words, the CFP offers the service as a bundle which is composed of computing and wireless/wired communication resources. The energy consumption for the computing and communication is naturally accounted in the bundle.

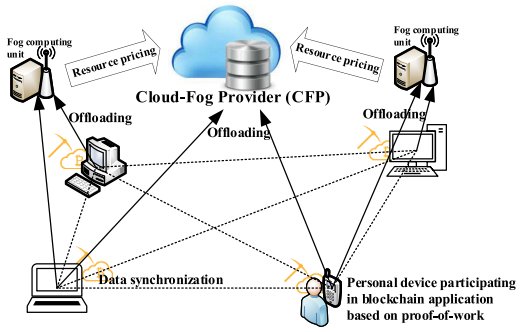


Fig. 1. System model of public blockchain application involving PoW.

Each miner $i \in \mathcal{N}$ determines their individual service demand, denoted by x_i. Additionally, we consider $x_i \in [\underline{x}, \bar{x}]$, in which $\underline{x}$ is the minimum service demand, e.g., for blockchain data synchronization, and $\bar{x}$ is the maximum service demand governed by the CFP. Note that each miner has no incentive to unboundedly increase its service demand due to its financial burden. Then, let $\mathbf{x} \triangleq (x_1, \ldots, x_N)$ and $\mathbf{x}_{-i}$ represent the service demand profile of all the miners and all other miners except miner i, respectively. As such, the miner $i \in \mathcal{N}$ with the service demand x_i has a relative computing power (hash power) α_i with respect to the total hash power of the network, which is defined as follows:

$$\alpha_i(x_i, \mathbf{x}_{-i}) = \frac{x_i}{\sum_{j \in \mathcal{N}} x_j}, \alpha_i > 0 \tag{1}$$

such that $\sum_{j \in \mathcal{N}} \alpha_j = 1$.

In the blockchain network, miners compete against each other in order to be the first one to solve the PoW puzzle and receive the reward from the speed game accordingly. The occurrence of solving the puzzle can be modeled as a random variable following a Poisson process with mean $\lambda = (1/600\ \text{s})$ [26]. Note that our model is general that can be applied with other values of λ easily. The set of transactions to be included in a block chosen by miner i is denoted as t_i. Once the miner successfully solves the puzzle, the miner needs to propagate its solution to the whole blockchain network and its solution needs to reach consensus. Because there is no centralized authority to verify the validate a newly mined block, a mechanism for reaching network consensus must be employed. In this mechanism, the verification needs to be processed by other miners before the new mined block is appended to the current blockchain.

The first miner to successfully mine a block that reaches consensus earns the reward. The reward consists of a fixed reward denoted by R, and a variable reward which is defined as rt_i, where r denotes a given variable reward factor and t_i denotes the number of transactions included in the block mined by miner i [26]. Additionally, the process of solving the puzzle incurs an associated cost, i.e., the payment from miner i to the CFP, p_i. The objective of the miners is to maximize their individual expected utility, and for miner i, it is defined as follows:

$$u_i = (R + rt_i) P_i(\alpha_i(x_i, \mathbf{x}_{-i}), t_i) - p_i x_i \tag{2}$$

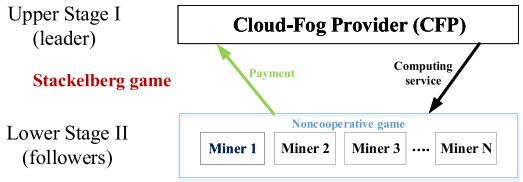


Fig. 2. Two-stage Stackelberg game model of the interactions among the CFP and miners in the blockchain network.

where $P(\alpha_i(x_i, \mathbf{x}_{-i}), t_i)$ is the probability that miner i successfully mines the block and its solutions reach consensus, i.e., miner i wins the mining reward.

The process of successfully mining a block consists of two steps, i.e., the mining step and the propagation step. In the mining step, the probability that miner i mines the block is directly proportional to its relative computing power α_i. Furthermore, there are diminishing chances of wining if one miner chooses to propagate a block that propagates slowly to other miners in the propagation step. In other words, even though one miner may find the first valid block, if its mined block is large, then this block will be likely to be discarded because of long latency, which is called orphaning [26]. Considering this fact, the probability of successful mining by miner i is discounted by the chances that the block is orphaned, $\mathbb{P}_{\text{orphan}}(t_i)$, which is expressed by

$$P_i(\alpha_i(x_i, \mathbf{x}_{-i}), t_i) = \alpha_i\big(1 - \mathbb{P}_{\text{orphan}}(t_i)\big). \tag{3}$$

Using the fact that block mining times follow the Poisson distribution aforementioned, the orphaning probability is approximated as [39]:

$$\mathbb{P}_{\text{orphan}}(t_i) = 1 - e^{-\lambda\tau(t_i)} \tag{4}$$

where $\tau(t_i)$ is the block propagation time, which is a function of the block size. In other words, the propagation time needed for a block to reach consensus is dependent on its size t_i, i.e., the number of transactions in it [26], [40]. Thus, the bigger the block is, the more time needed to propagate the block to the whole blockchain network [41]. Same as [26], we assume this time function is linear, i.e., $\tau(t_i) = z \times t_i$ with $z > 0$ represents a given delay factor. Note that this linear approximation is acceptable according to the numerical results from [26]. Additionally, it would be more appropriate to add a constant term in this function [41], but apparently this constant term has no effect on our subsequent analytical results. Thus, the probability that the miner i successfully mines a block and its solution reaches consensus is expressed as follows:

$$P_i(\alpha_i(x_i, \mathbf{x}_{-i}), t_i) = \alpha_i e^{-\lambda z t_i} \tag{5}$$

where $\alpha_i(x_i, \mathbf{x}_{-i})$ is given in (1).

B. Two-Stage Stackelberg Game Formulation

The interaction between the CFP and miners can be modeled as a two-stage Stackelberg game, as illustrated in Fig. 2. The CFP, i.e., the leader, sets the price in the upper Stage I. The miners, i.e., the followers, decide on their optimal computing service demand for offloading in the lower Stage II, being aware of the price set by the CFP. By using backward induction, we formulate the optimization problems for the leader and followers as follows.

1) Miners' Mining Strategies in Stage II: Given the pricing of the CFP and other miners' strategies, the miner i determines its computing service demand for its hash power maximizing the expected utility which is given as

$$u_i(x_i, \mathbf{x}_{-i}, p_i) = (R + rt_i)\frac{x_i}{\sum_{j\in\mathcal{N}} x_j} e^{-\lambda z t_i} - p_i x_i \tag{6}$$

where p_i is the price per unit for service demand of miner i. The miner subgame problem can be written as follows.

Problem 1 (Miner i Subgame):

$$\begin{aligned} \underset{x_i}{\text{maximize}} \quad & u_i(x_i, \mathbf{x}_{-i}, p_i) \\ \text{subject to} \quad & x_i \in [\underline{x}, \bar{x}]. \end{aligned} \tag{7}$$

2) CFP's Pricing Strategies in Stage I: The profit of the CFP is the revenue obtained from charging the miners for computing service minus the service cost. The service cost is directly related to the time that the miner takes to mine a block, the cost of electricity, c, and the other cost that is a function of the service demand x_i. Therefore, the CFP decides the pricing within the strategy space $\{\mathbf{p} = [p_i]_{i\in\mathcal{N}} : 0 \le p_i \le \bar{p}\}$ to maximize its profit which is represented as

$$\Pi(\mathbf{p}, \mathbf{x}) = \sum\nolimits_{i\in\mathcal{N}} p_i x_i - \sum\nolimits_{i\in\mathcal{N}} cTx_i. \tag{8}$$

Note that practically the price is bounded by maximum price constraint that is denoted by $\bar{p}$. Then, the profit maximization problem of the CFP is formulated as follows.

Problem 2 (CFP Subgame):

$$\begin{aligned} \underset{\mathbf{p}}{\text{maximize}} \quad & \Pi(\mathbf{p}, \mathbf{x}) \\ \text{subject to} \quad & 0 \le p_i \le \bar{p}. \end{aligned} \tag{9}$$

Problem 1 and Problem 2 together form the Stackelberg game, and the objective of this game is to find the Stackelberg equilibrium. The Stackelberg equilibrium ensures that the profit of the CFP is maximized given that the miners generate their demands following the best responses, i.e., the Nash equilibrium. This means that the demands from the miners maximize the utility. In our problem, the Stackelberg equilibrium can be written as follows.

Definition 1: Let $\mathbf{x}^*$ and $\mathbf{p}^*$ denote the optimal service demand vector of all the miners and optimal unit price vector of computing service, respectively. Then, the point $(\mathbf{x}^*, \mathbf{p}^*)$ is the Stackelberg equilibrium if the following conditions:

$$\Pi(\mathbf{p}^*, \mathbf{x}^*) \ge \Pi(\mathbf{p}, \mathbf{x}^*) \tag{10}$$

and

$$u_i(x_i^*, \mathbf{x}_{-i}^*, \mathbf{p}^*) \ge u_i(x_i, \mathbf{x}_{-i}^*, \mathbf{p}^*) \quad \forall x_i \ge 0; \ \forall i \tag{11}$$

are satisfied, where $\mathbf{x}_{-i}^*$ is the best response service demand vector for all the miners except miner i.

Note that the same or different prices can be applied to the miners, which we refer to them as the uniform and discriminatory pricing schemes, respectively. In the following, we investigate these two pricing schemes for resource management in blockchain networks. The Stackelberg equilibrium ensures that the profit of the CFP is maximized given that the miners generate their demands following the best responses,

i.e., the Nash equilibrium. This means that the demands from the miners maximize the utility. The Stackelberg equilibrium under the uniform pricing scheme contains only one single price that the CFP imposes to the miners identically. On the contrary, the equilibrium under the discriminatory pricing scheme contains different prices, each of which the CFP imposes to each miner separately.

