Social Welfare Maximization Auction in Edge Computing Resource Allocation for Mobile Blockchain

Yutao Jiao, Ping Wang, Dusit Niyato, and Zehui Xiong
School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798

***Abstract*—Blockchain, an emerging decentralized security system, has been applied in many applications, such as bitcoin, smart grid, and Internet-of-Things. However, running the mining process may cost too much energy consumption and computing resource usage on handheld devices, which restricts the use of blockchain in mobile environments. In this paper, we consider deploying edge computing service to support the mobile blockchain. We propose an auction-based edge computing resource allocation mechanism for the edge computing service provider. Since there is competition among miners, the allocative externalities are taken into account in the model. In our auction mechanism, we maximize the social welfare while guaranteeing the truthfulness, individual rationality and computational efficiency. Through extensive simulations, we evaluate the performance of our auction mechanism which shows that the proposed mechanism can efficiently solve the social welfare maximization problem for the edge computing service provider.**

***Index Terms*—mobile blockchain, auction, edge computing, pricing, resources allocation, proof of work**

I. Introduction

In contrast to traditional currencies, decentralized cryptocurrencies are traded among participants over a peer-to-peer (P2P) network without relying on trusted third parties like banks or financial regulatory authorities [1]. As the backbone technology, blockchain protocol provides an effective consensus mechanism to successfully solve problems about incentive, tamper-resistance, trust and so on [2]. Recently, blockchain has heralded many applications in various fields, such as Internet of Things [3] and cognitive radio [4].

The security and reliability of blockchains depend on a distributed consensus mechanism. Specifically, a group of participants in the blockchain network, called *miners,* try to solve a computationally difficult problem, i.e., the *proof of work* (PoW) puzzle, where the process is called *mining*. First, each miner receives and selects certain number of transaction records from public. Once solving the puzzle, the miner will broadcast a *block* which combines the transaction records and relevant information to the blockchain network. Next, this block will be verified by the majority of other miners for consensus and then finally be added to the blockchain. The miner which successfully finishes the above steps will receive a fixed reward and certain transaction fees as incentives of mining.

However, blockchain applications in mobile environments are still seldom realized because solving the PoW puzzle needs high computing power and large amount of energy which mobile devices cannot afford. In this paper, we consider the edge computing services for mobile users to deploy their mining tasks and thus support the mobile blockchain applications. Specifically, we discuss the allocation and pricing issue for edge computing resource. We first propose an auction-based market model. The market consists of three entities, i.e., blockchain owner, edge computing service provider (ESP) and miners. Considering the competition among miners [2] and network effects of blockchain by nature [5], we then study the auction mechanism with allocative externalities to maximize the social welfare. Allocative externalities refers to that one bidder cares about what another bidder wins in the auction. Our social maximization mechanism is truthful, individually rational and computationally efficient. Based on our real-world experiment of mobile blockchain, we analyze the probability of successfully mining a block and verify the probability function. Our simulation results show that the proposed auction mechanism can not only help the ESP to make practical sale strategies, but also assist the blockchain owner in adjusting the blockchain protocol. To the best of our knowledge, this is the first work that investigates resource management and pricing in the mobile blockchain with an auction model.

The rest of this paper is organized as follows. Section II reviews related work, and the system model of edge computing resource allocation for mobile blockchain is introduced in Section III. Section IV formulates the social welfare maximization problem and gives theoretical analysis. Section V presents experimental results of mobile blockchain and performance analysis. Finally, Section VI concludes the paper.

II. Related Work

As one of the pioneer papers, the authors in [6] modeled the mining process as a game played by miners. Each miner's strategy is to choose which branch of blockchain to mine on. They proved the existence of a Nash equilibrium when all miners behave as expected by Bitcoin designer. Further, they explored the case that some miners may deviate from the expected behavior, which makes blockchain network unstable and vulnerable. The authors in [7] proposed a game model in which the occurrence of solving the PoW puzzle is modeled as a Poisson process. Miners have to decide the size of block

978-1-5386-3180-5/18/$31.00 ©2018 IEEE

to broadcast as their response. Analytical solutions to the Nash equilibrium in a two-miner case was given. In [8], the authors designed a cooperative game model to investigate the mining pool. In the pool, miners form a coalition to accumulate their computational power and have steady reward. However, these works only studied the internal mining scheme and paid little attention to the actual running of blockchain in more dynamic environments, e.g., mobile blockchain. The auction design has been widely studied in other resource allocation problems, such as spectrum trading [9] and data crowdsensing [10]. However, none of these works can be directly applied to edge computing applications for mobile blockchain, since they only focused on the specific properties constrained by the studied topics. The authors in [11] used deep learning to recover the classical optimal auction for revenue maximization and applied it in the edge computing resources allocation. However, it only considers a unit of resource in the auction.

