IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 31, 2017, accepted January 31, 2018, date of publication March 5, 2018, date of current version April 23, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2805837

A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications

JINGZHONG WANG[1], (Member, IEEE), MENGRU LI[1], YUNHUA HE[1], (Member, IEEE), HONG LI[2], (Member, IEEE), KE XIAO[1], AND CHAO WANG[1]

[1]Department of Computer Science, North China University of Technology, Beijing 100144, China
[2]Beijing Key Laboratory IOT Information Security Technology, Chinese Academy of Sciences, Beijing 100093, China

Corresponding author: Yunhua He (heyunhua@ncut.edu.cn)

This work was supported in part by the National Key Technology R&D Program under Grant 2017YFB0802300, in part by the Beijing Natural Science Foundation under Grant 4184085, in part by the National Natural Science Foundation of China under Grant 61702503, Grant 61602053, and Grant 61672415, in part by the Youth Science and Technology Innovation Foundation (North China University of Technology) under Grant 1473009, in part by the Dominant Discipline Construction Project (Computer Science and Technology, College of Computer Science, North China University of Technology) under Grant X2044, and in part by the International Cooperation Program of Institute of Information Engineering, CAS, under Grant Y7Z0461104.

ABSTRACT Crowdsensing applications utilize the pervasive smartphone users to collect large-scale sensing data efficiently. The quality of sensing data depends on the participation of highly skilled users. To motivate these skilled users to participate, they should receive enough rewards for compensating their resource consumption. Available incentive mechanisms mainly consider the truthfulness of the mechanism, but mostly ignore the issues of security and privacy caused by a ''trustful'' center. In this paper, we propose a privacy-preserving blockchain incentive mechanism in crowdsensing applications, in which a cryptocurrency built on blockchains is used as a secure incentive way. High quality contributors will get their payments that are recorded in transaction blocks. The miners will verify the transaction according to the sensing data assessment criteria published by the server. As the transaction information can disclose users' privacy, a node cooperation verification approach is proposed to achieve k-anonymity privacy protection. Through theoretical analysis and simulation experiments, we show the feasibility and security of our incentive mechanism.

INDEX TERMS Blockchain, crowdsensing, incentive mechanism, node cooperation, privacy-preserving, signcryption.

I. INTRODUCTION

With the proliferation of powerful sensor embedded smartphones, crowdsensing has become a leading paradigm which leverages the pervasive smartphone users to collect data efficiently. In a typical crowdsensing application, a server posts the required sensing information and recruits a set of smartphone users to collect sensing data. After smartphone users send sensing data to the server, the server aggregates the sensing data to measure phenomena of common interest, i.e., real-time traffic conditions, environmental pollution quality or environmental noise pollution.

The accuracy of estimating the common interest depends on the high quality contributions of highly skilled users. While providing the high quality contributions, smartphone users consume their energy and the resources of their smartphones such as battery, storage and computing power. In addition, users may expose themselves to potential privacy threats as the sensed data contain time or location tags. Thus, the contributors should be given enough rewards to compensate for their resource consumption or potential privacy leaks. As is known to all, a user wants to maximize her own profit, and may lie or impersonate others to get more payment. Therefore, the design of a secure and truthful incentive mechanism is particularly important.

Many incentive mechanisms have been proposed and implemented, such as the reputation systems and monetary approaches. Reputation systems [1] can help identify uncooperative users, but ignore a formal specification and analysis of the incentive types and suffer sybil attacks [2] and whitewash attacks [3]. Monetary approaches [26] could be the most promising due to their explicit and flexible incentive methods. Most monetary schemes use pricing strategies to design truthful incentive mechanisms, in which the server and smartphone users cannot increase their utility by cheating or colluding with others. While some other privacy-preserving incentive mechanisms have been proposed for protecting

users' asking price privacy. However, these schemes either rely on a central authority or do not give an explicit digital currency system which is provably secure, leading to possible system collapses or potential privacy disclosure caused by the 'trusted' center.

Blockchain cryptocurrencies are provably decentralized secure, and have gained a noticeable popularity. The security of blockchain cryptocurrencies depends on a majority of the computing power instead of a central authority, thus eliminating the risks of one taking control over the system, generating inflation, or completely shutting down the system [34]. In this paper, we exploit a blockchain cryptocurrency to incentivize high skilled users to provide valuable or effective data for crowdsensing applications.

We consider the scenario where there is one server, multiple smartphone users, and some miners in the blockchain system. When the server publishes a sensing task contained explicit evaluation criteria of sensing data quality in blockchain, it would make a certain deposit for promising to reward. The users who try to get the reward upload the sensing data to the peer-to-peer network. Instead of the server, the initiative miners are responsible for quantifying and validating the quality. After the validation, the sensing data are transferred to the server while it's hash digests are reserved in the peer-to-peer network. If someone in the blockchain doubts the miners' work of validation, then he or she can check. Even though there are some failed or offline miners, the distributed network of blockchain won't be impacted since the others can take the place of them. Finally, the high quality contributors will obtain appropriate rewards from the server. We use an extended bitcoin transaction syntax to implement a secure pricing strategy, in which the server distributes the rewards to participating users in accordance with the predefined transfer conditions in the transaction script. The transaction verification uses commutative encryptions to defend against impersonation attacks by miners. As the transaction script record who uploads data and what is the quality of the uploaded data, a node cooperation privacy protection method in the blockchain is used to protect user privacy. In the node cooperation method, the miners can determine all the sensing data from a group, but cannot distinguish the data of a group member from other $k-1$ group members. A node in the blockchain may play a 'user' role for uploading sensing data or a 'miner' role for evaluating the sensing data or verifying the transaction, even she/he could be both the roles. Our main contributions are listed as follows:

- We propose a blockchain based secure crowdsensing incentive mechanism in which the miners' verifiable data quality evaluation can eliminate the security and privacy issues caused by a central authority;
- We use an extended transaction syntax to implement a secure reward distribution in accordance with the predefined transfer conditions in the transaction script;
- We propose a node cooperation privacy protection method for participating users to achieve k-anonymity privacy protection;
- We further employ a theoretical analysis and simulation study to demonstrate the security and efficiency of our incentive mechanism.

The remainder of the paper is structured as follows. Section II outlines the related work. In Section III, we introduce a crowdsensing system model in this paper. Our blockchain based incentive scheme is detailed in Section IV, followed by a comprehensive security analysis and evaluation in Section V. The paper is concluded in Section VI.

II. RELATED WORK

The incentive mechanisms in crowdsensing application mainly include the reputation mechanism, the reciprocity mechanism and the monetary incentive mechanism [4]–[6].

The reputation mechanism is evaluated by reputation values of users [28], [29], and the users with high reputation value could get superior service. Xie *et al.* [5] used the reputation mechanism in the crowdsensing system to reject low-level workers, motivate high-level workers to participate in sensing tasks, and then achieve high-quality mission solutions. But the reputation incentive mechanism is neither specific nor susceptible for Sybil attack and Whitewashing attack. The reciprocity mechanism matches the equivalent service according to the users' contribution. But it is necessary for the reciprocity mechanism to establish long-term communication or reciprocal relationship, and it is unsuitable for some individualized crowdsensing requirements.

The monetary incentive mechanism motivates users to participate in crowdsensing tasks by electronic money. Today, monetary incentive mechanisms are centralized. Jiang *et al.* [30] proposed a quality-aware incentive mechanism (QAIM) based on the reverse auction framework to meet the quality requirement of data reliability. The incentive mechanism proposed by Peng *et al.* [6] solved the problem that the quality of sensing data is uneven and affects the quality of service of the crowdsensing network. They incorporated the consideration of data quality into the design of incentive mechanism for crowdsensing, and proposed to pay the participants as how well they do, to motivate the rational participants to perform data sensing efficiently. But the centralized incentives are dependent on trusted centers, which are hardly achieved in reality. The trusted centers not only may sell users' privacy data or involve in collusion attacks with some users for personal gain, but also are vulnerable to be attacked, once captured, will lead to confusion in the incentive mechanism.