The significance of each pricing scheme is as follows. Under the uniform pricing scheme, the equilibrium ensures a fair price applied to all miners. The miners are indifferent to choose the services. However, the CFP has limited degree of freedom to maximize its profit. By contrast, under the discriminatory pricing scheme, the CFP can customize the price for each miner, matching with the miner's demand and preference. As such, the profit obtained under the discriminatory pricing scheme is expected to be superior to that of the uniform pricing scheme in terms of the higher profit for the CFP.

IV. Equilibrium Analysis for Cloud/Fog Computing Resource Management

In this section, we propose the uniform pricing and discriminatory pricing schemes for resource management in blockchain application involving PoW assisted by the CFP. We then analyze the optimal service demand of miners as well as the profit maximization of the CFP under both pricing schemes.

A. Uniform Pricing Scheme

We first consider the uniform pricing scheme, in which the CFP charges all the miners the same unit price for their computing service demand, i.e., $p_i = p, \forall i$. Given the payoff functions defined in Section III, we use backward induction to analyze the Stackelberg game.

1) Stage II (Miners' Demand Game): Given the price p decided by the CFP, in Stage II, the miners compete with each other to maximize their own utility by choosing their individual service demand, which forms the noncooperative miners' demand game (MDG) $\mathcal{G}^u = \{\mathcal{N}, \{x_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}}\}$, where $\mathcal{N}$ is the set of miners, $\{x_i\}_{i\in\mathcal{N}}$ is the strategy set, and u_i is the utility, i.e., payoff, function of miner i. Specifically, each miner $i \in \mathcal{N}$ selects its strategy to maximize its utility function $u_i(x_i, \mathbf{x}_{-i}, p)$. We next analyze the existence and uniqueness of the Nash equilibrium in the MDG.

Definition 2: A demand vector $\mathbf{x}^* = (x_1^*, \ldots, x_N^*)$ is the Nash equilibrium of the MDG $\mathcal{G}^u = \{\mathcal{N}, \{x_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}}\}$, if, for every miner $i \in \mathcal{N}$, $u_i(x_i^*, \mathbf{x}_{-i}^*, p) \geq u_i(x_i', \mathbf{x}_{-i}^*, p)$ for all $x_i' \in [\underline{x}, \bar{x}]$, where $u_i(x_i, \mathbf{x}_{-i})$ is the resulting utility of the miner i, given the other miners' demand $\mathbf{x}_{-i}$

$$x_i^* = \mathscr{F}_i(\mathbf{x}) = \begin{cases} \underline{x}, & \sqrt{\frac{(R+rt_i)\sum_{i\neq j} x_j}{pe^{-\lambda z t_i}}} - \sum_{i\neq j} x_j < \underline{x} \\ \sqrt{\frac{(R+rt_i)\sum_{i\neq j} x_j}{pe^{-\lambda z t_i}}} - \sum_{i\neq j} x_j, & \underline{x} \leq \sqrt{\frac{(R+rt_i)\sum_{i\neq j} x_j}{pe^{-\lambda z t_i}}} - \sum_{i\neq j} x_j \leq \bar{x} \\ \bar{x}, & \sqrt{\frac{(R+rt_i)\sum_{i\neq j} x_j}{pe^{-\lambda z t_i}}} - \sum_{i\neq j} x_j > \bar{x}. \end{cases} \tag{12}$$

Theorem 1: A Nash equilibrium exists in MDG $\mathcal{G}^u = \{\mathcal{N}, \{x_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}}\}$.

Proof: First, the strategy space for each miner is defined to be $[\underline{x}, \bar{x}]$, which is a nonempty, convex, and compact subset of the Euclidean space. From (6), u_i is apparently continuous in $[\underline{x}, \bar{x}]$. Then, we take the first-order and second-order derivatives of (6) with respect to x_i to prove its concavity, which can be written as follows:

$$\frac{\partial u_i}{\partial x_i} = (R + rt_i)e^{-\lambda z t_i}\frac{\partial \alpha_i}{\partial x_i} - p \tag{13}$$

$$\frac{\partial^2 u_i}{\partial {x_i}^2} = (R + rt_i)e^{-\lambda z t_i}\frac{\partial^2 \alpha_i}{\partial {x_i}^2} < 0 \tag{14}$$

where $(\partial\alpha_i/\partial x_i) = [(\sum_{i\neq j} x_j)/(\sum_{i\in\mathcal{N}} x_j)^2] > 0$, and $(\partial^2\alpha_i/\partial {x_i}^2) = -2[(\sum_{i\neq j} x_j)/(\sum_{i\in\mathcal{N}} x_j)^3] < 0$.

Therefore, we have proved that u_i is strictly concave with respect to x_i. Accordingly, the Nash equilibrium exists in this noncooperative MDG $\mathcal{G}^u$ [42]. The proof is now completed. ■

Further, based on the first-order derivative condition, we have

$$\frac{\partial u_i}{\partial x_i} = (R + rt_i)e^{-\lambda z t_i}\frac{\partial \alpha_i}{\partial x_i} - p = 0 \tag{15}$$

and we obtain the best response function of miner i by solving (15), as shown in (12).

Theorem 2: The uniqueness of the Nash equilibrium in the noncooperative MDG is guaranteed given the following condition:

$$\frac{2(N-1)e^{-\lambda z t_i}}{R + rt_i} < \sum_{i\in\mathcal{N}} \frac{e^{-\lambda z t_i}}{R + rt_i} \tag{16}$$

is satisfied.

Proof: Let $\mathbf{x}^*$ denote the Nash equilibrium of the MDG. By definition, the Nash equilibrium needs to satisfy $\mathbf{x} = \mathscr{F}(\mathbf{x})$, in which $\mathscr{F}(\mathbf{x}) = (\mathscr{F}_1(\mathbf{x}), \mathscr{F}_2(\mathbf{x}), \ldots, \mathscr{F}_N(\mathbf{x}))$. In particular, $\mathscr{F}_i(\mathbf{x})$ is the best response function of miner i, given the demand strategies of other miners. The uniqueness of the Nash equilibrium can be proved by showing that the best response function of miner i, i.e., as given in (12), is the standard function [42].

Definition 3: A function $\mathscr{F}(\mathbf{x})$ is a standard function when the following properties are guaranteed [42].

1) *Positivity:* $\mathscr{F}(\mathbf{x}) > \mathbf{0}$.
2) *Monotonicity:* If $\mathbf{x} \leq \mathbf{x}'$, then $\mathscr{F}(\mathbf{x}) \leq \mathscr{F}(\mathbf{x}')$.
3) *Scalability:* For all $\lambda > 1$, $\lambda\mathscr{F}(\mathbf{x}) > \mathscr{F}(\lambda\mathbf{x})$.

First, for the positivity, under the condition in (16), we have (from Lemma 1)

$$\sum_{i\neq j} x_j < \frac{R + rt_i}{pe^{-\lambda z t_i}} < \frac{R + rt_i}{4pe^{-\lambda z t_i}} \tag{17}$$

then we can conclude that

$$\sum_{i\neq j} x_j < \sqrt{\frac{R+rt_i\sum_{i\neq j}x_j}{pe^{-\lambda z t_i}}}. \tag{18}$$

Thus, we can prove that

$$\mathscr{F}_i(\mathbf{x}) = \sqrt{\frac{R+rt_i\sum_{i\neq j}x_j}{pe^{-\lambda z t_i}}} - \sum_{i\neq j} x_j > 0 \tag{19}$$

$$\begin{aligned}\mathcal{F}_i(\mathbf{x}') - \mathcal{F}_i(\mathbf{x}) &= \sqrt{\frac{R+rt_i\sum_{i\neq j}x_j'}{pe^{-\lambda z t_i}}} - \sum_{i\neq j}x_j' - \sqrt{\frac{(R+rt_i)\sum_{i\neq j}x_j}{pe^{-\lambda z t_i}}} - \sum_{i\neq j}x_j \\ &= \left(\sqrt{\frac{R+rt_i}{pe^{-\lambda z t_i}}} - \sqrt{\sum_{i\neq j}x_j'} - \sqrt{\sum_{i\neq j}x_j}\right)\left(\sqrt{\sum_{i\neq j}x_j'} - \sqrt{\sum_{i\neq j}x_j}\right)\end{aligned} \tag{20}$$

$$\begin{aligned}\lambda\mathcal{F}_i(\mathbf{x}) - \mathcal{F}_i(\lambda\mathbf{x}) &= \lambda\sqrt{\frac{(R+rt_i)\sum_{i\neq j}x_j}{pe^{-\lambda z t_i}}} - \lambda\sum_{i\neq j}x_j \\ &\quad - \sqrt{\frac{(R+rt_i)\sum_{i\neq j}\lambda x_j}{pe^{-\lambda z t_i}}} - \sum_{i\neq j}\lambda x_j \\ &= \left(\lambda - \sqrt{\lambda}\right)\sqrt{\frac{(R+rt_i)\sum_{i\neq j}x_j}{pe^{-\lambda z t_i}}} > 0 \quad \forall\lambda > 1\end{aligned} \tag{21}$$

which is the positivity condition. Second, we prove the monotonicity of (12). Let $\mathbf{x}' > \mathbf{x}$, we can further simplify the expression of $\mathcal{F}_i(\mathbf{x}') - \mathcal{F}_i(\mathbf{x})$, which is shown in (20). In particular, we have $\sqrt{\sum_{i\neq j}x_j'} - \sqrt{\sum_{i\neq j}x_j} > 0$, and we can easily verify that

$$\begin{aligned}&\sqrt{\frac{R+rt_i}{pe^{-\lambda z t_i}}} - \sqrt{\sum_{i\neq j}x_j'} - \sqrt{\sum_{i\neq j}x_j} \\ &\in \left(\sqrt{\frac{R+rt_i}{pe^{-\lambda z t_i}}} - 2\sqrt{\sum_{i\neq j}x_j'}, \sqrt{\frac{R+rt_i}{pe^{-\lambda z t_i}}} - 2\sqrt{\sum_{i\neq j}x_j}\right).\end{aligned} \tag{22}$$

Under the condition in (30), we can prove that

$$\sqrt{\frac{R+rt_i}{pe^{-\lambda z t_i}}} - 2\sqrt{\sum_{i\neq j}x_j} > 0 \quad \forall x_j. \tag{23}$$

Thus, the best response function of miner i in (12) is always positive.

