URIM: Utility-Oriented Role-Centric Incentive Mechanism Design for Blockchain-Based Crowdsensing

Zheng Xu[1,2,3], Chaofan Liu[1,2,3], Peng Zhang[1,2,3(✉)], Tun Lu[1,2,3(✉)], and Ning Gu[1,2,3]

[1] School of Computer Science, Fudan University, Shanghai, China
{zxu17,cfliu18,zhangpeng_,lutun,ninggu}@fudan.edu.cn
[2] Shanghai Key Laboratory of Data Science, Fudan University, Shanghai, China
[3] Shanghai Institute of Intelligent Electronics and Systems, Shanghai, China

Abstract. Crowdsensing is a prominent paradigm that collects data by outsourcing to individuals with sensing devices. However, most existing crowdsensing systems are based on centralized architecture which suffers from poor data quality, high service charge, single point of failure, etc. Some studies have explored decentralized architectures and implementations for crowdsensing based on blockchain, while incentive mechanisms for worker participation and miner participation, which serve as a crucial role in blockchain-based crowdsensing systems (BCSs), are ignored. To address this issue, we propose an incentive mechanism design named URIM to maximize participants' utilities, which consists of worker-centric and miner-centric incentive mechanisms for BCSs. For the worker-centric incentive mechanism, we model it as a reverse auction, in which dynamic programming is utilized to select workers, and payments are determined based on the Vickrey-Clarke-Groves scheme. We also prove this incentive mechanism is computationally efficient, individually rational and truthful. For the miner-centric incentive mechanism, we model interactions among the requester and miners as a Stackelberg game and adopt the backward induction to analyze its equilibrium at which the utilities of the requester and miners are optimized. Finally, we demonstrate the significant performance of URIM through extensive simulations.

Keywords: Crowdsensing · Blockchain · Incentive mechanism · Reverse auction · Game theory

1 Introduction

In recent years, sensing devices (such as smartphones, wearable devices and tablets) have been emerging in our daily life. The proliferation of devices capable of sensing and computing leads to the prosperity of a new sensing paradigm called crowdsensing. Crowdsensing leverages "humans-as-sensors" to enable traditional Internet of Things (IoT) application by combing perception capabilities

C. S. Jensen et al. (Eds.): DASFAA 2021, LNCS 12683, pp. 358–374, 2021.
https://doi.org/10.1007/978-3-030-73200-4_25

and crowdsourcing in many important fields, such as intelligent transportation, public safety, environmental monitoring and urban public management.

In the previous studies, most research on crowdsensing adopted centralized system architecture which generally consists of three roles: centralized platform, task requesters, and crowdsensing workers (also known as the data providers) [10]. However, there exists some drawbacks in the centralized crowdsensing systems, such as poor data quality, high service charge, single point of failure and privacy disclosure [13]. Therefore, some studies have explored decentralized techniques for crowdsensing systems, wherein a very popular solution is blockchain. Blockchain-based crowdsensing systems (BCSs) have following advantages. The decentralization, immutability and security of blockchain can facilitate the cooperation among mutually distrusted participants without service fees charged by the centralized platform and ensure the audibility of the crowdsensing data. Moreover, the decentralized blockchain architecture can avoid the single point of failure which may cause shutdown of traditional centralized systems. The anonymity of blockchain transactions can reduce risks of privacy disclosure.

Existing studies of BCSs mainly focus on architecture design and smart contracts implementation, while the incentive mechanisms for user engagement, which serve as a crucial role in crowdsensing systems, are ignored. Nowadays, most incentive mechanisms are designed for traditional centralized crowdsensing systems [15,19]. However, BCSs operate automatically via smart contracts without a centralized reliable intermediary. Thus, the incentive mechanism of BCSs is designed to optimize the utilities of participants when interacting with the blockchain, rather than the centralized platform. Although there are some studies on the incentive mechanisms for BCSs, they mainly focus on selection and reward allocation for workers [2,3,9]. They omit an exclusive and important role called miner in BCSs to handle and validate all operations. Existing incentive mechanisms generally involve the task requesters and workers, but ignore miners. Hence, existing incentive mechanisms are not fully compatible with BCSs. Due to the lack of appropriate incentive mechanisms, the utilities of participants cannot be maximized, and the efficiency of BCSs decreases.

There is an urgent need to design appropriate incentive mechanisms for BCSs, but it is a challenging task. First, BCSs allow participants to exchange data without a centralized truthful intermediary. It is crucial and challenging to build a system model of BCSs that can be compatible with holistic incentive mechanism design. Second, it is difficult to formalize how multiple roles interact with each other and how to optimize their utilities. Compared with traditional crowdsensing systems, a new role called miner is involved in BCSs. Miners directly determine the operating efficiency and security of BCSs, while how to select efficient miners in a safe and reliable way is not easy. Meanwhile, there are complex interactions between workers, miners and requesters, which aggravate the complexity of utility optimization in the incentive mechanism design.

