Received: 26 November 2021 | Revised: 22 April 2022 | Accepted: 19 May 2022

DOI: 10.1002/cpe.7253

RESEARCH ARTICLE

WILEY

Three-stage auction scheme for computation offloading on mobile blockchain with edge computing

Chengpeng Xia[1] | **Yalan Wu**[2] | **Long Chen**[3] | **Yawen Chen**[1] | **Jigang Wu**[3]

[1]Department of Computer Science, University of Otago, Dunedin, New Zealand

[2]School of Intergrated Circuits, Guangdong University of Technology, Guangzhou, China

[3]School of Computers, Guangdong University of Technology, Guangzhou, China

Correspondence
Yalan Wu, School of Intergrated Circuits, Guangdong University of Technology, Guangzhou, China.
Email: wuyalan93@outlook.com

Funding information
Guangdong Basic and Applied Basic Research Foundation, Grant/Award Number: 2021B1515120010; National Natural Science Foundation of China, Grant/Award Numbers: 62072118, 62106052

Summary

Blockchain has been applied in wide range of fields to guarantee security. However, it has been very challenging for blockchain to flourish in mobile environment with limited resources. Existing studies mainly assume that single mobile user can buy the whole resources from edge servers in mobile blockchain. This paper formulates the problem of maximizing the social welfare for computation offloading in mobile blockchain. A three-stage auction scheme with approximation ratio of $(1-\epsilon)$ based on group-buying mechanism is proposed to allocate edge server resources for mobile blockchain applications. In the first stage, the miners are divided into groups, and a Vickrey–Clarke–Groves based auction is proposed to determine the bid of each group for each edge server. In the second stage, a matching algorithm is proposed to match edge servers and Access Points for maximizing the profit of edge servers. In the third stage, the edge server resources are allocated to mobile users for mining base on the results in the above stages. We prove that our auction scheme guarantees truthfulness, individual rationality and budget balance. Simulation results show that, the social welfare of our scheme is improved by 33.78%, 21.84%, 19.69%, and 6.69% for 1000 miners, compared with the existing works.

KEYWORDS

auction, edge computing, mobile blockchain, resource allocation

1 | INTRODUCTION

Blockchain technology has attracted attentions since the first decentralized cryptocurrency Bitcoin was launched in 2008.[1] As a distributed ledger, blockchain is designed to achieve peer-to-peer (P2P) electronic currency directly, without the support of a trusted third-party organization. Traditional blockchian has been applied to data storage, decentralized terminal transmission and cryptography due to the anonymity, decentralization, security and nontamperable nature of blockchain.[2,3] Recently, studies are exploring the wider applications of blockchain in other fields, such as finance,[4] cognitive radio network[5] and so on. According to the report of Tractica,[6] it is expected that the annual revenue for blockchain companies will increase to 19.9 billion by 2025.

In blockchain network, all peers serve as nodes participate in solving a hash-based mathematical problem guaranteeing integrity of transactions. Transaction information is packaged as a block which is joined to the existing blockchain. The above generating of blockchain complies with a consensus mechanism which is called proof of work (PoW). In addition to the PoW mechanism, there are some consensus mechanisms that are also widely used, such as proof of stake (PoS), delegated proof of stake (DPoS), et al. Specifically, there are some nodes in the blockchain network which are hardware with computing power, called *miners*. Miners try to solve a computationally puzzle, that is, PoW puzzle, in which the process is called *mining*.[7] Mining plays a vital role in verifying, broadcasting and recording transaction to the public ledger in the blockchian operation. For new block creating, once a miner has found out a hash value that satisfies the condition, miner will pack the transaction information into the block with

a timestamp, and broadcasts the block to the blockchain network. Finally, the block which is the first to pass the certification will be joined to the main chain after verification, and the first miner will receive a reward.

In recent years, the data generated on a daily basis has exploded and the network environment has become increasingly complex which can cause security related issues, and also provide opportunity for mobile blockchain. The application fields of the mobile blockchain are considered to be extensive, such as Internet of Things (IoT)[8] and cloud data auditing.[9] Specifically, a blockchain-based cloud data auditing system enables users to execute data audits locally which can avoid data from being attacked in the process of transmission. Overall, we mainly consider the following aspects. On the one hand, developers can quickly self-organize a reliable separate private blockchain or consortium blockchain to support various decentralized applications (DApps). On the other hand, mobile devices can be added to the public blockchain to get a certain reward.

However, solving the PoW puzzle problem needs high computing power and energy consumption. Running a blockchain based on the PoW protocol in the mobile environment has to rely on the support of personal computers and mining machines. Miners cannot rely solely on mobile devices to complete the process. It remains a challenge for blockchain to flourish in the mobile environment.[10] Mobile edge computing is a new paradigm to improve the computing performance of mobile devices by providing more computing resource at the edge of pervasive radio access networks.[11] In the network architecture, the configurations of cloudlets[12] and fog nodes[13] help mobile users to complete the tasks which are offloaded to the cell base station. As the provider of computing resources, the base station can obtain a certain return, which means mobile users need to pay the corresponding fee for serving of base station through some monetary compensation. Users can also choose different service base stations according to their preferences and locations. Moreover, the studies on dynamic offloading and resource scheduling optimization also help users to reduce communication latency and energy consumption in edge computing.[14,15] Hence, the introduce of edge computing for resource allocation is a promising solution to support mobile blockchain operation.

To maximize the energy-efficiency and the number of accessed miners for edge servers in mobile blockchain, it is particularly important to design an efficient and reliable allocation algorithm. Auction theory[16] is now seen as an important component of economics and it has been used to solve such task and resource allocation problems. Auctions allocate resources to users reasonably and maximally by evaluating the utilities of sellers and buyers. It can motivate more edge servers to participate in the resource sharing. In particular, auction scheme is suitable for mobile blockchain network, because there are multiple edge servers and multiple miners that act as sellers and buyers, respectively. The auction-based algorithms must meet certain economic theories, such as truthfulness, budget balance and individual rationality.[17] Many existing auction and incentive schemes cannot be directly applied to the mobile blockchain. A three stages auction model was proposed to allocate resources in Reference 18, and the feasibility of edge server placement for task offloading has been proved in Reference 19. However, all of the above works only guarantee incentive compatibility and revenue gain for the edge servers. The utility of other participants are not guaranteed. It is very challenging that designing an auction scheme to maximize the utility for participators and ensure the individual rationality.

To effectively allocate computation resources of edge severs in the task offloading process of miners in mobile blockchain, we need to solve the following challenging problems: (i) The edge servers are heterogeneous, and the budget and demand for each mobile miner are different. Meanwhile, the distances from miners to access points (APs) and edge servers are different, and the assignable resources of each edge server are also different. It is a challenge problem to model the mobile blockchain and determine winning prices of miners. (ii) For the edge servers, offloading computation will consume its electric energy and computation power. Meanwhile, for the access points, they need to provide relay service for miners. Due to the selfishness nature of each participant, they should be incentivized. It is vital to design a reliable allocation algorithm that can provide monetary compensation. (iii) Auction should meet economic properties which are truthfulness, individual rationality, budget balance and computational efficiency. It is a challenge problem to ensure the economic properties in the mobile blockchain.

The main contributions of this work can be summarized as follows.

- We propose a mobile blockchain model where the mobile miners can offload the compute-intensive PoW puzzle to the edge servers. We introduce the group-buying mechanism to inspire edge servers to share their resource for mobile blockchain, and it can guarantee that miners are affordable.
- We present a three-stage auction scheme to allocate resources in edge servers. In the first stage, we select some miners to be the potential winners for each edge server in each group, and it can determine the bids of APs. In the second stage, APs are matched with edge servers according to their bids. In the third stage, we allocate the edge servers to corresponding groups, then miners offload the mining tasks to the edge servers.
- We prove that the proposed algorithms are truthful, individual rational, computational efficient and budget balanced. We prove that the proposed scheme is a $(1-\epsilon)$-approximation scheme.
- Extensive simulation results show that, the social welfare of proposed scheme is improved by 33.78%, 21.84%, 19.69%, and 6.69% for 1000 miners, respectively, compared with the existing studies.

The rest of the paper is organized as follows. Section 2 discusses the related works. The system model and formulating the resource allocation problem are introduced in Section 3. Section 4 describes our algorithms in the auction model. Section 5 gives theoretical analysis of our auction scheme. Simulation results are given in Section 6. Finally, Section 7 concludes the paper.

2 | RELATED WORK

In the last few years, some research focused on the areas of blockchain operations and applications. For example, authors in Reference 20 studied the motivation of Bitcoin users to spread transactions and join in the blockchain. Decker et al. modeled and explained the way of transaction propagating in Bitcoin network.[21] Besides, to improve the mining process, Houy[22] showed the situation of being a Nash Equilibrium in a two-miner case of mining game. The mining process based on solving PoW puzzle modeled as Poisson process with time dependence in Reference 23. Kraft[23] proposed an analytical method to improve the stability of block-times by changing the network-difficulty. Based on the above blockchain operation models, people began to explore the application of the mining process in mobile devices, that is, mobile blockchain. A blockchain-based permissions management framework was designed in Android system,[24] in which blockchain was applied to authenticate the results obtained and make them veritable and auditable. However, The mining process of this framework was executed in the personal computers and mining machines instead of mobile devices. Reference 10 proposed a mobile commerce application, that the mining process execute in Android mobile devices. In addition, authors in Reference 25 designed a mobile blockchain model that mobile users offload their mining process to an edge computing service provider, and adopted a two-stage Stackelberg game to manage the resources. However, both of the above studies did not consider the utility of miners and edge servers.

