A Blockchain-based Reward Mechanism for Mobile Crowdsensing

Jiejun Hu, Kun Yang, *Senior Member, IEEE,* Kezhi Wang, and Kai Zhang

***Abstract*—Mobile CrowdSensing (MCS) is a novel sensing scenario of Cyber-Physical-Social Systems. MCS has been widely adopted in smart cities, personal health care, and environment monitor areas. MCS applications recruit participants to obtain sensory data from the target area by allocating reward to them. Reward mechanisms are crucial in stimulating participants to join and provide sensory data. However, while the MCS applications execute the reward mechanisms, sensory data and personal private information can be in great danger, because of malicious task initiators/participants and hackers. This work proposes a novel blockchain-based MCS framework that preserves privacy and which secures both the sensing process and the incentive mechanism by leveraging the emergent blockchain technology. Moreover, to provide a fair incentive mechanism, this paper has considered an MCS scenario as a sensory data market, where the market separates the participants into two categories: monthly-pay participants and instant-pay participants. By analysing two different kinds of participants and the task initiator, this paper proposes an incentive mechanism aided by a three-stage Stackelberg game. Through theoretical analysis and simulation, the evaluation addresses two aspects: the reward mechanism and the performance of the blockchain-based MCS. The proposed reward mechanism achieves up to a ten percent improvement of the task initiator's utility compared with a traditional Stackelberg game. It can also maintain the required market share for monthly-pay participants whilst achieving sustainable sensory data provision. The evaluation of the blockchain-based MCS shows that the latency increases in a tolerable manner as the number of participants grows. Finally, the paper discusses the future challenges of blockchain-based MCS.**

***Index Terms*—Mobile crowdsensing, blockchain, reward mechanism, Stackelberg game, sensory data market**

I. Introduction

THE development of network technology, sensing devices, and social networks has increased the deployment of the next generation of Internet of Things (IoT) – Mobile CrowdSensing (MCS). MCS is a novel sensing framework, which is assisted by smartphone sensors and with the inclusion of human intelligence in the loop. MCS has become a typical application in Cyber-Physical-Social Systems (CPSS) [1], [2] because it adopts the multi-disciplinary approach where knowledge from communication, computer science, computer network, economic, psychology, and social research unite to provide a solution of a sensing task.

Jiejun Hu and Kun Yang are with the School of Computer Sciences and Electrical Engineering, University of Essex, CO4 3SQ, Colchester, U.K.

Kezhi Wang is with Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne, NE1, 8ST, U.K.

Kai Zhang is with the Department of Economics, University of Essex, CO4 3SQ, Colchester, U.K.

Manuscript received *** **, 2019; revised **** **, 2019.

Compared with traditional IoT Frameworks, MCS has the advantages of broad sensing coverage, spatiotemporality of sensory data, feasibility and flexibility of deployment, and so on. MCS has been widely adopted in different scenarios, such as personal health care [3], smart cities [4], [5], environmental monitoring [6] and disaster recovery [7], [8]. Furthermore, it has drawn the attention of both academia and industry. The challenges in MCS that have been studied include: the incentive mechanism [9], sensory data transmission [10], sensing tasks execution [11], [12] and offloading [13], quality of sensory data [14], and coverage [15].

MCS is becoming an essential part of daily life, it collects the sensory data along with the participants' private data (such as location data). The leakage of participants' private data is inherent when participants join an MCS application. Additionally, an MCS scenario faces several challenges during deployment and operation:

1) Untrustworthy participants: A participant who may forge his identity or reputation, for example, adversary attack. A malicious participant may steal sensory data causing privacy leakage.
2) Untrustworthy task initiator: A task initiator may publish a sensing task without a reward guarantee, it may also try to steal the private information from participants when there is communication between them.
3) Untrustworthy reward transaction: Due to the mobility of participants in MCS, the reward allocation procedure will be disturbed when a mobile user/participant moves from one target area to another. As a result, a participant will have difficulty in redeeming his/her reward.
4) High operational cost of the system: MCS needs an authority to process all the communications between the sensing task initiator and the participants. Considering the architecture of MCS is usually centralised, MCS may suffer a single point failure and add additional operational cost to the whole scenario.

To address the above privacy and security challenges, this paper has proposed a blockchain-based reward mechanism to provide privacy and security features to the MCS. The concept of Bitcoin [16] has drawn more attention than blockchain technology. Bitcoin was created in 2009, following with a white paper which provided all the details of blockchain technology. Blockchain technology is a disruptive technology and often stated to be the fifth computing revolution after the mainframe, personal computer, internet and social networking [17]. The vital feature of the blockchain technology is that it is a distributed ledger that records transactions in a conventional

and permanent way, which makes it a potential solution for a distributed sensing scenario.

Blockchain technology has the potential to collaborate with the MCS because it operates the transactions in a decentralised, anonymous, and trustful fashion [18]. Firstly, by adopting blockchain technology, it will reduce the additional cost of the third party in MCS. Secondly, considering the anonymity feature of blockchain, it can protect the participants' private information when they participate in the sensing task. Last but not least, the smart contract [19] can support the automation of sensing task allocation, participant selection, sensing task execution, and reward allocation. The smart contract can make it easier for the intricate reward allocation. We will address this in detail in the next section.

This work proposes a blockchain-based MCS which can achieve participant identity anonymization, decentralised rewards allocation, and transparent transactions without an ordinary trusted third party. The main contribution of this work involves three aspects:

- Proposing a blockchain-based MCS framework, which provides the protection of participants' privacy, as well as a secure sensing process and rewards allocation mechanism by leveraging the novel blockchain technology. The proposed work uses hybrid base stations as miners to verify and validate the identities of the participants and the sensing task, the sensing procedure, and the reward allocation.
- Designing the workflow of blockchain-based MCS and a set of smart contracts to assist the sensing task execution automation of MCS. Once all the identities of the participants are verified on the blockchain, the sensing task execution procedure will be triggered. When the task initiator has collected the sensory data, the rewards allocation procedure will start to execute. Smart contracts can guarantee the automation and security of MCS framework.
- Studying the features of the sensory data market and the participants. This work classifies the participants into monthly-pay participants, instant-pay participants, and the task initiator. It provides an economic approach to analyse the incentive mechanism. By leveraging a three-stage Stackelberg game reward mechanism, it can achieve a fair and efficient sensory data market in MCS.

The remainder of this paper is organised as follows. Section II presents the related work. The blockchain-based MCS framework and smart contracts are introduced in Section III. The three-stage Stackelberg game and the incentive mechanism are presented in Section IV, respectively. The performance and simulation of the mechanism are analysed in Section VI. This paper also identifies the future challenges of blockchain-based sensing technology in Section VII. In Section VIII, the conclusions of this work are presented.

II. Related work

This work adopts the blockchain in cooperation with MCS to deploy an automated, secured sensing paradigm. Blockchain technology with its disruptive features has made it possible to connect the world seamlessly, including computers, sensors, smartphones, tablets, and wearable devices. Application scenarios of blockchain technology are not merely limited to the financial sector as before. New applications, such as energy supplement chain, secure information transmission, and so on, have also emerged.

IoT and MCS applications have deployed in the distributed fashion. The deployment depends on a centric server to support the sensing tasks, which is in danger of single point failure. Furthermore, in an environment with a large number of sensors, the traditional framework is short of proper security guarantee. By adopting blockchain technology, it would solve the challenges of traditional IoT faces. [20] surveyed research issues and the challenges of IoT security aspects in cooperation with the blockchain technology. Kshetri et al. [21] proposed a blockchain-based identity and access management systems, which can be leveraged to strengthen IoT security. As defined in this work, many companies have joined a group which hopes to establish a blockchain protocol to build IoT devices, applications, and networks. Christidis et al. [22] adopted blockchain technology into IoT, which used a smart contract to deploy the automation of the complex multi-process in IoT. Alphand et al. [23] proposed IoTChain, a scheme that combined the object security architecture (OSCAR) for the IoT and the authentication and authorisation for constrained environment (ACE) framework to provide an end-to-end solution for secure authorised access to IoT resources. This paper addressed the details of the whole framework and the authorisation flow. It simulated the proposed framework with an Ethereum private testnet. Zhang et al. [24] proposed a blockchain-based IoT in E-business aspect to support the feature of decentralisation and traceability. Cao et al. [25] discussed the main ideas of the consensus mechanisms and their limitations in IoT. Blockchain can solve the authentication of IoT devices, because it uses consensus mechanism to verify the identities of the IoT devices without the third party. However the consensus mechanism of sensing task execution has not been well investigated in these works. Thus, it motivates us to consider to propose a secure task execution by leveraging blockchain.

Related works on the collaboration of MCS and blockchain were proposed to provide secure sensing procedure to MCS. Li et al. [26] proposed a novel framework of blockchain and crowdsensing, which deployed a software prototype on Ethereum. In [27], a privacy-preserved incentive mechanism was proposed for crowdsourcing applications. This work used a series of encryption algorithms to solve the security issues in crowdsourcing. Delgado et al. [28] presented Paysense, a general framework that incentivises user participation and provides a mechanism to validate the quality of collected data based on users' reputation. This work focused on analysing user participation, data sensing quality and user anonymity. The related works focused on the improvement of security by proposing new encryption algorithms. However spatiotemporality is crucial to MCS task, complicated encryption algorithms may lead to long latency. The features of MCS need to be considered when adopting blockchain.