III. System Model: Mobile Blockchain and Market Model

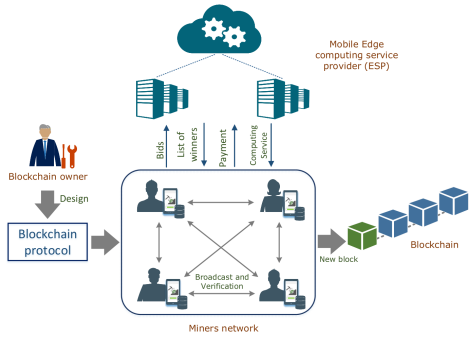


Fig. 1. Edge computing resource market for mobile blockchain.

A. Mobile Blockchain

Blockchain can be used to develop applications with mobile devices, as indicated in our earlier study [12]. To support the blockchain based service, there are a set of miners continuously running a consensus protocol [1] to confirm and secure distributed data or transactions at backend. Miners are required to solve a PoW puzzle. The mining process is conducted in a tournament structure, and miners chase each other to obtain the solution. Specifically, the PoW algorithm involves finding a nonce value that the output satisfies a given condition. If the nonce is found, the miner will combine it and additional fields into a block and then broadcast the block to peers in the blockchain network for verification and reaching consensus. Finally, the new block can be linked to the existing accepted chain of blocks. However, for a mobile user, it is unrealistic to continuously run such a computationally difficult program which requires a large volume of energy and time. Because the outstanding characteristics of edge computing: low latency, mobility and wide-spread geographical distribution, we consider offloading the mining tasks to the edge servers.

B. Edge Computing Resources Trading

As shown in Fig. 1, we consider a scenario where there is one ESP, one blockchain owner and a community of mobile users $\mathcal{N}=\{1,\ldots,N\}$. Due to the computing limitation on their devices, mobile users want to offload the task of solving PoW to the nearby edge computing servers deployed by the ESP. In particular, the ESP first announces its service and relevant information to mobile users. Then, the mobile users submit their resource demand profile $\mathbf{d}=(d_1,\ldots,d_N)$ and corresponding bids $\mathbf{b}=(b_1,\ldots,b_N)$ which represent their valuations of the offered services. After receiving the demands and bids, the ESP selects the winners and notifies the mobile users the allocation $\mathbf{x}=(x_1,\ldots,x_N)$ and the service price $\mathbf{p}=(p_1,\ldots,p_N)$. The setting $x_i=1$ means user i is within the winner list and being allocated resources that it demands for while $x_i=0$ is for no resource[1]. p_i is the sale price that user i is charged by the ESP[2].

C. Blockchain Mining with Edge Computing Service

With the allocation x_i and demand d_i, miner i's hash power γ_i relative to other miners' allocated resources can be calculated by:

$$\gamma_i(\mathbf{d},\mathbf{x})=\frac{d_i^{\alpha}x_i}{\sum_{j\in\mathcal{N}}d_j^{\alpha}x_j} \tag{1}$$

which is a fraction function that $\sum_{i\in\mathcal{N}}\gamma_i=1$. α is the curve fitting parameter of the hash power function $\gamma_i(\mathbf{d},\mathbf{x})$ verified by our real-world experiment, the detail of which will be presented in Section V.

In the mining tournament, miners compete to be the first to solve PoW with correct nonce value and propagate the block to reach consensus. The generation of new blocks follows a Poisson process with a constant rate $\frac{1}{\lambda}$ throughout the whole blockchain network [13]. Before the tournament, miners collect unconfirmed transactions into their blocks. We represent the size of transactions of each miner by $\mathbf{s}=(s_1,\ldots,s_N)$. When miner i propagates its block to the mobile blockchain network for consensus, the time for verifying each transaction is affected by the size of transactions s_i. The first miner which successfully has its block achieve consensus can get a reward R. The reward is composed of a fixed bonus T for mining a new block and a flexible transaction fee determined by the size of its collected transactions s and the transaction fee rate r [7]. Thus, miner i's expected reward R_i can be expressed by:

$$R_i=(T+rs_i)\mathbb{P}_i(\gamma_i(\mathbf{d},\mathbf{x}),s_i), \tag{2}$$

where $\mathbb{P}_i(\gamma_i(\mathbf{d},\mathbf{x}),s_i)$ is the probability that miner i receives the reward by contributing a block to the blockchain.