Based on the above background, we focus on: *How to design holistic incentive mechanisms for BCSs to maximize utilities of participating roles?* To solve this problem, we propose a utility-oriented role-centric incentive mechanism design

named URIM which aims to maximize utilities of participating roles in BCSs. According to the processes and participants of BCSs, workers and miners directly determines the performance of BCSs. Hence, URIM is designed to consist of worker-centric and miner-centric incentive mechanisms. In the worker-centric incentive mechanism (WCIM), the task requester publishes its task to BCSs through smart contracts. Then each worker submits its solution of the task and corresponding bidding price. Smart contracts on BCSs automatically selects workers by a dynamic programming algorithm and determines their payments by Vickrey-Clarke-Groves (VCG) scheme. The above interactions among the task requester, workers and smart contracts are modeled as a reverse auction. In the miner-centric incentive mechanism (MCIM), we first adopt cryptographic sortition to select eligible miners. For motivating miners to validate transactions and mine blocks, the task requester announces total transaction fees shared by all transactions related with its task. Then miners decide their mining strategies to validate different number of transactions and compete for the corresponding transaction fee. The above interactions among the task requester and miners are modeled as a Stackelberg game to optimize utilities of the task requester and miners. The main contributions of this paper are as follows:

- We propose a utility-oriented role-centric incentive mechanism design named URIM for BCSs. To the best of our knowledge, this is the first work on holistic incentive mechanism design for BCSs to ensure the utility maximization of all roles.
- We design a reverse auction based WCIM which adopts dynamic programming to select desirable workers and determine payments based on VCG scheme. We theoretically prove that WCIM is computationally efficient, individually rational and truthful.
- We design the MCIM that selects miners by cryptographic sortition and formulates mining competition by a two-stage Stackelberg game. Through backward induction, we analyze and validate the best response strategies of miners and the unique Stackelberg equilibrium where the utilities of the requester and miners are jointly maximized.
- We demonstrate the significant performance of URIM through extensive simulations.

The remainder of the paper is organized as follows. In Sect. 2, we review the related work of blockchain-based crowdsensing systems and incentive mechanisms for crowdsensing. In Sect. 3, we present the system model of BCSs with the design of URIM. We then present two compositions of URIM in Sect. 4 and 5. We present performance evaluations in Sect. 6. Finally, we conclude this paper in Sect. 7.

2 Related Work

In this section, we mainly review related research on the blockchain-based crowdsensing systems and incentive mechanisms for crowdsensing.

Blockchain-Based Crowdsensing Systems. Blockchain and automated execution of smart contracts greatly enhance the decentralized communication and cooperation without an intermediary in many fields [5]. In particular, the crowdsensing system can take the benefits of blockchain to achieve fair and trust-less collaboration. Crowdbc [13] proposes a decentralized crowdsensing framework based on blockchain and implements the main concepts in the framework through the usage of smart contracts. Zebralancer [14] shows how an anonymous decentralized crowdsensing system can be implemented on top of blockchain, which ensure the privacy of the crowdsensing data while preserves the transparency of blockchain systems. In [2], authors build a decentralized crowdsensing platform for data trading on blockchain. The research of homomorphic encryption for fair and secure BCSs is discussed in [21]. Zero-knowledge proof technique is proposed to enable data providers to submit data through a privacy preserving and secure way in BCSs [6]. The location privacy attack in the crowdsensing system is discussed in [20]. This work proposes a blockchain-based privacy preservation framework for protecting location of workers. These efforts are mainly aimed at how to implement crowdsensing on the blockchain.

Incentive Mechanism for Crowdsensing. The existing incentive mechanisms for crowdsensing systems can be divided into monetary and non-monetary incentive mechanisms. In monetary incentive mechanisms, auction is a common approach to pay workers with either real money or virtual tokens [7,11]. The radp-vpc mechanism is proposed in [12], which aims to minimize the platform cost and maintain the participation level of workers. Yang *et al.* propose a reverse auction based incentive mechanism to determine winners and their payments [19]. Some studies have attempted to provide monetary incentive mechanisms based on BCSs. An *et al.* propose a blockchain-based crowdsensing data trading system with truthful and confidential incentive mechanisms in [2]. Truthful and cost-optimal incentives for mobile user participation are designed in [3]. Hu *et al.* design the workflow of BCSs with the help of automatic smart contracts and they leverage a three stage Stackelberg game to motivate participants in [9]. The above works [2,3,9] only consider the participation of workers, but they ignore the mining competition and consensus achievement. Non-monetary incentive mechanisms provide comprehensive and long-term incentives for participants. In [1], a reputation management framework is proposed to evaluate both the contributions quality and the trust level of participants. Crowdsensing data trustworthiness are quantified based on statistical and vote-based reputation scores in [17].

3 System Overview

In this section, we present the system model of BCSs with the holistic incentive mechanism design. As shown in Fig. 1, there generally exists three roles participating in BCSs: the task requester, workers and miners. The task requester and workers can also be regarded as miners when they join in the mining competition.

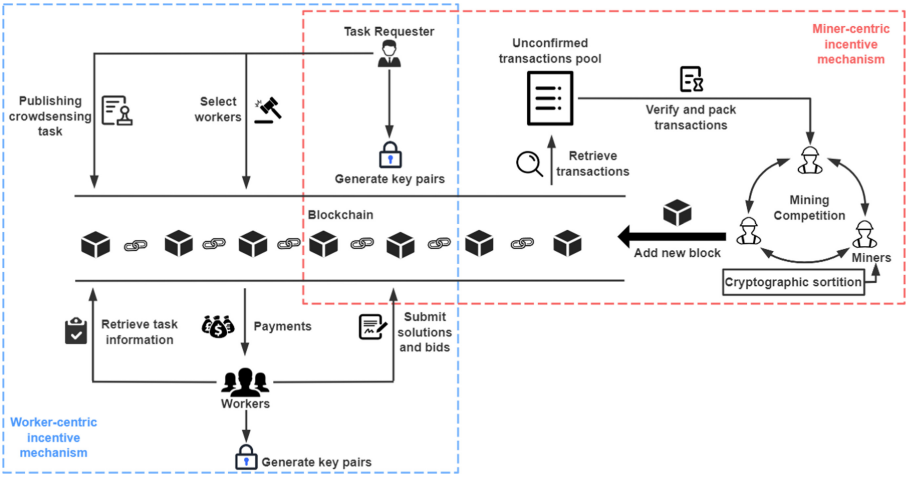

Fig. 1. System model of blockchain-based crowdsensing.