Resource allocation in edge computing has been widely studied in other field, such as truthful auction mechanisms,[26] where the authors proposed two truthful auction mechanisms for homogeneous tasks and heterogeneous tasks assignment. Authors proposed a user mobility prediction model to optimize edge server selection for enhancing the resource utilization of edge servers by using machine learning approach.[27] A cloudlet deployment model was proposed to allocate resources.[18] However, these works cannot be directly applied to mobile blockchain,[28] because the studies only concentrate on the specific constraints for their research topics. To design a resource allocation algorithm for mobile blockchain, both References 28 and 29 presented an auction mechanism for edge computing resource allocation respectively, where the auction in Reference 29 was based on deep learning. However, their studies assumed one mobile user can afford to buy those expensive edge servers, without considering the most important factor to incentivize the edge servers to offer its edge computing service.

In summary, the aforementioned works motivate us to study a resource allocation mechanism for mobile blockchain. Hence, we introduce a group-buying mechanism into mobile blockchian, and allocate the resources of edge servers to the small groups.

3 | SYSTEM MODEL AND PROBLEM FORMULATION

In this section, we first introduce the system model of the mobile blockchain network as well as the three-stage auction scheme which is called TCMB. Then, we formulate the problem and present the auction model for mobile blockchain.

3.1 | System model

Figure 1 illustrates the system model of our three-stage auction scheme for mobile blockchain. Mobile devices that execute the blockchain application are miners. In the process of mining, there is a set of miners required to execute a consensus protocol in order to find a new hash for the last block to store the verified transaction, that is, solving the PoW puzzle. The block of the miner who solves the puzzle firstly can be included in the blockchain. Remarkably, we only discuss blockchain technology which is based on PoW in this paper. However, solving the PoW puzzle requires high electricity and computing power from mobile devices. Hence, edge servers are introduced to share their resources to address this problem.

We build a group-buying model among mobile users, and set the independent miners into groups based on the related APs, which can resolve delays and energy consumption caused by long distance. We try to share the resources of edge servers to a group of miners instead of one miner. Therefore, in our three-stage auction model, the miners act as the buyers that buy resources by a group-buying way. The edge servers act as the sellers which provide resources. The APs act as the auctioneers that are the trusted third parties. In particular, miners of each group can obtain resources being able to afford those expensive edge servers, and the edge servers can share theirs resources and be rewarded in an effective way. Moreover, we consider that an edge server is constituted by a group of computers which are resource-rich, Internet-well-connected, and trusted. In order to prevent the monopoly of hashing power, blockchain developer designs the system that edge servers are not allowed mining by themselves in this paper. It is worth noting that we mainly focus on the blockchain environment that mobile devices have lower movement speed. The scenarios of cross AP are not within the scope of this paper. For the clarity of our algorithms, the key acronyms are summarized in Table 1.

We assume that $A = \{A_1, A_2, \dots, A_n\}$ represents the set of APs, and $E = \{E_1, E_2, \dots, E_K\}$ denotes the set of edge servers. In the first stage, there are a number of miners which are divided into n small groups according to the distance between miners and APs, and each group has n_i miners. The jth miner in the ith AP is denoted by U_i^j where $U_i = \{U_i^1, U_i^2, \dots, U_i^{n_i}\}$ in group A_i. We use that $\mathbb{U} = \bigcup_{i=1}^{n} U_i$ to denote the set of all miners. For edge server E_k, miner U_i^j submits budget $b_i^j(k)$ ($j \in \{1, 2, \dots, n_i\}$) as public information and resource demand r_i^j($j \in \{1, 2, \dots, n_i\}$) to AP. APs determine the

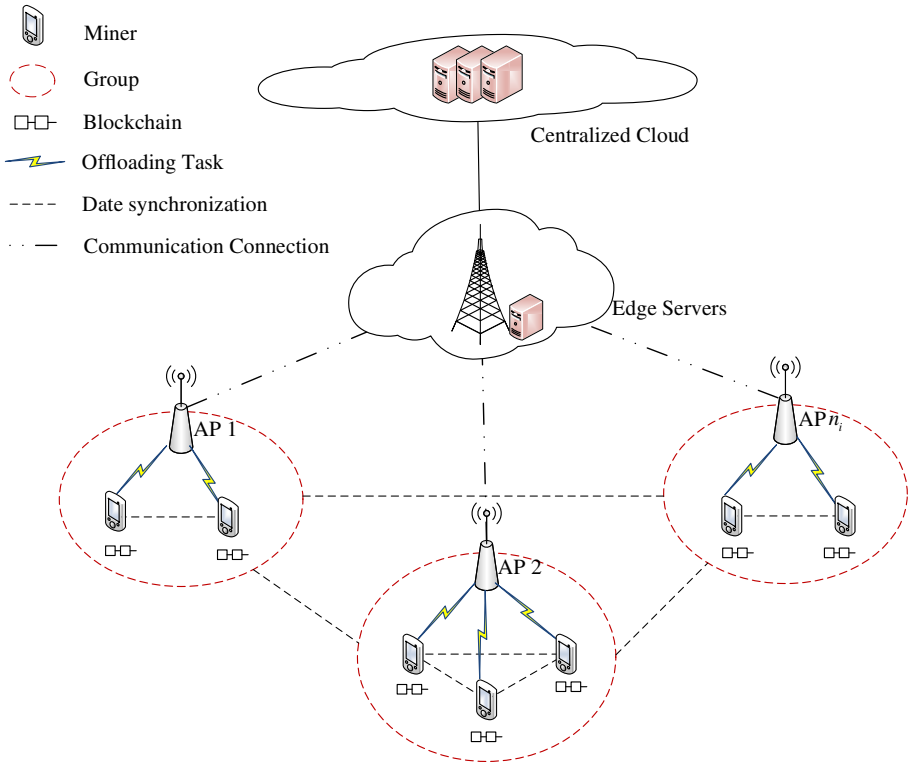

FIGURE 1 An illustration of mobile blockchain systems with three-stage resource allocation auction.

TABLE 1 Acronyms for system model

Acronyms	Meaning
TCMB	Three-stage auction scheme on blockchain
IoT	Internet of Things
AP	Access point
PoW	Proof-of-Work puzzle
VCG	Vickrey–Clarke–Groves auction
PWD	Potential winners determining algorithm
PGA	Payment getting algorithm
AM	APs matching algorithm

potential winner matrix and potential payment in this stage, and we use ω_i^k and $p_i^j(k)$ to denote the potential winner matrix and potential payment in group A_i for edge server E_k.

In the second stage, AP has a budget for each edge server which is calculated by summing the potential payments of miners in the group. Let b_i^k be the budget of group A_i bidding for E_k, and APs submit the budgets to the corresponding edge servers. After that, we match APs with edge servers, and we use θ_i^k to describe the edge server allocation.

In the third stage, We find the finally winers for edge servers according to the matching rule which is determined by the algorithm of the first two stages. AP charges the corresponding fee p_i^j in the potential winners set, and winner offloads the mining process to the edge server.

We use $x_i^j(k)$ to describe the computational resource allocation profile which can be defined as,

$$x_i^j(k) = \begin{cases} 1, & \text{if } U_i^j \text{ wins its bid for } E_k, \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

For the clarity of our system model, the key notations are summarized in Table 2.

TABLE 2 Notations for system model

Notations	Meaning
A_i	ith AP
E_k	kth edge server
U_i^j	jth miner of the ith AP group
n_i	Number of miners the ith AP group
r_i^j	Source demand of U_i^j
$b_i^j(k)$	Budget of U_i^j for E_k
F_i^k	Actual revenue of E_k of A_i
$p_i^j(k)$	Potential payment of A_i for E_k
$x_i^j(k)$	Statement whether U_i^j wins E_k
ξ_i^j	Computer power of U_i^j
S_B	Number of transactions in a new block
R_i^j	Reward of U_i^j from the mining process
ψ	Fixed bonus
η	Transaction fee rate
λ	Average block time
ζ	Variable reward factor
RS_k	Assignable resources of E_k
$w(k)$	The amount of allocated resources of E_k
$cs(k)$	Cost factor of E_k
RP_k	Reserve price of E_k
δ	Degree of competition in the market
p_i^j	Fee the AP charging the potential winner sets.
u_i^j	Utility of U_i^j
u_i	Utility of A_i
u^k	Utility of E_k
P_i	Fee a_i pays to E_k
P^k	Clearing price of APs
SW	Total social welfare

3.2 | Problem formulation

If U_i^j finds a new block successfully, it has a ξ_i^j percent chance of receiving a block reward from the blockchain. ξ_i^j is determined by the relative power in the whole network, which is defined as follows.[10,25]

$$\xi_i^j = \frac{r_i^j x_i^j(k)}{\sum_{i=1}^{n}\sum_{j=1}^{n_i} r_i^j x_i^j(k)}, \quad \xi_i^j > 0, \tag{2}$$

which satisfies that $\sum_{i\in n}\sum_{j\in n_i}\xi_i^j = 1$.

If a block is overtaken by other block at the time of propagation, it will be discarded, which be called *orphaned*.[30] Therefore, the miner who has solved the PoW puzzle firstly may not be certified and not be rewarded, when its block is overtaken by other block. We define the expected reward R_i^j of U_i^j as,

$$R_i^j = (\psi + \zeta \cdot S_B) \cdot P(\xi_i^j, S_B) = (\psi + \zeta \cdot S_B) \cdot \xi_i^j e^{-\frac{1}{\lambda}\eta S_B}, \tag{3}$$

where R_i^j consists of a variable bonus and a fixed reward ψ. We use $\zeta \cdot S_B$ to denote the variable bonus, where ζ is a given variable reward factor with $\zeta \geq 0$. $P(\xi_i^j, S_B)$ is the probability of miner receiving reward, λ is the average block time and η is the transaction fee rate. The detail of formulation for expected reward of miner is showed in Appendix A.