From the mining tournament above, winning the reward depends on the successful mining and instant propagation. The probability of mining a new block P_i^m is equal to miner

[1]The user becomes a miner if it wins the auction.

[2]The payment for user which is not allocated any resource is zero, i.e., $p=0$.

i's hash power γ_i, i.e., $P_i^m = \gamma_i$. However, the miner may even lose the tournament if its new block does not achieve consensus as the first. This kind of mined block that cannot be added on to the blockchain is called orphaned block [7]. Moreover, the block containing larger size of transactions has higher chance becoming orphaned. This is because a larger block needs more propagation time, thus causing higher delay for consensus. Here, we assume miner i's block propagation time τ_i is linear to the size of transactions in its block, i.e., $\tau_i = \xi s_i$. ξ is a constant that reflects the impact of s_i on τ_i. Since the arrival of new blocks follows a Poisson distribution, miner i's orphaning probability can be approximated by $P_i^o = 1 - \exp(-\frac{1}{\lambda}\tau_i)$ [14]. After substituting τ_i, we can express $\mathbb{P}_i$ as follows:

$$\mathbb{P}_i = P_i^m(1 - P_i^o) = \gamma_i e^{-\frac{1}{\lambda}\xi s_i}. \tag{3}$$

D. Blockchain Management

The blockchain owner maintains the blockchain mining protocol that specifies the fixed bonus T for the contributing miner and the transaction fee rate r. Through adjusting the difficulty of finding a new block, the blockchain owner keeps the average time λ at a reasonable constant value[3]. Additionally, a blockchain in PoW systems is only as secure as the amount of computing power dedicated to mining it [5]. This results in positive network effects: as more users participate in mining and more computing resources are invested, the value of reward given to miners increases since the blockchain network is more stable and secure. Empirically, we define the network effects by a common S-shaped utility function [15]:

$$w(d_{\mathcal{N}}) = \frac{1 - e^{-\nu d_{\mathcal{N}}}}{1 + \mu e^{-\nu d_{\mathcal{N}}}}, \tag{4}$$

where $d_{\mathcal{N}} = \sum_{i\in\mathcal{N}} d_i x_i$ is the total quantity of allocated resources and μ, ν are positive parameters. The monotonic increase of network effect function begins slowly from 0, then accelerates (convexly), and then eventually slows down (concavely) and converges asymptotically to 1.

IV. Social Welfare Maximization Auction for Edge Computing Service

In this section, we propose an auction mechanism for the ESP to allocate edge computing resources efficiently. We focus on maximizing the social welfare while guaranteeing the truthfulness, individual rationality and computational efficiency.

A. Valuation of mobile users

To take part in the auction, a mobile user needs to give the bid representing its valuation to the auctioneer, i.e., the ESP. Since the mobile user i cannot know the number of winners and total supply of computing resources until auction ends, its hash power γ_i is assumed to be 1. Hence, it can only give the bid b_i according to its expected reward R_i with $\gamma_i = 1$, which is also called *ex-ante* valuation v_i', i.e., $v_i' = R_i$.

Once the auction result is released, user i takes other users' received resources into consideration and has an *ex-post* valuation v_i'', which is defined by $v_i'' = R_i w$, where w is the network effect defined in (4). After substituting (1), (3) and (4), we have the specific expression of user i's ex-ante and ex-post valuation:

$$v_i' = (T + rs_i)e^{-\frac{1}{\lambda}\xi s_i}, \tag{5}$$

$$v_i'' = \frac{d_i^\alpha x_i}{\sum_{j\in\mathcal{N}} d_j^\alpha x_j} \frac{1 - e^{-\nu\sum_{i\in\mathcal{N}} d_i x_i}}{1 + \mu e^{-\nu\sum_{i\in\mathcal{N}} d_i x_i}} (T + rs_i)e^{-\frac{1}{\lambda}\xi s_i}. \tag{6}$$