The blockchain is a kind of distributed hyperledger with irreversibility and traceability. The Blockchain [27] based incentive mechanism is a preferred and secure distributed incentive that is primarily used for secure multiparty computation to ensure fairness currently [32]. Andrychowicz *et al.* [24] proposed a version of Bitcoin-based timed commitments: fulfill the commitment task within a limited time, or be punished if not implement commitment. They constructed protocols for secure multiparty lotteries

using the Bitcoin currency, without relying on a trusted authority. The commitment ensures that the gambler complies with the agreement to ensure the fairness of the lottery agreement. In their other work [25], Marcin extended the Bitcoin transaction syntax to support timed commitments and the modified Bitcoin currency system can be used to obtain fairness in any two-party secure computation protocol. Bentov and Kumaresan [19] proposed a more common Bitcoin incentive framework that could monetarily penalize an adversary of violating the agreement. Cecchetti *et al.* [31] presented a protocol *Solidus* for confidential transactions on public blockchains and the protocol hides both transaction values and the transaction graph while maintaining the public verifiability. Li *et al.* [33] conceptualized a blockchain-based decentralized framework for crowdsourcing named CrowdBC, in which a requester's task can be solved by a crowd of workers without relying on any third trusted institution. But the CrowdBC doesn't present the evaluation mechanism that is a decisive factor of users' participating enthusiasm and the fairness of the mechanism. Furthermore, there is no detailed implementation for the verification of miners, which may cause the impersonation attacks. For example, the miners in the public blockchain may take the to-be-verified crowdsourcing data as their own, then they could take users' payment by imitating them.

This paper is different from previous works, we proposed a blockchain based secure crowdsensing incentive mechanism in which verifiable data qualities evaluating by miners can eliminate the security and privacy issues caused by a central authority. We present a detailed process of data evaluation via the EM algorithm. In addition, we propose a node cooperation privacy protection incentive mechanism against impersonation attacks. We not only protect the privacies of sensing data and identity information, but also prevent the impersonation attacks.

III. SYSTEM MODEL AND PROBLEM DESCRIPTION

In this section, we present the model of crowdsensing. The crowdsensing system model is mainly composed by the server S and a set of participating users U, the sensing process is performed as follows [6]: 1) The server S releases sensing tasks, payment commitment and quality requirements. Participants $U = \{u_1, u_2, \ldots, u_i, \ldots, u_n\}$ carry mobile devices with embedded sensors. Each user $u_i \in U$ has an estimated sensing cost c_i, that is, the energy of u_i and the resource consumption of her smart phone. 2) The user u_i will carry out the sensing task when she estimates the sensing reward r_i is not less than the sensing cost c_i. After the task finished, u_i uploads the sensing data $Data_{u_i}$ to the server S. 3) The server S pays a certain amount of reward according to users' contribution. For each user u_i, a certain amount of reward is given according to her effective contribution which should meet the payment standard of S. So the user will get more payment if she has higher contribution, and get less payment if she has lower, even get nothing if her contribution can't meet the standard. Table 1 lists frequently used notations.

TABLE 1. Key notations.

Notation	Definition
U	Set of users
D	Set of observed sensing data
P	Set of missing true noise interval indictors
E	Set of unknown effort matrices
$L(E;P,D)$	Likelihood function of E
$\{d_1, ..., d_n\}$	Set of discrete noise intervals
r^*	Optimal quality based reward
c_i	Sensing cost of u_i
$Data_{u_i}$	Sensing data of u_i
q_{u_i}	Quality of u_i's sensing data
e^{u_i}	Effort matrix of u_i
$e^{u_i}_{lm}$	Probability that u_i submits data in interval d_m while the true interval is d_l
$d_t^{u_i}$	Noise interval that u_i's sensing data for task t falls into
$I(d_t^{u_i} = d_m)$	Indicator function for the event $d_t^{u_i} = d_m$
$\{\pi_1, ..., \pi_n\}$	Noise interval distribution
P^t	True noise interval indicator for task t
p_l^t	Probability of task t with true noise interval being d_l
$c_n(q_{u_i})$	Effective contribution of sensing data of quality q_{u_i}
V	Value gained from qualified sensing data
r_i	Reward to u_i for her contribution

But the incentive mechanism is mainly faced with the following questions.

- First, fully trusted server often does not exist in reality, the server may abuse of the information management rights and sell users' private information for the temptation of the interests, and the private information disclosure problem may reduce the enthusiasm of users;
- Second, the server S, is responsible for assessing sensing data and paying users, so the server may cheat users for minimizing the cost by paying less even nothing when taking the sensing data. This fairness problem may reduce the enthusiasm of users;
- Third, the server that holds the user information, is the most vulnerable part of the network model as the bull's-eye of adversaries. Once the server is captured by adversaries, the user information may be disclosed and the system may collapse.
- Finally, the electronic currency, token, or credits that paid by the servers may be not credible, because the currency issuers or managers may manipulate at the back for private interests.

IV. BLOCKCHAIN BASED INCENTIVE MECHANISM

In this paper, our incentive mechanism encourages users to submit high quality sensing data based the blockchain structure which is maintained by miner nodes. The distributed and traceable structure eliminates the security issues caused by

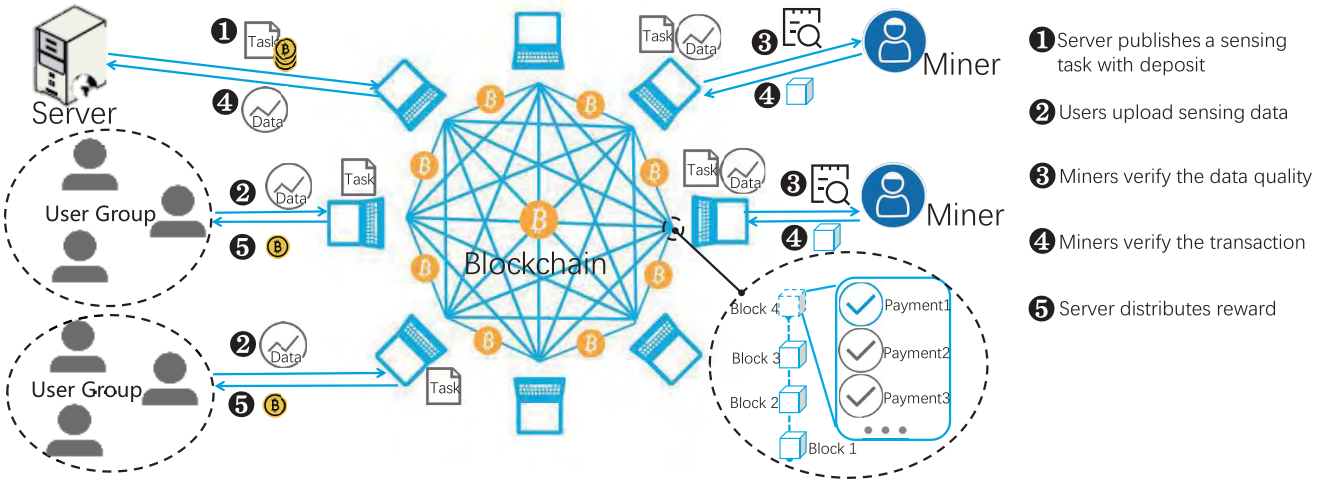


FIGURE 1. Incentive framework Based on Blockchain.

a central authority. A user gets different payment according to different data quality. The process that the user u_i uploads the sensing data and the server S pays for the data is treated as a transaction. The miners verify each new transaction and record them on the peer-to-peer network. There will be a new block to be mined out at intervals. Each block contains all the transactions occurred from the generation of last block up to now. These transactions are added to the blockchain in turn. Aforementioned process and the management of block are inspired by the transaction in blockchain [35]. We call the transaction included in the block and added to the chain as a confirmed transaction. The user u_i will receive her reward after the transaction has been confirmed. We assume there are payment rules for miners in the blockchain structure. Anyone in the blockchain could be a 'user' if she uploads the sensing data, or a 'miner' if she evaluates the data quality or the whole transaction. Thus a node may be a 'user' or 'miner' due to her work, even both of them.