For edge server E_k, we assume that the total resources in each edge server are different because of the heterogeneity of edge servers. The cost function of E_k can be quantified as,[31]

$$Cos(k) = cs(k) \cdot w(k), \tag{4}$$

where $w(k)$ is the amount of resources which are offloaded in the mining process by miners, and $cs(k)$ is the cost factor of E_k. We use RS_k to denote the assignable resources. The reserve price of E_k can be quantified as,

$$RP_k = cs(k) \cdot RS_k + \delta. \tag{5}$$

Edge servers will not sell the resources to miner whose payment is lower than reserve price, due to selfishness nature. Obviously, the reserve price for each edge server is different, since the edge servers may be heterogeneous and their cost factor is different. We assume that RS_k cannot changed after E_k submits to AP, and it is fixed during an auction. The parameter δ reflects market competition which increases with the increase of market competition, contrarily it will decrease. This is not the focus of our research, and we set $\delta = 0$ in this paper.

There is a preference for each miner, because the service quality provided by each edge server is different. Preferences are known only by themselves. Miners submit different bids according to their preferences. They prefer to pay higher prices for good service, and the budget $b_i^j(k)$ is higher also. When our three-stage auction is done, APs will charge miners according to the winners set, and miners will offload the mining tasks to the edge servers.

If U_i^j is a winner, its expected reward is R_i^j which is the gaining benefits from mobile blockchain, and it should pay p_i^j after the auction. Therefore, the utility of U_i^j can be defined as,

$$u_i^j = \begin{cases} R_i^j - p_i^j, & \text{if } U_i^j \in x_i^j(k), \\ 0, & \text{otherwise.} \end{cases} \tag{6}$$

If a miner is not a winner, its utility is 0. For the utility of AP, A_i will get an actual revenue from miners when A_i is in the winner set θ_i^k, and we use F_i^k to denote the actual revenue for edge server E_k. It pays P_i to edge server. We can quantify the utility of A_i^j as,

$$u_i = \begin{cases} F_i^k - P_i, & \text{if } A_i \in \theta_i^k, \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Similarly, E_k will get a reward if it is contained in the winner set θ_i^k, that is, the payment of AP P^k. $Cos(k)$ is the cost of E_k. The utility of edge server is defined as,

$$u^k = \begin{cases} P^k - Cos(k), & \text{if } E_k \in \theta_i^k, \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

We aim to maximize the total utilities of all participants by seeking the optimal offloading task and resource allocation. We introduce the social welfare SW to evaluate the efficiency of our auction scheme, which is defined as,

$$SW = \sum_{i=1}^{n} \sum_{j=i}^{n_i} u_i^j + \sum_{i=1}^{n} u_i + \sum_{k=1}^{K} u^k. \tag{9}$$

Hence, we formulate the optimization problem as a social welfare maximization problem as follows.

$$\begin{aligned} &\max\ SW, \\ &s.t. \sum_{j=1}^{n_i} x_i^j(k) r_i^j \leq RS_k, \quad \forall A_i \in a, \quad \forall E_k \in E, \\ &\sum_{k=1}^{K} x_i^j(k) = 1, \quad \forall U_i^j \in \mathbb{U}. \end{aligned} \tag{10}$$

Moreover, the social welfare maximization problem defined in (10) is NP-hard. It is a considerably challenge to design a scheme for maximizing the social welfare. The detail of NP-hardness proof is showed in Appendix B.

3.3 | Example application: Decentralized IoT authentication

To illustrate the application of our system and demonstrate the availability of concepts in this paper, we use a blockchain-based IoT authentication in Reference 32 as an example. In this system, each mobile devices is regarded as a requester to access data resources from IoT devices and sensors. However, mobile user does not have enough trust and right to access the IoT system. In this context, deploying a blockchain-based authentication by developer can be seen as a viable solution in IoT information system protection. Mobile users can self-organize a secure blockchain with the available edge server computing resources based on the designed smart contract.

In this blockchain-based IoT authentication system, there is a mobile block-chain with PoW consensus. For user registration, certificate issuer verifies the validity of user's registration request and updates the information to blockchain. The system verifies the identity of the transaction initiator by verifying the transaction signature in the blockchain for user authentication. Due to the computing resources and energy limitation of mobile devices, they are expected to buy resources from edge servers for blockchain operation. Hence, the three-stage auction is designed to execute the resources allocation. Users submit the bids and the demands to APs who will calculate the allocation results and the payments according to our auction scheme. Meanwhile, the auction scheme need guarantee the truthfulness and non-negative of each participant and maximize the social welfare. Finally, The winning miners offload the mining process to contribute new blocks containing the authentication information and corresponding transaction records to the blockchain, or verify user's identity information from the blockchain when user sends an access request.

4 | THREE-STAGE AUCTION SCHEME

In this section, we describe the proposed three-stage auction scheme for mobile blockchain. We first propose an optimal potential winner determination algorithm, and propose a payment calculation algorithm which is based on Vickrey-Clarke-Groves (VCG) auction. Then, we design a truthful AP match algorithm. The proposed group-buying auction scheme is truthfulness, individual rationality and optimization social welfare.

Figure 2 illustrates the overview of proposed three-stage auction scheme. In the scheme, APs determine the potential winners for each edge server from their group of miners, and decide their payments based on the bid of winning miners in the first stage. AP calculates its revenue R_i^k, where $i \in \{1, 2, \ldots, n\}$ and $k \in \{1, 2, \ldots, K\}$. In the second stage, APs bid for edge servers with budget equal to R_i^k. We match edge servers with APs according to their bids and reserve price RP_k. In the third stage, we match miners with edge servers where the miners are the potential winners determined in the first stage. After paying the resources, we place the edge servers in the winner APs, and allocate resources to the miners.

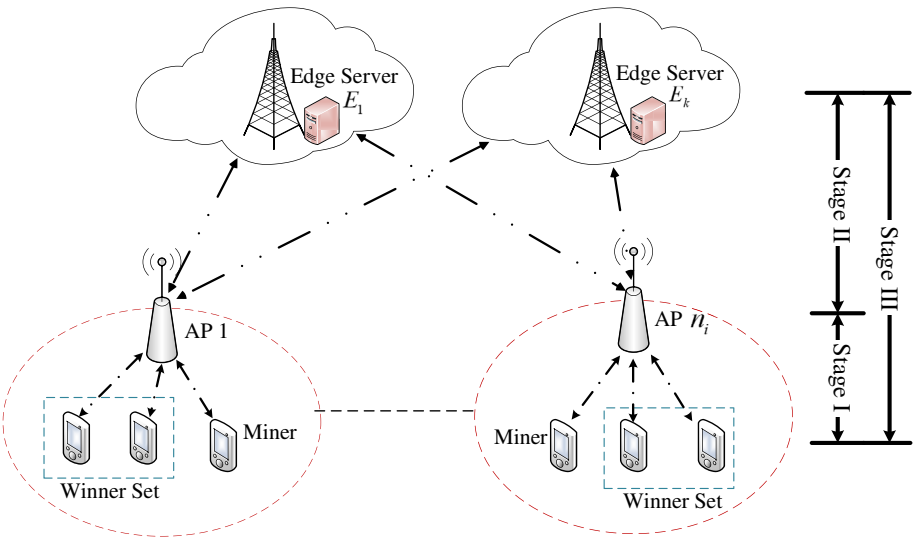

FIGURE 2 The overview of three-stage auction scheme

4.1 | Stage I: Matching potential winner

As shown in Algorithm 1, we first introduce a matching strategy to help APs select the potential winners. We design a greedy algorithm receiving resources as much as possible for miners. There is a different preference in terms of the quality of service and distance, and miners submit different bids for disparate edge servers. After they submit resource demand, we can obtain *cost performance ratio*, and define it as,

$$c_i^j(k) = \frac{b_i^j(k)}{r_i^j}, \tag{11}$$

where r_i^j is the resource demand of miner U_i^j, and b_i^j is the bid. Obviously, the cost performance ratio of miner is in direct proportion to the bid because the resource demand is fixed. Proposed algorithm can ensure to get resources as much miners as possible, and calculate the revenues of APs. The detail of the processes is presented in Algorithms 1 and 2.

In each group, let L_i^k be the number of resources which have been allocated in the process of matching between A_i and E_k. AP sorts miners in descending order according to the cost performance ratio and stores them to set M_i^k, which is the descending miner set between A_i and E_k. At first, AP selects the first miner for E_k from M_i^k, that is, the miner whose *cost performance ratio* is the largest. Then AP determines that whether the total resource demands exceed the total assignable resources. If r_i^k meets that $L_i^k + r_i^j \le RS_k$, AP will add U_i^j to the potential winner set ω_i^k, that is, $\omega_i^k = 1$, remove U_i^j from M_i^j, and update L_i^k by $L_i^k = L_i^k + r_i^j$. We choose the next miner, until we find out the miner whose demand satisfies that $L_i^k + r_i^j \ge RS_k$. After that, algorithm calculates the clearing price by potential winner matrix ω_i^k.

We design a VCG-based payment calculation algorithm. VCG mechanism is one of the most popular auctions with truthfulness. Winner will be paid with the 'opportunity cost' in VCG auction. We use $V_{\mathbb{B}}^{\mathbb{U}}$ and $V_{\mathbb{B}\setminus b_i^j(k)}^{\mathbb{U}}$ to denote the total bids under the above potential winner determination scheme, with and without the presence of bid $b_i^j(k)$ and miner U_i^j. Noted that $V_{\mathbb{B}}^{\mathbb{U}} - \omega_i^k b_i^j(k)$ denotes the total bids except for bid $b_i^j(k)$ under the above potential winner determination scheme. The miner's payment $p_i^j(k)$ is called 'opportunity cost', and it can be derived as the difference between $V_{\mathbb{B}\setminus b_i^j(k)}^{\mathbb{U}}$ and $V_{\mathbb{B}}^{\mathbb{U}} - \omega_i^k b_i^j(k)$, as follows.

$$p_i^j(k) = V_{\mathbb{B}\setminus b_i^j(k)}^{\mathbb{U}} - \left(V_{\mathbb{B}}^{\mathbb{U}} - \omega_i^k b_i^j(k)\right). \tag{12}$$

The detail of the VCG-based payment calculation algorithm is presented in Algorithm 2. If a miner is not a potential winner, its payment $p_i^j(k) = 0$. Hence, the revenue of A_i is the sum of $\{p_i^j(k)\}$, that is, $F_i^k = \sum_{j=1}^{n_i} p_i^j(k)$. If A_i wins the edge server C_k in next stage, it will charges $p_i^j(k)$ on miners.