B. Auction Maximizing Social Welfare

Once receiving bids $\mathbf{b}$ from all the mobile users, ESP will select winners and determine corresponding payments to maximize the social welfare. Let c denote the unit cost of running the edge computing service. ESP's total cost is $C(d_{\mathcal{N}}) = cd_{\mathcal{N}}$. Thus, designing such an auction becomes solving an optimization problem:

$$\max_{\mathbf{x}} \sum_{i\in\mathcal{N}} \frac{d_i^\alpha x_i}{\sum_{j\in\mathcal{N}} d_j^\alpha x_j} \frac{1 - e^{-\nu\sum_{i\in\mathcal{N}} d_i x_i}}{1 + \mu e^{-\nu\sum_{i\in\mathcal{N}} d_i x_i}} (T + rs_i)e^{-\frac{1}{\lambda}\xi s_i} - \sum_{i\in\mathcal{N}} cd_i x_i \tag{7}$$

$$\text{s.t.} \sum_{i\in\mathcal{N}} d_i x_i \le D \text{ and } x_i \in \{0,1\}, \forall i \in \mathcal{N} \tag{8}$$

where the objective function in (7) is the social welfare of the blockchain network, i.e., the difference between the sum of all users' ex-post valuations and ESP's total cost. The constraint in (8) defines the maximum quantity of computing resources that ESP can offer denoted by D.

Based on the above system model, we first consider a simple case where all mobile users submit various bids to compete for a fixed quantity of resources. Without loss of generality, we set $d_i = 1, \forall i \in \mathcal{N}$. Then, the optimization problem can be expressed as follows:

$$\max_{\mathbf{x}} \sum_{i\in\mathcal{N}} \frac{x_i}{\sum_{j\in\mathcal{N}} x_j} \frac{1 - e^{-\nu\sum_{i\in\mathcal{N}} x_i}}{1 + \mu e^{-\nu\sum_{i\in\mathcal{N}} x_i}} (T + rs_i)e^{-\frac{1}{\lambda}\xi s_i} - \sum_{i\in\mathcal{N}} cx_i \tag{9}$$

$$\text{s.t.} \sum_{i\in\mathcal{N}} x_i \le D \text{ and } x_i \in \{0,1\}, \forall i \in \mathcal{N} \tag{10}$$

We aim to solve this integer program efficiently while making the auction process truthful and individually rational. The proposed auction is based on the Myerson's well-known characterization [16] as described in Theorem 1.

Theorem 1. *([17, Theorem 13.6]) An auction is truthful if and only if it satisfies the following two properties:*

[3]It is worth noting that the blockchain owner is not a central entity that controls the data storage and mining strategies of the miners. Similar to the bitcoin protocol [1], the blockchain owner in this paper only designs the protocol specifies the value of T, r and λ, and does not affect the decentralization and security of blockchain.

Algorithm 1 Social Welfare Maximization Auction

Input: Mobile users' bid profile $\mathbf{b} = (b_1, \ldots, b_N)$.

Output: Resource allocation profile $\mathbf{x} = (x_1, \ldots, x_N)$ and payment profile $\mathbf{p} = (p_1, \ldots, p_N)$.

1: **begin**
2: **for each** $i \in \mathcal{N}$ **do**
3: $x_i \leftarrow 0, p_i \leftarrow 0$
4: **end for**
5: $\mathcal{W} \leftarrow \varnothing, \mathcal{W}_t \leftarrow \varnothing, S \leftarrow 0, S_t \leftarrow 0$
▷ $\mathcal{W}$ is the set of winners.
6: **while** $S \leq S', \mathcal{W} \neq \mathcal{N}, |\mathcal{W}| \leq D$ **do**
7: $j \leftarrow \arg\max_{j \in \mathcal{N} \setminus \mathcal{W}} b_j$
8: $\mathcal{W} \leftarrow \mathcal{W}_t$
9: $\mathcal{W}_t \leftarrow \mathcal{W} \cup \{j\}, S \leftarrow S_t$
10: $S_t \leftarrow \frac{1}{|\mathcal{W}_t|} \frac{1-e^{-\nu|\mathcal{W}_t|}}{1+\mu e^{-\nu|\mathcal{W}_t|}} \sum_{l \in \mathcal{W}_t} b_l - c\,|\mathcal{W}_t|$
11: **end while**
12: **for each** $j \in \mathcal{W}$ **do**
13: $x_j \leftarrow 1$
14: $\mathcal{N}_{-j} \leftarrow \mathcal{N} \setminus \{j\}, \mathcal{W}_{-j} \leftarrow \mathcal{W} \setminus \{j\}$
15: $\mathcal{W}' \leftarrow \varnothing, \mathcal{W}'_t \leftarrow \varnothing, S' \leftarrow 0, S'_t \leftarrow 0$
16: **while** $S' \leq S'_t, \mathcal{W}' \neq \mathcal{N}_{-j}, |\mathcal{W}| \leq D$ **do**
17: $k \leftarrow \arg\max_{k \in \mathcal{N}_{-j} \setminus \mathcal{W}'} b_k$
18: $\mathcal{W}' \leftarrow \mathcal{W}'_t$
19: $\mathcal{W}'_t \leftarrow \mathcal{W}' \cup \{k\}, S' \leftarrow S'_t$
20: $S'_t \leftarrow \frac{1}{|\mathcal{W}'_t|} \frac{1-e^{-\nu|\mathcal{W}'_t|}}{1+\mu e^{-\nu|\mathcal{W}'_t|}} \sum_{l \in \mathcal{W}'_t} b_l - c\,|\mathcal{W}'_t|$
21: **end while**
22: $p_j = S' - \frac{1}{|\mathcal{W}_{-j}|} \frac{1-e^{-\nu|\mathcal{W}_{-j}|}}{1+\mu e^{-\nu|\mathcal{W}_{-j}|}} \sum_{l \in \mathcal{W}_{-j}} b_l + c\,|\mathcal{W}_{-j}|$
23: **end for**
24: **end**