Related works attempted to provide secure incentive mechanism of MCS aided by blockchain. Chatzopoulos et al. [29]

proposed a truthful, cost-optimal auction that minimises the payments from the crowdsensing providers to mobile users based on a blockchain-aided mobile crowdsensing architecture. With the help of four smart contracts, it deployed a novel incentive mechanism in the blockchain. Feng et al. [30] investigated the limitation of the existing IoT frameworks and proposed a purely decentralised platform of crowdsensing by adopting permissionless blockchain technology. The author formulated a noncooperative game to analysis the competitive situations among the sensors. Cai et al. [31] addressed several challenges including the sensory data's safeguarding issue, knowledge monetisation and streamlined sensory data in the crowdsensing scenario. This work proposed a crowdsensing framework that enables privacy-preserving knowledge discovery and full-fledged blockchain-based knowledge monetisation. However, it did not give the detail on how to allocate the reward to each participant. Shi et al. [32] proposed a fault-tolerant incentivisation mechanism for mobile P2P crowd service (MPCS). They designed an MPCSToken smart contract to facilitate the service auction, task execution and payment settlement process with the help of blockchain technology. Jia et al. [33] proposed a blockchain-based location privacy protection incentive mechanism in MCS. It took privacy protection as a supplement of the monetary incentive mechanism and addressed the problem in a cryptographic approach. However, related works only used the classic incentive mechanisms, such as auction, noncooperative game, and so on, for one time stimulation. They have not considered to provide MCS application sustainable sensory data. The related works have not considered that blockchain can improve security of the system when the transactions keep growing.

Thus, this motivates us to propose a novel blockchain-based MCS framework that preserves privacy and which secures both the sensing process and the incentive mechanism by leveraging the emergent blockchain technology. Firstly, we proposed the architecture of the blockchain-based MCS and its workflow. We design a novel set of smart contracts from participants' registration, sensing task execution, to reward allocation. Based on the framework, we provide the solution of participants' privacy and sensing procedure security. Secondly, different from the related works, we consider the participants into different roles and propose a three stage Stackelberg game. This incentive mechanism makes sure the sensory data is sustainable provided by the participants and the utility of the task initiator is maximized. Thirdly, we have simulate the proposed framework on the Ethereum testnet to proof the efficiency.

III. Blockchain-based MCS framework

A. The architecture of blockchain-based MCS

This section introduces the framework of blockchain-based MCS and the entities in the framework. In an MCS scenario, a task initiator would like to collect as much good quality sensory data as possible under a specific budget. In some particular application, he even prefers long-term sensory data gathering. Thus according to an enterprise system, we classify the workers (participants) in MCS into contract workers who are paid monthly and temporary workers who are paid instantly after work. In this case, contract workers will contribute the sensory data in a long-term and stable manner and the temporary worker can make compensation whether when the budget is limited, or the sensory data is not sufficient. In the following paper, we will call contract workers "monthly-pay participants", and temporary workers "instant-pay participants". Thus this framework includes:

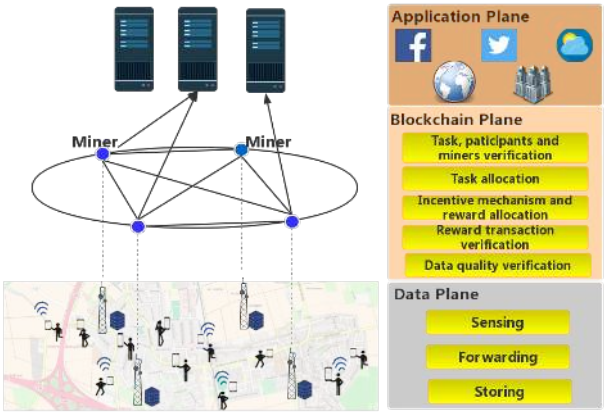


Fig. 1. Architecture of blockchain-based MCS

1) Task initiator: The initiator who publishes the sensing task and allocates the reward to monthly-pay and instant-pay participants through blockchain.
2) Participant: The participants are classified into two different roles, participants who will get paid instant after finishing the sensing task and participants who will get paid monthly. The instant-pay participants' reward is according to the sensory data quality and his reputation, the monthly-pay participants' reward is their salaries according to the number of the task they accomplish and their reputation.
3) Miner: Adding authorised miners aims to verify all the participants' identity and transactions between them. In this scenario, the hybrid base stations serve as authorised miners in blockchain-based MCS. A hybrid base station not only can execute the communication, but also server as storage and computation resource. By using blockchain, task initiator, participants and miners are on the blockchain working in cooperation anonymously. Besides the authorised miners also verify the identities of the task initiator and participants before continuing the sensing task of MCS. Smart contracts are deployed on the miners for the sensing task execution. The miners store all the blocks in the storage, thus they are in charge of verifying the registration of task initiator and participants, transactions, quality control of sensory data.

The architecture of blockchain-based MCS shows in Fig. 1. This work proposes a three-layer architecture for blockchain-based MCS, which consists of data plane, blockchain plane and application plane. Fundamental functions, such as sensing, data forwarding, and storing, can be operated on data plane

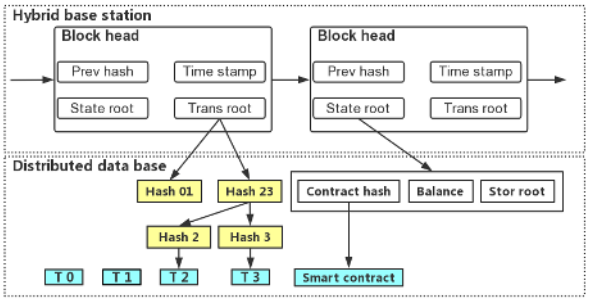


Fig. 2. Structure of block in blockchain-based MCS

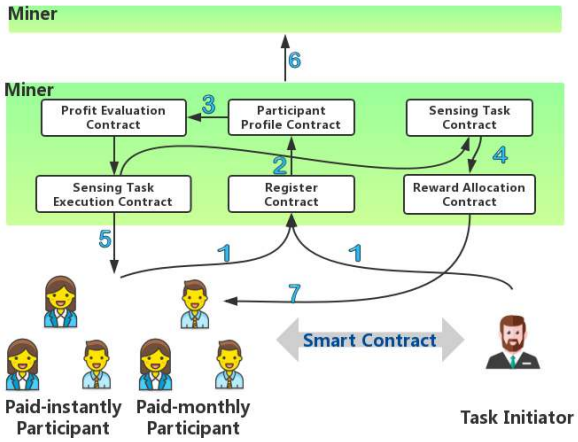


Fig. 3. Workflow of blockchain-based MCS

by smartphone users. This architecture introduces an extra abstract layer called blockchain plane to help an MCS application to verify the identities of participants, allocate the sensing task/rewards, operate the transactions and control the sensory data quality. Application plane can deal with the request from a specific organisation and process the sensory data to extract the knowledge.

In this work, hybrid base stations are equipped with servers and capable to operate communication and computation tasks. The miners store the whole blockchain information locally. The blockchain and the structure of a block are shown in Fig. 2. The chain in the miner starts with a genesis block. The new blocks the system generates are appended after the genesis block. In each block, it consists the block head, the previous hash of the block, time stamp, state root, transactions root, and so on. The state root and the transactions root are the root of Merkel tree. The transactions root stores all the hash value of the transactions between the participants. In the state root, it includes the contract hash, which is the hash value of the smart contract, balance, and the storage root. All the actual data is stored in distributed data base, which could be in the server of the hybrid base station.

B. The workflow of blockchain-based MCS

This section presents the workflow of blockchain-based MCS. Fig. 3 depicts the workflow of smart contracts between each entity in blockchain-based MCS. The task initiator communicates with the participants through the set of smart contracts, which are deployed on the miner. The details of the smart contracts will be introduced in the following section. We assume that the participants (including the task initiator) have registered and enrolled with the certificate authority (CA) and received back necessary cryptographic material, which is used to authenticate when sensing task starts.

1) **System initializaiton**: Task initiator and participants sign in for the MCS application. They will send their identities, public/private keys, certificates, etc. to the closest miner. The miner will run the "Registration Contract", and verify the identities of the participants and the task initiator with other miners by consensus mechanism. And then the miners will send confirmations to the task initiator if the participants' identities are valid. When the registration procedure completes, it will trigger the next step. Task initiator will send the description of the sensing task to the corresponding miners. The miners will verify the sensing task, and then broadcast the sensing task to all the registered participants.
2) **Incentive mechanism deployment (three-stage Stackelberg game)**: After system initialisation, the role of each identity will be clarified. Thus the incentive mechanism will be triggered by running the "Participant Profile Contract" and the "Sensing Task Contract". We will introduce this procedure in detail in the following sections.
3) **Token allocation**: After the incentive mechanism completes, all the participants receive the message of the reward, size of the sensory data. They need to inspect the message, if the message is legitimate, then they execute the sensing task according to the reward. Each of the participants will be allocated with a token, which indicates the sensing task and reward. For this function, we set a "credit & token bank" in every miner to enable token allocation.
4) **Sensory data uploading**: Since every participant has had the promised reward for accomplishing the sensing task, they will upload the promised sensory data to the task initiator via miner. At this step, instant-pay participants will get their reward from the credit bank of the miner.
5) **New block generation**: The miners will process the proof-of-work and build the new block with all the transactions of the sensing task on the chain. The new block will be audited and finally added on the blockchain.
6) **Token redemption and task accomplishment**: After the new block is added, all the participants have the tokens, and the sensing task completes, the tokens will

be redeemed whenever or wherever the participants need.

C. Smart contracts of blockchain-base MCS

The concept of the smart contract was firstly introduced in 1997 [19]. A smart contract is an agreement, which tells each party how to act when they trust each other. We assume that all the smart contracts are authorized before deployment. In the proposed blockchain-based MCS framework, a novel set of smart contracts is designed to operate the the transactions and verification. According to the workflow of blockchain-based MCS, the novel set of smart contracts are proposed.

1) Registration contract: All the participants including task initiator register run registration contract as it shows in TABLE. I. All the participants will send their address and roles in the secure communication channel to the miner to verify their identities. After the consensus among the miners finishes, the participants without the legitimate signature will be detected. This paper omits the technical details of cryptography algorithms in the blockchain. We adopt the asymmetric cryptography algorithms to provide the secure communication channel.