Algorithm 1. *PWD /* potential winners determining */*

Input: The cost performance ratio of miners $\{c_i^k(k)\}$, assignable resources set $\{RS_k\}$
Output: Potential winner matrix ω_i^k, potential clearing price $\{p_i^j(k)\}$ and revenue set $\{F_i^k\}$

```
for k = 1 to K do
    Sort miners in descending order according to the c_i^j(k) and store to M_i^k
    for y = 1 to n_i do
        Choose the miner with the largest c_i^j(k) from M_i^k
        if L_i + r_i^j ≤ RS_k then
            ω_i^k = ω_i^k ∪ U_i^j
            L_i = L_i + r_i^j
            Remove U_i^j from M_i^k
        else
            Remove U_i^j from M_i^k
        end if
    end for
    for i = 1 to n do
        p_i^j(k) = PGA(i, j, k, c_i^k(k), RS_k ω_i^k)
    end for
    F_i^k = Σ_{j=1}^{n_i} p_i^j(k)
end for
```

Algorithm 2. *PGA /* payment getting algorithm */*

Input: i, j, k, cost performance ratio $\{c_i^k(k)\}$, assignable resources set $\{RS_k\}$, potential winners matrix ω_i^k

Output: Potential clearing price $\{p_i^j(k)\}$

$V_{\mathbb{B}}^{\mathbb{U}} = \sum_{U_i^j \in \omega_i^k} b_i^j(k)$

Remove U_i^j from M_i^k

for $y = 1$ to n_i **do**

  Choose the miner with the largest $c_i^{j'}(k)$ from M_i^k

  if $L_i + r_i^{j'} \le RS^k$ **then**

    $\bar{\omega}_i^k = \bar{\omega}_i^k \cup U_i^{j'}$

    $L_i = L_i + r_i^{j'}$

    Remove $U_i^{j'}$ from M_i^k

  else

    Remove $U_i^{j'}$ from M_i^k

  end if

end for

$V_{\mathbb{B}\setminus b_i^j(k)}^{\mathbb{U}} = \sum_{U_i^j \in \bar{\omega}} b_i^j(k)$

if $U_i^j \in \omega_i^k$ **then**

  $p_i^j(k) = V_{\mathbb{B}\setminus b_i^j(k)}^{\mathbb{U}} - (V_{\mathbb{B}}^{\mathbb{U}} - \omega_i^k b_i^j(k))$

else

  $p_i^j(k) = 0$

end ifreturn p_i^j

Note that the algorithms cannot be directly applied to our model in Reference 18. The reason is that their pricing strategy will cause a local optimal, and its payment is larger than our algorithms. Therefore, its algorithm cannot achieve a great utility both for miners and other participants. The specific analysis will be presented in the simulation section.

To illustrate the details of Algorithm 1, we assume that there are 2 APs $\{A_1, A_2\}$ and an edge server E_1 with its assignable resource $RS_k = 7$. We divide miners into groups based APs as $(U_1^1, U_1^2, U_1^3, U_2^4)$, $(U_2^1, U_2^2, U_2^3, U_2^4)$ with their bids for E_1 as $\{4, 1, 5, 2\}$, $\{2, 3, 5, 3\}$, and assume their resource demands are $\{3, 1, 4, 1\}$, $\{3, 3.5, 5, 1.5\}$. First, according the performance ratio $c_i^j(k)$ where $c_i^j(k) = b_i^j(k)/r_i^j$, we calculate the performance ratio among the miners for E_1, that is, $\{1.33, 1, 1.25, 2\}$ and $\{0.67, 0.86, 1, 2\}$. Then, we have $M_1^1 = \{U_1^4, U_1^1, U_1^3, U_1^2\}$ which is sorted by the performance ratio $c_i^j(1)$. The largest U_1^4 is selected and judged by whether $L_1^1 + r_1^4 \ge RS_1$. Since $L_1^1 = 2$ at this moment, m_1^4 is added to the potential winner set ω_1^1 for E_1, and U_i^k is removed from M_i^k. Similarly, U_1^1 is also a winner, and $L_1^1 = 2 + 4 = 6$. So far, the remaining resource needs of miners are greater than the distributable resources. Therefore, we have potential winner set that $\omega_1^1 = \{U_1^4, U_1^1\}$. By analog, the potential winner set of A_2 for E_1 is that $\omega_2^1 = \{U_2^4, U_2^2\}$.

For Algorithm 2, we propose a simple example as follows. Same as the assumption of Algorithm 1, there is an edge server E_1 with its assignable resource 7 and a miner group with 4 members $\{U_1^1, U_1^2, U_1^3, U_1^4\}$ based on A_1. The bids, source demands and performance ratios are $\{4, 1, 5, 2\}$, $\{3, 1, 4, 1\}$ and $\{1.33, 1, 1.25, 2\}$. Its potential miner winner set is $\{U_1^4, U_1^1\}$ which is obtained in Algorithm 1. We calculate the payment of U_1^4 according to the VCG-based algorithm. The total bid of A_1 is that $V_{\mathbb{B}}^{\mathbb{U}} = b_1^1 + b_1^4 = 6$ and the total bid except b_1^4 is that $V_{\mathbb{B}}^{\mathbb{U}} - \omega_1^1 b_1^4(1) = 6 - 2 = 4$. The total bids under the above potential winner determination scheme without the presence of bid $b_1^4(1)$ and miner U_1^4 is $V_{\mathbb{B}\setminus b_1^4(1)}^{\mathbb{U}}$, in this case, U_1^1 and U_1^3 will win the auction, that is, $V_{\mathbb{B}\setminus b_1^4(1)}^{\mathbb{U}} = b_1^1 + b_1^3 = 9$. Therefore, the payment of U_1^4 is that $p_1^4(1) = V_{\mathbb{B}\setminus b_1^4(1)}^{\mathbb{U}} - (V_{\mathbb{B}}^{\mathbb{U}} - \omega_1^1 b_1^4(1)) = 9 - 4 = 5$. U_1^1 means without miner U_1^1 and bid b_1^1, so the potential winner set is $\{U_1^4, U_1^3, U_1^2\}$, that is, $V_{N\setminus b_1^1(1)}^{\mathbb{U}} = b_1^4 + b_1^3 + b_1^2 = 8$. The payment of U_1^1 is that $p_1^1(1) = V_{\mathbb{B}\setminus b_1^1(1)}^{\mathbb{U}} - (V_{\mathbb{B}}^{\mathbb{U}} - \omega_1^1 b_1^1(1)) = 6$.

4.2 | Stage II: Matching edge server for AP

In this stage, we select the optimal AP for each edge server. First, AP submits its bid b_i^k which equals to its revenue F_i^k, to keep the auction truthful. We use that $d_i^k = b_i^k - RP_k$ to denote the profit of E_k.[33] D is the set of d_i^k. The profit vector D_i is the ith row in the matrix D.

We try to design an optimal matching with the maximizing profit while ensuring the truthfulness of auction. The process of matching APs with edge servers is shown in the Algorithm 3. We assume that *num* is a small random integer. In this paper, the *num* is set between 0 and 2 in the algorithm for the truthfulness, that is, $num \in [0, 2]$. We select the *num*th element d_i^k in D. For this AP-edge server matching, the profit is d_i^k. The Algorithm 3 judges whether the budget of A_i is larger than the reserve price of E_k, and the profit is a positive value when $d_i^k > 0$. If $d_i^k < 0$, A_i fails to be matched

Algorithm 3. *AM* /* APs matching with edge servers */

Input: $\{b_i^k\}, \{RP_k\}, \{D\}$
Output: The match matrix X, $\{P_i\}$, $\{P^k\}$
for $k = 1$ to K **do**
  for $i = 1$ to n **do**
    Find out the *num*-th profitable matching d_i^k from D.
    if exist b_j^k, s.t. $b_i^k \geq b_j^k \geq \cdots \geq RP_k$ **then**
      $\theta_i^k = 1$
      $P_i = P^k = B_j^k$
      Setting the values of elements in ith row and kth column of D to 0.
    else
      $d_i^k = 0$
      $\theta_i^k = 0$
    end if
  end for
end for

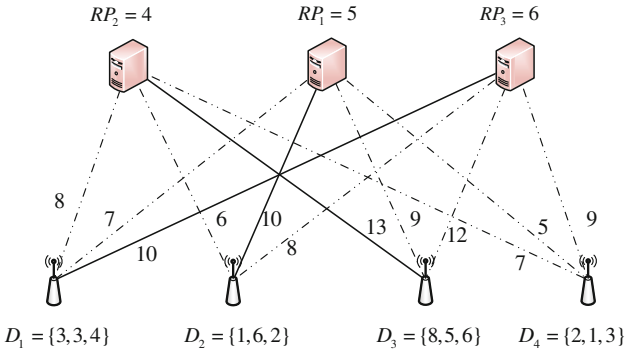

FIGURE 3 Example for *AM*

with E_k, and $\theta_i^k = 0$, which is the allocated matrix between APs and edge servers. If $d_i^k > 0$, we should find a bid b_j^k for edge server E_k from the other AP, where b_j^k meets $b_i^k \geq b_j^k \geq \cdots \geq RP_k$ and $i \neq j$. In other words, the selected bid has the maximum value for E_k without the bid b_i^k. Then, we allocate E_k on A_i, and set $\theta_i^k = 1$. If there is no such b_j^k meets the condition, we set $\theta_i^k = 0$ also. The clearing prices of A_i and E_k equal to b_j^k which is the largest bid between b_i^k and RP_k. Particularly, the revenue of E_k is equal to the clearing prices, so we have that $P_i = P^k = b_j^k$. Finally, we set the values of all elements in the ith row and kth column for matrix D, respectively.