1) *Monotonicity of winner selection rule: If user i wins the auction with bid b_i, then it will also win with any higher bid $b'_i > b_i$.*
2) *Critical payment: The payment by a winner is the smallest value needed in order to win the auction.*

Our auction mechanism is illustrated in Algorithm 1. In Lines 5-11, the winner selection process is conducted with a greedy scheme. We define a winner set $\mathcal{W}$. Including a user i in the set is equivalent to assigning $x_i = 1$. Thus, we rewrite the problem in an alternative form as follows:

$$\max_{\mathcal{W} \subseteq \mathcal{N}} S(\mathcal{W})$$
$$s.t. S(\mathcal{W}) = \sum_{i \in \mathcal{W}} \frac{1}{|\mathcal{W}|} \frac{1 - e^{-\nu|\mathcal{W}|}}{1 + \mu e^{-\nu|\mathcal{W}|}} b_i - c\,|\mathcal{W}|$$
$$|\mathcal{W}| \leq D$$

where $|\mathcal{W}|$ measures the number of winners in $\mathcal{W}$, $S(\mathcal{W})$ is social welfare of $\mathcal{W}$ and $b_i = v'_i = (T + rs_i)e^{-\lambda k s_i}$ because the auction is truthful. In the winner selection process (Lines 6-11), mobile users are first sorted in a descending order according to their bids. We then add one user sequentially to the winner set $\mathcal{W}$, which will be stopped before the corresponding social welfare $S(\mathcal{W})$ decreases. Finally, the solution $\mathcal{W}$ is output by the algorithm.

Proposition 2. *The resource allocation $\mathbf{x}$ output by Algorithm 1 is globally optimal to the social welfare maximization problem given in (9)-(10).*

Proof: With proof by contradiction, this result follows from Claim 3. ■

Claim 3. Let $\mathcal{W}_A$ be the solution output by Algorithm 1 on input $\mathbf{b}$, and $\mathcal{W}_O$ the optimal solution. If $\mathcal{W}_A \neq \mathcal{W}_O$, then we can construct another solution $\mathcal{W}^*_O$ the social welfare of which $S(\mathcal{W}^*_O)$ is even larger than $\mathcal{W}_O$.

Proof: Without loss of generality, we assume $b_1 \geq \cdots \geq b_N$ and $\mathcal{W}_A \neq \mathcal{W}_O$. Let m be the first element (while-loop Lines 6-11) where $m \notin \mathcal{W}_O$. Since (b_m is minimal by assumption) m is maximal, we must have $1, \ldots, m-1 \in \mathcal{W}_O$ and in particular, the set of corresponding bid $\mathbf{b}_{\mathcal{W}_O}$ has the form $\mathbf{b}_{\mathcal{W}_O} = \{b_1, b_2, \ldots, b_{m-1}, b'_m, b'_{m+1}, \ldots, b'_{|\mathcal{W}_O|}\}$, where the bids $b_1, \ldots, b'_{|\mathcal{W}_O|}$ are listed in the descending order. Meanwhile, Algorithm 1 chooses $\mathbf{b}_{\mathcal{W}_A} = \{b_1, b_2, \ldots, b_{m-1}, b_m, b_{m+1}, \ldots, b_{|\mathcal{W}_O|}\}$ and there must be $b_m > b'_j$ for all $j \geq m$. In particular, we have $b_m > b'_m$. Hence, we define $\mathbf{b}_{\mathcal{W}^*_O} = \mathbf{b}_{\mathcal{W}_O} \cup \{b_m\} \setminus \{b'_m\}$, i.e., we obtain $\mathbf{b}_{\mathcal{W}^*_O}$ by deleting the mth bid in $\mathbf{b}_{\mathcal{W}_O}$ and adding b_m. Now we have the social welfare of $\mathbf{b}_{\mathcal{W}^*_O}$:

$$S(\mathcal{W}^*_O) = S(\mathcal{W}_O) + \frac{1}{|\mathcal{W}_O|} \frac{1 - e^{-\nu|\mathcal{W}_O|}}{1 + \mu e^{-\nu|\mathcal{W}_O|}} (b_m - b'_m).$$