TABLE I
REGISTRATION CONTRACT

ID	Address	Type
P_1	Addr$\{P_1\}$	Initiator
P_2	Addr$\{P_2\}$	Instant-pay participant
P_3	Addr$\{P_3\}$	Monthly-pay participant
P_4	Addr$\{P_4\}$	Miner

2) Participant profile contract: When the miners collect all the information from the participants, their profile will be built to assist the participant selection procedure, sensing task execution procedure and rewards allocation procedure. A participant's profile contains the participant's reputation, expecting the reward of sensing task, participant's status and so on, as it is shown in TABLE. II.

TABLE II
PARTICIPANT PROFILE CONTRACT

Address	Profile	Sensing Task ID	Reward of Task
Addr$\{P_1\}$	Profile$\{P_1\}$	T_1	R_1
Addr$\{P_2\}$	Profile$\{P_2\}$	t_1	r_1
Addr$\{P_3\}$	Profile$\{P_3\}$	t_2	r_2
Addr$\{P_4\}$	Profile$\{P_4\}$	t_2	0

3) Sensing task contract: The sensing task contract consists the ID, execution status, deposit and rewards plan of sensing tasks. The execution status of a sensing task is a binary variable in TABLE. III. When the status is 0, it means the sensing task is unfinished and vice versa. There are also parameters, such as sensing task's deposit which can guarantee the promised rewards to the participants and its reward plan which gives guidance of rewards allocation.

TABLE III
SENSING TASK CONTRACT

Sensing Task ID	Status	Deposit	Reward Plan
T_1	0	D_1	R_1
T_2	1	D_2	R_2

4) Profit Evaluation Contract: When the participants register on the chain, the miners obtain all the information to evaluate the rewards allocation plan by running the profit evaluation contract. Due to the deployment of the three-stage Stackelberg game, all the participants, including the task initiator have the profit evaluation contract to calculate if a specific scenario will maximise their profit, according to equation (1), (3) and (4). This procedure will be introduced in the following sections. We denote $U(\cdot)$ as the profit function of participant with sensing plan in TABLE. IV.

TABLE IV
PROFIT EVALUATION CONTRACT

ID	Expecting reward	Sensing task ID	Device ability	Profit $U(\cdot)$
P_1	r_1	T_1	$D(P_1)$	$U_1(\cdot)$
P_2	r_2	T_2	$D(P_2)$	$U_2(\cdot)$

5) Sensing Task Execution Contract: When the participants calculate the maximum profit according to the details of the sensing task, reward and so on, they will obtain the sensing plan, including the quality of sensory data and the sensory data size. The participants will follow the sensing task execution contract, in TABLE. V, to execute the sensing task. So the sensing task execution contract will be triggered.

TABLE V
SENSING TASK EXECUTION CONTRACT

ID	Profit $U(\cdot)$	Sensing task ID	Status
P_1	$U_1(\cdot)$	T_1	0
P_2	$U_2(\cdot)$	T_2	1

6) Reward allocation contract: The key algorithms of this paper will be deployed in a sensing task contract according to the participant profile contract. This algorithm will give the result of the reward plan of the sensing task. Meanwhile, during this procedure, reward will be allocated as tokens to the participants, which is enabled by the reward allocation contract in TABLE. VI.

TABLE VI
REWARD ALLOCATION CONTRACT

Sensing Task ID	Status	Participant's ID	Token
T_1	0	P_1	$Token_1$
T_2	1	P_2	$Token_2$

D. Consensus mechanism of blockchain-base MCS

In this work, we use Proof-of-Work (PoW) as the consensus mechanism. PoW requires a great amount of computation power to create a set of transactions (the block). PoW is the practice of solving block equations to verify if the each transaction is legitimate in the block. The miner starts PoW by choosing a number "nonce", along with the hash of the previous block, and the Merkel root, he could get an answer of the equation. He repeats changing the "nonce" till he calculate the right answer. Once the PoW completes, the block of transactions is confirmed and becomes public. PoW can reduce the risk of a 51% attack, because the equation is very hard to solve. And it doesn't rely on any third party, which enables to build a transparent network.

In this work, we adopt the PoW in Ethereum without any optimization. In future work, our study will be focused on the distributed consensus mechanism.

IV. SYSTEM MODEL OF THE INCENTIVE MECHANISM

The incentive mechanism is the crucial research aspect in the MCS. A task initiator can obtain the sensory data and price the sensory data in the MCS framework as a sensory data market. A sensory data market should conform to market rules. Thus adopting a primary economic method is necessary.

In blockchain-based MCS, the framework consists of a set $\mathbf{p}$ of participants. We consider a set of the instant-pay participants as $\mathbf{p^I} = \{1, 2, ..., p^I\}$ and a set of the monthly-pay as $\mathbf{p^M} = \{p^I+1, p^I+2, ..., p^I+p^M\}$, where $\mathbf{p^I} \bigcup \mathbf{p^M} = \mathbf{p}$. In this scenario, there exists multiple hybrid base stations acting as miners. We denote miner as $\mathbf{m} = \{1, 2, ..., m\}$. A task initiator will publish a sensing task $t = (R, D, B)$ to the participants. Here D denotes the required sensory data size, R denotes the reputation of the participants, and B denotes the budget of reward. The sensory data size each participant in $\mathbf{p^I}$ and $\mathbf{p^M}$ provides is $\mathbf{d} = \{d_1, ..., d_{p^I}, ..., d_{p^I+p^M}\}$.

In this blockchain-based MCS sensory data market, to have more sustainable participants for sensing tasks, task initiator prefers more monthly-pay participants. Thus, in the first stage of the game, monthly-pay participants dominate the market over task initiator. In the second stage, task initiator should dominate the market when he/she negotiates with instant-pay participants. In the third stage, instant-pay participants adjust the sensory data size according to the reward the task initiator provides. The formal definitions of the players and their strategies in the three-stage Stackelberg game [34] are as following.

- **Monthly-pay participant** signs in for long-term and gets paid monthly. The strategy profile of monthly-pay participants are their salary, which denote as a set $\mathbf{r_{p^M}} = \{r_{p^I+1}, ..., r_{p^I+p^M}\}$. They can only redeem their payments monthly;
- **Task initiator** who starts a sensing task, selects the monthly-pay participants according to the sensing task's requirements, and then offers the instant-pay participants the reward to execute the sensing task. Thus the strategy profile of task initiator includes two parts: sensory data size $\mathbf{d_{p^M}} = \{d_{p^I+1}, ..., d_{p^I+p^M}\}$ and the reward to instant-pay participants $\mathbf{r_{p^I}} = \{r_1, ..., r_{p^I}\}$;
- **Instant-pay participant** who gets paid after each task according to the sensory data size and reputation. According to the reward offered by the task initiator, instant-pay participants can decide the sensory data size. The strategy profile is the sensory data size $\mathbf{d_{p^I}} = \{d_1, ..., d_{p^I}\}$.

TABLE VII
NOTATION AND DESCRIPTIONS

Notation	Description
$\mathbf{p}$	A set of participants
$\mathbf{p^I}$	A set of instant-pay participants
$\mathbf{p^M}$	A set of monthly-pay participants
$\mathbf{m}$	A set of base stations / miners
$\mathbf{d}$	A set of sensory data size
$R_{\mathbf{p}}$	Reputation of participant $\mathbf{p}$
$\mathbf{r}$	A set of payment/reward to participants
α	Market domination indicator
γ	Default value of reputation
$\omega_{\mathbf{p}}$	Processing ability of sensing device in participant set $\mathbf{p}$
β	Network condition
B	Reward Budget of task initiator
D	Total sensory data size of the task

A. Problem formulation

1) Utility of task initiator: A task initiator aims to maximise his profit which consists of two parts: revenue by accomplishing the sensing task and cost by paying the participants. When a task initiator announces a sensing task to all the participants, they must have a set of specific parameters to guarantee the quality of the result of the sensing task. Moreover, task initiator will take the reputation [14], [35], [36] of participant into consideration as well. Task initiator will have a set of payment $\mathbf{r} = \{r_1, ..., r_{p^I}, ..., r_{p^I+p^M}\}$ to participants, where $\mathbf{r}$ is the value of one unit of the sensory data. We also denote the data quantity as $\mathbf{d} = \{d_1, ..., d_{p^I}, ..., d_{p^I+p^M}\}$. Let d_i denote as instant-pay participants where $i \in \mathbf{p^I}$ and d_j denote as monthly-pay participants where $j \in \mathbf{p^M}$.

In order to obtain long and stable sensory data, a sensing task initiator is willing to recruit more monthly-pay participants. Instant-pay participants are part-time workers, who complement the sensory data market. For example when the budget is limited, possibly more instant-pay participants will join the market. Thus, in this model monthly-pay participants will dominate the market. In this paper, the Stackelberg game is adopted to naturally grand monthly-pay participants the

"first mover advantage", which means the first mover in the game will dominate the market [37].

The profit a task initiator can gain depends on the sensory data size d_i and d_j, the reputation of the participants R_i and R_j, and his expense to pay them r_i and r_j as well. The utility function of the task initiator is defined as:

$$U_I = \sum_{i \in \mathbf{p^I}} d_i h(R_i) + \sum_{j \in \mathbf{p^M}} {d_j}^2 h(R_j) - (\sum_{i \in \mathbf{p^I}} r_i d_i + \sum_{j \in \mathbf{p^M}} r_j d_j) \tag{1}$$

where $h(\cdot)$ is the reputation function of participants. Note that we have added quadratic d_j, which indicates the task initiator prefers monthly-pay participants to obtain more income. The reputation function [38] $h(\cdot)$ of the participants $\mathbf{p}$ is defined as:

$$h(R_{\mathbf{p}}) = \begin{cases} \gamma + (1-\gamma) ln(1+\varepsilon) & \text{if} \quad R \leq R_{\mathbf{p}} \leq R_{max} \\ \gamma e^{(R_{\mathbf{p}} - R)} & \text{if} \quad R_{min} \leq R_{\mathbf{p}} \leq R \end{cases} \tag{2}$$

where γ is a default value, R is the required reputation of the task initiator. Here $\varepsilon = \frac{(e-1)(R_{\mathbf{p}} - R)}{R_{max} - R}$. The reputation function implies that when the reputation of a participant is lower than the required reputation of the sensing task, $h(\cdot)$ will decrease sharply, conversely $h(\cdot)$ will markedly increase.