We illustrate our incentive mechanism in FIGURE 1 and briefly describe it as follows. First, S releases the sensing task with evaluation criteria of the data quality, and prepays a deposit. Then the users perform the sensing task and upload the sensing data onto peer-to-peer network; miners verify the quality q_{u_i} of the sensing data with the knowledge of evaluation function achieved from S, quantify the contribution $c_{q_{u_i}}$, and determine the payment criteria r^*; the miners verify the transaction of S and the user u_i. Finally, according to the payment criteria, S pays payment r^* to the user u_i after the verifications of sensing data and user's identity passed. The new block includes the verified transaction and other transactions within a certain period. After the transaction is verified, the sensing data is sent to the server and the hash digest of the data is stored in the blockchain. Note that the work of verification in the traceable public blockchain can be checked by everyone As the miners can obtain transaction contents when verifying the data, they may launch

$Task\_Claim(\mathbf{in}: T_y)$

in - script: $Sig_{SK_S}(TaskClaim) \,||\, e^{u_{unknown}} \,||\, n \,||\, Sig(Hash(Data_{u_{unknown}})) \,||\, Data_{u_{unknown}}$

out - script:
Verify $Data_{u_{unknown}}$

$q_{u_{unknown}} = g(e^{u_{unknown}}) = \sum_l \frac{e_{ll}^{u_{unknown}}}{n}$

Verify $u_{unknown}$
$Data_{sign} = Sig(Hash(Data_{u_{unknown}}))$;
if $(Data_{u_{unknown}} = Hash(De - sign(Data_{sign})))$
return true;

value: M *coins*

time - lock: τ

FIGURE 2. Task_Claim:

an impersonation attack or collusion attacks to get payment illegally. To solve this problem, we propose a transaction verification method of the node cooperation, which will keep the user's privacy information within a group from attacking of adversaries.

A. PUBLISH A SENSING TASK WITH DEPOSIT

The sensing task is issued by the server S. We use the urban noise map data sensing [21] as an example to illustrate our incentive mechanism design. The server S creates a transaction task Task_Claim and attaches payment commitment to the transaction, in which the server releases the quality certification standard and the method of sensing data collected by users. The server S makes the corresponding commitment and grants the deposit on the transaction task [9]–[11]. The transaction tasks syntax expression is shown in FIGURE 2, and the meanings of the symbols in FIGURE 2 are as follows. $Sig_{SK_S}(Task\_Claim)$ is the signature of S to the published task to manifest the server that requests the task; The Task_Claim

attach the the method of quality estimation for user $u_{unknown}$ to *Verify* $Data_{u_{unknown}}$ by miners, and the method will be explained detailedly at Section IV-B. The user $u_{unknown}$ signs her identity information by her secret key, and the server *Verify* $u_{unknown}$ for de-signing the information by user's public key.The value M is the number of deposits paid by S. The time-lock τ is the task deadline.

B. UPLOAD SENSING DATA AND VERIFY THE QUALITY

When a user receives the Task_Claim issued by S, she evaluates the sensing cost c_i including spending time, energy cost, traffic cost, equipment computing and storage cost, etc. Then the user u_i compares sensing payment with the cost c_i and decides to participate the crowdsensing or not. In this paper, These users are commonly assumed to be rational, and would not make contributions unless there are sufficient incentives. The goal of the user u_i is to maximize their interests and minimize the cost. The profit of the user u_i is:

$$profit_{u_i} = r_i - \min_i c_i. \tag{1}$$

The user u_i performs sensing task when the expected sensing reward is more pleasurable than the cost c_i or equal it. After uploading the sensing data by u_i, the miner estimates the quality of the sensing data following the rules made by the server, that is, miners don't have to learn additional field knowledge. S takes the quality as a reference to pay for u_i. The smaller the granularity of data quality interval division is, the more accurate the estimation of quality is, and the more complex the incentive mechanism is. Because too narrow intervals can enlarge the quality estimation complexity, S will set a right granularity to maximize its benefit by weighing the accuracy and complexity. In our mechanism, S distributes payment according to the different quality, thus it encourages users to upload high-quality data.

The quality of sensing data is regarded as the value of user's sensing level, and the initiative miners estimate an effort matrix e^{u_i} for user u_i. For the noise sensing data, the estimation of the sensing quality would divide the noise into $\{d_1, d_2, \ldots, d_n\}$ intervals and the exact readings of sensing noise fall in different intervals. Each interval spans over a range of decibels. We assume it is common knowledge that the probability that uploaded data from user falls within n intervals is normal distribution. We estimate probability matrix $E_{n\times n} = \{e_{lm}^{u_i} | l = 1, 2, \ldots, n, m = 1, 2, \ldots, n\}$ that the user u_i submits sensing data in the interval d_l,$e_{lm}^{u_i} \in [0, 1]$. d_l is the smallest error interval, and the error is growing farther from d_l on the coordinate axis. We assume that the sensing level of the user u_i is constant for a certain period, so that the sensing data quality $q_{u_i} = g(e^{u_i})$ can be estimated based on the $\sum_i y_i$ sensing tasks execution.

1) QUALITY ESTIMATION

We use the expectation maximization (EM) algorithm to estimate the probability matrix e^{u_i} of the user u_i and the probabilities $p^t \in P$ of the true noise interval d_l with the highest accuracy and minimum error in each task [12]. We assume that the participants' sensing costs follow a probability distribution, with a probability distribution function $f(c_i)$, and a cumulative distribution function $F(c)$. We can asymptotically learn the distribution $f(c_{u_i}, e^{u_i})$ of sensing cost and effort matrix and we assume that the distribution is common knowledge.

Given the sensing data D, the unknown exact noise intervals P, the probability matrix E, and the probability density function f, the likelihood function of E is $L(E; P, D) = f(P, D|E)$. In order to find the maximum likelihood estimation, the EM algorithm runs the following two steps iteratively until convergence.

E-step: given observation D, current estimation E and conditional distribution P, we calculate the expected value of the likelihood function:

$$Q(E|\widehat{E}^t) = E_{P|D,\widehat{E}^t}[L(E; P, D)], \tag{2}$$

where $\widehat{E}^t$ is the current E values after t iterations.

M-step: we find the maximized estimation $\widehat{E}$ of the expectation function.

$$\widehat{E}^{t+1} = \underset{E}{\operatorname{argmax}}\, Q(E|\widehat{E}^t). \tag{3}$$

Iterate **E-step** and **M-step** until the estimation converges.