Since $b_m - b'_m > 0$ and $|\mathcal{W}^*_O| = |\mathcal{W}_O|$, $S(\mathcal{W}^*_O)$ is strictly larger than $S(\mathcal{W}_O)$, which is in contradiction to that $\mathcal{W}_O$ is the optimal solution. This proves the claim. ■

In Lines 12-23, for each iteration, we exclude one winner from the user set and rerun the winner selection process to calculate the payment for the winner. The payment calculation is based on the Vickrey–Clarke–Groves (VCG) mechanism [18].

Proposition 4. *The Social Welfare Maximization Auction (Algorithm 1) is truthful.*

Proof: Since the calculation of payment by the algorithm relies on VCG mechanism, it directly satisfies the second condition in Theorem 1. For the first condition about monotonicity, we only need to show that if a winner i raises its bid from b_i to $b_i^+$where $b_i^+ > b_i$, it still stays in the set of winners. We denote the original set of winners as $\mathcal{W}$ and the new set of winners $\mathcal{W}_+$ after winner i changes its bid to b_i^+. The original bid set is $\mathbf{b} = \{b_1, \ldots, b_i, \ldots b_N\}$ ($i \leq |\mathcal{W}|$) sorted in the descending order. In addition, we define $S(\mathbf{b}_\mathcal{U}) = S(\mathcal{U}), \forall \mathcal{U} \subseteq \mathcal{N}$ which means the social welfare of a set of bids is equal to the set of its corresponding users. We discuss the monotonicity in two cases:

1) Case 1: $b_{i-1} \geq b_i^+ \geq b_i \geq b_{i+1}$. The new set of ordered

$$S(\{b_1,\dots b_{k-1},b_k\})=\frac{1-\mathrm{e}^{-\nu k}}{(1+\mu\mathrm{e}^{-\nu k})k}\left(\sum_{j=1}^{k-1}b_j+b_k\right)<\frac{1-\mathrm{e}^{-\nu k}}{(1+\mu\mathrm{e}^{-\nu k})k}\left(\sum_{j=1}^{k-1}b_j+b_i^+\right)=S\left(\{b_1,\dots,b_{k-1},b_i^+\}\right) \quad (11)$$

bids is $\mathbf{b}^+=\{b_1,\dots,b_{i-1},b_i^+,b_{i+1},\dots b_N\}$. We have

$$\begin{aligned}S(\{b_1,\dots,b_i^+\})=&\frac{1-e^{-\nu i}}{(1+\mu e^{-\nu i})i}\left(\sum_{j=1}^{i-1}b_j+b_i^+\right)-ci\\ >&S(\{b_1,\dots,b_i\})=\sum_{j=1}^{i}\frac{1-e^{-\nu i}}{(1+\mu e^{-\nu i})\,i}b_j-ci.\end{aligned} \quad (12)$$

The social welfare of new set of bids $\{b_1,\dots,b_i^+\}$ is larger than that of original set of bids $\{b_1,\dots,b_i\}$, which guarantees b_i^+ being in the set of winning bids.

2) Case 2: $b_{k-1}\geq b_i^+\geq b_k\geq\dots\geq b_i$, $1<k<i$. The new set of ordered bids is $\mathbf{b}^+=\{b_1,\dots,b_{k-1},b_i^+,b_k,\dots,b_{i+1},\dots b_N\}$. We have

$$S(\{b_1,\dots,b_{k-1},b_i^+\})=\frac{1-\mathrm{e}^{-\nu k}}{(1+\mu\mathrm{e}^{-\nu k})k}\left(\sum_{j=1}^{k-1}b_j+b_i^+\right)-ck, \quad (13)$$

$$S(\{b_1,\dots b_{k-1},b_k\})=\frac{1-\mathrm{e}^{-\nu k}}{(1+\mu\mathrm{e}^{-\nu k})k}\sum_{j=1}^{k}b_j-ck, \quad (14)$$

$$S(\{b_1,\dots,b_{k-1}\})=\frac{1-\mathrm{e}^{-\nu(k-1)}}{(1+\mu\mathrm{e}^{-\nu(k-1)})(k-1)}\sum_{j=1}^{k-1}b_j-c(k-1). \quad (15)$$