At last, as for scalability, we need to prove that $\lambda\mathscr{F}(x) > \mathscr{F}(\lambda x)$, for $\lambda > 1$. The steps of proving the positivity of $\lambda\mathcal{F}(x) - \mathcal{F}(\lambda x)$ are shown in (20). Therefore, $\lambda\mathscr{F}(x) > \mathscr{F}(\lambda x)$ is always satisfied for $\lambda > 1$. Until now, we have proved that the best response function in (12) satisfies three properties described in Definition 2. Therefore, the Nash equilibrium of MDG $\mathcal{G}^u = \{\mathcal{N}, \{x_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}}\}$ is unique. The proof is now completed. ■

Theorem 3: The unique Nash equilibrium for miner i in the MDG is given by

$${x_i}^* = \frac{N-1}{\sum_{j\in\mathcal{N}}\frac{pe^{-\lambda z t_j}}{R+rt_j}} - \left(\frac{N-1}{\sum_{j\in\mathcal{N}}\frac{pe^{-\lambda z t_j}}{R+rt_j}}\right)^2\frac{pe^{-\lambda z t_i}}{R+rt_i} \quad \forall i \tag{24}$$

provided that the condition in (16) holds.

Proof: According to (13), for each miner i, we have the mathematical expression

$$\frac{\sum_{i\neq j}x_j}{\left(\sum_{j\in\mathcal{N}}x_j\right)^2} = \frac{pe^{-\lambda z t_i}}{R+rt_i}. \tag{25}$$

Then, we calculate the summation of this expression for all the miners as follows:

$$\frac{(N-1)\sum_{j\in\mathcal{N}}x_j}{\left(\sum_{j\in\mathcal{N}}x_j\right)^2} = \sum_{i\in\mathcal{N}}\frac{pe^{-\lambda z t_i}}{R+rt_i} \tag{26}$$

which means $[(N-1)/(\sum_{j\in\mathcal{N}}x_j)] = \sum_{i\in\mathcal{N}}([pe^{-\lambda z t_i}]/[R+rt_i])$. Thus, we have

$$\sum_{j\in\mathcal{N}}x_j = \frac{N-1}{\sum_{i\in\mathcal{N}}\frac{pe^{-\lambda z t_i}}{R+rt_i}}. \tag{27}$$

Recall from (12), according to the first-order derivative condition, we have

$$\sum_{j\in\mathcal{N}}x_j = \sqrt{\frac{(R+rt_i)\sum_{i\neq j}x_j}{pe^{-\lambda z t_i}}}. \tag{28}$$

By substituting (28) into (27), we have

$$\frac{N-1}{\sum_{i\in\mathcal{N}}\frac{pe^{-\lambda z t_i}}{R+rt_i}} = \sqrt{\frac{R+rt_i}{pe^{-\lambda z t_i}}\left(\frac{N-1}{\sum_{i\in\mathcal{N}}\frac{pe^{-\lambda z t_i}}{R+rt_i}} - x_i\right)}. \tag{29}$$

After squaring both sides, we have

$$\left(\frac{N-1}{\sum_{i\in\mathcal{N}}\frac{pe^{-\lambda z t_i}}{R+rt_i}}\right)^2 = \frac{R+rt_i}{pe^{-\lambda z t_i}}\left(\frac{N-1}{\sum_{i\in\mathcal{N}}\frac{pe^{-\lambda z t_i}}{R+rt_i}} - x_i\right).$$

With simple transformations, we obtain the Nash equilibrium for miner i as shown in (24). ■

Lemma 1: Given

$$\frac{2(N-1)e^{-\lambda z t_i}}{R+rt_i} < \sum_{i\in\mathcal{N}}\frac{e^{-\lambda z t_i}}{R+rt_i} \tag{30}$$

the following condition:

$$\sum_{i\neq j}x_j < \frac{R+rt_i}{4pe^{-\lambda z t_i}} \tag{31}$$

is satisfied.

Proof: According to (24) and (27), we can obtain

$$\sum_{j\neq i}x_j = \left(\frac{N-1}{\sum_{j\in\mathcal{N}}\frac{pe^{-\lambda z t_j}}{R+rt_j}}\right)^2\frac{pe^{-\lambda z t_i}}{R+rt_i}. \tag{32}$$

After substituting (30) into (32), we have

$$\frac{2(N-1)pe^{-\lambda z t_i}}{R+rt_i} < \sum_{i\in\mathcal{N}}\frac{pe^{-\lambda z t_i}}{R+rt_i} \tag{33}$$

which means that the condition in (30) needs to be ensured. On the contrary, if the condition in (30) holds, then, the condition in (32) is satisfied. The proof is now completed. ■

Generally, we can use the best-response dynamics for obtaining the Nash equilibrium of the N-player noncooperative game in Stage II [42]. In the following, we analyze the profit maximization of the CFP in Stage I under uniform pricing.

2) Stage I (CFP's Profit Maximization): Based on the Nash equilibrium of the computing service demand in the MDG $\mathcal{G}^u = \{\mathcal{N}, \{x_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}}\}$ in Stage II, the leader of the Stackelberg game, i.e., the CFP, can optimize its pricing strategy in Stage I to maximize its profit defined in (8). Thus, the optimal pricing can be formulated as an optimization problem. By substituting (24) into (8), the profit maximization of the CFP is simplified as follows:

$$\begin{aligned} \underset{p>0}{\text{maximize}} \quad & \Pi(p) = (p - cT)\frac{N-1}{\sum_{j\in\mathcal{N}} \frac{pe^{-\lambda z t_j}}{R+rt_j}} \\ \text{subject to} \quad & 0 \le p \le \overline{p}. \end{aligned} \tag{34}$$

Theorem 4: Under uniform pricing, the CFP achieves the globally optimal profit, i.e., profit maximization, under the unique optimal price.

Proof: From (34), we have

$$\Pi(p) = \frac{p - cT}{p}\frac{N-1}{\sum_{j\in\mathcal{N}} \frac{e^{-\lambda z t_j}}{R+rt_j}}. \tag{35}$$

The first and second derivatives of profit $\Pi(p)$ with respect to price p are given as follows:

$$\frac{d\Pi(p)}{dp} = \frac{cT}{p^2}\frac{N-1}{\sum_{j\in\mathcal{N}} \frac{e^{-\lambda z t_j}}{R+rt_j}} \tag{36}$$

and

$$\frac{d^2\Pi(p)}{dp^2} = -\frac{2cT}{p^2}\frac{N-1}{\sum_{j\in\mathcal{N}} \frac{e^{-\lambda z t_j}}{R+rt_j}} < 0. \tag{37}$$

Due to the negativity of (37), the strict concavity of the objective function is ensured. Thus, the CFP is able to achieve the maximum profit with the unique optimal price. The proof is now completed. ∎

Note that the profit maximization defined in (34) is a convex optimization problem, and thus it can be solved by standard convex optimization algorithms, e.g., gradient assisted binary search. Under uniform pricing, we have proved that the Nash equilibrium in Stage II is unique and the optimal price in Stage I is also unique. Thus, we can conclude that the Stackelberg equilibrium is unique and accordingly the best-response dynamics algorithm can achieve this unique Stackelberg equilibrium [42].

B. Discriminatory Pricing Scheme

Then, we consider the discriminatory pricing scheme, in which the CFP is able to set different unit prices of service demand for different miners. Again, we use the backward induction to analyze the optimal service demand of miners and the profit maximization of the CFP.

1) Stage II (Miners' Demand Game): Under discriminatory pricing scheme, the strategy space of the CFP becomes $\{\mathbf{p} = [p_i]_{i\in\mathcal{N}} : 0 \le p_i \le \overline{p}\}$. Recall that we prove the existence and uniqueness of MDG $\mathcal{G}^u = \{\mathcal{N}, \{x_i\}_{i\in\mathcal{N}}, \{u_i\}_{i\in\mathcal{N}}\}$, given the fixed price from the CFP. Thus, under discriminatory pricing, the existence and uniqueness of the MDG can be still guaranteed. With minor change from Theorem 3, we have the following theorem immediately.

Theorem 5: Under uniform pricing, the unique Nash equilibrium demand of miner i can be obtained as follows:

$${x_i}^* = \frac{N-1}{\sum_{j\in\mathcal{N}} \frac{p_j e^{-\lambda z t_j}}{R+rt_j}} - \left(\frac{N-1}{\sum_{j\in\mathcal{N}} \frac{p_j e^{-\lambda z t_j}}{R+rt_j}}\right)^2 \frac{p_i e^{-\lambda z t_i}}{R+rt_i}, \forall i \tag{38}$$

if the following condition:

$$\frac{2(N-1)p_i e^{-\lambda z t_i}}{R+rt_i} < \sum_{j\in\mathcal{N}} \frac{p_j e^{-\lambda z t_j}}{R+rt_j} \tag{39}$$

holds.

Proof: The steps of proof are similar to those in the case of uniform pricing as shown in Section IV-A1, and thus we omit them for brevity. ∎

We next analyze the profit maximization of the CFP in Stage I under discriminatory pricing to further investigate the Stackelberg equilibrium.