1. **Task requester.** Let R be the task requester (hereinafter referred to as requester), and R publishes crowdsensing task ST to the BCS. ST defines the sensing requirement including the task budget B, task duration and description of target data. To motivate workers to enhance the quality of sensing information, and miners to validate transactions related with ST, a certain amount of compensation will be paid to workers and miners respectively.
2. **Worker.** Let $W = \{w_1, w_2, \cdots, w_m\}$ be the set of all workers. Worker w_i should submit its solution SL_i and bidding price b_i before the task ending time if w_i is interested in task ST.
3. **Miner.** The responsibility of miners is to secure the blockchain network and to deal with every transaction in it. Each miner validate transactions in its block to compete for the mining reward which includes a specific block reward and fees sent with validated transactions. Miners are selected from those requesters and workers by a specific selection manner.

In Fig. 1, the workflow of BCSs with utility-oriented role-centric incentive mechanism contains five stages as follows:

1. **Participants register.** In the beginning, the requester and workers join in this system. Each registered participant has a unique public/private key pair to secure its transactions.
2. **Publish crowdsensing task.** In this stage, the requester publishes the crowdsensing task to BCSs via smart contracts.
3. **Submit crowdsensing information.** Workers can retrieve crowdsensing tasks they are interested in by interacting with blockchain. Workers submit crowdsensing solutions and bidding prices before the task deadline.
4. **Select workers and determine payments.** After receiving crowdsensing solutions, BCSs automatically select desirable workers and determine their payments via smart contracts.

5. **Select miners and generate blocks.** Based on participants' computing power, cryptographic sortition is adopted to randomly and unpredictably select miners. Selected miners pack bundled transactions into a block, then compete for mining rewards with proof of work (PoW) consensus.

The goal of incentive mechanism design for BCSs is to motivate participants and maximize their utilities. Other issues in the design and implementation of smart contracts in BCSs is out of the scope of our paper. People can refer to [2,13,21] for these issues. Both workers and miners play an important role in determining the performance of BCSs, so we need to design incentive mechanisms for them. In Stage 4, we propose a worker-centric incentive mechanism, in which eligible workers are paid a reasonable return according to their contribution and bidding price. In Stage 5, we propose a miner-centric incentive mechanism, in which miners compete with each other for a total transaction fee.

4 Worker-Centric Incentive Mechanism

In this section, we propose a reverse-auction-based worker-centric incentive mechanism named WCIM to select workers by dynamic programming, and determine their payments through VCG scheme.

After the requester R posts the task ST on BCSs, reverse-auction-based WCIM will output a subset of workers $S \in W$ as winners and determine the payment for each winner $w_i \in S$ by taking workers' contribution v_i and bidding price b_i as input. These processes are performed automatically on smart contracts. The sum of all winners' contributions is represented as $\sum_{w_i \in S} v_i$. The utility of R is the difference between winners' contributions and their social costs, which is represented as $\sum_{w_i \in S} (v_i - b_i)$. WCIM aims to maximize the utility of R while satisfying the budget control. Hence, WCIM can be formulated as follows:

$$Maximize \sum_{w_i \in S} (v_i - b_i), \quad Subject\ to \sum_{w_i \in S} b_i \leq B. \tag{1}$$

The WCIM is designed to satisfy properties as follows:

- **Computational Efficiency.** The incentive mechanism is computationally efficient if its computation runs in polynomial time.
- **Individual Rationality.** The incentive mechanism is individually rational if each worker has non-negative utility.
- **Truthfulness.** The incentive mechanism is truthful if no worker could obtain higher utility by reporting a false bid that deviates from its true cost no matter what others report.

4.1 Implementation of WCIM

From the above, WCIM consists of workers selection and payment determination.

Wokrers Selection. We reduce the workers selection to 0–1 Knapsack problem which is constructed as follows and use dynamic programming for the optimal solution in Algorithm 1.

Workers are denoted by set $W = \{w_1, \cdots, w_m\}$. Workers' bidding prices and contributions are denoted by $\{b_1, \cdots, b_m\}$ and $\{v_1, \cdots, v_m\}$. We map workers' bidding set $\{b_1, \cdots, b_m\}$ to a non-negative integer set $\{\beta b_1, \cdots, \beta b_m\}$ by multiplying each bidding price with amplification factor β. Meanwhile, we use $x_i \in \{0, 1\}$, $i \in \{1, \cdots, m\}$ to represent if worker w_i will be selected. The workers selection problem is constructed to determine $X = \{x_1, \cdots, x_m\}$ to

$$Maximize \sum_{i=1}^{m} (v_i - b_i) \cdot x_i, \quad Subject\ to \sum_{i=1}^{m} \beta b_i x_i \leq \beta B. \tag{2}$$

Payment Determination. We propose a VCG [18] based payment determination algorithm illustrated in Algorithm 2. In the generalized VCG auction, each winner is required to pay "harm" imposed on other workers, i.e., the difference between the optimal utility of the requester with and without this winner [18]. We define $V(S)_W^{-w_i}$ as the optimal utility of R excluding the contribution of worker w_i, which can be represented as

$$V(S)_W^{-w_i} = V(S)_W - (v_i - b_i). \tag{3}$$

Then, we define $V(S)_{W \setminus \{w_i\}}$ as the optimal utility of R excluding the participation of worker w_i. Thus, the payment p_i of worker w_i can be represented as

$$p_i = v_i - \left(V(S)_{W \setminus \{w_i\}} - V(S)_W^{-w_i}\right). \tag{4}$$

4.2 Theoretical Analysis of WCIM Properties

In this subsection, we prove that WCIM satisfies mentioned three properties: computational efficiency (Lemma 1), the individual rationality (Lemma 2) and the truthfulness (Lemma 3).