2) Utility of monthly-pay participant: The utility function of the participant $j \in \mathbf{p^M}$ who gets paid monthly is based on the sensory data size d_j and the cost of sensing and uploading. We assume that every participant keeps the sensing history on record to estimate the expecting salary for the next month and then report the salary to the task initiator. Thus we have the utility function of monthly-pay participant j

$$U_j^{PM} = r_j d_j - [s_j(d_j, R_j) + u(d_j)] \tag{3}$$

where $s_j(\cdot)$ is function of sensing cost and $u(\cdot)$ is function of sensory data uploading cost. Function $s_j(\cdot)$ and $u(\cdot)$ increase as the size of sensory data increases. A rational participant will keep his utility function positive.

3) Utility of instant-pay participant: Instant-pay participant $i \in \mathbf{p^I}$ will receive a reward offer from task initiator. Then according to the reward, he will decide the sensory data size d_i he can contribute to the task initiator. The revenue for p_i^I will be the reward r_i he/she can get after accomplishing a single sensory task. The cost depends on the size of sensory data d_i, participant's reputation $h(R_i)$ and the uploading cost $u(d_i)$. The objective of the participants is to maximise their individual expected utility. Thus the utility function U_i^{PI} of instant-pay participant i is:

$$U_i^{PI} = r_i d_i - [s_i(d_i, R_i) + u(d_i)] \tag{4}$$

Furthermore, the sensing cost function $s_i(\cdot)$ and sensory data uploading function $u(\cdot)$ are defined in detail:

$$s_i(d_i, R_i) = \omega_i \cdot h(R_i) {d_i}^2 \tag{5}$$

$$s_j(d_j, R_j) = \omega_j \cdot h(R_j) d_j \tag{6}$$

$$u(d_{\mathbf{p}}) = \beta \cdot d_{\mathbf{p}} \tag{7}$$

where $\omega_{\mathbf{p}}$ represents the processing ability of the sensing devices, which is the CPU ability of encoding the data before sending it out. The network condition denoted as β, which means that a greater β indicates a poorer network condition, it will require more cost to upload the sensory data. Note that we design different sensing cost function for different participants, the instant-pay participants will have greater cost comparing to the monthly-pay participants, because the task initiator prefers more monthly-pay participants in the system.

V. THREE-STAGE GAME AND EQUILIBRIUM

This section will present the solution of the three-stage Stackelberg game. This game aims to maximise the utility of task initiator and maximise the utility of the participants, at the same time achieve the maximum sensory data quality.

To solve a traditional Stackelberg game, we adopt backwards induction which solves the equilibria of the subgames first. In the three-stage Stackelberg game, there are three subgames, which means we need to obtain three perfect equilibria [39] of the three subgames.

A. Subgames equilibria and Stackelberg equilibrium

For every player i with strategy profile τ_i, we assume the state after executing strategy profile τ_i is $O_{\mathfrak{h}}(\tau_i)$ according to history $\mathfrak{h}$.

Definition (Subgame perfect equilibrium) The strategy profile τ^* is a subgame perfect equilibrium if, the utility of state $O_{\mathfrak{h}}(\tau^*)$ is at least as good as the utility of state $O_{\mathfrak{h}}(\tau_i, \tau^*_{-i})$, where the strategy profile (τ_i, τ^*_{-i}) represents player i chooses τ_i while every other player $-i$ chooses τ^*_{-i}. Equivalently, for every player i and every history $\mathfrak{h}$ after which it is player i's turn to move,

$$U_i(O_{\mathfrak{h}}(\tau^*)) \geq U_i(O_{\mathfrak{h}}(\tau_i, \tau^*_{-i})) \tag{8}$$

where U_i is a utiltiy function that represents player i's preferences.

The definition above is the general definition for subgame perfect equilibrium. For example, in this work, when an instant-pay participant wants to decide his strategy of sensory data size d_i, he will take the previous stage's strategy as given, which is the reward strategy r_i from task initiator, to derive his optimal strategy ${d_i}^*$. The subgame perfect equilibrium can be interpreted in the following two aspects:

- **The subgame is Nash Equilibrium, so the follower's strategy is optimal, given the leader's strategy.**
  In three-stage Stackelberg game, the leader is monthly-pay participants, and follower is task initiator in stage I. Then the leader is task initiator, and the followers are the instant-pay participants in stage II. Finally, the players are an instant-pay participants in non-cooperate game stage III. Thus in this three-stage Stackelberg game, the Nash equilibrium can be obtained.
- **According to the strategy history, the followers' strategy is optimal.**
  As it is in a Stackelberg game, the subgame will play dynamically. According to the strategy history and preferences of the leader, the followers will repeatedly engage

in the same game with different strategy profile until they reach the optimal solutions.

When every subgame can admit a subgame perfect equilibrium, the Stackelberg game achieves the Stackelberg equilibrium. Now we give the definition of Stackelberg equilibrium of the proposed game.

Definition (Stackelberg equilibrium) The strategy profile $(\mathbf{r}^*_{\mathbf{p^M}}, \mathbf{d}^*_{\mathbf{p^M}}, \mathbf{r}^*_{\mathbf{p^I}}, \mathbf{d}^*_{\mathbf{p^I}})$ is a Stackelberg equilibrium if it satisfies

$$U^{PI}(\mathbf{d}^*_{\mathbf{p^I}}) \geq U^{PI}(d_i, \mathbf{d}^*_{-i}) \tag{9}$$

$$U^{I}(\mathbf{d}^*_{\mathbf{p^M}}, \mathbf{r}^*_{\mathbf{p^I}}) \geq U^{I}(d_j, \mathbf{d}^*_{-j}, r_i, \mathbf{r}^*_{-i}) \tag{10}$$

$$U^{PM}(\mathbf{r}^*_{\mathbf{p^M}}) \geq U^{PM}(r_j, \mathbf{r}^*_{-j}) \tag{11}$$

where $\mathbf{d}^*_{\mathbf{p^I}}$ is the equilibrium sensory data size strategies of instant-pay participants, d_i is the sensory data size strategy of participant i, d^*_{-i} is the equilibrium strategies of all the participants expect participant i in (9). The rest of the notation in (10) and (11) has the same meaning as in (9). (9), (10) and (11) are subgame equilibria of stage III, stage II and stage I, respectively, in the whole Stackelberg game. When all the subgames admit perfect equilibria, we derive the Stackelberg equilibrium. The subgame perfect equilibria of the three subgames will be analysed in the following sections.

B. Stage III: Instant-pay participants' strategy profile

According to backward induction, the task initiator's reward plan $\mathbf{r}_{\mathbf{p^I}}$ is taken as given to solve the profit maximisation problem of instant-pay participants in Stage III. According to equation (4), (5) and (7)

$$\begin{aligned} \max_{d_i \in \mathbf{d}_{\mathbf{p^I}}} \quad & U_i^{PI} = r_i d_i - \omega_i h(R_i) {d_i}^2 - \beta d_i \\ s.t. \quad & U_i^{PI} > 0 \\ & R_i \geq R \end{aligned} \tag{12}$$

where $h(\cdot)$ is defined in (2). Firstly, the utility function should be greater than 0, because every participant is rational. Secondly, there is a requirement in the sensing task description which indicates the participants' reputation to fulfil R. (12) is concave maximisation problem in strategy space $[d_{min}, d_{max}]$. According to the derivation of d_i, the optimal ${d_i}^*$ is

$${d_i}^* = \frac{r_i - \beta}{2 w_i h(R_i)} \tag{13}$$

The optimal strategy profile of sensory data size $d_i^*(r_i)$ of instant-pay participant i obtains, which is a subgame perfect equilibrium. This work assumes that the task initiator will set a minimum sensory data size d_{min} for every participant and participants' sensing ability is fixed which is not more than d^{max}.

C. Stage II: Task initiator's strategy profile

Given salary plan $\mathbf{r}_{\mathbf{p^M}}$ of monthly-pay participants, task initiator aims to maximise his profit by deciding the equilibrium strategy profile of reward $\mathbf{r}_{\mathbf{p^I}}$ for instant-pay participants and the strategy profile of the sensory data size $\mathbf{d}_{\mathbf{d^M}}$ for monthly-pay participants. Since the salary plan of monthly-pay participants is given, the sensory data size of them obtains. According to (3), (6) and (7)

$$\begin{aligned} \max_{r_i \in \mathbf{r}_{\mathbf{p^I}}, d_j \in \mathbf{d}_{\mathbf{p^M}}} \quad & U^I \\ s.t. \quad & \textstyle\sum_i r_i + \sum_j r_j \leq B \\ & \textstyle\sum_i d_i + \sum_j d_j \geq D \\ & d_j \leq D_j^{max} \\ & U^I > 0 \end{aligned} \tag{14}$$

The first constraint is the total reward to all the participants is under budget B. The second constraint means that the total sensory data size is greater than the required sensory data size D. The third constraint is the sensory data of monthly-pay participants contributes can not exceed the maximum sensory data D_j^{max}. The last constraint requires the utility should not below 0. It shows the concavity of (14) and the convexity of the constraints. Thus it is a concave maximisation problem. Given monthly-pay participants' strategy r_j and the optimal data strategy ${d_i}^*$ of instant-pay participants from (13), the Lagrange function of (14) is:

$$\begin{aligned} &\mathcal{L}(\mathbf{r}_{\mathbf{p^I}}, \mathbf{d}_{\mathbf{p^M}}, \lambda, \mu, \kappa_{\mathbf{p^M}}) \\ &= -\sum_{i \in \mathbf{p^I}} \frac{r_i(r_i - \beta)}{2 w_i h(R_i)} - \sum_{j \in \mathbf{p^M}} r_j d_j + \Big(\sum_{i \in \mathbf{p^I}} \frac{r_i - \beta}{2 w_i h(R_i)} h(R_i) \\ &\quad + \sum_{j \in \mathbf{p^M}} \eta {d_j}^2 h(R_j)\Big) + \lambda\Big(B - \sum_{i \in \mathbf{p^I}} r_i - \sum_{j \in \mathbf{p^M}} r_j\Big) \\ &\quad + \mu\Big(\sum_{i \in \mathbf{p^I}} \frac{r_i - \beta}{2 w_i h(R_i)} + \sum_{j \in \mathbf{p^M}} d_j - D\Big) + \sum_{j \in \mathbf{p^M}} \kappa_j (D_j^{max} - d_j) \end{aligned} \tag{15}$$

where λ, μ and $\kappa_{\mathbf{p^M}}$ are non-negative Lagrange multipliers associated with constraints in (14). According to (15), we can solve r_i and d_j from (14) by the derivations of all the r_i and all the d_j, respectively.