2) Stage I (CFP's Profit Maximization): Similar to that in Section IV-A2, we analyze the profit maximization with the analytical result from Theorem 5, i.e., the Nash equilibrium of the computing service demand in Stage II. After substituting (38) into (8), we have the following optimization:

$$\begin{aligned} \underset{\mathbf{p}>\mathbf{0}}{\text{maximize}} \quad & \Pi(\mathbf{p}) = \sum_{i\in\mathcal{N}} \left(p_i - cT\frac{N-1}{\sum_{j\in\mathcal{N}} \frac{p_j e^{-\lambda z t_j}}{R+rt_j}}\right) \\ \text{subject to} \quad & 0 \le p_i \le \overline{p} \quad \forall i. \end{aligned} \tag{40}$$

Theorem 6: $\Pi(\mathbf{p})$ is concave on each p_i, when $\sum_{i\neq j}(a_i + a_j)(1 - [N(p_j/a_j)/\sum_{j\in\mathcal{N}}(p_j/a_j)]) \le 0$, and decreasing on each p_i when $\sum_{i\neq j}(a_i + a_j)(1 - [N(p_j/a_j)]/[\sum_{j\in\mathcal{N}}(p_j/a_j)]) > 0$, provided that the following condition:

$$\frac{p_i}{a_i} \ge \frac{\sum_{j\in\mathcal{N}} \frac{p_j}{a_j}}{(N-1)^2} \tag{41}$$

is satisfied, where $a_i = (R + rt_i)e^{-\lambda z t_i}$.

Proof: We first decompose the objective function in (40) into two parts, namely, $\sum_i cT x_i^*$ and $\sum_i p_i x_i^*$. Then, we analyze the properties of each part. We define

$$f(\mathbf{p}) = -cT{x_i}^* = -cT\frac{N-1}{\sum_{j\in\mathcal{N}} \frac{p_j e^{-\lambda z t_j}}{R+rt_j}}. \tag{46}$$

Let $a_j = (R + rt_j)e^{-\lambda z t_j}$, and we have $f(\mathbf{p}) = ([-cT(N-1)]/[\sum_{j\in\mathcal{N}}(p_j/a_j)])$. Then, we obtain the first and the second partial derivatives of (46) with respect to p_i as follows:

$$\frac{\partial f(\mathbf{p})}{\partial p_i} = \frac{(N-1)cT}{a_i\left(\sum_{j\in\mathcal{N}} \frac{p_j}{a_j}\right)^2} \tag{47}$$

$$\frac{\partial^2 f(\mathbf{p})}{\partial {p_i}^2} = \frac{-2(N-1)cT}{{a_i}^2\left(\sum_{j\in\mathcal{N}} \frac{p_j}{a_j}\right)^3}. \tag{48}$$

Further, we have

$$\frac{\partial f(\mathbf{p})}{\partial p_i p_j} = \frac{-2(N-1)cT}{a_i a_j \left(\sum_{j\in\mathcal{N}} \frac{p_j}{a_j}\right)^3}. \tag{49}$$

Thus, we can obtain the Hessian matrix of $f(\mathbf{p})$, which is expressed as

$$\nabla^2 f(\mathbf{p}) = \frac{-2(N-1)cT}{\left(\sum_{j\in\mathcal{N}} \frac{p_j}{a_j}\right)^3} \begin{bmatrix} \frac{1}{{a_1}^2} & \frac{1}{a_1 a_2} & \cdots & \frac{1}{a_1 a_N} \\ \frac{1}{a_2 a_1} & \frac{1}{{a_2}^2} & \cdots & \frac{1}{a_2 a_N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_N a_1} & \frac{1}{a_N a_2} & \cdots & \frac{1}{{a_N}^2} \end{bmatrix}. \tag{50}$$

For each $i \in \mathcal{N}$, we have $(1/{a_i}^2) > 0$. Thus, the diagonal elements of the Hessian matrix are all larger than zero, and the principle minors are equal to zero. Therefore, the Hessian matrix of $f(\mathbf{p})$ is semi-negative definite.

Then, we analyze the properties of $\sum_i p_i x_i^*$. We first define

$$g(\mathbf{p}) = \sum_{i\in\mathcal{N}} p_i {x_i}^* = \frac{\sum_{j\neq i} a_i x_i x_j}{\left(\sum_{j\neq i} x_j\right)^2}. \tag{51}$$

By substituting (38) into (51), we can obtain the final expression for $g(\mathbf{p})$, which can be rewritten as (42), shown at the bottom of this page. Then, we derive the first-order and the second partial derivatives of (42) with respect to p_i as shown in (43), at the bottom of this page, and (52), at the bottom of the next page. Since we have

$$\begin{aligned} x_i &= \frac{N-1}{\sum_{h\in\mathcal{N}} \frac{p_h}{a_h}} - \frac{p_i}{a_i}\left(\frac{N-1}{\sum_{h\in\mathcal{N}} \frac{p_h}{a_h}}\right)^2 \\ &= \frac{N-1}{\sum_{h\in\mathcal{N}} \frac{p_h}{a_h}}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}} \frac{p_h}{a_h}}\frac{p_i}{a_i}\right) > 0 \end{aligned}$$

then

$$1 - \frac{N-1}{\sum_{h\in\mathcal{N}} \frac{p_h}{a_h}}\frac{p_i}{a_i} > 0.$$

When $\sum_{i\neq j}(a_i + a_j)(1 - [N(p_j/a_j)]/[\sum_{j\in\mathcal{N}}(p_j/a_j)]) \leq 0$, it is observed from (53), shown at the bottom of the next page, that $[\partial^2 g(\mathbf{p})/\partial {p_i}^2] < 0$, i.e., $g(\mathbf{p})$ is concave on each p_i. Now we prove that $\Pi(\mathbf{p})$ is a monotonically decreasing function with respect to p_i, when $\sum_{i\neq j}(a_i + a_j)(1 - [N(p_j/a_j)]/[\sum_{j\in\mathcal{N}}(p_j/a_j)]) > 0$. The steps are shown in (45), at the bottom of the next page, where $p_{\min} = \min\{p_1, p_2, \ldots, p_N\}$. Practically, $p_{\min} > cT$. Thus, with some manipulations, we can prove $(\partial\Pi/\partial p_i) < 0$ when $\sum_{i\neq j}(a_i + a_j)(1 - [N(p_j/a_j)]/[\sum_{j\in\mathcal{N}}(p_j/a_j)]) > 0$, if the condition in (41) holds. The proof is now completed. ■

Theorem 7: Under discriminatory pricing, the CFP achieves the profit maximization by finding the unique optimal pricing vector.

Proof: From Theorem 6, we know that $\Pi(\mathbf{p})$ is concave on each p_i, when $\sum_{i\neq j}(a_i + a_j)(1 - [N(p_j/a_j)]/[\sum_{j\in\mathcal{N}}(p_j/a_j)]) \leq 0$, and decreasing on each p_i when $\sum_{i\neq j}(a_i + a_j)(1 - [N(p_j/a_j)]/[\sum_{j\in\mathcal{N}}(p_j/a_j)]) > 0$. In other words, when $\Pi(\mathbf{p})$ is concave on p_i, p_i needs to be smaller than a certain threshold, and $\Pi(\mathbf{p})$ is decreasing on p_i when p_i is larger than this threshold. Then, it can be concluded that if the price is higher than the threshold, the miner is not willing to purchase the computing service from the CFP. Therefore, we know that the optimal value of profit of the CFP, i.e., $\Pi^*(\mathbf{p})$ is achieved in the concave parts when $\sum_{i\neq j}(a_i + a_j)(1 - [N(p_j/a_j)]/[\sum_{j\in\mathcal{N}}(p_j/a_j)]) \leq 0$. Clearly, the maximization of profit $\Pi(\mathbf{p})$ is achieved either in the boundary of domain area or in the local maximization point. Since we know that the optimal value of profit, i.e., $\Pi^*(\mathbf{p})$ is achieved in the interior area, and thus $\mathbf{p}^*$ exists. In the following, we prove that there exists at most one optimal solution by using VI theory [43], from which the uniqueness of the optimal solution, i.e., the Stackelberg equilibrium, follows.

Let the set

$$\mathcal{K} = \left\{\mathbf{p} = [p_1, \ldots, p_N]^\top \middle| \sum_{i\neq j}(a_i + a_j)\left(1 - \frac{N\frac{p_j}{a_j}}{\sum_{j\in\mathcal{N}}\frac{p_j}{a_j}}\right) \leq 0 \quad \forall i \in \mathcal{N}\right\}.$$

The constraint can be rewritten as follows:

$$\sum_{i\neq j}\left((a_i + a_j)\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h} - N\frac{p_j}{a_j}\right)\right) \leq 0. \tag{54}$$

$$g(\mathbf{p}) = \sum_{j\neq h}\left(a_h\left(1 - \frac{p_h}{a_h}\frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\right)\left(1 - \frac{p_j}{a_j}\frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\right)\right) \tag{42}$$

$$\frac{\partial g(\mathbf{p})}{\partial p_i} = \sum_{j\neq i}\left((a_i + a_j)\left(\frac{-\frac{N-1}{a_i}\sum_{h\neq i}\frac{p_h}{a_h}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right) + \frac{\frac{N-1}{a_i}\frac{p_j}{a_j}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i}{a_i}\right)\right)\right) \tag{43}$$

$$\begin{aligned} &\sum_{i\neq j}\left((a_i + a_j)\left(\sum_{h\in\mathcal{N}}\frac{\lambda p_h' + (1-\lambda)p_h''}{a_h} - N\frac{\lambda p_j' + (1-\lambda)p_j''}{a_j}\right)\right) \\ &= \sum_{i\neq j}\left((a_i + a_j)\left(\lambda\sum_{h\in\mathcal{N}}\frac{p_h'}{a_h} - (1-\lambda)\sum_{h\in\mathcal{N}}\frac{p_h''}{a_h} - \lambda N\frac{p_j'}{a_j} - (1-\lambda)N\frac{p_j''}{a_j}\right)\right) \\ &= \lambda\sum_{i\neq j}\left((a_i + a_j)\left(\sum_{h\in\mathcal{N}}\frac{p_h'}{a_h} - N\frac{p_j''}{a_j}\right)\right) + (1-\lambda)\sum_{i\neq j}\left((a_i + a_j)\left((1-\lambda)\sum_{h\in\mathcal{N}}\frac{p_h'}{a_h} - N\frac{p_j''}{a_j}\right)\right) \leq 0 \end{aligned} \tag{44}$$

Thus, we redefine the set $\mathcal{K}$ as $\{\mathbf{p} = [p_1, \ldots, p_N]^\top | \sum_{i\neq j}((a_i + a_j)(\sum_{h\in\mathcal{N}}(p_h/a_h) - N(p_j/a_j))) \leq 0, \forall i \in \mathcal{N}\}$. Then, we formulate an equivalent problem to (40) as follows:

$$\begin{aligned} \underset{\mathbf{p}>\mathbf{0}}{\text{minimize}} \quad & -\Pi(\mathbf{p}) \\ \text{subject to} \quad & \mathbf{p} \in \mathcal{K}. \end{aligned} \tag{55}$$

Let $F(\mathbf{p}) = \nabla(-\Pi(\mathbf{p})) = -[\nabla_{p_i}\Pi]^\top_{i\in\mathcal{N}}$. Accordingly, the optimization problem in (55) is equivalent to find a point set $\mathbf{p}^* \in \mathcal{K}$, such that $(\mathbf{p} - \mathbf{p}^*)F(\mathbf{p}^*) \geq 0, \forall \mathbf{p} \in \mathcal{K}$, which is the VI problem: VI($\mathcal{K}, F$).