To illustrate the above process, we use Figure 3 as an example. There are 3 edge servers $\{E_1, E_2, E_3\}$ with their reserve price RP_k as $\{5, 4, 6\}$ and 3 APs $\{A_1, A_2, A_3, A_4\}$ with their bids for edge servers b_i^k as $\{8, 7, 10\}$, $\{6, 10, 8\}$, $\{13, 9, 12\}$, $\{7, 5, 9\}$, hence their corresponding profits are $\{3, 3, 4\}$, $\{1, 6, 2\}$, $\{8, 5, 6\}$, $\{2, 1, 3\}$ which are calculated by $d_i^k = b_i^k - RP_k$. First, we assume that the random number *num* is equal to 1 and select the *num*th d_i^k from D, that is, $d_3^1 = 8$. Since there is a b_1^1 where $b_3^1 = 13 > b_1^1 = 8 > RP_k$, we set $\theta_3^1 = 1$ which means we allocate E_1 to A_3, and the payment of A_3 is $P_3 = P^1 = b_1^1 = 8$. The ith row and the kth column of D are set to 0, so, $D = \{\{0, 3, 4\}, \{0, 6, 2\}, \{0, 0, 0\}, \{0, 1, 3\}\}$. Therefore, we select *num*th d_i^k again and assume $num = 2$. b_1^3 can be chosen satisfying that $d_1^3 = 10 \geq d_2^2 = 10 > RP_k$. We allocate E_3 to A_1, the payment of A_1 is $P_1 = P^3 = b_2^2 = 10$. Finally, we obtain that E_2 matches with A_2 and the payment is 5.

4.3 | Stage III: Allocation of the resource

We get the winner APs and the matching matrix of APs with edge servers in stage II. APs charge the potential winner miners price $p_i^j(k)$ which is confirmed in stage I in their group. For each AP A_i, it will pay P^k to the corresponding E_k. The edge servers will be placed in the corresponding APs, and resources will be allocated to the miners. The miners will offload the mining program to edge servers to solve the PoW puzzle.

5 | THEORETICAL ANALYSIS

Given the utility function defined in (10), we now analyze the performance of the proposed auction. As shown in Definition 1, we introduce a definition to prove that our auction guarantees the economic properties. Moreover, an approximation algorithm is guarantee of good performance for NP-hard problem solving which will be proved by Definition 2.

Definition 1 (Definition 13.6 34). An auction is truthful if and only if it satisfies the following two conditions:

1) the winner selection rule is *monotonic*, that is, if miner U_i wins the auction with bid $b_i^j(k)$, then it will also win with any higher bid $b_i^j(k) > b_i^j(k)'$.
2) the payment of each winner is the *critical payment*, and it is the smallest value needed.

Definition 2 (Definition 1.2 35). A polynomial-time approximation scheme is a family of algorithms A_ϵ, where there is an algorithm for each $\epsilon > 0$, such that A_ϵ is a $(1-\epsilon)$-approximation algorithm for maximization problems.

5.1 | Truthfulness

To demonstrate the truthfulness, we should prove that miners are truthful in each stage of our auction.

Theorem 1. *The auction is truthful in Stage I.*

Proof. Suppose that the bid $b_i^n(k)$ of m_i^j is the winning bid in the n-th step with algorithm 1. Let $(b_i^1(k), b_i^2(k), \ldots, b_i^n(k))$ be the first n winners in AP a_i. There are $n-1$ miners winning the auction before U_i^n. Assume that there is a bid $b_i^{n'}(k)$ which replaces bid $b_i^n(k)$, where $b_i^{n'}(k) = b_i^n(k) + \theta,\ (\theta > 0)$. We can easily to obtain that bid $b_i^{n'}(k)$ will certainly win in the nth step or even earlier step. Thus, the Algorithm 1 is monotonic that is, it satisfies the first condition Definition 1. For the critical payment, since Algorithm 2, which is the calculation of payment based on VCG mechanism, it directly satisfies the second condition in Definition 1. ∎

Theorem 2. *The auction is truthful in Stage II.*

Proof. Algorithm 3 is similar to the *fixed price auction* in Reference 33, which has been proved to be truthful. We only alter the method of profit parameter determination. When the *num* is equal to 2, the algorithm is truthful, which has also been proved. In addition, the payments in the stage II are independent to edge servers and APs. Thus, the auction scheme in stage II is truthful. ∎

5.2 | Budget balance

Theorem 3. *The three-stage auction scheme is budget balanced.*

Proof. The budget balance for the proposed scheme can be proved as follows. If $\theta_i^k = 1$, E_k was matched to A_i, and the total payment of winning miners is that $ear_1 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} p_i^j$. The total profits for edge servers are that $ear_2 = \sum_{k=1}^{K} P^k$. Similarly, the total profits of APs are that $ear_3 = \sum_{i=1}^{n}(F_i^k - P_i)$. The total budget of APs ear_4 is equal to the value of ear_1, where $ear_4 = \sum_{i=1}^{n} b_i^k$. We can obtain that $ear_4 \geq ear_2 + ear_3$ by Algorithm 3, and calculate that $ear_1 \geq ear_2 + ear_3$. The final result is that,

$$\sum_{i=1}^{n}\sum_{j=1}^{n_i} p_i^j \geq \sum_{k=1}^{K} P^k + \left(\sum_{i=1}^{n} F_i^k - \sum_{i=1}^{n} P_i\right). \tag{13}$$

∎

5.3 | Individual rationality

Theorem 4. *The three-stage auction scheme is subject to the individual rationality.*

Proof. In the first stage, if U_i^j wins the edge server E_k. According to properties of the VCG mechanism[36] and Algorithms 1 and 2, it directly proves $p_i^j \leq b_i^j(k)$, and the payment mechanism in the first stage guarantees the individual rationality.

For APs, as mentioned above, $b_i^k = F_i^k . b_j^k \le b_i^k$ and $b_j^k = P_i$ according to Algorithm 3. Hence, $F_i^k = b_i^k \ge P_i$. Moreover, the payment for edge servers cannot be smaller than their requirement, that is, $P^k \ge RP_k$. ∎

5.4 | Computational efficiency

Theorem 5. *The time complexity of the proposed scheme is $O(K \cdot n^2)$.*

Proof. For the first stage, the sorting needs $O(n\log n)$ time, choosing the winners takes in $O(n)$, and the time complexity of the payment calculation of potential winners is $O(n\log n)$ in algorithm 2. Hence, the time complexity of the first stage is $O(K \cdot n\log n)$. For Algorithm 3, finding out the numth d_i^k takes in $O(n)$. Thus, the time of the second stage is $O(K \cdot n^2)$. To sum up, both two stages have polynomial-time complexity, and it is $O(K \cdot n^2)$, which proves the above theorem. ∎

5.5 | Approximation ratio

Theorem 6. *The proposed scheme is a $(1-\epsilon)$-approximation scheme.*

Proof. We relax the indicator variable constraint (1) temporarily and have $x_i^j(k) \in \{0, 1\}$. According to (6), (7), (8), and (9), we can obtain the optimal solution of social welfare SW_{opt} as:

$$SW_{opt} = \sum_{i=1}^{n}\sum_{j=i}^{n_i}\left(x_i^j(k)R_i^j - cs(k)\cdot s_i^j(k)\right), \tag{14}$$

where $s_i^j(k)$ is the amount of resource that miner U_i^j obtained from E_k with the optimal solution. The SW_{opt} is the total utility of both sellers, auctioneers and buyers when all resources of server are allocated. In our scheme, some user tasks cannot be executed by the edge server due to the resources constraints.

It should be noted that, the resource demands of buyers and the total resources that sellers owned should satisfy:

$$\sum_{k=1}^{K} RS_k \le \sum_{i=1}^{n}\sum_{j=i}^{n_i} r_i^j. \tag{15}$$

But due to the resource constraints, the number of resources being allocated cannot exceed the resources sellers provide. We have following constraint:

$$\sum_{i=1}^{n}\sum_{j=i}^{n_i} x_i^j(k) r_i^j \le \sum_{k=1}^{K} RS_k. \tag{16}$$

When a task matches successfully, the utility is

$$\Theta = x_i^j(k)R_i^j - x_i^j(k)r_i^j cs(k). \tag{17}$$

The $SW_{opt} = \sum_{i=1}^{n}\sum_{j=1}^{n_i}\sum_{k=1}^{K}\Theta + SW_{rest}$, where

$$SW_{rest} = \sum_{i=1}^{n}\sum_{j=i}^{n_i}\sum_{k=1}^{K}\left(s_i^j(k) - x_i^j(k)r_i^j\right)cs(k). \tag{18}$$

Then, putting (17) and (18) into (14) we obtain:

$$\begin{aligned} SW_{opt} &= \sum_{i=1}^{n}\sum_{j=i}^{n_i}\sum_{k=1}^{K}\left(\Theta + (s_i^j(k) - x_i^j(k)r_i^j)cs(k)\right) \\ &\le \sum_{k=1}^{K} RS_k \cdot cs(k) \\ &\quad + \sum_{i=1}^{n}\sum_{j=i}^{n_i}\sum_{k=1}^{K}\left(s_i^j(k) - x_i^j(k)r_i^j\right)cs(k) \\ &\le SW \cdot (1+\epsilon'), \end{aligned} \tag{19}$$

where $\epsilon' = (\sum_{i=1}^{n}\sum_{j=1}^{n_i}(\sum_{k=1}^{K}s_i^j(k) - x_i^j(k)r_i^j))/\sum_{k=1}^{K}RS_k$. According to (16), the relation of the $s_i^j(k)$, r_i^j and RS_k is

$$\sum_{i=1}^{n}\sum_{j=1}^{n_i}x_i^j(k)r_i^j \le \sum_{i=1}^{n}\sum_{j=1}^{n_i}\sum_{k=1}^{K}s_i^j(k) \le \sum_{k=1}^{K}RS_k. \tag{20}$$

According to (20), we can obtain that $\epsilon' \in [0, 1]$. Let $\epsilon'' = 1 + \epsilon'$ and $\epsilon = \frac{\epsilon'}{\epsilon''}$. We have

$$\begin{aligned} SW &\ge \left(1 - \frac{\epsilon'}{\epsilon''}\right) SW_{opt} \\ &= (1 - \epsilon)SW_{opt}. \end{aligned} \tag{21}$$

We can also obtain that $\epsilon \in [0, 1]$. According to definition 2, our scheme can achieve a $(1 - \epsilon)$ approximation ratio, and it is a $(1 - \epsilon)$-approximation scheme. ∎

6 | EXPERIMENTAL RESULTS

6.1 | Simulation setup

In this section, we conduct experiments to demonstrate the performance of our scheme on MATLAB R2016a. In the experiments, the number of miners follows the uniform distribution $U(600, 1200)$. The reward of the successful miners is composed of a flexible fee $\eta \cdot S_B$ and a fixed bonus ψ, where the fixed bonus $\psi = 25$ and the transaction fee rate η ranges from 0.002 to 0.008. We set the correlation constant $\xi = 1$ and the size of transaction S_B follows the uniform distribution $U(0, 1000)$. Since achievement of a new block follows a Poisson distribution as mentioned above, we try to change the difficulty of finding a new block by changing the value of λ, where λ ranges from 250 to 1750 with increment of 250, according to References 10 and 10.