The steps of quality estimation are as follows: step 1, initialize probability distribution of the true noise interval for the task $t \in T$. $I(d_t^{u_i} = d_m) = 1$ when the perception data $d_t^{u_i}$ falls in the true interval d_m;

$$p_l^t = p(d_t^0 = d_l) = \frac{\sum_{u_i \in U_t} I(d_t^{u_i} = d_l)}{|\ U_t\ |} \tag{4}$$

The step 2, we estimate the likelihood estimation of the sensing probability matrix $e_{lm}^{u_i}$:

$$\widehat{e}_{lm}^{u_i} = \frac{\sum_{t \in T^{u_i}} p_l^t I(d_t^{u_i} = d_m)}{\sum_{t \in T^{u_i}} p_l^t}, \quad m = 1, 2, \ldots, n \tag{5}$$

The true noise interval is

$$\widehat{\pi}_l = \frac{\sum p_l^t}{|\ T\ |}, \quad l = 1, 2, \ldots, n \tag{6}$$

The step 3, we estimate the noise interval distribution. Given the sensing data D, the sensing effort matrix E, and the noise interval distribution $\{\pi_1, \ldots \pi_n\}$. We estimate the true noise interval P via the Bayesian inference, then we calculate the distribution of the true noise interval P_i^t according to the following formula:

$$p_l^t = \frac{\pi_l \prod_{u_i \subseteq U_t} \prod_m (e_{lm}^{u_i})^{I(d_t^{u_i} = d_m)}}{\sum_q \pi_q \prod_{u_i \subseteq U_t} \prod_m (e_{qm}^{u_i})^{I(d_t^{u_i} = d_m)}}, \quad i = 1, 2, \ldots, n \tag{7}$$

Finally, iterative step 2 and step 3 until the two estimation converge, i.e $|\ \widehat{E}^{t+1} - \widehat{E}^t\ | < \varepsilon$, $|\ \widehat{P}^{t+1} - \widehat{P}^t\ | < \eta$, $\varepsilon > 0, \eta > 0$. At last, we get the sensing data quality of the node user u_i.

According to the estimate of the effort matrix e^{u_i}, we can get the sensing data quality by the mapping function. Set $q_{u_i} = g(e^{u_i}) = \sum_l e_{ll}^{u_i}/n$. In the light of the noise interval indicator $P^t = \{P_1^t, P_2^t, \ldots, P_n^t\}$ of Task_Claim, the interval d_k^* to be delivered is the one with maximum possibility, e.i.$d_k^* = \underset{k}{\text{argmax}} p_k^t$.

2) CONTRIBUTION QUANTIFICATION

In addition, similar to the capacity of a noisy channel [22], the contribution of the sensing data can be expressed as mutual information. We use the mutual information to quantify the effective contribution $c_n(q_{u_i})$ of sensing quality q_{u_i}. In the signal transmission system, the input signal is perfect but interfered by the noisy channel with the probability $1-q_{u_i}$. Thus, the output signal is equivalent to received information on sensing data of quality q_{u_i}. In the crowdsensing, the sensing data uploaded by users is high quality data with the probability of q_{u_i}, that is, the noise reading falls in the exact interval d_l, and low quality data with the probability of $1 - q_{u_i}$.

Given the sensing data, the information uncertainty is

$$h_b(q_{u_i}) = -qlog(q_{u_i}) - (1 - q_{u_i})log(1 - q_{u_i}) \tag{8}$$

Generally, if quality restriction in the signal transmission system is not a binary random variable, but distributed with q_{u_i} in the correct interval d_l and equal probability $(1 - q_{u_i})/(n - 1)$ for each of the $(n - 1)$ rest intervals, then the information uncertainty is calculated as

$$h_n(q_{u_i}) = -q_{u_i}log(q_{u_i}) - \sum_{n-1}(\frac{1 - q_{u_i}}{n-1})log(\frac{1 - q_{u_i}}{n-1}) \tag{9}$$

Therefore, the effective contribution to sensing data of quality q_{u_i} can be formulated as

$$c_n(q_{u_i}) = log(n) + q_{u_i}log(q_{u_i}) + (1 - q_{u_i})log((1 - q_{u_i})/(n - 1)) \tag{10}$$

When the sensing data of quality q_{u_i} equals 1, we have $h_n(1) = 0$, i.e., minimal uncertainty, and $c_n(1) = log(n)$, i.e., maximal contribution. For convenience, we only consider and reward sensing data of quality within the range [0.5, 1] and regard the range [0, 0.5) as the disqualification.

After the quality estimation and contribution quantification of user u_i by the miners, then S pays users the sensing reward according to it.

C. VERIFY THE TRANSACTION AND DISTRIBUTE REWARD

From the probability density function $f(c_i)$ and the cumulative distribution function $F(c)$ of the sensing cost, the profit is defined as the difference between value V gained from the sensing data, and the reward r to user, formulated as

$$Profit_S(c_i, r) = \begin{cases} 0, & r < c_i \\ V - r, & r \geq c_i. \end{cases} \tag{11}$$

While the distribution of c_i is independent of value V and reward r, the expected profit can be calculated as

$$\begin{aligned} Profit_S(r) &= \int_0^{\infty} Profit_S(c_i, r) f(c_i)\, dc_i \\ &= \int_0^{r} (V - r) f(c_i)\, dc_i = F(r)(V - r). \end{aligned} \tag{12}$$

Therefore, the server S can maximize her profit by calculating the first derivative of the function $Profit_S(r)$. We get the optimal reward r^* by the following equation,

$$r^* = V - \frac{F(r^*)}{f(r^*)}. \tag{13}$$

The server rewards the user u_i proportionally to her quantified contribution, i.e., $r(q_{u_i}) = rc_n(q_{u_i})$, where r is a benchmark reward.

The profit $Profit_S$ that S gains from the sensing data is

$$Profit_S(c_i, e^{u_i}, r) = \begin{cases} 0, & rc_n(g(e^{u_i})) < c_i \\ V - rc_n(g(e^{u_i})), & rc_n(g(e^{u_i})) \geq c_i. \end{cases} \tag{14}$$

Then, the optimal quality based reward is determined by

$$\begin{aligned} r^* &= \underset{r}{\text{argmax}}\ Profit_S(r) \\ &= \underset{r}{\text{argmax}} \int_{e^{u_i}} \int_0^{\infty} Profit_S(c_i, e^{u_i}, r) f(c_i, e^{u_i}) dc_i de^{u_i}. \end{aligned} \tag{15}$$

With the estimated data quality and quantified contribution by miners, the server S pays for the corresponding payment to the user u_i after verifying her identity information, as shown in FIGUER 3. The server S pays $Payment_{S \to u_i}$ to u_i after the verification $Sig(Hash_{SK_{u_i}}(Data_{u_i}))$ of the sensing data to the user u_i. Miners verify user's signature in uploaded sensing data and calculate the optimal reward r_*, and the method of the calculation will be explained detailedly at Section IV-B. The time-lock τ is the task deadline. In a distributed transaction, S and user u_i trade as two parties, and their transaction data is packed into a block. The block including the transaction verified by miners along with other transactions within a certain period inserts the blockchain.

However, the miners are in charge of the task of verifying the sensing data in the incentive framework. As we all know, the blockchain has no central authority that controls the transaction. All the transactions are listed openly, so the miner can obtain the user's identity information. Moreover, miners verify the sensing data. Therefore, the miner could get identity and uploaded data of the user in the incentive framework. Consequently, miners may launch an impersonation attack and take the place of users to get payment impersonation. Even if not to obtain absolute payment, miners could obtain users' identity information, so the user will bear the threat of privacy disclosure.

Thus if S wants to dispel doubts to privacy risks of the users in the implementation of the sensing tasks to motivate

$Payment_{S\to u_i}(\mathbf{in}: Deposit_S)$

in-script: $Sig_{SK_S}(Payment_{S\to u_i}) \| n \| r \| Sig(Hash_{SK_{u_i}}(Data_{u_i})) \| q_{u_i}$

out-script: $Ver_{Miner}(Sig_{SK_S}(Payment_{S\to u_i}))$; $Ver_S(Sig(Hash_{SK_{u_i}}(Data_{u_i})))$;
Calculate r^*
if $(q_{u_i} \geq 0.5 \,\&\&\, q_{u_i} \leq 1)$
$r^* = r \times \log(n) + q_{u_i}\log(q_{u_i}) + (1-q_{u_i})\log((1-q_{u_i})/(n-1))$
else
$r^* = 0$

value: r^*

time-lock: τ

FIGURE 3. Crowdsensing payment.

users energetically, besides the monetary incentive mentioned above, a reasonable incentive mechanism should also consider the protection of the user privacy information.