By adopting Karush Kuhn Tucker (KKT) conditions [40], the optimal strategy profile of instant-pay participants' reward ${\mathbf{r}_{\mathbf{p^I}}}^*(r_j)$ and ${\mathbf{d}_{\mathbf{p^M}}}^*(r_j)$ can be obtained by solving linear equations. The results depend on r_j from Stage I. The subgame perfect equilibrium can be derived by obtaining the optimal value in Stage II.

Lemma 1. In Stage II, given the strategy $\mathbf{r}_{\mathbf{p^M}}$ of monthly-pay participants, the task initiator's optimal strategy can be obtained.

The solution of Stage II and proof of Lemma 1 can be found in Appendix. A.

D. Stage I: monthly-pay participants' strategy profile

In Stage I, given the monthly-pay sensory data strategy of $\mathbf{d}_{\mathbf{p^M}}(\mathbf{r}_{\mathbf{p^M}})$, monthly-pay participants will adjust their salary strategy $\mathbf{r}_{\mathbf{p^M}}$ to maximise their profit function. According to (3), that is

$$\begin{aligned} \max_{r_j \in \mathbf{r}_{\mathbf{p^M}}} \quad & U_j^{PM} = r_j d_j - \omega_j h(R_j) d_j - \beta d_j \\ s.t. \quad & U_j^{PM} > 0 \\ & R_j \geq R_{\mathbb{I}}^b \end{aligned} \tag{16}$$

where $h(\cdot)$ is defined in (2). According to equation (28), the optimal data size strategy $\mathbf{d_{p^M}}^*(r_j)$ of monthly-pay participant is an increasing function on r_j, as a result, the objective function in (16) is convex. Due to the constraints, the optimal salary strategy for monthly-pay participants can be obtained.

Lemma 2. In Stage I, the strategy $\mathbf{r_{p^M}}$ of monthly-pay participants satisfies

$$U_j(\mathbf{r}^*_{\mathbf{p^M}}) \geq U_j(r_j, \mathbf{r}^*_{-j}) \tag{17}$$

By analysing the optimal strategy $\mathbf{d_{p^M}}^*$ in equation (28), the salary of one monthly-pay participant relates with all the other monthly-pay participants. This indicates that the subgame in Stage I is a cooperative game, which means the co-workers (monthly-pay participants) work in the union form and fight for each other for a better salary. The optimal strategy $\mathbf{r_{p^M}}^*$ can be achieved.

- When $d_j^* = D_j^{max}$, the objective function is an increasing function, thus $r_j^* = r_j^{max}$.
- When $d_j^* = \frac{r_j}{2h(R_j)}$, the objective function is

$$U_j^{PM} = \frac{r_j^2}{2h(R_j)} - \omega_j h(R_j)\frac{r_j}{2h(R_j)} - \beta\frac{r_j}{2h(R_j)}$$

  and it is concave, thus $r_j^* = r_j^{max}$.
- When $d_j^* = \xi(D - \tau + \sum_{i\in\mathbf{p^L}} A_i \sum_{j\in\mathbf{p^M}} r_j + \sum_{j\in\mathbf{p^M}} \frac{r_j - r_{j-1}}{2h(R_{j-1})})$, d_j^* is a function on $\sum_j r_j$, which is $d_j^* = \sum_j r_j$. The objective function is a binary primary concave function, at the same time the constant terms are all greater than zero. Thus r_j^* is in the range of $[r_j^{min}, r_j^{max}]$.

Thus the optimal strategy ${r_j}^*$ of monthly-pay participants of Stage I can be obtained. The subgame equilibrium of Stage I can be reached in the situations above.

E. Existence and uniqueness of Nash equilibrium

Theorem 1. *(Existence of subgame perfect equilibrium)* Every finite extensive game with perfect information has a subgame equilibrium.

Proof 1. The proposed three-stage Stackelberg game is an extensive game with all the given information, also it is with a finite strategy space, such as $[d_{min}, d_{max}]$ and $[r_{min}, r_{max}]$. Thus the subgame equilibrium can be obtained.

Theorem 2. *(Existence of Stackelberg Equilibrium)* There exists Stackelberg equilibrium in the proposed three-stage game.

Proof 2. The existence of Stackelberg equilibrium depends on the subgame perfect equilibrium. In the proposed three-stage game, the set of subgame perfect equilibria of a finite strategy space extensive game with perfect information is equal to the set of strategy profiles isolated by the procedure of backward induction [39]. According to the analysis of the proposed three-stage game, Stackelberg equilibrium can be obtained.

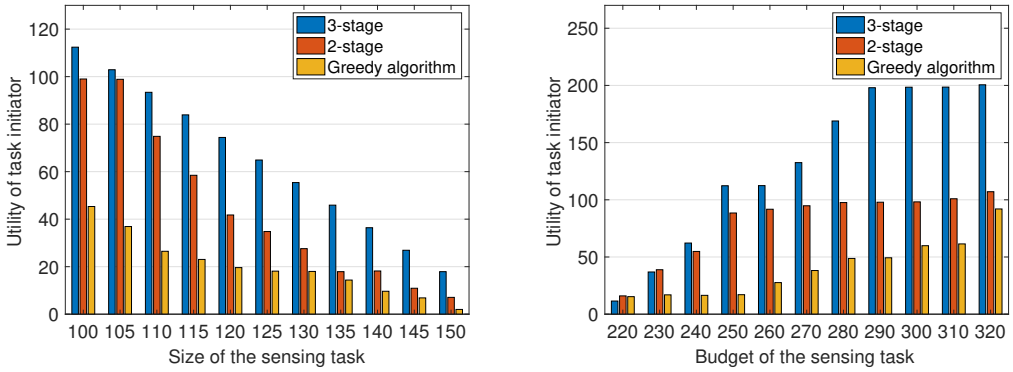
VI. SIMULATION

This section presents the simulation results of the proposed framework in two aspects. We first evaluate the three-stage Stackelberg algorithms. And then the performance of blockchain-based MCS architecture is assessed by Ethereum testnet.

A. Incentive mechanism performance analysis

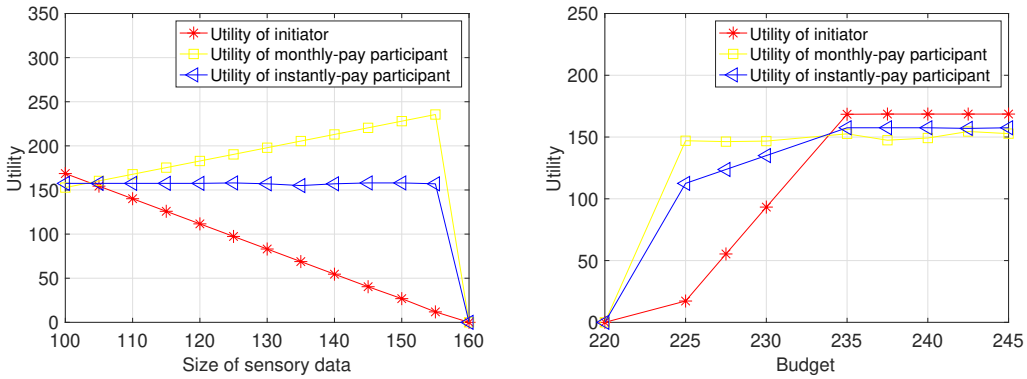
To benchmark the performance of the proposed algorithm, we implement the traditional Stackelberg algorithm [11] and the greedy reward allocation algorithm. Notice that the traditional Stackelberg algorithm takes only one kind of participants, and the greedy algorithm is centralized. We show the dynamics of the task initiator's utility in terms of different sensory data requirement with limited budget. Fig. 4(a) shows that when the size of the sensing task increases, the task initiator's utility decreases slower than 2-stage and the greedy algorithm. Fig. 4(b) demonstrates the three different algorithms with different budget and the same size of sensing task. We observe that when the budget increases, the proposed algorithm can achieve higher initiator's utility. It can provide the sensory data market with a reasonable pricing strategy, which leads the system to a better utility. To investigate the impact of sensory data size and budget, we then implement the simulations with different size of sensory data requirement B in Fig. 5(a). We see that when the size of the sensing task increases, the task initiator's utility decreases. However the utility of monthly-pay participants increases. There is a joint point when the size is 105 MB, which means the equilibrium point in this setting of the simulation. When the size of the sensing task is too big, there is not enough budget, which makes the utilities become zero. We also implement the simulations with different budget D in Fig. 5(b). We see that when the budget increases, the utilities become stable. Because the computation ability of the participants is bounded.