Definition 4: If F is strictly monotone on $\mathcal{K}$, then VI($\mathcal{K}, F$) has at most one solution, where $\mathcal{K} \in \mathbb{R}^N$ is a convex closed set, and the mapping $F : \mathcal{K} \mapsto \mathbb{R}^N$ is continuous [43].

Let $\lambda \in (0, 1)$, $\mathbf{p}', \mathbf{p}'' \in \mathcal{K}$, it can be concluded that $\lambda\mathbf{p}' + (1 - \lambda)\mathbf{p}' \in \mathcal{K}$, which is shown in (44), at the bottom of the previous page. Accordingly, $\mathcal{K}$ is a convex and closed set. To prove that the mapping $F : \mathcal{K} \mapsto \mathbb{R}^N$ is strictly monotone on $\mathcal{K}$, we check the positivity of $(\mathbf{p}' - \mathbf{p}'')^\top(F(\mathbf{p}') - F(\mathbf{p}'')), \forall \mathbf{p}', \ \mathbf{p}'' \in \mathcal{K}$ and $\mathbf{p}' \neq \mathbf{p}''$. We know

$$\begin{aligned} &(\mathbf{p}' - \mathbf{p}'')^\top(F(\mathbf{p}') - F(\mathbf{p}'')) \\ &= \sum_{i\in\mathcal{N}}\left((p_i' - p_i'')\left(-\nabla_{p_i}\Pi\big|_{p_i=p_i'} + \nabla_{p_i}\Pi\big|_{p_i=p_i''}\right)\right) \end{aligned} \tag{56}$$

and from Theorem 6, we have

$$\frac{\partial^2\Pi(\mathbf{p})}{\partial {p_i}^2} = \frac{\partial^2(f(\mathbf{p}) + g(\mathbf{p}))}{\partial {p_i}^2} < 0. \tag{57}$$

Thus, $\nabla_{p_i}\Pi$ is decreasing on each p_i, and $-\nabla_{p_i}\Pi$ is increasing on each p_i. It can be concluded that

$$-\nabla_{p_i}\Pi\big|_{p_i=p_i'} + \nabla_{p_i}\Pi\big|_{p_i=p_i''} = \begin{cases} \geq 0, p_i' \geq p_i'' \\ < 0, p_i' < p_i''. \end{cases} \tag{58}$$

$$\begin{aligned} \frac{\partial\Pi(\mathbf{p})}{\partial p_i} &= \sum_{j\neq i}\left((a_i + a_j)\left(\frac{\frac{N-1}{a_i}\sum_{h\neq i}\frac{p_h}{a_h}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right) + \frac{\frac{N-1}{a_i a_j}p_j}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i}{a_i}\right)\right)\right) + \frac{\frac{N-1}{a_i}cT}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2} \\ &\leq \frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(\sum_{j\neq i}\left((a_i + a_j)\left(-\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right) + \frac{p_j}{a_j}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i}{a_i}\right)\right)\right) + cT\right) \\ &= \underbrace{-\frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\sum_{j\neq i}\left((a_i + a_j)\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\left(1 - \frac{N}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right)\right)\right)}_{<0} + \frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(cT - \sum_{j\neq i}\left((a_i + a_j)\frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i}{a_i}\frac{p_j}{a_j}\right)\right) \\ &= -\frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\sum_{j\neq i}\left((a_i + a_j)\left(-\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\left(1 - \frac{N}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right)\right)\right) + \frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(cT - \sum_{j\neq i}\left(\underbrace{\frac{a_i + a_j}{a_j}}_{<1}\frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i p_j}{a_i}\right)\right) \\ &\leq -\frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\sum_{j\neq i}\left((a_i + a_j)\left(-\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\left(1 - \frac{N}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right)\right)\right) + \frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(cT - p_{\min}\frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{N-1p_i}{a_i}\right) \\ &= \underbrace{-\frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\sum_{j\neq i}\left((a_i + a_j)\left(-\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\left(1 - \frac{N}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right)\right)\right)}_{<0} + \underbrace{\frac{\frac{N-1}{a_i}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^2}\left(cT - p_{\min}\frac{(N-1)^2}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i}{a_i}\right)}_{<0} < 0 \end{aligned} \tag{45}$$

$$\frac{\partial^2 g(\mathbf{p})}{\partial {p_i}^2} = \sum_{j\neq i}\left((a_i + a_j)\left(\frac{2\frac{N-1}{{a_i}^2}\sum_{h\neq i}\frac{p_h}{a_h}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^3}\left(1 - 2\frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right) - \frac{2\frac{N-1}{{a_i}^2}\frac{p_j}{a_j}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^3}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i}{a_i}\right)\right)\right) \tag{52}$$

$$\begin{aligned} \frac{\partial^2 g(\mathbf{p})}{\partial {p_i}^2} &= \frac{2\frac{N-1}{{a_i}^2}\sum_{h\neq i}\frac{p_h}{a_h}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^3}\sum_{j\neq i}\left((a_i + a_j)\left(1 - 2\frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right)\right) - \frac{2\frac{N-1}{{a_i}^2}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^3}\sum_{j\neq i}\left((a_i + a_j)\frac{p_j}{a_j}\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i}{a_i}\right)\right) \\ &\leq \frac{2\frac{N-1}{{a_i}^2}\sum_{h\neq i}\frac{p_h}{a_h}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^3}\underbrace{\sum_{j\neq i}\left((a_i + a_j)\left(1 - \frac{N}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_j}{a_j}\right)\right)}_{\leq 0} - \frac{2\frac{N-1}{{a_i}^2}}{\left(\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}\right)^3}\sum_{j\neq i}\left((a_i + a_j)\frac{p_j}{a_j}\underbrace{\left(1 - \frac{N-1}{\sum_{h\in\mathcal{N}}\frac{p_h}{a_h}}\frac{p_i}{a_i}\right)}_{\geq 0}\right) \end{aligned} \tag{53}$$

Algorithm 1 Gradient Iterative Algorithm to Find Stackelberg Equilibrium Under Discriminatory Pricing

1: **Initialization:**
Select initial input $\mathbf{p} = [p_i]_{i\in\mathcal{N}}$ where $p_i \in [0, \overline{p}]$, $k \leftarrow 1$, precision threshold ε;
2: **repeat**
3: Each miner i decides its computing service demand $x_i^{[k]}$ based on (12);
4: CFP updates the prices using a gradient assisted searching algorithm, i.e.,

$$\mathbf{p}(t+1) = \mathbf{p}(t) + \mu\nabla\Pi(\mathbf{p}(t)), \tag{60}$$

where μ is the step size of the price update and $\mu\nabla\Pi(\mathbf{p}(t))$ is the gradient with $\frac{\partial\Pi(\mathbf{p}(t))}{\partial\mathbf{p}(t)}$. The price information is sent to all miners;
5: $k \leftarrow k+1$;
6: **until** $\frac{\left\|\mathbf{p}^{[k]}-\mathbf{p}^{[k-1]}\right\|_1}{\left\|\mathbf{p}^{[k-1]}\right\|_1} < \varepsilon$
7: **Output:** optimal demand $\mathbf{x}^{*[k]}$ and optimal price $\mathbf{p}^{*[k]}$.

Then, we have

$$\left((p_i' - p_i'')\left(-\nabla_{p_i}\Pi\big|_{p_i=p_i'} + \nabla_{p_i}\Pi\big|_{p_i=p_i''}\right)\right) \geq 0 \quad \forall i \in \mathcal{N} \tag{59}$$

and we know $\mathbf{p}' \neq \mathbf{p}''$, and accordingly there exists at least one $j \in \mathcal{N}$ which satisfies the constraint in (59). Therefore, we have proved that F is strictly monotone on $\mathcal{K}$ and continuous. Until now, we have proved that VI($\mathcal{K}, F$) has at most one solution according to [43, Definition 4]. Thus, the equivalent problem admits at most one optimal solution. Since we know the existence of a single optimal solution, and thus the uniqueness of the optimal solution is validated. The proof is now completed. ■

Similar to that in Section IV-A, we can apply the low-complexity gradient-based searching algorithm to achieve the maximized profit $\Pi(\mathbf{p})$ of the CFP. In particular, we adopt Algorithm 1 to obtain the unique Stackelberg equilibrium, under which the CFP achieves the profit maximization according to Theorem 7. The basic description is explained as follows: for the given prices imposed by the CFP, the followers' subgame is solved first. After substituting the best responses of the followers' subgame into the leader subgame, the optimal prices can be obtained by a gradient-based algorithm. The similar algorithm can be used for uniform pricing as well.