D. PRIVACY PROTECTION ENHANCED MECHANISMS

When a cryptocurrency such as Bitcoin and Monero is used to motivate a node to complete a sensing task in a crowdsensing application, the miner could obtain the privacy of the nodes by verifying the transaction. To solve this challenge, we study the privacy protection incentive mechanism based on node cooperation in crowdsensing applications.

Miners can obtain the node's private information mainly due to their verification work of sensing data and identify information, so it is necessary that a part of the verification work of the miners is allocated to the other party. Because verification committed by a single participating node will increase the overhead of storage, computing and communication, meanwhile it is easy to track users through IP addresses. So it is essential to study the user collaboration based transaction validation model. According considerations as above, we present a transaction verification model based on node cooperation method, as shown in FIGURE 4. K users form a trading group. The server S trades with a group G_i. The sensing data of users in a group are integrated into a group data. Then S pays the group $Payment_{S\to G_i}$ and the group distributes the payment for every users in the group. The model divides the verification process into two phases: an intra-group negotiation phase and a group transaction verification phase of miners.

1) INTRA-GROUP NEGOTIATION

In this phase, we form a transaction group of at least K nodes in the network through K-anonymity privacy protection mechanism. The nodes prepay deposit that will be confiscated if nodes violate the agreement. So the users in a group are semi-honesters who will fully comply with the agreement. Therefore, node users in a transaction group trust each other in a certain extent and negotiate to verify the identity information and sensing data of the nodes in the group.

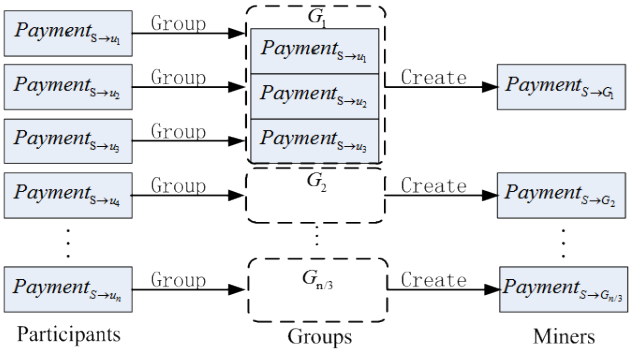


FIGURE 4. Transaction verification model based on node cooperation.

a: K-ANONYMITY PRIVACY PROTECTION

We make up a transaction group composed by unverified close nodes. Namely, nodes in a group are friends who trust each other. Each group contains K nodes to meet the objective of K-anonymity protection. K-anonymity [8], [13] is an anonymity privacy protection technique proposed by Samarati and L. Sweeney for public databases or microdata release in 1998, which can avoid privacy information leaking by means of link attacks effectively when the information is published.

K-anonymity requires that only one element (record) can be fixed in a set (data set) with a probability of no more than $1/k$ (k is a constant) substantially, that is, requires any element (record) possesses $k-1$ identical copy elements at least in the set.

K users in a group G_i meet that the data properties of user u_i are $(A_1, A_2, \cdots, A_n)$ associated with the quasi-identifier $QI_T = \{A_i, \cdots, A_j\} \subseteq \{A_1, A_2, \cdots, A_n\}$. Each of the ordered values appearing in $T[QI]$ appears k times at least. The users group G_i satisfies the purpose of K-anonymity privacy protection. The sponsor of group is the group administrator.

b: LEGALITY CHECK

When the sensing data of a user are transmitted over the public network, it is required to sign and encrypt the data for traceability and security. When examining a cryptographic algorithm, one needs to take into account not only the strength or level of security the algorithm can offer, but also the computational time and the resulting message expansion of it.

Therefore we use signcryption technique [14] that the efficiency enhances dramatically relative to the signature and encryption. We use signcryption schemes based on bilinear maps to complete the verification of node users in a group. In the paper, we use the five algorithms shown below to complete the checking legality of sensing data.

We illustrate the employing of the signcryption mechanism in the group with the example the user u_R in group $Group_i$ verifies the user u_S. Signcryption schemes based on bilinear maps show as follows:

Firstly, in the system initialization algorithm Setup(1^k), select the set of bilinear maps groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$with the order prime p, which meets the requirement $2^{k-1} < p < 2^k$, the generator $(g_1, g_2) \in \mathbb{G}_1 \times \mathbb{G}_2$ and $g_1 = \Psi(g_2), g_2 \overset{R}{\leftarrow} \mathbb{G}_2$; choose the symmetric cryptographic scheme $DES = (Enc, Dec)$, the key space K, and the ciphertext space C; select a hash function: $H' : \{0,1\}^* \rightarrow \{0,1\}$, $H_1 : \{0,1\}^* \rightarrow Z_q$, $H_2 : \mathbb{G}_1^3 \rightarrow \{0,1\}^{k+1}$, $H_3 : \{0,1\}^k \rightarrow K$, thereupon get the parameter $param \leftarrow (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, g_1, g_2, DES, H', H_1, H_2, H_3)$.

Then in the key generation algorithm KeyGen(*param*), we get the key pair (sk, pk) through the computation of $x_U \overset{R}{\leftarrow} Z_P^*; y_U \leftarrow g_2^{x_U}; sk \leftarrow x_U; pk \leftarrow y_U$.

After the preparation of system initialization Setup(1^k) and key generation KeyGen(*param*), signcrypt and unsigncrypt the sensing data $Data_{u_i}$ by the Algorithm 1 and Algorithm 2 as following.

Algorithm 1 *Signcrypt*$(param, sk_{u_S}, sk_{u_R}, Data_{u_S})$

Inputs: The parameter *param*; the secret keys sk_{u_S} and sk_{u_R} of u_S and u_R; the sensing data $Data_{u_S}$ of user u_S; sk_{u_S} will be resolved as (x_{u_S}, y_{u_S}); pk_{u_R} will be resolved as y_{u_R}.

if $y_{u_S}, y_{u_R} \notin \mathbb{G}_2 \backslash \{1\}$ **then**
  return$\perp$
end if

$m \leftarrow Data_{u_S}; \gamma \overset{R}{\leftarrow} Z_P^*; b_m \longleftarrow H'(sk_{u_S}, m)$

$r \leftarrow \frac{\gamma}{H_1(b_m||m||pk_S)+x_S} mod\ p$

$\theta_1 \leftarrow g_1^r; \theta_2 \leftarrow (\gamma \ || \ b_m \ || \ y_{u_R} \ || \ \Psi(y_{u_R})^r)$

$\tau \leftarrow H_3(\gamma \ || \ b_m \ || \ y_{u_R} \ || \ \Psi(y_{u_R})^r)$

$\theta_1 \leftarrow Enc_\tau(m); c \leftarrow (\theta_1, \theta_2, \theta_3)$

return ciphertext c;

Algorithm 2 *Unsigncrypt*$(param, pk_{u_S}, sk_{u_R}, c)$

Inputs: The parameter *param*; the public key pk_{u_S} of user u_S; the secret key sk_{u_R} of user u_R; the ciphertext c; sk_{u_S} will be resolved as (x_{u_R}, y_{u_R}); pk_{u_S} will be resolved as y_{u_S},c will be resolved as $(\theta_1, \theta_2, \theta_3)$.

if $\theta_1 \notin \mathbb{G}_1, \theta_2 \notin \{0,1\}^{k+1}$ *or* $\theta_3 \notin C$ **then**
  return$\perp$
end if

$(\gamma \ || \ b_m) \leftarrow \theta_2 \oplus H_2(\theta_1 \ || \ y_R \ || \ \theta_1^{x_{u_R}})$

if $\gamma \notin Z_P^*$ **then**
  $\perp$
end if

$\tau \leftarrow H_3(\gamma \ || \ b_m \ || \ y_R \ || \ c_1^{x_{u_R}}); m \leftarrow Dec_\tau(\theta_3); \sigma \leftarrow \theta_1^{\gamma^{-1}}$

if $e(\sigma, y_{u_S} \cdot g_2^{H_1(b_m||m||pk_{u_S})}) \neq e(g_1, g_2)$ **then**
  return $\perp$
end if

return $(m \ || \ b_m \ || \ \sigma)$

c: QUALITY VERIFICATION

When the signcryption algorithm is completed, the user has verified the identity information of user u_S. When the verification of signature is passed, the user verifies $Data_{u_S}$ after unsigncryption.