In our simulation, for each edge server such as E_k, the assignable resources of E_k follows the normal distribution $N(25, 5)$ and $10 \le E_k \le 30$. The cost factor $cs(k)$ is of uniform distribution $U(0.75, 0.1)$ and $0.5 \le cs(k) \le 1$. Since we can get reserve price RP_k from (5). We generate small groups in terms of APs, and the number of miners in a_i is of uniform distribution $U(5, 30)$. Moreover, the resources demand r_i^j of each miner follows the normal distribution $N(2, 1)$ and $1 \le r_i^j \le 3$. Their bids for each edge server are following the uniform distribution $U(1, 15)$.

To better illustrate the performance of our auction scheme which is called TCMB, we apply the Brute Force (BF) algorithm, the heaviest access point first mechanism (HAF) in Reference 37, the Three-stage auction scheme for cloudlet deployment mechanism (TACD) in Reference 18, the two-stage auction for relay aided computation resource allocation (TARCO) in Reference 38 and the social welfare maximization auction for mobile blockchain (SWM) in Reference 28 to our mobile blockchain. We compare our scheme with other three mechanisms.

The HAF is an allocation mechanism based on greedy strategy without auction: they sort the total resource requirements of APs in descending order, and sort the assignable resources of edge server in descending order. They assign edge servers to APs according to the order, one by one. In other words, HAF matches the first edge server whose assignable resources is the biggest for the first AP whose resources demand is biggest, and matches the second edge server for the second AP et cetera. For TACD mechanism, its pricing strategy is that the payment of miner equals to its resources demand multiply by cost performance ratio which is the next miner of the last winner, that is, $p_i^j = r_i^j \cdot c_i^{j'}(k)$, where $c_i^{j'}(k)$ is the largest cost performance ratio except winners. TARCO is a two-stage auction resource allocation mechanism which divides mobile users into some groups, and introduces small cell user equipment as a group-leader in each group. Mobile users can be allowed to access the base station by relaying the computation data via group-leader relays. SWM aims to maximize the social welfare, and its rationale is based on the well-known Myerson's characterization. The social welfare in SWM is formulated as the difference between the sum of all miners' valuations and the edge server's total cost which means that SWM only focuses on maximizing the utility of miners. Hence, we did not obtain the utilities of other participants for SWM. BF is used to obtain the upper bound, and due to the limitation of computing power, BF will be illustrated by smaller settings.

6.2 | Simulation results

We first examine the impact of the number of miners on utility of TCMB, TACD, HAF, and TARCO. The utility of edge servers, APs, and miners are as shown in Figures 4, 5, and 6, respectively. We vary the number of miners from 600 to 1200, and set the number of edge servers equal to the number of APs, that is, $K = n$ in order to balance the market. The variable reward factor and constant rate related with Poisson distribution are fixed at $\eta = 0.006$, $\lambda = 800$ for better experimental results which are analyzed in the following experiment. It is shown both in three figures that the utility of edge servers increases with increasing number of miners. This happens due to the fact that the more mobile users take part in the mobile

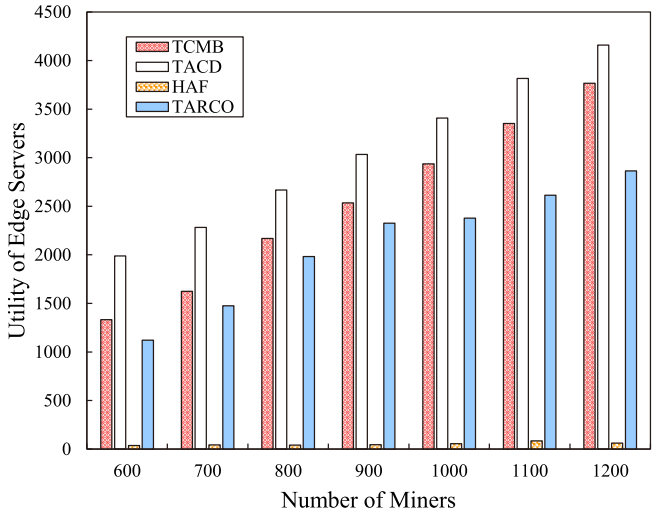

FIGURE 4 Utility of edge servers with the number of miners

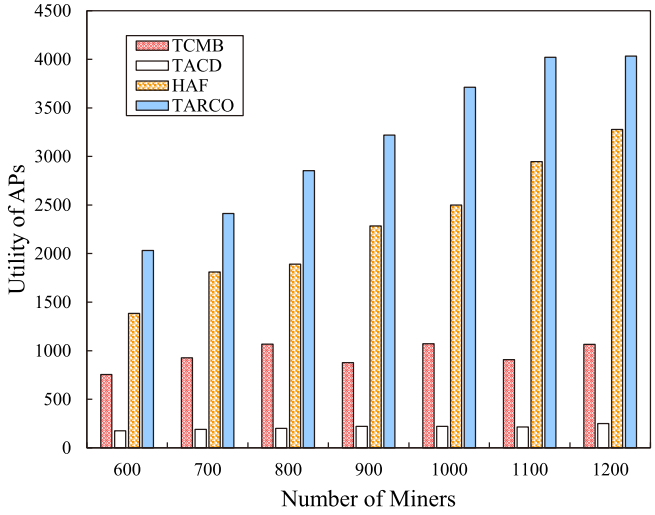

FIGURE 5 Utility of APs with the number of miners

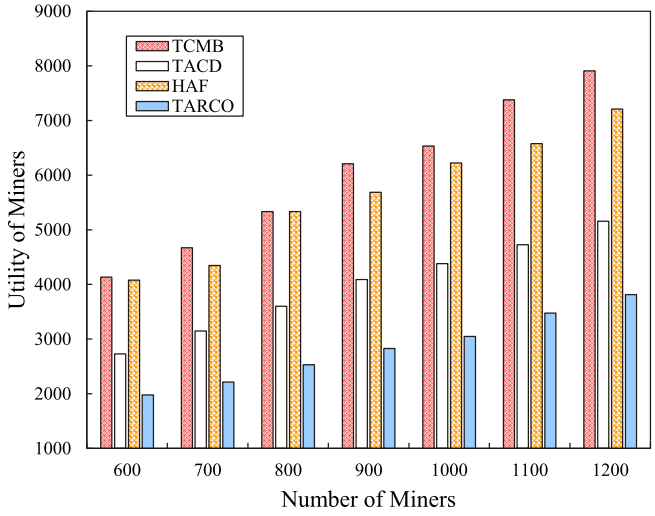

FIGURE 6 Utility of miners with the number of miners

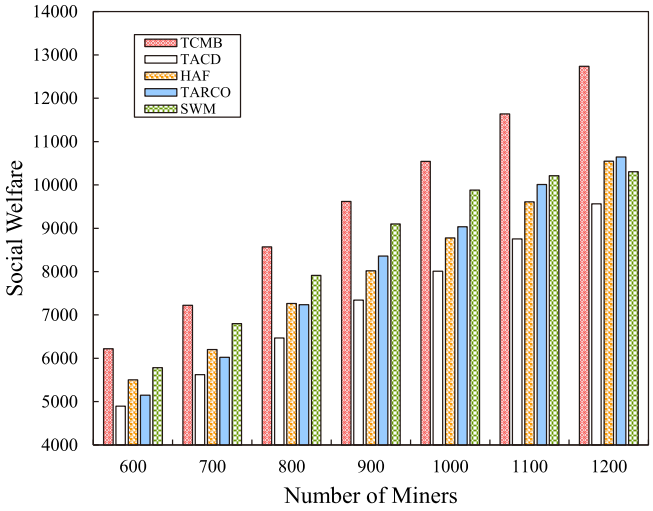

FIGURE 7 Social welfare with the number of miners

TABLE 3 Running time of each algorithm with number of miners

Number of miners	50	60	70	80	90	100
BF	25.2911 s	84.3574 s	191.2412 s	410.3641 s	1053.6625 s	2045.1765 s
TCMB	0.014241 s	0.013045 s	0.016968 s	0.021293 s	0.026172 s	0.031657 s
TACD	0.015948 s	0.015161 s	0.011502 s	0.014112 s	0.017538 s	0.020269 s
HAF	0.004435 s	0.004280 s	0.003939 s	0.003092 s	0.002769 s	0.004288 s
TARCO	0.776798 s	1.174561 s	2.093426 s	3.507182 s	5.761514 s	9.554813 s
SWM	0.012439 s	0.012895 s	0.014216 s	0.015415 s	0.018617 s	0.018645 s

blockchain, the more utility can be produced by blockchain network. Figure 4 shows the utility of edge servers that there is a difference between HAF mechanism and other schemes. The utility of proposed scheme is much higher than that in HAF, which is close to 0 in the HAF.