V. Performance Evaluation

In this section, we first perform the real experiment on the PoW-based blockchain mining to validate the proposed utility function of the miner. Then, we conduct the extensive numerical simulations to evaluate the performance of our proposed price-based computing resource management to support blockchain application involving PoW.

A. Environmental Setup

We first set up the real blockchain mining experiment based on Ethereum and consider the smart phones as limited devices, as illustrated in Fig. 3. The experiment is performed on a workstation with Intel Xeon CPU E5-1630, and Android devices (smart phones) installing a mobile blockchain client application. The mobile blockchain client application is implemented by the Android Studio and Software Development Kits

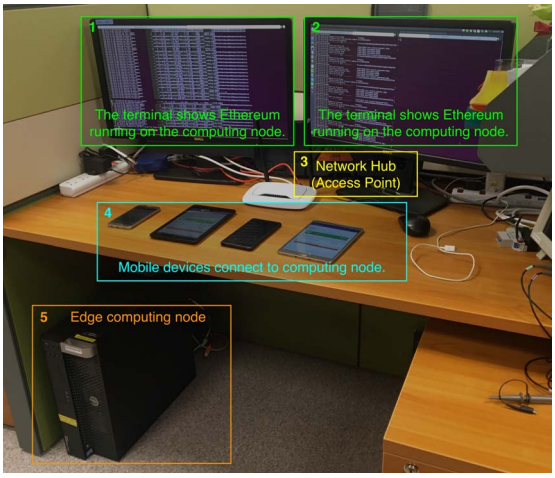


Fig. 3. Real mobile blockchain mining experimental setup with Ethereum which is a popular open ledger.

tools. All transactions are created by the mobile blockchain client application.[4] Each miner's working environment has one CPU core as its processor. The miner's processor and its CPU utilization rate are generated and managed by the Docker platform [45]. The mobile device of each miner has installed Ubuntu 16.04 LTS (Xenial Xerus) and Go-Ethereum [46] as the operation system and the blockchain framework, respectively.

In Fig. 3, from Box 1 and 2, the screen of computer terminal shows that the Ethereum is running on the host, i.e., edge device (Box 5). The mobile devices in Box 4 are connected to the edge computing node through network hub (Box 3) using mobile blockchain client application. The basic steps can be implemented as follows. The mobile users, i.e., miners use the Android device to connect to the edge computing node through network hub, i.e., access point. Then, the miners can request the service from edge node, and mine the block with the assistance of Ethereum service provided accordingly.

We create 1000 blocks employing Node.js and use the mobile device to mine these blocks in the experiment. We consider two cases with three miners and four miners. In the three-miner case, we first fix the other two miners' service demand (CPU utilization) at 40 and 60, and then vary one miner's service demand. In the four-miner case, we first fix other three miners' service demand as 40, 50, and 60, and then vary one miner's service demand. For our experiment, the number of transactions in each mined block is 10, i.e., the size of block is the same. The comparison of the real experimental results and our proposed analytical model is shown in Fig. 4. As expected, there is not much difference between the

[4]In our experiment, each mobile device sends transactions to the server, and the size of each transaction is around 1 kB [44]. Then, the server will collect and pack all the transactions into a block and proceed to solve the proof-of-work puzzle, where each block consists of block information and hash numbers. As mentioned in this paper, the number of transactions in each mined block is 10, and thus the size of the data from mobile device sent to the server is approximately 10 kB in total. Likewise, the size of a block including 10 hash numbers that is sent from the server to the mobile device is around 1.5 kB. The detailed description can be found in our previous work [44].

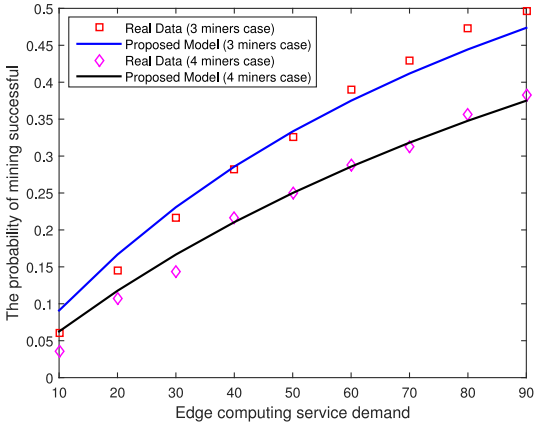


Fig. 4. Comparison of real experiment results with our proposed model.

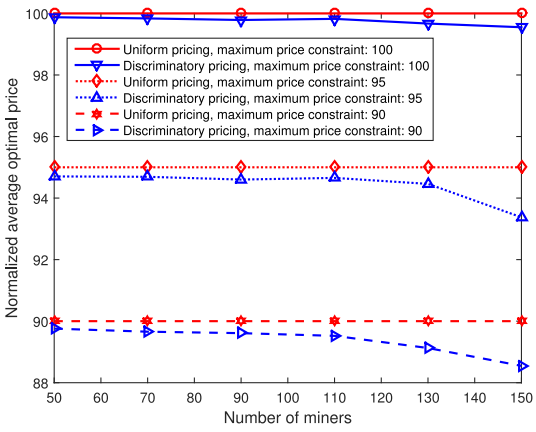


Fig. 5. Normalized average optimal price versus the number of miners.

real results and our analytical model. This is because the probability that the miner successfully mines the block is directly proportional to its relative computing power when the block size are identical. Note that the delay effects are negligible. In the sequel, we present the numerical results to evaluate the performance of the proposed price-based computing resource management for supporting blockchain application involving PoW.

B. Numerical Results

To illustrate the impacts of different parameters from the proposed model on the performance, we consider a group of N miners, e.g., mobile users in the blockchain application involving PoW assisted by the CFP. We assume the size of a block mined by miner i follows the normal distribution $\mathcal{N}(\mu_t, \sigma^2)$. The default parameter values are set as follows: $\underline{x} = 10^{-2}$, $\bar{x} = 100$, $\bar{p} = 100$, $\mu_t = 200$, $\sigma^2 = 5$, $R = 10^4$, $r = 20$, $z = 5 \times 10^{-3}$, $c = 10^{-3}$, and $N = 100$. Further, we employ the "fix" function in MATLAB to round each t_i to the nearest integer toward zero. Note that some of these parameters are varied according to the evaluation scenarios. We evaluate the performance of uniform pricing and discriminatory pricing in the following.

1) Investigation on Total Service Demand of Miners and the Profit of the CFP:

a) Comparison of uniform pricing and discriminatory pricing: We first address the comparison of uniform pricing and discriminatory pricing schemes. Fig. 5 demonstrates the comparison of the normalized average optimal price under two proposed pricing schemes. It is worth noting that the optimal price under uniform pricing is the same as the maximum price, which can be explained by (36). Specifically, the expression in (36) is always positive, and thus the profit of the CFP increases with the increase of price. This means that the maximum price is the optimal value for profit maximization of the CFP under uniform pricing. Thus, we have the following conclusion: the CFP intends to set the maximum possible value as optimal price under uniform pricing. This conclusion is still useful even when the CFP does not have the complete information about the miners.

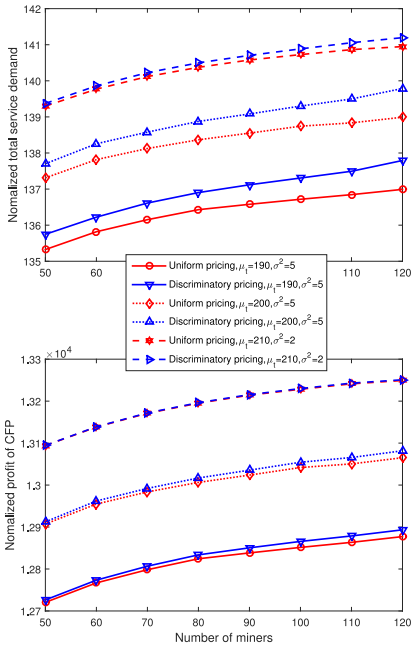


Fig. 6. Normalized total service demand of miners and the profit of the CFP versus the number of miners.

Further, we find that the average optimal price of discriminatory pricing is slightly lower than that of uniform pricing. The intuition is that, under discriminatory pricing, the CFP can set different unit prices of service demand for different miners. For the details of operation of discriminatory pricing, we conduct the case study in Section V-B2. In this case, the CFP can significantly encourage the higher total service demand from miners and achieve greater profit gain under discriminatory pricing, which is also consistent with the following results. As shown in Figs. 6–8, in all cases, the total service demand from miners and the profit of the CFP under the uniform pricing scheme is slightly smaller than that under the discriminatory pricing scheme.

From Fig. 6, we find that when σ^2 decreases, the results under uniform pricing scheme is close to that under discriminatory pricing. This is because the heterogeneity of miners in blockchain is reduced as σ^2 decreases. We may consider

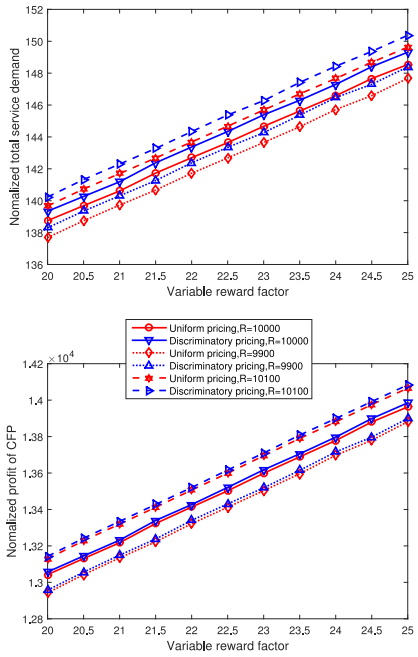


Fig. 7. Normalized total service demand of miners and the profit of the CFP versus the variable reward factor.