As the coefficient $\frac{1}{|\mathcal{W}|}\left(\nu_1\left(1-\mathrm{e}^{-\nu_2|\mathcal{W}|}\right)-\nu_3\right)$ in $S(\mathcal{W})$ is a monotonically decreasing function of $|\mathcal{W}|$, increasing b_i may change the winner set $\mathcal{W}$ and reduce the number of winners. Since in the original set of bids $\mathbf{b}$, $\{b_{1,\dots},b_{k-1},b_k,\dots,b_i\}$ are all selected as winning bids, $S(\{b_1,\dots b_{k-1},b_k\})>S(\{b_1,\dots,b_{k-1}\})$. Because the inequality in (11), we have $S(\{b_1,\dots,b_{k-1},b_i^+\})>S(\{b_1,\dots,b_{k-1}\})$,which implies that b_i^+still wins the auction. This concludes the proof. ■

Proposition 5. *The Social Welfare Maximization Auction (Algorithm 1) is computationally efficient and individually rational.*

Proof: Since the time complexity of finding the maximum miner's bid is $O(\min(N,D))$ and the number of winners is at most N, the time complexity of the winner selection process (while-loop, Lines 6-11) is $O(\min^2(N,D))$. In each iteration of payment calculation process (Lines 12-23), a similar winner selection process is executed. Therefore, the whole auction process can be performed in polynomial time with the time complexity of $O(\min^3(N,D))$ which is polynomial. According to Proposition 2 and the properties of the VCG mechanism [18], the payment scheme in Algorithm 1 guarantees the individual rationality. ■

V. Experiment Results and Performance Analysis

In this section, we provide simulation results of the proposed auction, from which we can further obtain useful decision making strategies for ESP and the blockchain owner.

A. Verification for Hash Power Function

An earlier real-world mobile blockchain mining experiment has been done in [12], [19]. In the experiment, we designed a mobile blockchain client application in the Android platform and implemented it on three mobile devices (miners). Each of the three client applications generates transactions and then starts mining with one CPU core. The miners' CPU utilization rate is managed and measured on the Docker platform [20]. Each mobile device mines the block under Go-Ethereum [21] blockchain framework. To verify the hash power function (1), we vary one miner's service demand while fixing the other two miners' service demand (CPU utilization) at 40 and 60. Besides, we set the number of transactions in each mined block to be 10 for all miners. Figure 2 shows the change of the hash power, i.e., the probability of successfully mining a block, with different amount of computing resources. We note that the hash power function defined in (1) can well fit the actual experimental data. From these results, we choose the hash power function with parameter $\alpha=1.2$ in the rest of this section.

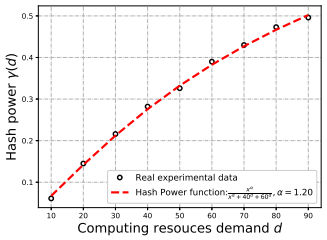
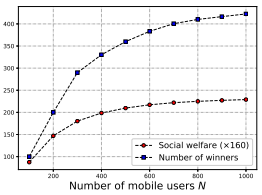


Fig. 2. Estimation of the hash power function $\gamma(d)$.

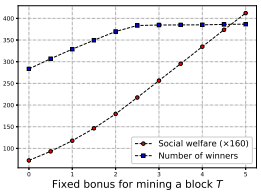
B. Simulation Results

We vary the number of mobiles users N from 100 to 1000, the mining bonus T from 0 to 5, and the transaction fee rate r from 0.001 to 0.009. We set $\mu=0.5$, $\nu=0.005$, $\xi=1$ and $c=0.02$. The transaction size s of each user is uniformly distributed over $[0,1000]$. Since the blockchain owner can adjust the average time of mining a block, we also varied the average time of mining a block λ from 100 to 1800 with increment of 212.5. Each measurement is averaged over 100 instances.

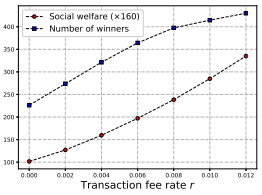
1) *Impact of the number of mobile users N:* Figure 3a shows the impact of the total number of mobile users N



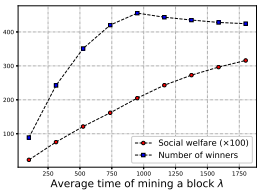
(a) Impact of the number of mobile users N.