Fig. 6(a) demonstrates the domination of monthly-pay participants in the proposed sensory data market considering a scenario with different CPU ability w_j of monthly-pay participants. With higher CPU ability, the sensing cost will increase for monthly-pay participants, then more instant-pay participants will join the sensing task. However, because of the "first mover's advantage" of monthly-pay participants, they will still dominate the sensory data market. For a further understanding of the "first-mover advantage" and the sensory data market share, this paper evaluates the proposed model with different ratio of monthly-pay participants and instant-pay participants considering 20 participants in this scenario with sensory data amount of 50MB, 60MB and 70MB. As shown in Fig. 6(b), when the ratio increases, the task initiator's utility gradually increases. However, with a small sensory data amount requirement, the utility stays stable at some point. The result is because the ratio of participants is sufficient for the specific scenario. To verify that the proposed algorithms can reach convergent, we further the dynamic of the reward for participants in Fig. 7. There are 20 participants with 500 units of reward and 200 units of sensory data. The proposed algorithm obtains the optimal reward strategy within



(a) With different sensory data size D (b) With different budget B

Fig. 4. Utility of task initiator



(a) With different sensory data size D (b) With different budget B

Fig. 5. Utilities of participants and the task initiator

ten iterations. The result of the simulation infers the feasibility of the proposed strategy in real life.

B. Blockchain performance analysis

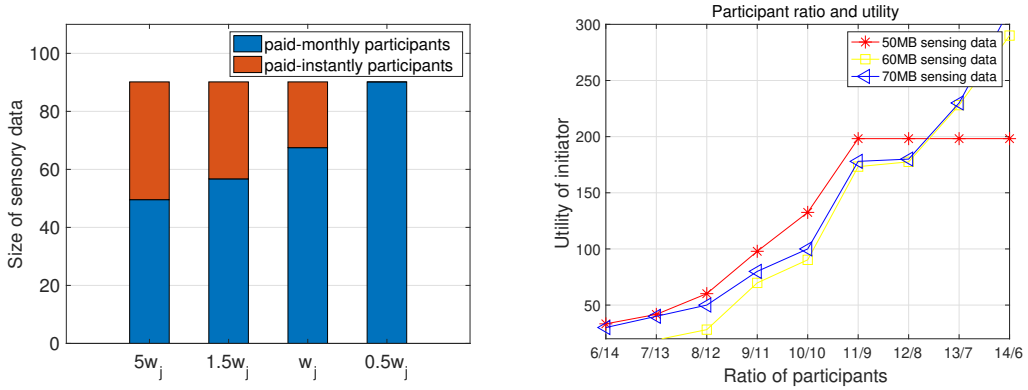
Previous simulations on mobile devices based blockchain have been done in [41]. In this section, the performance of the proposed blockchain-based MCS has been presented. We implemented the Ethereum testnet on a computer with Intel Core i5 CPU @ 1.3 GHz and 4 GB of RAM. The simulation considers a blockchain-based MCS including different numbers of the monthly-pay participants and instant-pay participants, three miner, and one task initiator, which makes the topology of the MCS. In this topology, every participant can communicate with the miner and each other.

Firstly miners will run the **Registration contract** to register all the participants, including monthly-pay/instant-pay participants and task initiator. Secondly, after the miners consent the participants' identities by consensus mechanism, The miners will broadcast the sensing task and run the **Participant profile contract** and the **Sensing task contract** to negotiate with task initiator. Thirdly all the miners will run the **Profit evaluation contract** to compute their optimal strategy individually and execute the sensing task by the **Sensing task execution contract**. At last, the miners will run the **Reward allocation contract** to compensate all the participants. Periodically, the miners will verify all the transactions and build a new block. As shown in Fig. 8, we deploy the contracts of the blockchain-based MCS framework, including the key functions, such as system initialization, verification, the three-stage game algorithms, and mining. It demonstrates the proposed framework with a different number of participants. With the expansion, the proposed framework still shows a tolerable latency of each function.

VII. Future Challenges

Blockchain technology has shown significant influence in the Internet of Things, Internet of Vehicles and Mobile Crowdsensing with the advantages of decentralisation, trustworthiness, traceability, flexibility and so on. However, there are still open issues need to be considered in the future when adopting blockchain technology into MCS.

The Computation overhead of Blockchain-based MCS. Mobile devices work as sensors in the MCS with limited power supplement, computation capacity and storage, with complex communication networks conditions at the same time. For the sensing and personal data privacy, blockchain will adopt more complicated cryptographic algorithms to resolve the issue, which mobile devices could not afford. Xiong et al. [42] considered edge computing as the network enabler for mobile blockchain. However, this work focused mostly on the pricing



(a) Monthly-pay participants with different computation ability w_j

(b) With different ratio of participants in the sensory data market

Fig. 6. Market share in blockchain-based MCS

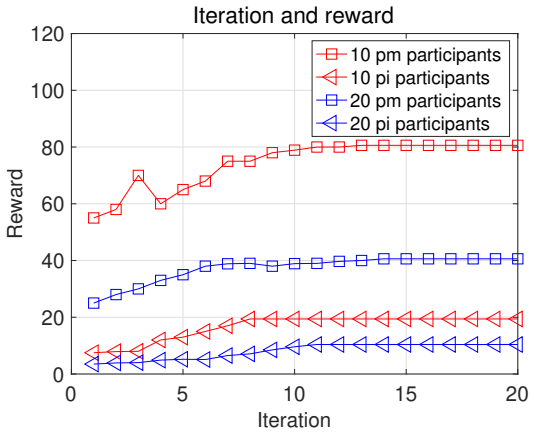


Fig. 7. The convergence of the proposed algorithm

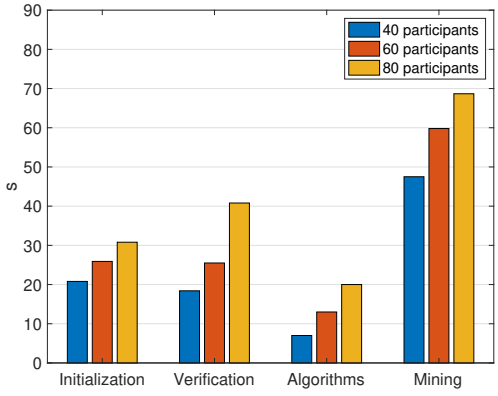


Fig. 8. The latency of blockchain-based MCS

scheme of edge computing resources, but not the details in cooperation with blockchain technology. Moreover, MCS requires real-time sensory data, which also enhance the need for high computation capacity. The challenge is improving the performance of the blockchain-based MCS without sacrificing the security feature of the system.

Privacy and trustworthiness of blockchain-based MCS. Although MCS is a novel form of traditional IoT, it has unique features, such as the selfishness, mobility, intelligence of the users of the mobile devices. These features add more requirements when it comes to privacy guarantee. In future research, dynamic access control is a crucial function to guarantee the security in blockchain-based MCS where mobile devices users may join the sensing task anytime and anywhere, due to mobility.

Human-in-the-loop framework. MCS is a human-centric sensing framework. With the feature of automation in blockchain, the human-centric feature can drift the framework from autonomy to intelligence by leveraging human-in-the-loop. For example, by designing a human-centric trust model [43], an MCS funded by grass-rooted participants can perform services like an expert.

Sensory data market. MCS needs rational incentive mechanisms to stimulate mobile devices users to participate in sensing tasks. Pricing the sensory data is one of the essential incentive mechanism in MCS. According to the applications of blockchain-based cryptocurrencies, such as bitcoin, a blockchain-based sensory data market will make sure that the pricing scheme is fair and secure.

Trade-off among performance, security and resource. An MCS application requires real-time sensory data from more participants, which requires higher performance from a blockchain-based MCS when participants increase. To achieve high performance and efficient resource allocates while maintaining a high security level for the system is a crucial task in blockchain-based MCS. Initial attempt has been made by Wang et al. [44]. This work proposed asynchronous consensus zones to scale blockchain system linearly without compromising security.

VIII. Conclusion

The work presented in this paper has two main contributions towards solving the challenges of MCS. Firstly, it proposes a blockchain-based MCS framework with a novel set of smart contracts. Secondly, this work designs a three-stage Stackelberg game to maintain the number of participants by considering this MCS scenario as a sensory data market. In the three-

stage Stackelberg game, the participants are classified into monthly-pay participants and instant-pay participants. This allows the monthly-pay participants to have a guarantee of the sustainable contribution of the sensory data. Furthermore, the game preserves the fairness of the sensory data market in cooperation with a secure reward allocation scheme aided by blockchain technology.

The simulation of the proposed blockchain-based MCS framework is twofold. Firstly, we simulate the performance of the three-stage game. In terms of the utility of the task initiator, the improvement of the proposed reward strategy ranges from two to ten percent, under the same participants' reputation, compared with the two-stage game. It also ranges from 2 to 20 percent comparing with the average reward strategy. It can also maintain the required market share for monthly-pay participants whilst achieving sustainable sensory data provision. Secondly, we simulate the performance of the block-based MCS with a set of smart contracts to prove the feasibility of the proposed work. Finally, this paper also discusses the future challenges in the cooperation of blockchain technology and MCS to enlighten future works.

Currently, the bottleneck of blockchain deployment is the consensus mechanism. Consensus mechanisms, such as the computationally-intensive PoW, Byzantine Fault Tolerance (BFT), can not support large numbers of IoT devices. So in future work, we will study the consensus mechanism of blockchain to support improved efficiency and scalability.