Lemma 1. *WCIM is computationally efficient.*

Proof. The winners selection has been reduced to 0–1 Knapsack problem, as illustrated in Algorithm 1 and it takes $O(n\beta B)$ time. The payment determination illustrated in Algorithm 2 takes $O(mn\beta B)$ time. WCIM is executed by Algorithm 1 and 2 sequentially and its running time is the sum of them. Hence, WCIM is a polynomial-time mechanism and computationally efficient. □

Lemma 2. *WCIM is individually rational.*

Proof. Based on (4), we have

$$\begin{aligned} p_i = v_i - \left(V(S)_{W \setminus \{m_i\}} - V(S)_W^{-m_i}\right) &= v_i - \left(V(S)_{W \setminus \{m_i\}} - V(S)_W + v_i - b_i\right) \\ &= V(S)_W - V(S)_{W \setminus \{m_i\}} + b_i. \end{aligned} \tag{5}$$

Algorithm 1. The Winners Selection Algorithm

Input: The worker set $\{w_1, w_2, \cdots, w_m\}$, their bid set $\{b_1, b_2, \cdots, b_m\}$, their contribution set $\{v_1, v_2, \cdots, v_m\}$ and the budget B, the amplification factor β;
Output: The selected worker set S;

$S \leftarrow \oslash$, $H[i,j] \leftarrow 0$;
for i from 1 to m **do**
  for j from 0 to βB **do**
    if $\beta b_i \leq j$ && $H[i-1, j-\beta b_i] + (v_i - b_i) > H[i-1, j]$ **then**
      $H[i,j] \leftarrow H[i-1, j-\beta b_i] + (v_i - b_i)$;
      $X[i,j] \leftarrow 1$;
    else
      $H[i,j] \leftarrow H[i-1, j]$;
      $X[i,j] \leftarrow 0$;
    end if
  end for
end for
$V \leftarrow H[m, \beta B]$;
$B' \leftarrow 0$;
for j from βB downto 0 **do**
  if $H[m,j] == V$ **then**
    $B' \leftarrow j/\beta$;
  end if
end for
for i from m downto 0 **do**
  if $X[i, \beta B'] == 1$ **then**
    $S \leftarrow S \cup \{w_i\}$;
    $B' = B' - b_i$;
  end if
end for
return S;

Since S is the winner set, it is easy to find $V(S)_W \geq V(S)_{W \setminus \{m_i\}}$, and thus $p_i \geq b_i$. Hence, WCIM is individually rational. □

Lemma 3. *WCIM is truthful.*

Proof. If w_i reports a truthful bidding price, its utility can be represented as follows:

$$\begin{aligned} U(w_i) = p_i - b_i &= V(S)_W - V(S)_{W \setminus \{w_i\}} + b_i - b_i \\ &= V(S)_W - V(S)_{W \setminus \{w_i\}}. \end{aligned} \tag{6}$$

In (6), w_i is unable to influence the value of $V(S)_{W \setminus \{w_i\}}$. After reporting the untruthful bidding price $b_i^{'}$ from the truthful bidding price b_i, the utility of w_i is changed as follows:

$$\begin{aligned} \Delta U(w_i) = U\left(w_i^{'}\right) - U(w_i) &= V(S)_{W'} - V(S)_{W' \setminus \{w_i\}} - \left(V(S)_W - V(S)_{W \setminus \{w_i\}}\right) \\ &= V(S)_{W'} - V(S)_W \end{aligned} \tag{7}$$

From Lemma 2, we can obtain $V(S)_{W'} \leq V(S)_W$, and then $\Delta U(w_i) \leq 0$. Thus, the worker w_i cannot get higher utility by reporting an untruthful bidding price. Hence, WCIM is truthful. □

Algorithm 2. The Payment Determination Algorithm

Input: Winner set $S = \{w_1, w_2, \cdots, w_m\}$, their bid set $\{b_1, b_2, \cdots, b_m\}$ and contribution set $\{v_1, v_2, \cdots, v_m\}$;
Output: The winner payment set P;

$P \leftarrow \oslash$;
for j from 1 to m **do**
  $V(S)_S^{-w_i} = V(S)_S - (v_i - b_i)$
  Calculate $V(S)_{S\setminus\{w_i\}}$ according to Algorithm 1
  $p_i = v_i - \left(V(S)_{S\setminus\{w_i\}} - V(S)_S^{-w_i}\right)$
  $P \leftarrow P \cup \{p_i\}$
end for
return P;

5 Miner-Centric Incentive Mechanism

In this section, we model the miner-centric incentive mechanism as a Stackelberg game to decide how to optimize the utility of the requester and miners.