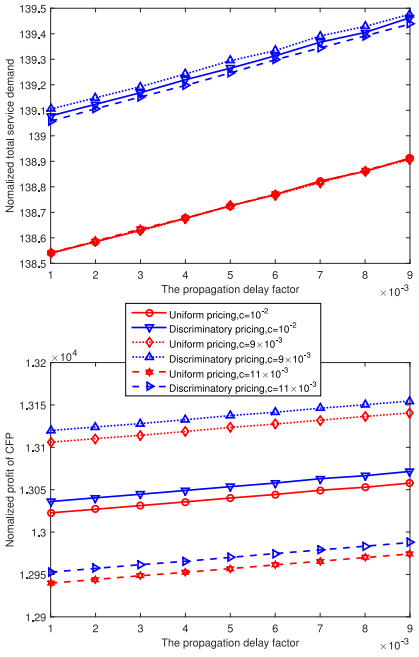


Fig. 8. Normalized total service demand of miners and the profit of the CFP versus the propagation delay factor.

one symmetric case, where the miners are homogeneous with the same size of blocks to mine, i.e., $\sigma^2 = 0$. In this case, the discriminatory pricing scheme yields the same results as those of the uniform pricing scheme.

b) Impacts of the number of miners: We next evaluate the impacts brought by the number of miners, and the results are shown in Fig. 6. From Fig. 6, we find that the total service demand of miners and the profit of the CFP increase with the increase of the number of miners in blockchain. This is due to the fact that having more miners will intensify the competition among the miners, which potentially motivates them to have higher service demand. Further, the coming miners have their service demand, and thus the total service demand from miners is increased. In turn, the CFP extracts more surplus from miners and thereby has greater profit gain. Additionally, it is observed that the rate of service demand increment decreases as the number of miners increases. This is from the fact that the incentive of miners to increase their service demand is weakened because the probability of their successful mining is reduced when the number of miners is increasing. Comparing different results, it is also observed that the total service demand of miners and the profit of the CFP increase as μ_t increases. This is because when μ_t increases, i.e., the average size of one block becomes larger, the variable reward for each miner also increases. The potential incentive of miners to increase their service demand is improved, and accordingly the total service demand of miners increases. Consequently, the CFP achieves greater profit gain.

c) Impacts of reward for successful mining: Then, we investigate the impacts of variable reward and fixed reward on miners and the CFP, which are shown in Fig. 7. It is observed that with the increase of variable reward factor, both the total service demand of miners and the profit of the CFP increase. This is from the fact that the increased variable reward enhances the motivation of miners for higher service demand, and the total service demand is enhanced accordingly. As a result, the CFP achieves greater profit gain. Further, by comparing curves with different value of fixed reward, we find that as the fixed reward increases, the total service demand of miners and the profit of the CFP also increase. Similarly, this is because the increased fixed reward induces greater incentive of miners, which in turn improves the total service demand of miners and the profit of the CFP.

d) Impacts of propagation delay: At last, we examine the impact of propagation delay on miners and the CFP, as illustrated in Fig. 8. It is observed that as the propagation delay factor increases, the total service demand and the profit of the CFP increase. This is because when the propagation delay effects are strong, the miners with larger mined block need to have higher service demand to reduce the propagation delay of their propagated solutions. At the same time, a miner with smaller mined block is also incentivized from the demand competition with the other miners. Therefore, the total service demand increases, which in turn improves the profit of the CFP. Additionally, we observe that as the value of service cost factor increases, the total service demand decreases under discriminatory pricing and remains unchanged under uniform pricing. On the contrary, the profit of the CFP increases in both schemes. Recall from Fig. 5, the reason is that the optimal price under uniform pricing remains unchanged from varying the value of service cost factor, and thus the service demand remains unchanged under uniform pricing. Correspondingly, the CFP achieves greater profit gain from the lower cost under uniform pricing. However, under discriminatory pricing, when the service cost decreases, the CFP has an incentive to set lower price for some miners to encourage higher total service demand. On the contrary, when the value of service cost factor

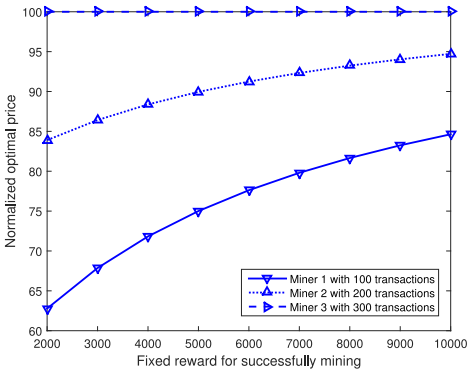


Fig. 9. Normalized optimal price versus the fixed reward for mining successfully under discriminatory pricing.

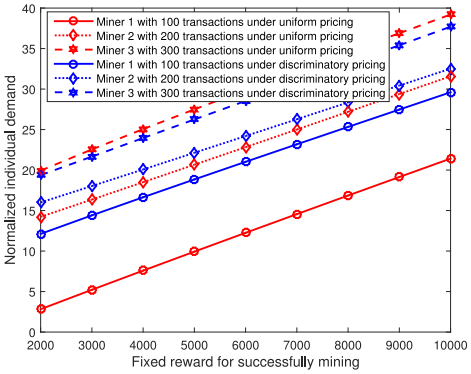


Fig. 11. Normalized individual demand versus the fixed reward for mining successful.

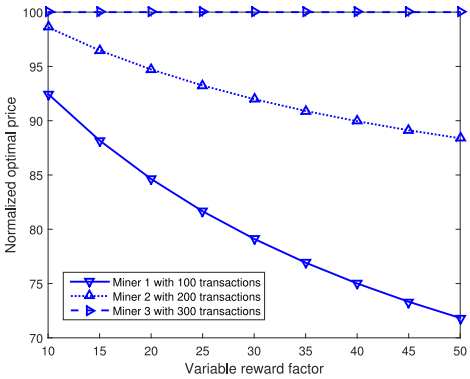


Fig. 10. Normalized optimal price versus the variable reward factor under discriminatory pricing.

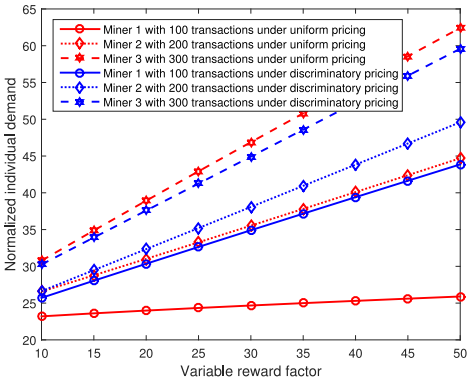


Fig. 12. Normalized individual demand versus the variable reward factor.

increases, the CFP has no incentive to set lower price for these miners, since the higher total service demand results in higher cost for the CFP. Therefore, as the value of service cost factor decreases, the total service demand and the profit of CFP increase.

2) Investigation on Optimal Price Under Uniform and Discriminatory Pricing Schemes: Then, to explore the impacts of discriminatory pricing on each specific miner, we investigate the optimal price and resulting individual computing service demand from miners. We conduct a case study for three-miner mining with the following parameters: $t_1 = 100$, $t_2 = 200$, $t_3 = 300$, $\underline{x} = 10^{-2}$, $\bar{x} = 100$, $\bar{p} = 100$, $R = 10^4$, $r = 20$, $z = 5 \times 10^{-3}$, and $c = 10^{-3}$.

As expected, we observe from Figs. 9 and 10 that the optimal price charging to the miners with the smaller block is lower, e.g., miners 1 and 2. This is because the variable reward of miners 1 and 2 for successful mining is smaller than that of miner 3. Thus, the miners 1 and 2 have no incentive to pay a high price for their service demand as miner 3. In this case, the CFP can greatly improve the individual service demand of miners 1 and 2 by setting lower prices to attract them, as illustrated in Figs. 11 and 12. Due to the competition from other two miners, the miner 3 also has the potential incentive to increase its service demand. However, due to the high service unit price, as a result, the miner 3 reduces its service demand for saving cost. Nevertheless, the increase of service demand from miners 1 and 2 are greater. Therefore, the total service demand and the profit of the CFP are still improved under discriminatory pricing compared with uniform pricing.

Further, from Fig. 9, we observe that the optimal prices for miners 1 and 2 increase with the increase of fixed reward. This is because as the fixed reward increases, the incentives of miners 1 and 2 to have higher service demand is greater. In this case, the CFP is able to raise the price and charge more for higher revenue, and thus achieves greater profit. Therefore, for each miner, the individual service demand increases as the fixed reward increases, as shown in Fig. 11. Additionally, we observe from Fig. 10 that the optimal prices for miners 1 and 2 decrease as the variable reward factor increases. This is because when the variable reward factor increases, the incentive of each miner to have higher service demand is greater. However, the incentives of the miners with smaller block to mine, i.e., the miners 1 and 2 are still not much as that of miner 3, and become smaller than that of miner 3 as the variable reward factor increases. Therefore, the CFP intends to set the lower price for miners 1 and 2 which may induce more individual service demand as shown in Fig. 12.

Note that the Stackelberg game of the edge/fog computing service for blockchain aims at maximizing the profit of the CFP. Alternatively, social welfare, i.e., utility of miners, are also important and should be maximized. As such, auction [47] is a suitable tool to achieve this objective in which some preliminary modeling and results are presented in [35].

VI. Conclusion

In this paper, we have investigated the price-based computing resource management, for supporting offloading mining tasks to CFP in proof-of-work-based public blockchain networks. In particular, we have adopted the two-stage Stackelberg game model to jointly study the profit maximization of CFP and the utility maximization of miners. Through backward induction, we have derived the unique Nash equilibrium point of the game among the miners. The optimal resource management schemes including the uniform and discriminatory pricing for the CFP have been presented and examined. Further, the existence and uniqueness of the Stackelberg equilibrium have been proved analytically for both pricing schemes. We have performed the real experiment to validate the proposed analytical model. Additionally, we have conducted the numerical simulations to evaluate the network performance, which help the CFP to achieve optimal resource management and gain the highest profit. For the future work, we will further study the oligopoly market with multiple CFPs, where providers compete with each other for selling computing services to miners. Another direction is to study the optimal strategies of the provider and miners with the consideration of cyber-attacks, such as [48].