Figure 5 shows that our scheme is superior to TACD, while our scheme is lower than HAF and TARCO for utility of APs. This is because, our proposed scheme, we select the bid b_j^k as the payment instead of the largest bid b_i^k where $b_i^k \geq b_j^k \geq RP_k$ keeping the truthfulness of auction. However, HAF cannot satisfy the truthfulness, and after it finds the $b_i^k \geq RP_k$, HAF will selects RP_s as clearing price. As a result, the utility of edge servers in HAF is approximate equal to 0. Intuitively, TARCO obtains the highest utility of APs in Figure 5, it is because that the AP can obtain two incomes. One profit is made by offloading task and hosting the auction. Meanwhile, as a group-leader, AP can also be a miner to get reward in TARCO. Figure 6 shows that our scheme outperforms other mechanisms, and the utility of miners in TCMB is higher than others. Specifically, the introduction of the group-leader will increase the competition between APs and miners in TARCO, and the revenues of miners will decrease with the heighten of competition. Due to the payment algorithm, miners need to pay more for the same resources in TACD, and it can be observed that the utility of miners in TACD is lower than our scheme. Whereas, edge servers get more revenue when they sell the same resources, so the utility of edge servers is the highest as shown in Figure 4. Figure 7 shows the social welfare of our three-stage auction scheme is higher than SWM mechanism because SWM lacks consideration of the utilities of APs and edge servers, which only chooses to optimize the utility of miners instead of the total utility. On average, The social welfare in proposed scheme outperforms TACD, HAF, TARCO, and SWM by about 27.10%, 13.09%, 20.82%, and 7.58%, while the number of miners is 600. Moreover, when the number of miner is up to 1000, the social welfare achieves by our scheme are 33.78%, 21.84%, 19.69%, and 6.69% higher than that of TACD, HAF, TARCO, and SWM mechanisms, respectively.

For the simulations of BF, we assume that there are at most 100 miners allocated the resources. We investigate the upper bound of social welfare. The running time of five mechanisms are as shown in Table 3. We notice that with increasing number of miners, time cost by BF increase exponentially. It is much higher than running time of other mechanisms, and we cannot get the experimental results when the number of miners increases to a large extent.

Figure 8 demonstrates the relationships between BF and other four mechanisms on social welfare. There are almost the same trends that with the increasing number of miners, the social welfare grows accordingly. It is worth mentioning that BF is not agreed with the actual case and it cannot fully guarantee the economic properties, although it gets the best social welfare. The growth of the performance of BF mechanism is limited by

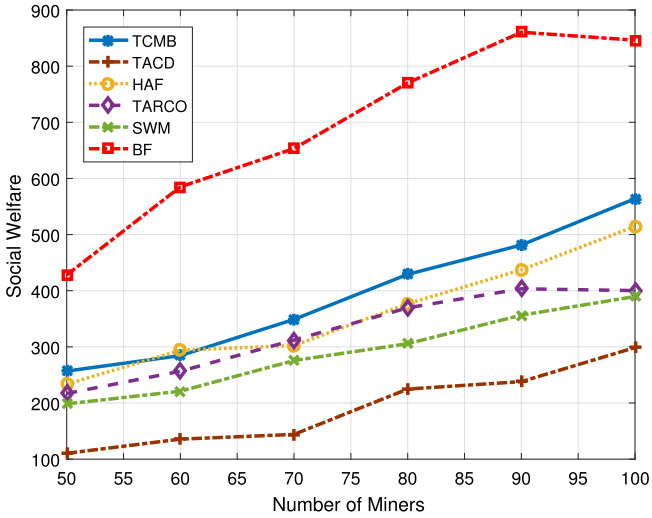

FIGURE 8 Upper bound of social welfare with the number of miners

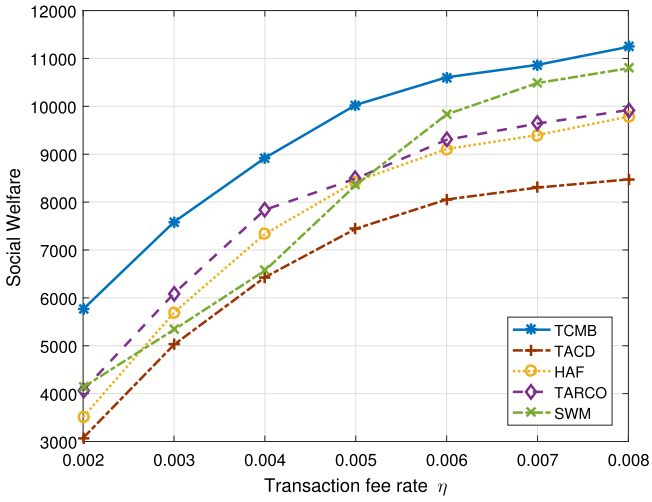

FIGURE 9 Impact of the transaction fee rate η on social welfare

the total assignable resources, when the number of miners increases to a certain amount. In conclusion, TCMB has the best performance in social welfare without the BF mechanism, and the BF achieves higher social welfare than that of our mechanism for about 50.08%, and about 183.33%, 64.49%, 111.46%, and 117.20% better than TACD, HAF, TARCO, and SWM, respectively. Moreover, TCMB outperforms TACD, HAF, TARCO, and SWM by 88.87%, 9.60%, 40.90%, and 44.72%, respectively.

We also investigate the impact of the transaction fee rate η. We fix the number of users, which is equal to 1000, and set that $\lambda = 800$. We vary the value of η from 0.002 to 0.008. As shown in Figure 9, all mechanisms can all generate large social welfare when blockchain owner increases the transaction fee rate. Because the valuation of miners increases with higher η, according to the definition in Equation (3). However, with the increasing of fee rate, the social welfare tends to be stable. Higher reward attracts more users to join which causes the competition in blockchain network increasing as the number of miners. We can also see that our mechanism is better than HAF, TACD, and TARCO in the whole process. In terms of the social welfare, TCMB outperforms TACD, HAF, TARCO, and SWM by about 34.74%, 18.97%, 18.12%, and 20.05% at $\eta = 0.005$, respectively.

In Figure 10, we set that $\eta = 0.006$, and fix the number of users to 1000, to observe the impact of the average time λ on the social welfare. We vary the value of λ from 250 to 1750. We obtain that the social welfare increases as the block time of mining a new block increases. Note that when the difficulty is low, the short broadcasting time will reduces the success rate of propagation for miners who have solved the PoW puzzle. If the difficulty λ becomes high, the success rate of propagation will be increased, and social welfare will increase. We also obtain that the increment of social welfare decreases. This is because the λ has less impact for the valuation of miners that can be seen from Equations (A2) and (3). Moreover, the social welfare of our mechanism is 30.36%, 8.59%, 6.60%, and 3.67% better than TACD, HAF, TARCO, and SWM at $\lambda = 1000$, respectively.

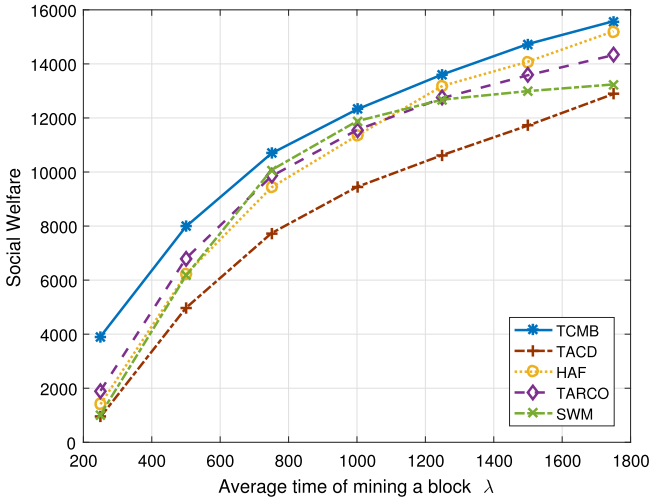

FIGURE 10 Impact of the block time λ on social welfare

7 | CONCLUSION

In this article, we have proposed a mobile blockchain model with edge computing. We have investigated the computation offloading decision and resources allocation strategy in mobile blockchian, which is formulated as a social welfare maximization problem. Three-stage auction scheme based on the group-buying mechanism has been designed to allocate resources which can ensure the benefits of participants. First, we have selected some miners to be potential winners for each edge server in each group. Then, AP represents a group that has been matched with edge server. Finally, miners offload the mining tasks to the corresponding edge servers for receiving expected reward. We have proved that our scheme is truthful, individual rational, budget balance and computational efficient. We have proved that the approximation ratio of proposed scheme is $(1-\epsilon)$. We have compared our proposed scheme with TACD, HAF, and TARCO. Extensive simulation results show that our scheme is 33.78%, 21.84%, 19.69%, and 6.69% higher than that of TACD, HAF, TARCO, and SWM mechanisms in terms of social welfare, respectively, when the number of miners is 1000. For the future work, A dynamic and high speed user movement network environment will be considered, and new on-line resource allocation algorithms will be designed for more efficient and practical blockchain system to adapt complicated communication environment.

ACKNOWLEDGMENT

Part of the works has been presented in 24th International Conference on Parallel and Distributed Systems (ICPADS 2018).[39] This work was supported by the National Natural Science Foundation of China under Grant Nos. 62106052 and 62072118, Guangdong Basic and Applied Basic Research Foundation under Grant No. 2021B1515120010, Guangdong Science and Technology Planning Project under Grant 2016A020210122.

CONFLICT OF INTERESTS

The authors declare no conflict of interests.