5.1 Blockchain Mining with Crowdsensing

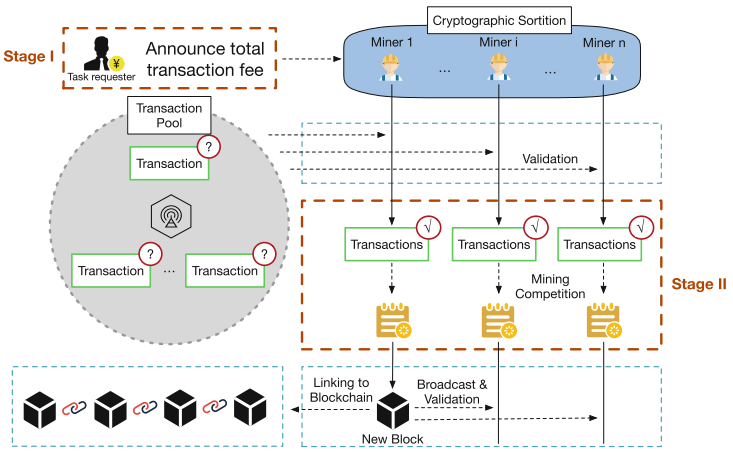

Fig. 2. Mining competition

As shown in Fig. 2, the block mining competition includes 5 steps that are, in order, miners selection, transaction fee announcement, transaction validation, block mining and block validation. In the beginning, eligible miners are selected by cryptographic sortition according to their computing power. Cryptographic sortition has sufficient randomness and unpredictability to eliminate manipulation of consensus led by the collusion among requesters, workers and miners [4]. We refer to and improve the work [16] so that participants with higher computing power could be selected with more chance.

Hence, a participant can be selected as the miner m_j at epoch τ if this condition is met: $\frac{HASH(\langle \tau \| rand(\tau) \rangle_{m_j})}{2^L} \cdot \frac{1-e^{-kI}}{1+e^{-kI}} \leq I_j^\tau$ where $rand(\tau)$ is a public randomness that can be extracted from the blockchain at epoch τ, $\langle \tau \| rand(\tau) \rangle_{m_j}$ is a signature of message $\tau \| rand(\tau)$ produced with private key of m_j, $HASH$ is a deterministic hash function, L is the bits of the output of $HASH$, I_j^τ is the fraction of m_j's computing power over all miners in BCSs at epoch τ.

Unlike traditional mining in which transaction fee is paid by each initiator, the requester R has to pay transaction fees to motivate miners to pack and validate transactions since all transactions are related to its task. After the selection of miners, R announces total transaction fee F that all miners compete for. If one miner successfully solves a crypto puzzle, it will broadcast its solution to BCSs. After the solution reaches Proof-of-Work (PoW) consensus, a new block is mined successfully and its miner obtains the mining reward which includes voluntary transaction fees of this block and a fixed block reward. The voluntary transaction fees depend on the number of transactions in the block, in other words, the miner can earn more voluntary transaction fees if it packs and validates more transactions.

Winning a mining reward depends on mining and propagating a block as quickly as possible. During the mining process, whether a miner can mine a new block depends on its relative computing power μ. However, the block may be orphaned by subsequent blocks and hence its miner will not be paid because of propagation time lag [8]. The occurrence of mining a block follows the Poisson distribution, and the probability of block being orphaned is $P_{orphan} = 1 - e^{-\lambda T(r)}$, where $\lambda = 1/600$ and $T(r)$ represents the block propagation time which depends linearly on r [8]. Therefore, the probability of winning the mining reward is denoted by $P = \mu(1 - P_{orphan}) = \mu e^{-\lambda \varepsilon r}$, where ε is a delay factor reflecting the impact of r on $T(r)$.

Given the set of selected miners, denoted by $M = \{m_1, \cdots, m_n\}$, each miner $m_j \in M$ decides to include r_j transactions in its block. The utility of m_j is determined by two parts: 1) the mining reward, and 2) the electricity and other costs associated with mining. Thus, the utility of m_j is presented by

$$U_m^j = \left(\frac{r_j F}{\sum_{m_n \in S} r_n} + D \right) P_j - c_j = \left(\frac{r_j F}{\sum_{m_n \in S} r_n} + D \right) \mu_j e^{-\lambda \varepsilon r_j} - c_j \quad (8)$$

where $\frac{r_j F}{\sum_{m_n \in S} r_n}$ means transaction fees obtained by m_j according to the ratio of its number of transactions, and D means the fixed block reward. The utility of the requester R is

$$U_R(F) = f(r_1, \cdots, r_n) - F \quad (9)$$

where $f(r_1, \cdots, r_n)$ is the satisfaction function with respect to the number of verified transactions from selected miners. We made a realistic and general assumption that $f(0, \cdots, 0) = 0$ and $f(r_1, \cdots, r_n)$ is a strictly concave function in variables $r_1, \cdots, r_n$ and monotonically increasing in each r_j [19].

5.2 Two-Stage Stackelberg Game Formulation

According to Sect. 5.1, we can formulate MCIM as a two-stage Stackelberg game. In the stage I of MCIM, R announces a total transaction fee F to motivate miners to pack transactions into their blocks. Since no rational miners will join in the mining competition with negative earnings, so we consider that $F > 0$. In the stage II of MCIM, each miner $m_j \in M$ decides to pack a different amount of transactions r_j in block mining competition to maximize its utility. Let $\Phi = \{r_1, \cdots, r_n\}$ denote the strategy profiles consisting of all miners' strategies and Φ_{-j} denotes the strategy profile excluding r_j. Thus in MCIM, the requester is the leader and miners are the followers. The objective of MCIM is to find the Stackelberg equilibrium where R can maximize its utility with the response strategies of miners, which is represented as follows:

– In stage I:

$$Maximize\ U_R^{\Phi}(F), \quad Subject\ to\ F > 0. \tag{10}$$

– In stage II:

$$Maximize\ U_m^j, \quad Subject\ to\ r_j \geq 0. \tag{11}$$

5.3 Equilibrium Analysis for MCIM

In this section, we analyze the optimal strategy of miners and the utility maximization of the requester. We apply the backward induction method to analyze the Stackelberg equilibrium of MCIM. In the stage II of MCIM, given the total transaction fee F, miners compete with each other to maximize their own utility by choosing their individual strategy, which can be considered as a block mining game (BMG) $G^M = \left\{M, \Phi, \left\{U_m^j\right\}_{m_j \in M}\right\}$, where M is the set of miners, Φ is miners' strategy set and U_m^j is the utility of miner m_j.