APPENDIX A
PROOF OF LEMMA 1

Based on Lagrange function (15) and according to KKT conditions, it follows

$$r_i \frac{\partial \mathcal{L}}{\partial (r_i)} = 0; \quad \frac{\partial \mathcal{L}}{\partial (r_i)} \leq 0; \quad r_i \geq 0 \tag{18}$$

$$d_j \frac{\partial \mathcal{L}}{\partial (d_j)} = 0; \quad \frac{\partial \mathcal{L}}{\partial (d_j)} \leq 0; \quad d_j \geq 0 \tag{19}$$

$$\lambda(\sum_{i\in\mathbf{p^L}} r_i + \sum_{j\in\mathbf{p^M}} r_j - B) = 0;$$
$$\sum_{i\in\mathbf{p^L}} r_i + \sum_{j\in\mathbf{p^M}} r_j - B \leq 0; \quad \lambda \geq 0 \tag{20}$$

$$\mu(A\sum_{i\in\mathbf{p^L}} r_i - \beta + \sum_{j\in\mathbf{p^M}} d_j - D^b) = 0;$$
$$A\sum_{i\in\mathbf{p^L}} (r_i - \beta) + \sum_{j\in\mathbf{p^M}} d_j - D^b \leq 0; \quad \mu \geq 0 \tag{21}$$

$$\sum_{j\in\mathbf{p^M}} \kappa_j (D_j^{max} - d_j) = 0;$$
$$D_j^{max} - d_j \leq 0; \sum_{j\in\mathbf{p^M}} \kappa_j \geq 0 \tag{22}$$

where (18), (19), (20) and (21) denote the complementary slackness condition, and (23), (24) are the first-order derivative conditions of (15) with respect to r_i and d_j, respectively.

$$\frac{\partial \mathcal{L}}{\partial r_i} = A_i h(R_i) - A_i(2r_i - \beta) - \lambda + \mu A_i \tag{23}$$
$$\frac{\partial \mathcal{L}}{\partial r_{i-1}} = A_{i-1} h(R_{i-1}) - A_{i-1}(2r_{i-1} - \beta) - \lambda + \mu A_{i-1}$$
$$\vdots$$
$$\frac{\partial \mathcal{L}}{\partial d_j} = 2d_j h(R_j) - r_j + \mu - \kappa_j \tag{24}$$
$$\frac{\partial \mathcal{L}}{\partial d_{j-1}} = 2d_{j-1} h(R_{j-1}) - r_{j-1} + \mu - \kappa_{j-1}$$
$$\vdots$$
$$\frac{\partial \mathcal{L}}{\partial \lambda} = \sum_{i\in\mathbf{p^L}} r_i + \sum_{j\in\mathbf{p^M}} r_j - B \tag{25}$$
$$\frac{\partial \mathcal{L}}{\partial \mu} = \sum_{i\in\mathbf{p^L}} A_i(r_i - \beta) + \sum_{j\in\mathbf{p^M}} d_j - D \tag{26}$$
$$\frac{\partial \mathcal{L}}{\partial \kappa_j} = D_j^{max} - d_j \tag{27}$$
$$\frac{\partial \mathcal{L}}{\partial \kappa_{j-1}} = D_{j-1}^{max} - d_{j-1}$$
$$\vdots$$

where $\frac{1}{2w_i h(R_i)} = A_i$. And then we will look for the interior solutions when

- when $\mu = 0$, $\kappa_j = 0$, and $\lambda = 0$, by solving the equations above, we can obtain the optimal strategy
$$r_i{}^* = \frac{1}{2}(h(R_i) + \beta)$$
$$d_j{}^* = \frac{r_j}{2h_j}$$
when $\sum_{j\in\mathbf{p^M}} r_j \in [0, \phi]$.
And when $\mu = 0$, $\kappa_j = 0$, and $\lambda \geq 0$, we can obtain the optimal strategy
$$\sum_{i\in\mathbf{p^L}} r_i{}^* = B - \sum_{j\in\mathbf{p^M}} r_j$$
$$d_j{}^* = \frac{r_j}{2h_j}$$
when $\sum_{j\in\mathbf{p^M}} r_j \in (\psi, \sum_{j\in\mathbf{p^M}} r_j^{max})$.
- when $\mu > 0$, $\kappa_j \geq 0$, and $\lambda = 0$, by solving the equations above, we can obtain the optimal strategy
$$r_i{}^* = \frac{1}{2}(h(R_i) + \beta)$$
$$d_j{}^* = D_j^{max}$$
when $\sum_{j\in\mathbf{p^M}} r_j \in (0, \psi)$.
And when $\mu = 0$, $\kappa_j = 0$, and $\lambda \geq 0$, we can obtain the optimal strategy
$$r_i{}^* = w_i[D - \sum_{j\in\mathbf{p^M}} D_j^{max} - \frac{1}{4w_i}\sum_{i\in\mathbf{p^L}} (h(R_{i-1}) - h(R_i))]$$
$$d_j{}^* = D_j^{max}$$

when $\sum_{j\in\mathbf{p^M}} r_j \in (\psi, \sum_{j\in\mathbf{p^M}} r_j^{max})$.

- When $\mu > 0$, $\kappa_j = 0$, and $\lambda = 0$, there is no solution for this optimisation problem.
  And when $\mu > 0$, $\kappa_j = 0$, and $\lambda \geq 0$, we can obtain the optimal strategy

$$r_i{}^* = w_i[D - \sum_{j\in\mathbf{p^M}} D_j^{max} - \frac{1}{4w_i}\sum_{i\in\mathbf{p^L}}(h(R_{i-1}) - h(R_i))]$$
$$d_j{}^* = \xi(D - \tau + \sum_{i\in\mathbf{p^L}} A_i \sum_{j\in\mathbf{p^M}} r_j + \sum_{j\in\mathbf{p^M}} \frac{r_j - r_{j-1}}{2h(R_{j-1})})$$

  when $\sum_{j\in\mathbf{p^M}} r_j \in (\varphi, \sum_{j\in\mathbf{p^M}} r_j^{max})$.
- When $\mu > 0$, $\kappa_j \geq 0$, and no matter $\lambda = 0$ or $\lambda \geq 0$, we can obtain the optimal strategy

$$r_i{}^* = \frac{1}{4}[2(B - \sum_{j\in\mathbf{p^M}} r_j) - \sum_{i\in\mathbf{p^L}}(h(R_{i-1}) - h(R_i))]$$
$$d_j{}^* = D_j^{max}$$

  when $\sum_{j\in\mathbf{p^M}} r_j \in (\psi, \sum_{j\in\mathbf{p^M}} r_j^{max})$.

We can obtain the result

$$d_j^* = \begin{cases} D_j^{max} & \text{if} \quad \sum_{j\in\mathbf{p^M}} r_j \in (0,\phi)(\psi, \sum_{j\in\mathbf{p^M}} r_j^{max}); \\ \frac{r_j}{2h(R_j)} & \text{if} \quad \sum_{j\in\mathbf{p^M}} r_j \in (\psi, \sum_{j\in\mathbf{p^M}} r_j^{max}); \\ \xi(D - \tau + \sum_{i\in\mathbf{p^L}} A_i \sum_{j\in\mathbf{p^M}} r_j + \sum_{j\in\mathbf{p^M}} \frac{r_j - r_{j-1}}{2h(R_{j-1})}) & \\ \quad \text{if} \quad \sum_{j\in\mathbf{p^M}} r_j \in (\varphi, \sum_{j\in\mathbf{p^M}} r_j^{max}) & \end{cases} \tag{28}$$

$$r_i^* = \begin{cases} \frac{h(R_i)}{2} & \text{if} \quad \sum_{j\in\mathbf{p^M}} r_j \in (0,\phi); \\ \frac{1}{4}[2(B - \sum_{j\in\mathbf{p^M}} r_j) - \sum_{i\in\mathbf{p^L}}(h(R_{i-1}) - h(R_i))] & \\ \quad \text{if} \quad \sum_{j\in\mathbf{p^M}} r_j \in (\psi, \sum_{j\in\mathbf{p^M}} r_j^{max}); & \\ w_i[D - \sum_{j\in\mathbf{p^M}} D_j^{max} - \frac{1}{4w_i}\sum_{i\in\mathbf{p^L}}(h(R_{i-1}) - h(R_i))] & \\ \quad \text{if} \quad \sum_{j\in\mathbf{p^M}} r_j \in (\varphi, \sum_{j\in\mathbf{p^M}} r_j^{max}) & \end{cases} \tag{29}$$

where

$$\begin{aligned} \xi &= \frac{1}{1 + h(R_j)\sum_{j\in\mathbf{p^M}} \frac{1}{h(R_{j-1})}} \\ \tau &= B\sum_{i\in\mathbf{p^L}} A_i - \sum_{i\in\mathbf{p^L}} A_i\beta \\ \phi &= 2\sum_{j\in\mathbf{p^M}} h_j D_j^{max} \\ \psi &= B - \frac{1}{2}\sum_{i\in\mathbf{p^L}} h_i \\ \varphi &= \sum_{j\in\mathbf{p^M}} \frac{1}{h(R_j)}(D - \frac{1}{4w_i}\sum_{i\in\mathbf{p^L}} h_i) \end{aligned} \tag{30}$$

Until now, this lemma is proved.

ACKNOWLEDGMENT

This work was carried out within the project SerIoT, which has received funding from the European Union???s Horizon 2020 Research and Innovation programme under grant agreement No 780139.