Verifying the two aspects bases on the premise of mutual trust of the nodes in the group: the identity information of the nodes in the group and the node data quality estimation. The identity information of the node has been verified by the signcryption algorithm. We verify the sensing data of the node in this section.

We use the EM algorithm in Section 4.2 to estimate the quality of the sensing data. Assume that the sensing data of a user u_i is verified by u_j, we get the estimated value of the data quality by iterating **E-step** and **M-step**.

E-step calculates the expected value $Q(E|\widehat{E}^t)$ of the likelihood function and **M-step** finds the estimate $\widehat{E}$ of expected value maximization. Finally, we get the sensing data quality of the node u_i. We quantify its contribution according to the contribution quantification method of the Section 4.2 and get payment $Payment_{S \rightarrow u_i}$ afterwards, then the calculation steps and results are transmitted to other users in the group. After all the users' payment is calculated, the group administrator calculates the payment $Pro_U = \{Pro_{u_i} | i = 1, 2, \ldots, k, \sum_i^k Pro_{u_i} = 1\}$ of all users proportionally according to the compensation standard $Payment_U = \{Payment_{s \rightarrow u_i} | i = 1, 2, \ldots, k\}$.

The privacy information involved identity of the user in the group is verified by intra-group negotiation through the aforementioned legality check. All the sensing data of the members in the group are merged together to form a group sensing data $Data_{Group_i}$, which will be verified by the miners.

The miners verify a group sensing data and that could reduce the probability of collusion attacks between the miners and users. The blockchain is a kind of hyperledger with clock stamp, so the miners' verifications, which are open in the blockchain, are traceable. Anyone who doubts a miner could check her works of verification.

2) GROUP TRANSACTION VERIFICATION

The users are responsible for the verification of the identity information of the nodes in the group, and the user's sensing data integrated is verified by the miners. We use a hash function to encrypt the sensing data of users in the group to ensure data security. For integrating users' data in the group, we use the Merkle tree structure to summarize the node data of the group.

a: MERKLE TREE

The Merkle tree is a hash binary tree, a data structure used to summarize quickly and validate the integrity of large-scale data. The binary tree contains an encrypted hash value. In the Bitcoin network, the Merkle tree is used to concatenate all transactions in a block [7].

Similar to the transactions in Bitcoin, we also use the Merkle tree structure to concatenate the sensing data of all users $U = \{u_i, u_{i+1}, \ldots, u_{i+k}\}$ in a group $Group_i$, generate

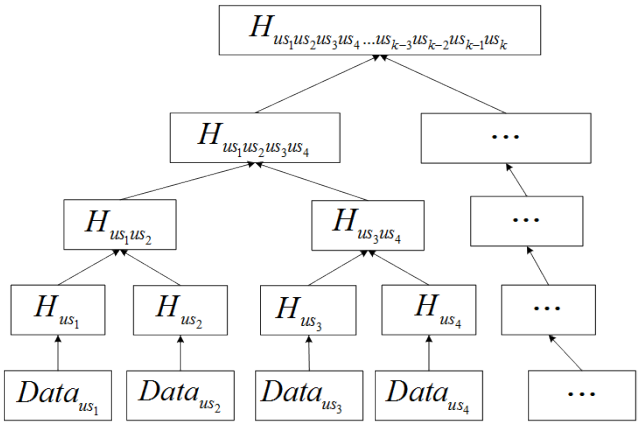


FIGURE 5. Merkle tree.

the digital fingerprints of the entire dataset, and provides an efficient way that checks the existence of the data $Data_{us_i}$ of a user us_i. Each user us_i in the group is a hash node. Generating a complete Merkle tree requires a recursive hash of the hash node pair and inserting the hash node generated newly into the Merkle tree. The Merkle tree is built from the bottom up. For the node users set in the $Group_i$, the sensing data set is $Data_{USER_{Group_i}} = \{Data_{us_1}, Data_{us_2}, \ldots, Data_{us_k}\}$. The concatenation of Merkle tree is as follows:

At the beginning, all the data have not been stored in the Merkle tree yet. We hash the data and store the hash in the corresponding leaf node shown in FIGURE 5. In this paper, we use the double-SHA256 encryption hash algorithm to hash the sensing data:

$$H \sim u_i = SHA256(SHA256(Data_{u_i})) \tag{16}$$

By concatenating the hash values of adjacent leaf nodes and hash it, the two leaf nodes are concatenated as a parent node, and repeat that until one node remained at the top which is the root of Merkle tree. Thus through the Merkle tree, all the sensing data of the nodes in $Group_i$ is concatenated into sensing data $Data_{Group_i}$, which is verified by miners.

b: VERIFY GROUP DATA

Miners verify the legitimacy and data quality of group data $Data_{Group_i}$. In addition, we check legitimacy by the group blind signature algorithm [22] and estimate the data quality by the EM algorithm in Section 4.2. The group member u_i signs the message, and miners verify the signature.

After the validity of the group is verified by the group blind signature, the EM algorithm is used to verify the quality of the sensing data, to verify the corresponding contribution standard and reward, and to calculate the corresponding reward standard of the node data.

$$Reward_{Group_i} = \sum_{i=1}^{k} Reward_{us_i}. \tag{17}$$

Miners make the calculated payment and details of indicators information published. The server S pays the group $Reward_{Group_i}$ after checking. The group allocates the total payment proportionally according to the verification. So, users get their specific reward $Reward_{us_i}$ according to the proportion Pro_{u_i} in the group.

After the verification, the miners sign a timestamp and encrypt the sensing data $Data_{Group_i}$ of $Group_i$ then S stores it as historical data: $Data_{History} = Sig_{Miner}(Hash(Data_{Group_i})) + Timetamp$.

V. SECURITY AND PERFORMANCE ANALYSIS

A. SECURITY ANALYSIS

We will analyze the security of the proposed mechanism by blockchain structure, K-anonymity and Unsigncrypt/Signcrypt this the section.

1) STRUCTURAL ADVANTAGES OF BLOCKCHAIN

The crowdsensing model based on blockchain is benefited from the structural characteristics of the blockchain which eliminates the security weakness of the crowdsensing incentive model due to the existence of the third party. The structural characteristics of the blockchain can also effectively prevent data from being tampered and stolen. In addition, the server S verifies the sensing data and pays the sensing reward of user in traditional incentive mechanism. Therefore, as a stakeholder, the user has reason to suspect that S will maliciously reduce estimated results of the quality level of the sensing data and pay less to users resulting to harm the interests of users. In crowdsensing model based on blockchain, miners are stakeholders for verifying the data, which can avoid the unfair treatment to users effectively.

2) K-ANONYMITY

Node cooperation model formed K-anonymity of the can prevent miners effectively from background knowledge attacks and link attacks to nodes in a group. In the event those adversaries can launch an identity attack on data-based query reasoning and functional dependence reasoning in the process of data release. The K-anonymity can effectively prevent sensitive data disclosure of user during this process. The security of the nodes is mainly dependent on the similarity of the quasi-identifier properties of the node group formed by the division and classification of K nodes. The greater the similarity is, the smaller the information loss caused by the aggregated data is.