Definition 1. *A set of strategies $\Phi^* = \{r_1^*, \cdots, r_n^*\}$ is the Nash equilibrium of the BMG if $U_m^j\left(r_j^*, \Phi_{-j}^*\right) \geq U_m^j\left(r_j, \Phi_{-j}^*\right)$ for any $r_j \geq 0$.*

Theorem 1. *A Nash equilibrium in BMG $G^M = \left\{M, \Phi, \left\{U_m^j\right\}_{m_j \in M}\right\}$ exists.*

Proof. We compute the first order and second order derivatives of U_m^j defined in (8) with respect to r_j:

$$\frac{\partial U_m^j}{\partial r_j} = \left(\frac{F\sum_{m_n \neq j \in S} r_n}{\left(\sum_{m_n \in S} r_n\right)^2} - \lambda\varepsilon\left(\frac{Fr_j}{\sum_{m_n \in S} r_n} + D\right)\right) \cdot \mu_j e^{-\lambda\varepsilon r_j} \tag{12}$$

and

$$\begin{aligned}\frac{\partial^2 U_m^j}{\partial r_j^2} = &-\lambda\epsilon\mu_j e^{-\lambda\varepsilon r_j}\left(\frac{F\sum_{m_n \neq j \in S} r_n}{\left(\sum_{m_n \in S} r_n\right)^2} - \lambda\varepsilon\left(\frac{Fr_j}{\sum_{m_n \in S} r_n} + D\right)\right) - \\ &\mu_j e^{-\lambda\varepsilon r_j}\left(\frac{2F\sum_{m_n \neq j \in S} r_n}{\left(\sum_{m_n \in S} r_n\right)^3} + \lambda\varepsilon\left(\frac{F\sum_{m_n \in S} r_n - Fr_j}{\left(\sum_{m_n \in S} r_n\right)^2}\right)\right) < 0.\end{aligned} \tag{13}$$

Thus, U_m^j is strictly concave with respect to r_j. Hence, given any $F > 0$ and any strategy profile Φ_{-j} of the other miners, the best response strategy of m_j is unique when $r_j \geq 0$. Accordingly, the Nash equilibrium of noncooperative BMG G^M exists.

Further, by setting the first derivative of U_m^j to 0, we have

$$\left(\frac{F\sum_{m_n\neq j\in S} r_n}{\left(\sum_{m_n\in S} r_n\right)^2} - \lambda\varepsilon\left(\frac{Fr_j}{\sum_{m_n\in S} r_n} + D\right)\right)\cdot \mu_j e^{-\lambda\varepsilon r_j} = 0, \tag{14}$$

and we can obtain the best response strategy of m_j which is denoted as $\beta(r_j)$ in (15):

$$\beta(r_j) = \begin{cases} 0, & \text{otherwise.} \\ \frac{\sqrt{F\lambda\varepsilon\left(F\lambda\varepsilon\sum_{m_n\neq j\in S} r_n + 4D + 4F\right)\sum_{m_n\neq j\in S} r_n} - \lambda\varepsilon(2D+F)\sum_{m_n\neq j\in S} r_n}{2\lambda\varepsilon(D+F)}, & F \geq 0. \end{cases} \tag{15}$$

According to (14), we have

$$\lambda\varepsilon D\left(\sum_{m_n\in S} r_n\right)^2 + \lambda\varepsilon F r_j \sum_{m_n\in S} r_n = F\sum_{m_n\neq j\in S} r_n. \tag{16}$$

Then, we can get $(\lambda\varepsilon|M|D + \lambda\varepsilon F)\sum_{m_n\in S} r_n = F(|M|-1)$ by summing up (16) over all selected miners. Thus,

$$\sum_{m_n\in S} r_n = \frac{F(|M|-1)}{\lambda\varepsilon|M|D + \lambda\varepsilon F}. \tag{17}$$

By substituting (17) into (16), we have the unique Nash equilibrium for miner m_j in BMG, as shown in (18):

$$r_j^* = \frac{\left(F^2 + DF\right)(|M|-1)}{\lambda\varepsilon|M|(|M|D+F)(F-D)}. \tag{18}$$

□

According to the above analysis, the requester knows that there exists a unique Nash equilibrium for selected miners for any $F > 0$. Thus the requester can maximize its utility by choosing the optimal transaction fee F.

Theorem 2. *There exists the unique Stackelberg Equilibrium* $\left(F^*, r_j^{ne}\right)$ *in the MCIM game, where* F^* *is the unique maximizer of the requester's utility in (9) and* r_j^{ne} *is given by (18) with* F^*.

Proof. Since rational miners will not participate in mining when $F = 0$, $U_R(F) = 0$ for $F = 0$ and approaches to $-\infty$ when F goes to ∞. Note that $f(r_1, \cdots, r_n)$ is a strictly concave function in variables $\{r_1, \cdots, r_n\}$, hence $U_R(F)$ has a unique maximum value when $F = F^*$ that can be efficiently calculated by either bisection or Newton's method [19]. Therefore, there exists a unique Stackelberg Equilibrium $\left(F^*, r_j^{ne}\right)$ in MCIM. □

6 Performance Evaluation

In this section, we conduct extensive simulations to evaluate and investigate impacts of key parameters on performance of URIM. We present simulation settings, metrics and results as follows.