References

[1] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing-based edge computing resource management in mobile blockchain," in *Proc. IEEE ICC*, Kansas City, MO, USA, May 2018, pp. 1–6.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, May 2008.

[3] W. Wang *et al.*, "A survey on consensus mechanisms and mining management in blockchain networks," *arXiv preprint arXiv:1805.02707*, 2018.

[4] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement.*, vol. 99. New Orleans, LA, USA, Feb. 1999, pp. 173–186.

[5] D. Ongaro and J. K. Ousterhout, "In search of an understandable consensus algorithm," in *Proc. USENIX Annu. Tech. Conf.*, Philadelphia, PA, USA, Jun. 2014, pp. 305–319.

[6] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Prob. Netw. Security (IFIP WG)*, Zürich, Switzerland, Oct. 2015, pp. 112–125.

[7] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Proc. 34th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. II Adv. Cryptol. (EUROCRYPT)*, Sofia, Bulgaria, Apr. 2015, pp. 281–310.

[8] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *Proc. IFIP Int. Conf. Distrib. Appl. Interoper. Syst.*, Neuchatel, Switzerland, Jun. 2017, pp. 206–220.

[9] W. Wang, D. Niyato, P. Wang, and A. Leshem, "Decentralized caching for content delivery based on blockchain: A game theoretic perspective," in *Proc. IEEE ICC*, Kansas City, MO, USA, May 2018, pp. 1–6.

[10] X. Chen *et al.*, "Framework for context-aware computation offloading in mobile cloud computing," *J. Cloud Comput.*, vol. 6, no. 1, p. 1, 2017.

[11] C. Huang, R. Lu, and K.-K. R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 105–111, Nov. 2017.

[12] R. Recabarren and B. Carbunar, "Hardening Stratum, the bitcoin pool mining protocol," in *Proc. Privacy Enhancing Technol.*, vol. 2017, no. 3, 2017, pp. 57–74.

[13] H. Zhang, Y. Zhang, Y. Gu, D. Niyato, and Z. Han, "A hierarchical game framework for resource management in fog computing," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 52–57, Aug. 2017.

[14] H. Zhang *et al.*, "A multi-leader multi-follower Stackelberg game for resource management in LTE unlicensed," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 348–361, Jan. 2017.

[15] C. Jiang, Y. Chen, K. R. Liu, and Y. Ren, "Optimal pricing strategy for operators in cognitive femtocell networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 5288–5301, Sep. 2014.

[16] J.-J. Laffont, P. Rey, and J. Tirole, "Network competition: II. Price discrimination," *RAND J. Econ.*, vol. 29, no. 1, pp. 38–56, 1998.

[17] T. T. A. Dinh *et al.*, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[18] 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.

[19] D. Chatzopoulos, M. Ahmadi, S. Kosta, and P. Hui, "Flopcoin: A cryptocurrency for computation offloading," *IEEE Trans. Mobile Comput.*, vol. 17, no. 5, pp. 1062–1075, May 2018.

[20] H. Kopp, D. Mödinger, F. Hauck, F. Kargl, and C. Bösch, "Design of a privacy-preserving decentralized file storage with financial incentives," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS PW)*, Paris, France, 2017, pp. 14–22.

[21] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," in *Proc. Internet Things Bus. Models Users Netw.*, Copenhagen, Denmark, Nov. 2017, pp. 1–8.

[22] J. Kang *et al.*, "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.

[23] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *Proc. ACM 18th Annu. Int. Conf. Mobile Comput. Netw.*, 2012, pp. 173–184.

[24] A. Chakeri and L. G. Jaimes, "An incentive mechanism for crowdsensing markets with multiple crowdsourcers," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 708–715, Apr. 2018.

[25] A. Chakeri and L. G. Jaimes, "An iterative incentive mechanism design for crowd sensing using best response dynamics," in *Proc. IEEE ICC*, Paris, France, May 2017, pp. 1–7.

[26] N. Houy, "The bitcoin mining game," *Ledger J.*, vol. 1, no. 13, pp. 53–68, 2016.

[27] J. I. Beccuti and C. Jaag, "The bitcoin mining game: On the optimality of honesty in proof-of-work consensus mechanism," Swiss Econ., Zürich, Switzerland, Working Papers 0060, Aug. 2017.

[28] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proc. ACM Conf. Econ. Comput. (EC)*, Maastricht, The Netherlands, Jul. 2016, pp. 365–382.

[29] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proc. ACM AAMAS*, Istanbul, Turkey, May 2015, pp. 919–927.

[30] B. A. Fisch, R. Pass, and A. Shelat, "Socially optimal mining pools," in *Proc. Int. Conf. Web Internet Econom.*, 2017, pp. 205–218.

[31] S. Kim, "Group bargaining based bitcoin mining scheme using incentive payment process," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 11, pp. 1486–1495, 2016.

[32] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, "On power splitting games in distributed computation: The case of bitcoin pooled mining," in *Proc. IEEE CSF*, Verona, Italy, Jul. 2015, pp. 397–411.

[33] 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.

[34] 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," in *Proc. IEEE ICC*, Kansas City, MO, USA, May 2018, pp. 1–6.

[35] Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maximization auction in edge computing resource allocation for mobile blockchain," in *Proc. IEEE ICC*, Kansas City, MO, USA, May 2018, pp. 1–6.

[36] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger (EIP-150 revision)," Ethereum Project, White Paper, 2017.

[37] D. K. Tosh *et al.*, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proc. IEEE/ACM CCGrid*, 2017, pp. 458–467.

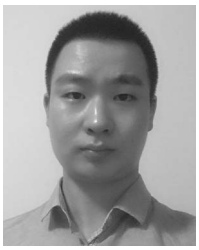
[38] N. Wang, B. Varghese, M. Matthaiou, and D. S. Nikolopoulos, "ENORM: A framework for edge node resource management," *IEEE Trans. Services Comput.*, to be published.

[39] *Orphan Probablity Approximation*. Accessed: Mar. 2013. [Online]. Available: https://gist.github.com/gavinandresen/5044482

[40] E. S. Robla, "Analysis of reward strategy and transaction selection in bitcoin block generation," Ph.D. dissertation, Dept. Elect. Eng., Univ. Washington, Seattle, WA, USA, 2015.
[41] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Proc. IEEE P2P*, Trento, Italy, Sep. 2013, pp. 1–10.
[42] Z. Han, D. Niyato, W. Saad, T. Baar, and A. Hjrungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[43] G. Scutari, D. P. Palomar, F. Facchinei, and J.-S. Pang, "Convex optimization, game theory, and variational inequality theory," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 35–49, May 2010.
[44] K. Suankaewmanee *et al.*, "Performance analysis and application of mobile blockchain," in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (ICNC)*, 2018, pp. 642–646.
[45] *Docker*. [Online]. Available: https://www.docker.com/community-edition
[46] *Go-ethereum*. Accessed: Jun. 2017. [Online]. Available: https://ethereum.github.io/go-ethereum/
[47] C. Jiang, Y. Chen, Q. Wang, and K. R. Liu, "Data-driven auction mechanism design in IAAS cloud computing," *IEEE Trans. Services Comput.*, to be published.
[48] S. Feng *et al.*, "On cyber risk management of blockchain networks: A game theoretic approach," *arXiv preprint arXiv:1804.10412*, 2018.

Zehui Xiong (S'17) received the B.Eng. degree (Hons.) in telecommunication engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2016. He is currently pursuing the Ph.D. degree at the School of Computer Science and Engineering, Nanyang Technological University, Singapore.

His current research interests include network economics, game theory for resource management, market models, and pricing.



Shaohan Feng (S'17) received the B.S. degree from Beihang University, Beijing, China, in 2014, and the M.Sc. degree from Zhejiang University, Hangzhou, China, in 2016. He is currently pursuing the Ph.D. degree at the School of Computer Science and Engineering, Nanyang Technological University, Singapore.

His current research interests include resource management in cloud computing and communication networks.

Wenbo Wang (S'13–M'17) received the B.S. and M.S. degrees from the School of Automation, Beijing Institute of Technology, Beijing, China, and the Ph.D. degree in computing and information sciences from the Rochester Institute of Technology, Rochester, NY, USA, in 2016.

He is currently a Research Fellow with the School of Computer Engineering, Nanyang Technological University, Singapore. His current research interests include cross-layer optimization in multimedia wireless networks, cognitive radio networks, game theoretical modeling and mechanism design in wireless networks, and Internet of Things.

Dusit Niyato (M'09–SM'15–F'17) 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 Full Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His current research interests include energy harvesting for wireless communication, Internet of Things, and sensor networks.

Ping Wang (M'08–SM'15) received the Ph.D. degree in electrical engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008.

She is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, York University, Toronto, ON, Canada. Her current research interests include resource allocation in multimedia wireless networks, cloud computing, and smart grid.

Dr. Wang was a co-recipient of the Best Paper Award of the IEEE Wireless Communications and Networking Conference in 2012 and the IEEE International Conference on Communications in 2007. She is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the *EURASIP Journal on Wireless Communications and Networking*, and the *International Journal of Ultra Wideband Communications and Systems*.

Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland at College Park, College Park, MD, USA, in 1999 and 2003, respectively.

From 2000 to 2002, he was a Research and Development Engineer with JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland at College Park. From 2006 to 2008, he was an Assistant Professor with Boise State University, Boise, ID, USA. He is currently a Professor with the Electrical and Computer Engineering Department and the Computer Science Department, University of Houston, Houston, TX, USA. His current research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid.

Dr. Han was a recipient of the NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for a paper published in the *Journal on Advances in Signal Processing* in 2015, the IEEE Leonard G. Abraham Prize in the field of communications systems (Best Paper Award in the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS) in 2016, and several Best Paper Awards at IEEE conferences. He is currently an IEEE Communications Society Distinguished Lecturer.