We calculate the degree of anonymity by the size of average equivalence class C_{AVG} [17]

$$C_{AVG} = (\frac{Total_{nodes}}{Group_{nodes}})/k \tag{18}$$

The number of nodes is closer to the K value in a group and the tinier information loss is, the higher the degree of anonymity is. Also, the modified discernibility metric C_{MDM} measures the anonymized degree of the data set:

$$C_{MDM} = \sum_{Group} (\mid num_{Group} \mid -k)^2 \tag{19}$$

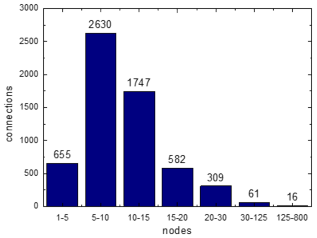


FIGURE 6. Distribution of group with different nodes.

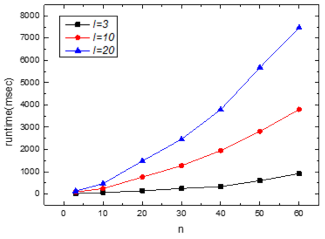


FIGURE 7. Impact of crowdsensing matrix.

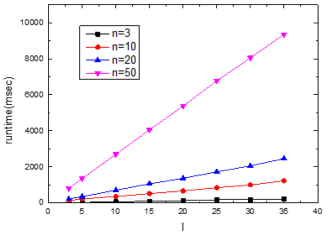


FIGURE 8. Impact of iteration times.

For all groups, the anonymization quality is measured by calculating the square of the difference between the number of nodes and the value of k. When all nodes are k ideally, the C_{MDM} is zero.

In the paper, we use Gervais's Bitcoin-Simulator to simulate blockchain and the number of block nodes [16], also the efficiency of K-anonymity.

FIGURE 6 shows that connection of 5-15 nodes in a group is most. The comparison of (a) and (b) in FIGURE 10 shows that when the k value is about 10, the number of anonymous groups with the best efficiency is the largest.

3) SECURITY ANALYSIS OF UNSIGNCRYPT/SIGNCRYPT

Compared with combining of signing and encrypting in a serial manner, the hidden signature as a 'one-time' Diffie-Hellman key in signcryption algorithm will save an exponential operation (a scalar multiplication operation on an elliptic curve actually). In addition to an inverse operation, the sender $Group_i$ just needs to calculate two exponential operations on $\mathbb{G}_1$. Note that the two exponential operations can be done offline (when the message is unknown). In fact, in the offline phase, the sender can choose random $r \overset{R}{\leftarrow} Z_P^*$, calculate $\theta_1 \leftarrow g_1^r$ and $w = \Psi(pk_R)^r$, and calculate $\gamma \leftarrow [H_1(b_m||m||pk_S) + sk_S] mod\ p$, $\theta_2 \leftarrow (\gamma\ ||\ b_m) \oplus H_2(c_1\ ||\ pk_R\ ||\ w)$, $\theta_3 \leftarrow Enc_{H_3(\gamma||b_m||y_R||w)}(m)$ after knowing the message m, as well. Note that, it is necessary to signcrypt with a different r to prevent the private key from leaking.

B. PERFORMANCE ANALYSIS

In this section, we analysis the social welfare of the server and users by EM algorithm relative to the uniform pricing scheme, EM algorithm performance in the different parameters of seed clusters, sensing matrices and iterations and Merkle tree calculation cost.

1) SOCIAL WELFARE

When simulating enough users to participate, the user gets a corresponding reward based on the estimated sensing quality in the EM algorithm, which has an overwhelming advantage over the uniform pricing scheme for all users. Not only the user's enthusiasm improves, but also the server reduces the loss of profits. The server's profit formula (14) shows that when using the uniform pricing scheme, the value V of the low quality nodes is less than the node's reward $rc_n(g(e^{u_i}))$, and thus server S's profit $Profit_S(c_i, e_{u_i}, r)$ is less than 0. The pricing mechanism $r^* = \text{argmax}_r Profit(r)$ in EM algorithm makes $Profit_S(c_i, e_{u_i}, r) \geqslant 0$, thereby effectively avoid the economic loss of S.

2) EM ALGORITHM PERFORMANCE

We simulated the effects of different parameters (seed clusters, sensing matrices, iterations) on the EM algorithm in the Ubuntu 16.04 environment:

There are observed value in rows and eigenvalues in columns of in the sensing matrix $E_{n\times n}$, $n = 1, 2, \ldots$, and the critical value ε calculated at the fourth step in EM algorithm. The influence of the computational cost on the known data cluster w, the number of iterations I, and the order of the matrix n is simulated:

As can be seen in FIGURE 11, when the set of parameters increases uniformly (the order of the sensing matrix $n = 10$; iteration number $I = 3$; critical value $\varepsilon = 0.001$), the efficiency cost (we use the algorithm running time to represent) increases linearly. But the time is almost constant when the number of clusters is 10-15. Therefore, We show more detailed simulation results about 10-15 clusters in FIGURE 11(b). The result shows the EM algorithm has the lowest cost when the number of clusters is 11. Hence the number of clusters should set at 11 when the data set is trained.

In FIGURE 7, when the order of the sensing matrix ($E_{n\times n, n=1,2,\ldots}$) increases uniformly (cluster $w = 2$, iteration number $I = 3$, critical value $\varepsilon = 0.001$), the algorithm cost increases exponentially.

In FIGURE 8, when the number of iterations increases uniformly (the order of sensing matrix $n = 10$, cluster $w = 5$, $\varepsilon = 0.001$), the cost increases linearly.

3) MERKLE TREE CALCULATION COST ANALYSIS

FIGURE 9 shows that we simulate the effect of different tree depths on the data hash efficiency of the Merkle tree.

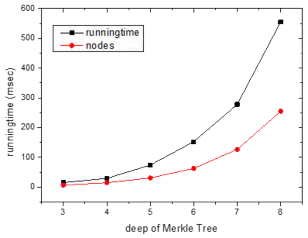
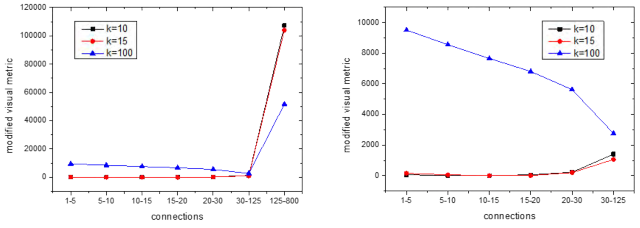
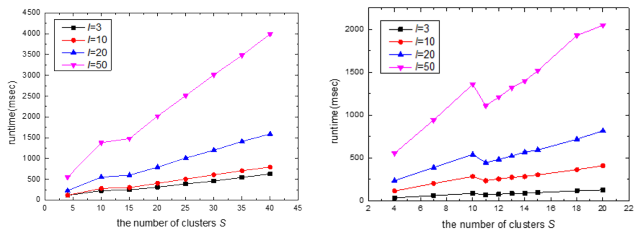


FIGURE 9. Impact of Merkle tree depths.



(a) (b)

FIGURE 10. C_{MDM} in different k value. (a) 125-800 nodes groups excluded. (b) 125-800 nodes groups included.



(a) (b)

FIGURE 11. Impact of cluster. (a) Cluster (3-40). (b) Cluster (5-10).

With the limited time, we did not really implement the integration of K nodes data in Merkle tree. We calculate the total hash calculation cost by adding the hash calculation cost of all nodes. FIGURE 5 shows that the number of nodes increases exponentially with the increasing of tree depth (Merkle tree is a full binary tree, the number of nodes $node_{num} = 2^{deep} - 1$, $deep$ is tree depth). With the number of nodes increasing, the computational cost increases more dramatically than the number of nodes, the hash cost (the black line) is steeper than the number of nodes (the red line) shown in FIGURE 9.