6.1 Simulation Setup

In the simulation, we consider multiple workers compete to complete the task, and submit their bidding prices and solutions. Then, miners are selected to pack transactions and compete for transaction fees. For evaluating the WCIM, the bidding price b and the contribution v of each worker is normally distributed over $[0.1, 1]$ and $[0.01, 0.5]$ respectively. The number of workers $|W|$ varies from 100 to 1000 with the increment of 100. For evaluating the MCIM, the utility of the requester is set as $U_R(F) = \theta \log\left(1 + \sum_{m_j \in M} r_j\right) - F$ that satisfies the assumptions in Sect. 5.1. We set θ to 10^4. The fixed block reward D is fixed at 100 and the delay factor is fixed at 10^{-4}. For each miner, its mining cost is randomly generated from $[10, 20]$ and μ is randomly generated from $[0.001, 0.1]$. All simulations are performed in Python 3.7.0 and Solidity 0.7.0 on a Windows machine with Intel Core i7-7700 CPU and 16 GB memory.

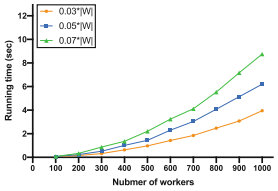

Fig. 3. Running time.

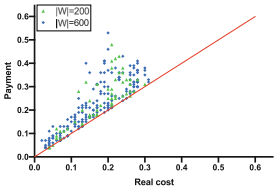

Fig. 4. Individual rationality.

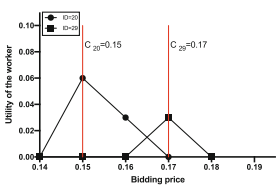

Fig. 5. Truthfulness.

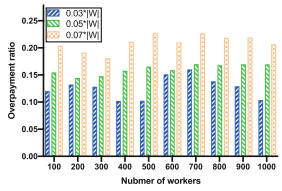

Fig. 6. Overpayment ratio at varied budgets.

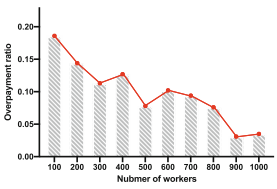

Fig. 7. Overpayment ratio at fixed budget.

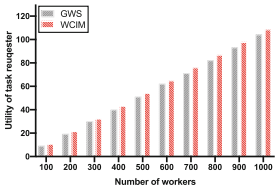

Fig. 8. Utility of requester.

6.2 Evaluation of the Worker-Centric Incentive Mechanism

To investigate the performance of WCIM, we present following metrics: running time, individual rationality, truthfulness, overpayment ratio and utility of requester. Furthermore, we compare WCIM with greedy winner selection (GWS) proposed in [2].

Running Time: We first demonstrate the running time of WCIM in Fig. 3. The budget is set as $|W|$ multiplied by $\{0.03, 0.05, 0.07\}$ respectively. We can find the running time increases slowly with increasing $|W|$. Additionally, the running time has slight changes when the budget increases. These results show WCIM can efficiently select workers and calculate their payments.

Individual Rationality and Truthfulness: Then we verify the individual rationality and truthfulness of WCIM. We demonstrate the individual rationality by comparing each payment and the related real cost (truthful bidding). We randomly set $|W|$ as 200 and 600 in Fig. 4, and we find each payment is greater than the related real cost. To verify the truthfulness, we randomly pick two winners (ID = 20, 29) and change their claimed bidding prices, then recalculate their utilities. We illustrate results in Fig. 5 and find two winners can only obtain their maximum utility if they bid the real cost $Cost_{20} = 0.15$, $Cost_{29} = 0.17$.

Overpayment Ratio: Figure 6 plots the overpayment ratio when $|W|$ changes from 100 to 1000 and the budget equals $|W|$ multiplied by $\{0.03, 0.05, 0.07\}$ respectively. Figure 7 shows the overpayment ratio decreases with the increase of $|W|$ when the budget is fixed at 1000. We find that the overpayment ratio is always less than 0.25, which means that the requester does not have to pay much extra money to induce truthfulness.

Utility of Requester: Figure 8 plots the utility of requester when $|W|$ change from 100 to 1000. $|W|$ multiplied by 0.05 is set as the budget. With the increase of workers and budget, more workers will be selected to complete the task and the utility of requester increase spontaneously. As seen from Fig. 8, WCIM outputs higher utility of requester than GWS because WCIM adopts dynamic programming which can always obtain the global optimal solution.

6.3 Evaluation of the Miner-Centric Incentive Mechanism

To evaluate MCIM, we reveal impacts of total transaction fee F and the number of miners $|M|$ on the number of total transactions TX and the utility of the requester $U_R(F)$.

Number of Total Transactions: Figure 9 depicts the impact of F on TX when $|M|$ is fixed at 1000. It is found that TX increases as F increases. This is because increased F incentivizes miners to pack more transactions into their blocks. Figure 10 depicts the impact of $|M|$ on TX when F is fixed at 20000. We can find that with the increase of $|M|$, TX increases with a slowdown, which is in line with (18). The reason is that more involved miners intensify the competition for the transaction fee, which incentivizes miners to validate more transactions.

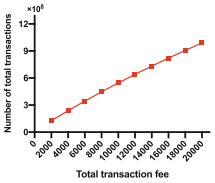

Fig. 9. Impact of F on TX.

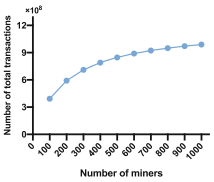

Fig. 10. Impact of $|M|$ on TX.

Fig. 11. Impact of F on $U_R(F)$.

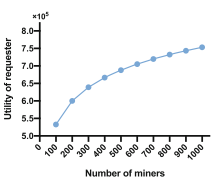

Fig. 12. Impact of $|M|$ on $U_R(F)$.

Fierce competition, however, reduces the probability of winning mining rewards. As a result, the growth trend of total transactions is slowing down.