(b) Impact of fixed bonus T.



(c) Impact of the transaction fee rate r.



(d) Impact of the parameter λ.

on the social welfare S and the number of participating users $|\mathcal{W}|$. We fix $T = 2.5$, $r = 0.007$ and $\lambda = 600$. We observe that $|\mathcal{W}|$ and S increase at diminishing rate as the base of mobile users becomes larger. Naturally, the ESP can select more winners as miners to increase the social welfare with more mobiles users. However, at the same time, the negative effects from the competition among a larger number of miners are apparent, which slows down the rise of the social welfare as well as the number of winners.

2) Impact of the fixed bonus T for mining a block and the transaction fee rate r: We set $N = 600$ and $\lambda = 600$. By fixing $r = 0.007$ and $T = 2.5$, we consider the impact of varied fixed bonus and transaction fee rate on the social welfare and the number of selected miners. From Figs. 3b and 3c, we note that if the blockchain owner raises the bonus or the transaction fee rate, more social welfare will be generated nearly in proportion. However, the number of winners increases and tends to be stable. This is because there will be fierce competition if too many miners participate in the blockchain network, which causes the loss of social welfare.
3) Impact of the average time λ for successfully mining a block: In Fig. 3d, we fix $N = 600$, $T = 2.5$ and $r = 0.007$. When the blockchain owner raises the difficulty of mining a block, represented by λ, the social welfare increases while the number of winners initially increases and then declines. Note that the user's expected reward R, i.e., the valuation for edge computing service, grows with increasing λ. When the difficulty λ is small and each user's valuation is also small, the ESP has to accept more users, i.e., more winners, to maximize the social welfare. However, if the difficulty of mining a block becomes high and each user values the service more, the ESP can reduce the number of winning users while achieving the optimal social welfare. Another reason for the decreasing number of winners is the increasingly intense competition among them.

VI. Conclusions

In this paper, we have investigated the edge computing services that enable mobile blockchain. To efficiently allocate computing resources, we have proposed an auction-based market model to maximize the social welfare. In the auction design, we have considered allocative externalities, including the competition among the miners as well as the network effects in the blockchain network. By theoretical analysis and simulation, we have proved that the auction mechanism is truthful, individually rational and computationally efficient and solves the social welfare maximization problem. For the future work, we will consider variable demands of mobile users.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*, EC '16, 2016.
[3] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[4] K. Kotobi and S. G. Bilén, "Blockchain-enabled spectrum access in cognitive radio networks," in *Proceedings of Wireless Telecommunications Symposium (WTS), 2017*, pp. 1–6, IEEE, 2017.
[5] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," tech. rep., National Bureau of Economic Research, 2016.
[6] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proceedings of WEIS*, 2013.
[7] N. Houy, "The bitcoin mining game," *Ledger*, vol. 1, pp. 53–68, 2016.
[8] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, 2015.
[9] L. Gao, Y. Xu, and X. Wang, "Map: Multiauctioneer progressive auction for dynamic spectrum access," *IEEE Transactions on Mobile Computing*, vol. 10, no. 8, pp. 1144–1161, 2011.
[10] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1732–1744, 2016.
[11] N. C. Luong, D. Niyato, P. Wang, and Z. Xiong, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," in *Proceedings of IEEE International Conference on Communications (ICC)*, May 2018.
[12] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, "Performance analysis and application of mobile blockchain," in *Proceedings of International Conference on Computing, Networking and Communications (ICNC)*, (Maui, Hawaii, USA), Mar. 2018.
[13] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Networking and Applications*, vol. 9, no. 2, pp. 397–413, 2016.
[14] P. R. Rizun, "A transaction fee market exists without a block size limit," *Block Size Limit Debate Working Paper*, 2015.
[15] M. O. Jackson, *Social and economic networks*. Princeton university press, 2010.
[16] R. B. Myerson, "Optimal auction design," *Mathematics of operations research*, vol. 6, no. 1, pp. 58–73, 1981.
[17] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic game theory*. Cambridge University Press Cambridge, 2007.
[18] V. Krishna, *Auction theory*. Academic press, 2009.
[19] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Edge computing resource management and pricing for mobile blockchain," *arXiv preprint arXiv:1710.01567*, 2017.
[20] "Docker," *https://www.docker.com/community-edition.*
[21] "Go-ethereum," *https://ethereum.github.io/go-ethereum/.*