REFERENCES

[1] Fei-Yue Wang. The emergence of intelligent enterprises: From cps to cpss. *IEEE Intelligent Systems*, 25(4):85–88, 2010.
[2] Nikolaos Vastardis and Kun Yang. Mobile social networks: Architectures, social properties, and key research challenges. *IEEE Communications Surveys & Tutorials*, 15(3):1355–1371, 2012.
[3] Rüdiger Pryss, Manfred Reichert, Jochen Herrmann, Berthold Langguth, and Winfried Schlee. Mobile crowd sensing in clinical and psychological trials–a case study. In *2015 IEEE 28th International Symposium on Computer-Based Medical Systems*, pages 23–24. IEEE, 2015.
[4] Pengfei Zhou, Yuanqing Zheng, and Mo Li. How long to wait?: predicting bus arrival time with mobile phone based participatory sensing. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, pages 379–392. ACM, 2012.
[5] Yoshito Tobe, Itaru Usami, Yusuke Kobana, Junji Takahashi, Guillaume Lopez, and Niwat Thepvilojanapong. vcity map: Crowdsensing towards visible cities. In *SENSORS, 2014 IEEE*, pages 17–20. IEEE, 2014.
[6] Francesco Calabrese, Massimo Colonna, Piero Lovisolo, Dario Parata, and Carlo Ratti. Real-time urban monitoring using cell phones: A case study in rome. *IEEE Transactions on Intelligent Transportation Systems*, 12(1):141–151, 2011.
[7] Carmen Fishwick. Tomnod–the online search party looking for malaysian airlines flight mh370. *The Guardian*, 14:37, 2014.
[8] Jinwei Liu, Haiying Shen, Lei Yu, Husnu Saner Narman, Jiannan Zhai, Jason O Hallstrom, and Yangyang He. Characterizing data deliverability of greedy routing in wireless sensor networks. *IEEE Transactions on Mobile Computing*, 17(3):543–559, 2018.
[9] Luis G Jaimes, Idalides J Vergara-Laurens, and Andrew Raij. A survey of incentive techniques for mobile crowd sensing. *IEEE Internet of Things Journal*, 2(5):370–380, 2015.
[10] Zheng Song, Chi Harold Liu, Jie Wu, Jian Ma, and Wendong Wang. Qoi-aware multitask-oriented dynamic participant selection with budget constraints. *IEEE Transactions on Vehicular Technology*, 63(9):4618–4632, 2014.
[11] Jiejun Hu, Kun Yang, Liang Hu, and Kezhi Wang. Reward-aided sensing task execution in mobile crowdsensing enabled by energy harvesting. *IEEE Access*, 2018.
[12] Kezhi Wang, Kun Yang, and Chathura Sarathchandra Magurawalage. Joint energy minimization and resource allocation in c-ran with mobile cloud. *IEEE Transactions on Cloud Computing*, 6(3):760–770, 2016.
[13] Kun Yang, Shumao Ou, and Hsiao-Hwa Chen. On effective offloading services for resource-constrained mobile devices running heavier mobile internet applications. *IEEE communications magazine*, 46(1):56–63, 2008.

[14] Cong Zhao, Shusen Yang, Ping Yan, Qing Yang, Xinyu Yang, and Julie McCann. Data quality guarantee for credible caching device selection in mobile crowdsensing systems. *IEEE Wireless Communications*, 25(3):58–64, 2018.

[15] Haoyi Xiong, Daqing Zhang, Guanling Chen, Leye Wang, and Vincent Gauthier. Crowdtasker: Maximizing coverage quality in piggyback crowdsensing under budget constraint. In *2015 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 55–62. IEEE, 2015.

[16] Satoshi Nakamoto. Bitcoin v0. 1 released. *The Mail Archive*, 9, 2009.

[17] Melanie Swan. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[18] Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 2017.

[19] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[20] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, and Helge Janicke. Blockchain technologies for the internet of things: Research issues and challenges. *arXiv preprint arXiv:1806.09099*, 2018.

[21] Nir Kshetri. Can blockchain strengthen the internet of things? *IT Professional*, 19(4):68–72, 2017.

[22] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *Ieee Access*, 4:2292–2303, 2016.

[23] Olivier Alphand, Michele Amoretti, Timothy Claeys, Simone Dall'Asta, Andrzej Duda, Gianluigi Ferrari, Franck Rousseau, Bernard Tourancheau, Luca Veltri, and Francesco Zanichelli. Iotchain: A blockchain security architecture for the internet of things. In *Wireless Communications and Networking Conference (WCNC), 2018 IEEE*, pages 1–6. IEEE, 2018.

[24] Yu Zhang and Jiangtao Wen. The iot electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, 10(4):983–994, 2017.

[25] Bin Cao, Yixin Li, Lei Zhang, Long Zhang, Shahid Mumtaz, Zhenyu Zhou, and Mugen Peng. When internet of things meets blockchain: challenges in distributed consensus. *arXiv preprint arXiv:1905.06022*, 2019.

[26] Ming Li, Jian Weng, Anjia Yang, Wei Lu, Yue Zhang, Lin Hou, Jia-Nan Liu, Yang Xiang, and Robert H Deng. Crowdbc: A blockchain-based decentralized framework for crowdsourcing. *IACR Cryptol. ePrint Arch., Univ. California, Santa Barbara, Santa Barbara, CA, USA, Tech. Rep*, 444:2017, 2017.

[27] Jingzhong Wang, Mengru Li, Yunhua He, Hong Li, Ke Xiao, and Chao Wang. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. *IEEE Access*, 6:17545–17556, 2018.

[28] Sergi Delgado-Segura, Cristian Tanas, and Jordi Herrera-Joancomartí. Reputation and reward: two sides of the same bitcoin. *Sensors*, 16(6):776, 2016.

[29] Dimitris Chatzopoulos, Sujit Gujar, Boi Faltings, and Pan Hui. Privacy preserving and cost optimal mobile crowdsensing using smart contracts on blockchain. *arXiv preprint arXiv:1808.04056*, 2018.

[30] Shaohan Feng, Wenbo Wang, Dusit Niyato, Dong In Kim, and Ping Wang. Competitive data trading in wireless-powered internet of things (iot) crowdsensing systems with blockchain. *arXiv preprint arXiv:1808.10217*, 2018.

[31] Chengjun Cai, Yifeng Zheng, and Cong Wang. Leveraging crowdsensed data streams to discover and sell knowledge: A secure and efficient realization. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pages 589–599. IEEE, 2018.

[32] Fengrui Shi, Zhijin Qin, Di Wu, and Julie McCann. Mpcstoken: Smart contract enabled fault-tolerant incentivisation for mobile p2p crowd services. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pages 961–971. IEEE, 2018.

[33] Bing Jia, Tao Zhou, Wuyungerile Li, Zhenchang Liu, and Jiantao Zhang. A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. *Sensors*, 18(11):3894, 2018.

[34] Hamed Shah-Mansouri, Vincent WS Wong, and Jianwei Huang. An incentive framework for mobile data offloading market under price competition. *IEEE Transactions on Mobile Computing*, 16(11):2983–2999, 2017.

[35] Maryam Pouryazdan, Burak Kantarci, Tolga Soyata, Luca Foschini, and Houbing Song. Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing. *IEEE Access*, 5:1382–1397, 2017.

[36] Tony T Luo, Salil S Kanhere, Jianwei Huang, Sajal K Das, and Fan Wu. Sustainable incentives for mobile crowdsensing. *arXiv preprint arXiv:1701.00248*, 2017.

[37] Heinrich Von Stackelberg. *Market structure and equilibrium*. Springer Science & Business Media, 2010.

[38] Ju Ren, Yaoxue Zhang, Kuan Zhang, and Xuemin Sherman Shen. Sacrm: Social aware crowdsourcing with reputation management in mobile sensing. *Computer Communications*, 65:55–65, 2015.

[39] Martin J Osborne et al. *An introduction to game theory*. Oxford university press New York, 2004.

[40] David Gale, Harold W Kuhn, and Albert W Tucker. Linear programming and the theory of games. *Activity analysis of production and allocation*, 13:317–335, 1951.

[41] Kongrath Suankaewmanee, Dinh Thai Hoang, Dusit Niyato, Suttinee Sawadsitang, Ping Wang, and Zhu Han. Performance analysis and application of mobile blockchain. In *2018 international conference on computing, networking and communications (ICNC)*, pages 642–646. IEEE, 2018.

[42] Zehui Xiong, Shaohan Feng, Dusit Niyato, Ping Wang, and Zhu Han. Optimal pricing-based edge computing resource management in mobile blockchain. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.

[43] Bin Yu, Jarod Wright, Surya Nepal, Liming Zhu, Joseph Liu, and Rajiv Ranjan. Iotchain: Establishing trust in the internet of things ecosystem using blockchain. *IEEE Cloud Computing*, 5(4):12–23, 2018.

[44] Jiaping Wang and Hao Wang. Monoxide: Scale out blockchains with asynchronous consensus zones. In *16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19)*, pages 95–112, 2019.

Jiejun Hu received her Ph.D. and MSc in the School of Computer Science and Technology of Jilin University, China, in 2019 and 2015, respectively. Currently she is a senior research officer in the University of Essex, UK. Her research areas are mobile crowdsensing, communication networks, future network and technology, blockchain and network security.

Kun Yang received his PhD from the Department of Electronic & Electrical Engineering of University College London (UCL), UK. He is currently a Chair Professor in the School of Computer Science & Electronic Engineering, University of Essex, leading the Network Convergence Laboratory (NCL), UK. Before joining in the University of Essex at 2003, he worked at UCL on several European Union (EU) research projects for several years. His main research interests include wireless networks and communications, IoT networking, data and energy integrated networks, mobile edge computing. He manages research projects funded by various sources such as UK EPSRC, EU FP7/H2020 and industries. He has published 150+ journal papers and filed 10 patents. He serves on the editorial boards of both IEEE and non-IEEE journals. He is a Senior Member of IEEE (since 2008) and a Fellow of IET (since 2009).

Kezhi Wang received his B.E. and M.E. degrees in School of Automation from Chongqing University, China, in 2008 and 2011, respectively. He received his Ph.D. degree in Engineering from the University of Warwick, U.K. in 2015. He was a Senior Research Officer in University of Essex, U.K. Currently he is a Senior Lecturer in Department of Computer and Information Sciences at Northumbria University, U.K. His research interests include wireless communications, mobile edge computing, UAV communication and machine learning.

Kai Zhang received the B.E. degree in Information and Computing Science from Anhui University of Technology, China, in 2011, and the M.E. degrees in Economics from Zhongnan University of Economics and Law, China, in 2014 and the University of Essex, U.K., in 2018. He is currently pursuing the Ph.D. degree in Economics from the University of Essex. His research interests include Game Theory and its applications, Contract Theory, Organizational Economics and Industrial Organization.