Utility of Requester: For the utility of requester, we first evaluate the impact of F on it when $|M|$ is fixed at 1000 and present results in Fig. 11. We find that as F increases, $U_R(F)$ decreases gradually. The intuitive reason is that, the margin utility descends with more transaction fees. Although the requester announces more transaction fees, there is a diminishing marginal effect on the contributions of miners, which fails to cover the corresponding increase of F. As shown in Fig. 12, we evaluate the impact of $|M|$ on $U_R(F)$ when F is fixed at 20000. It is found that the requester can achieve greater utility when more miners join in the mining, which indeed demonstrates diminishing returns when $|M|$ increases and is in line with $U_R(F)$. Combining Fig. 11 and 12, we find the requester can optimize its utility with more miners and fewer F.

7 Conclusion

In this paper, we have proposed a utility-oriented role-centric incentive mechanism design named URIM for BCSs, which consists of worker-centric and miner-centric incentive mechanisms. Through both rigorous theoretical analyses and extensive simulations, we have demonstrated that the worker-centric incentive mechanism is computationally efficient, individually rational and truthful, and the miner-centric incentive mechanism can maximize the utility of the requester based on optimal strategies of miners. In the future work, we will further explore non-monetary incentive mechanisms for BCSs and evaluate our design in real-world applications.

Acknowledgements. This work was supported by the Scientific Research Program of Science and Technology Commission of Shanghai Municipality under Grant No. 19511102203.

References

1. Amintoosi, H., Kanhere, S.S.: A reputation framework for social participatory sensing systems. Mob. Netw. Appl. **19**(1), 88–100 (2014)
2. An, B., Xiao, M., Liu, A., Gao, G., Zhao, H.: Truthful crowdsensed data trading based on reverse auction and blockchain. In: Li, G., Yang, J., Gama, J., Natwichai, J., Tong, Y. (eds.) DASFAA 2019. LNCS, vol. 11446, pp. 292–309. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-18576-3_18
3. Chatzopoulos, D., Gujar, S., Faltings, B., Hui, P.: Privacy preserving and cost optimal mobile crowdsensing using smart contracts on blockchain. In: 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 442–450. IEEE (2018)
4. Conti, M., Gangwal, A., Todero, M.: Blockchain trilemma solver algorand has dilemma over undecidable messages. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1–8 (2019)
5. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al.: Blockchain technology: beyond bitcoin. Appl. Innov. **2**(6–10), 71 (2016)
6. Duan, H., Zheng, Y., Du, Y., Zhou, A., Wang, C., Au, M.H.: Aggregating crowd wisdom via blockchain: a private, correct, and robust realization. In: 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom2019), pp. 43–52. IEEE (2019)
7. Feng, Z., Zhu, Y., Zhang, Q., Ni, L.M., Vasilakos, A.V.: TRAC: truthful auction for location-aware collaborative sensing in mobile crowdsourcing. In: IEEE INFOCOM 2014-IEEE Conference on Computer Communications, pp. 1231–1239. IEEE (2014)
8. Houy, N.: The bitcoin mining game. Available at SSRN 2407834 (2014)
9. Hu, J., Yang, K., Wang, K., Zhang, K.: A blockchain-based reward mechanism for mobile crowdsensing. IEEE Trans. Comput. Soc. Syst. **7**(1), 178–191 (2020)
10. Huang, J., et al.: Blockchain-based mobile crowd sensing in industrial systems. IEEE Trans. Ind. Inf. **16**(10), 6553–6563 (2020)
11. Koutsopoulos, I.: Optimal incentive-driven design of participatory sensing systems. In: 2013 Proceedings IEEE INFOCOM, pp. 1402–1410. IEEE (2013)
12. Lakhani, K.: Innocentive.com (a) (harvard business school case no. 608–170). Harvard Business School, Cambridge (2008)
13. Li, M., et al.: CrowdBC: a blockchain-based decentralized framework for crowdsourcing. IEEE Trans. Parallel Distrib. Syst. **30**(6), 1251–1266 (2018)
14. Lu, Y., Tang, Q., Wang, G.: ZebraLancer: private and anonymous crowdsourcing system atop open blockchain. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 853–865. IEEE (2018)
15. Ogie, R.I.: Adopting incentive mechanisms for large-scale participation in mobile crowdsensing: from literature review to a conceptual framework. Hum.-Cent. Comput. Inf. Sci. **6**(1), 24 (2016)
16. de Pedro, A.S., Levi, D., Cuende, L.I.: WitNet: a decentralized oracle network protocol. arXiv preprint arXiv:1711.09756 (2017)
17. Pouryazdan, M., Kantarci, B., Soyata, T., Foschini, L., Song, H.: Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowdsensing. IEEE Access **5**, 1382–1397 (2017)
18. Xu, J., Xiang, J., Yang, D.: Incentive mechanisms for time window dependent tasks in mobile crowdsensing. IEEE Trans. Wirel. Commun. **14**(11), 6353–6364 (2015)
19. Yang, D., Xue, G., Fang, X., Tang, J.: Incentive mechanisms for crowdsensing: crowdsourcing with smartphones. IEEE/ACM Trans. Netw. **24**(3), 1732–1744 (2015)

20. Yang, M., Zhu, T., Liang, K., Zhou, W., Deng, R.H.: A blockchain-based location privacy-preserving crowdsensing system. Futur. Gener. Comput. Syst. **94**, 408–418 (2019)
21. Zhang, J., Cui, W., Ma, J., Yang, C.: Blockchain-based secure and fair crowdsourcing scheme. Int. J. Distrib. Sens. Netw. **15**(7), 1550147719864890 (2019)