DATA AVAILABILITY STATEMENT

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request. The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Chengpeng Xia https://orcid.org/0000-0002-9520-0229

REFERENCES

1. Bitcoin NS. A peer-to-peer electronic cash system. *Consulted*. 2008;1(4):1-9. https://bitcoin.org/bitcoin.pdf
2. Tapscott D, Tapscott A. *Blockchain Revolution: how the Technology behind Bitcoin is Changing Money, Business, and the World*. Penguin; 2016.
3. Saad M, Spaulding J, Njilla L, et al. Exploring the attack surface of blockchain: a comprehensive survey. *IEEE Commun Surv Tutorials*. 2020;22(3):1977-2008.
4. Wang H, Ma S, Dai HN, Imran M, Wang T. Blockchain-based data privacy management with nudge theory in open banking. *Future Gener Comput Syst*. 2020;110:812-823.
5. Rathee G, Ahmad F, Kurugollu F, Azad MA, Iqbal R, Imran M. CRT-BIoV: a cognitive radio technique for blockchain-enabled internet of vehicles. *IEEE Trans Intell Trans Syst*. 2020;22(7):4005-4015.
6. Blockchain for enterprise applications. *Tractica*. 2018; https://www.tractica.com/research/blockchain-for-enterpriseapplications/.

7. Kiayias A, Koutsoupias E, Kyropoulou M, Tselekounis Y. Blockchain mining games. *ACM Conference on Economics and Computation*. ACM; 2016:365-382.
8. Tewari A, Gupta B. Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *J Supercomput*. 2017;73(3):1085-1102.
9. Mohan AP, Gladston A, Mohamed Asfak R. Merkle tree and Blockchain-based cloud data auditing. *Int J Cloud Appl Comput*. 2020;10(3):54-66.
10. Suankaewmanee K, Hoang DT, Niyato D, Sawadsitang S, Wang P, Han Z. Performance analysis and application of mobile blockchain. *IEEE International Conference on Computing, Networking and Communications*. IEEE; 2018:642-646.
11. Xu C, Lei J, Li W, Fu X. Efficient multi-user computation offloading for Mobile-edge cloud computing. *IEEE/ACM Trans Network*. 2016; 24(5):2795-2808.
12. Ma L, Wu J, Dota CL. Delay bounded optimal cloudlet deployment and user association in wmans. *17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. IEEE; 2017:196-203.
13. Andreev S, Galinina O, Pyattaev A, et al. Exploring synergy between communications, caching, and computing in 5G-grade deployments. *IEEE Commun Mag*. 2016;54(8):60-69.
14. Zhou S, Jadoon W, Shuja J. Machine learning-based offloading strategy for lightweight user mobile edge computing tasks. *Complexity*. 2021;2021:1-11.
15. Jehangiri AI, Maqsood T, Ahmad Z, et al. Mobility-aware computational offloading in mobile edge networks: a survey. *Cluster Comput*. 2021;24(4):2735-2756.
16. Menezes FM, Monteiro PK. *An Introduction to Auction Theory*. Oxford University Press; 2005.
17. Han Z, Niyato D, Saad W, Başar T, Hjørungnes A. Game theory in wireless and communication networks. *Theory, Models, and Applications*. Cambridge University Press; 2012.
18. Zhou G, Wu J, Chen L. Tacd: a three-stage auction scheme for cloudlet deployment in wireless access network. *International Conference on Wireless Algorithms, Systems, and Applications*. Springer; 2017:877-882.
19. Li X, Zeng F, Fang G, Huang Y, Tao X. Load balancing edge server placement method with QoS requirements in wireless metropolitan area networks. *IET Commun*. 2021;14(21):3907-3916.
20. Babaioff M, Dobzinski S, Oren S, Zohar A. On Bitcoin and red balloons. *ACM Sigecom Exch*. 2011;10(3):5-9.
21. Decker C, Wattenhofer R. Information propagation in the Bitcoin network. *IEEE Thirteenth International Conference on Peer-To-Peer Computing*. IEEE; 2013:1-10.
22. Houy N. The Bitcoin mining game. *Working Papers*. 2014;1-19. Available from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407834
23. Kraft D. Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Netw Appl*. 2016;9(2):397-413.
24. Ouaguid A, Abghour N, Ouzzif M. A novel security framework for managing android permissions using blockchain technology. *Int J Cloud Appl Comput*. 2018;8(1):55-79.
25. Xiong Z, Feng S, Wang W, Niyato D, Wang P, Han Z. Cloud/fog computing resource management and pricing for blockchain networks. *IEEE Internet Things J*. 2018;6(3):4585-4600.
26. Wang X, Chen X, Wu W. Towards truthful auction mechanisms for task assignment in mobile device clouds. *IEEE International Conference on Computer Communications*. IEEE; 2017:1-9.
27. Jehangiri AI, Maqsood T, Umar AI, et al. LiMPO: lightweight mobility prediction and offloading framework using machine learning for mobile edge computing. *Cluster Comput*. 2022;1-19.
28. Jiao Y, Wang P, Niyato D, Xiong Z. Social welfare maximization auction in edge computing resource allocation for mobile blockchain. *IEEE International Conference on Communications*. IEEE; 2018:1-6.
29. Luong NC, Xiong Z, Wang P, Niyato D. Optimal auction for edge computing resource management in mobile blockchain networks: a deep learning approach. *2018 IEEE International Conference on Communications*. IEEE; 2018:1-6.
30. Andresen G. Back-of-the-envelope calculations for marginal cost of transactions 2013. https://gist.github.com/gavinandresen/5044482.
31. Kang X, Sun S. Incentive mechanism design for mobile data offloading in heterogeneous networks. *IEEE International Conference on Communications*. IEEE; 2015:7731-7736.
32. Zhaofeng M, Jialin M, Jihui W, Zhiguang S. Blockchain-based decentralized authentication modeling scheme in edge and IoT environment. *IEEE Internet Things J*. 2020;8(4):2116-2123.
33. Goldberg AV, Hartline JD. Competitive auctions for multiple digital goods. *European Symposium on Algorithms Springer*; 2001:416-427.
34. Nisan N, Roughgarden T, Tardos E, Vazirani VV. *Algorithmic Game Theory*. Cambridge University Press; 2007.
35. Williamson DP, Shmoys DB. *The Design of Approximation Algorithms*. Cambridge university press; 2011.
36. Krishna V. *Auction theory*. Academic press. 2009.
37. Jia M, Cao J, Liang W. Optimal cloudlet placement and user to cloudlet allocation in wireless metropolitan area networks. *IEEE Trans Cloud Comput*. 2017;4:725-737.
38. Chen L, Wu J, Zhang X, Zhou G. TARCO: two-stage auction for D2D relay aided computation resource allocation in Hetnet. *IEEE Trans Services Comput*. 2018;14(1):1-14.
39. Xia C, Chen H, Liu X, Wu J, Chen L. Efficient three-stage resource allocation auction for Mobile Blockchain in edge computing. *24th International Conference on Parallel and Distributed Systems*. IEEE; 2018:701-705.
40. Chekuri C, Khanna S. A PTAS for the multiple knapsack problem. *SIAM J Comput*. 2005;35:713-728.

How to cite this article: Xia C, Wu Y, Chen L, Chen Y, Wu J. Three-stage auction scheme for computation offloading on mobile blockchain with edge computing. *Concurrency Computat Pract Exper*. 2022;34(25):e7253. doi: 10.1002/cpe.7253

APPENDIX A. PROBLEM FORMULATION FOR EXPECTED REWARD OF MINER

In the process of mining, the new block occurrence can be modeled as a process which follows a Poisson distribution with a constant rate λ[23] which is also known as the average block time. The new block will be broadcast in blockchain network once a miner has solved the PoW puzzle. However, if the block is overtaken by other block at the time of propagation, it will be orphaned, and the orphaning probability can be approximately defined as,

$$\mathcal{P}_{orphan}(\tau) = 1 - e^{-\frac{1}{\lambda}\tau}, \tag{A1}$$

where τ is the block propagation time. Without loss of generality, S_B is used to denote the block size and η is a constant that reflects the liner relationship between time and block size, that is, $\tau = \eta \cdot S_B$. It should be noted that the larger block size is, the more difficult it takes to reach consensus in the propagation process. Block size depends on the number of transactions in block. The first miner will receive mining reward who solves the PoW with a correct nonce value and reach consensus instead of orphaned. According to (2) and (A1), the probability of miner receiving reward can be defined as,

$$\begin{aligned} P(\xi_i^j, S_B) &= \xi_i^j(1 - \mathcal{P}_{orphan}(\tau)) \\ &= \xi_i^j e^{-\frac{1}{\lambda}\eta S_B}. \end{aligned} \tag{A2}$$

There are two parts of reward for miner, which are a variable bonus $\zeta \cdot S_B$ and a fixed reward ψ. Hence, the expected reward can be defined as,

$$\begin{aligned} R_i^j &= (\psi + \zeta \cdot S_B) \cdot P(\xi_i^j, S_B) \\ &= (\psi + \zeta \cdot S_B) \cdot \xi_i^j e^{-\frac{1}{\lambda}\eta S_B}. \end{aligned} \tag{A3}$$

APPENDIX B. NP-HARDNESS PROOF OF THE SOCIAL WELFARE MAXIMIZATION PROBLEM

In proposed three-stage auction mobile blockchain system, the APs need to determine the winning miners, and match the edge servers with miners. Such winner determination problem can be formulated as,

$$\begin{aligned} &\max \sum_{k=1}^{K}\sum_{i=1}^{n}\sum_{j=1}^{n_i} x_i^j(k) b_i^j(k), \\ &s.t. \sum_{j=1}^{n_i} x_i^j(k) r_i^j \le RS_k, \quad \forall A_i \in a, \quad \forall E_k \in E, \\ &\sum_{k=1}^{K} x_i^j(k) = 1, \quad \forall U_i^j \in \mathbb{U}. \end{aligned} \tag{B1}$$

In our auction scheme, the resource demand of each miner is different. As such, the winners determination problem defined in (B) is NP-hard in terms of the polynomial-time reduction from Multiple Knapsack problem.[40] Hence, it is considerably challenging to design a mechanism for determining the winners.