VI. CONCLUSION

In this paper, we propose a distributed incentive mechanism based blockchain which can eliminate the security issues caused by a 'trustful' center. In the distribute crowdsensing system, the sensing data qualities are evaluated via the EM algorithm and contributions are quantified via mutual information by miners. We use a signcryption method to prevent miners and other adversaries from violating users' privacy. The signcryption mechanism saves computing costs compared to operating sequentially of the signature and encryption. In addition, we use the node cooperation based privacy protection mechanism which makes users' privacy to be hidden in group to deal with the impersonation attacks in the open and transparent blockchain.

In the future, we will analyze the possibility and discuss solutions of collusion attacks between an anonymity group and miners, between miners and the server and between users and miners. Due to limited time and paper space, we will display the security experiment and more theoretical analysis in our future work.

REFERENCES

[1] Y. Zhang and M. van der Schaar, "Reputation-based incentive protocols in crowdsourcing applications," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 2140–2148.

[2] J. R. Douceur, "The sybil attack," in *Proc. Int. Workshop Peer-Peer Syst.*, 2002, pp. 251–260.

[3] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, "Free-riding and whitewashing in peer-to-peer systems," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 5, pp. 1010–1019, May 2006.

[4] X. Gong, X. Chen, J. Zhang, and H. V. Poor, "Exploiting social trust assisted reciprocity (STAR) toward utility-optimal socially-aware crowdsensing," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 1, no. 3, pp. 195–208, Sep. 2015.

[5] H. Xie, J. C. S. Lui, and D. Towsley, "Incentive and reputation mechanisms for Online crowdsourcing systems," in *Proc. IEEE IWQoS*, Jun. 2015, pp. 207–212.

[6] D. Peng, F. Wu, and G. Chen, "Pay as how well you do: A quality based incentive mechanism for crowdsensing," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 177–186.

[7] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol, CA, USA: O'Reilly Media, 2014.

[8] R. Xiangmin, Y. Jing, and Z. Jianpei, "An improved strategy of preventing privacy inference attacks based on k-anonymity data set," *Int. J. Adv. Comput. Technol.*, vol. e4, no. 10, pp. 346–355, 2012.

[9] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *Proc. 25th USENIX Secur. Symp.* 2016, pp. 279–296.

[10] R. Kumaresan, T. Moran, and I. Bentov, "How to use bitcoin to play decentralized poker," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 195–206.

[11] L. Luu, J. Teutsch, R. Kulkarni, and P. Saxena, "Demystifying incentives in the consensus computer," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 706–719.

[12] A. P. Dawid and A. M. Skene, "Maximum likelihood estimation of observer error-rates using the EM algorithm," *Appl. Statist.*, vol. 28, no. 1, pp. 20–28, 1979.

[13] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[14] A. W. Dent and Y. Zheng, *Practical Signcryption*. Heidelberg, Germany: Springer, 2010.

[15] A. Lysyanskaya and Z. Ramzan, "Group blind digital signatures: A scalable solution to electronic cash," in *Proc. Int. Conf. Financial Cryptogr.*, 1998, pp. 184–197.

[16] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 3–16.

[17] R. J. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *Proc. IEEE ICDE*, Apr. 2005, pp. 217–228.

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

[19] I. Bentov and R. Kumaresan, "How to use bitcoin to design fair protocols," in *Proc. Int. Cryptol. Conf.*, 2014, pp. 421–439.

[20] I. Miers, C. Garman, and M. Green, "Zerocoin: Anonymous distributed E-cash from bitcoin," in *Proc. IEEE Secur. Privacy (SP)*, May 2013, pp. 397–411.

[21] Noisetube. (2008). *Urban Noise Sensing*. [Online]. Available: http://www.noisetube.net/

[22] R. W. Yeung, *Information Theory and Network Coding*. Berlin, Germany: Springer, 2008.
[23] J. Wang, P. G. Ipeirotis, and F. Provost, "Quality-based pricing for crowdsourced workers," New York Univ., New York, NY, USA, Tech. Rep. CBA-13-06, 2013.
[24] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek, "Secure multiparty computations on bitcoin," in *Proc. IEEE Secur. Privacy (SP)*, May 2014, pp. 443–458.
[25] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek, "Fair two-party computations via bitcoin deposits," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2014, pp. 105–121.
[26] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. IEEE INFOCOM*, Mar./Apr. 2003, pp. 1987–1997.
[27] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. Secur. Privacy Workshops (SPW)*, May 2015, pp. 180–184.
[28] M. A. Alswailim, H. S. Hassanein, and M. Zulkernine, "A reputation system to evaluate participants for participatory sensing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.
[29] M. Pouryazdan, B. Kantarci, T. Soyata, L. Foschini, and H. Song, "Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing," *IEEE Access*, vol. 5, pp. 1382–1397, 2017.
[30] L.-Y. Jiang, F. He, Y. Wang, L.-J. Sun, and H.-P. Huang, "Quality-aware incentive mechanism for mobile crowd sensing," *J. Sensors*, vol. 2017, 2017, Art. no. 5757125.
[31] E. Cecchetti *et al.*, "Solidus: Confidential distributed ledger transactions via PVORM," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017.
[32] A. R. Choudhuri, M. Green, A. Jain, G. Kaptchuk, and I. Miers, "Fairness in an unfair world: Fair multiparty computation from public bulletin boards," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 719–728.
[33] M. Li *et al.*, "CrowdBC: A blockchain-based decentralized framework for crowdsourcing," IACR Cryptol. ePrint Arch., Univ. California, Santa Barbara, Santa Barbara, CA, USA, Tech. Rep. 2017/444, 2017.
[34] Y. He, H. Li, and X. Cheng, "A bitcoin based incentive mechanism for distributed P2P applications," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.*, 2017, pp. 457–468.
[35] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://bitcoin.org/bitcoin.pdf.

JINGZHONG WANG received the B.S. degree and M.S. degree from Inner Mongolia University. He is currently a Professor and the Dean of studies with the North China University of Technology. He has published 40 papers in internal and international conference and journals, and he has edited and translated six books. His research areas include digital image processing and application, computer communication network, and information security technology.

MENGRU LI received the bachelor's degree from Beijing Wuzi University. She is currently pursuing the master's degree with the North China University of Technology. Her research interests include Bitcoin-based incentive mechanism.

YUNHUA HE (M'17) received the Ph.D. degree in computer science from Xidian University, Xi'an, China, in 2016. He has been an Assistant Professor with the North China University of Technology, China, since 2016. His research interests include security and privacy in cyber-physical systems, Bitcoin-based incentive mechanism, security and privacy in vehicle ad hoc networks. He has published 16 research articles in refereed international conferences and premier journals. He received the Best Paper Award from the conference WASA 2017.

HONG LI (M'17) received the B.A. degree from Xi'an Jiaotong University and the Ph.D. degree from the University of the Chinese Academy of Sciences. He has been an Assistant Professor with the Chinese Academy of Sciences, China, since 2017. He has published 14 papers in refereed international conferences and premier journals. His primary research interests include security and privacy in Internet of Things, and security and privacy in mobile social networks. He received the Best Paper Award from the Conference WASA 2017.

KE XIAO received the Ph.D. degree in circuit and system from the Beijing University of Posts and Telecommunications, Beijing, China, in 2008. He has been an Associate Professor with the North China University of Technology, China, since 2012. He has long been involved in the research and development and teaching work of wireless communications, the Internet of Things, and embedded systems. He is a member of the IEEE Communications Society and the IEEE VTS Society. He serves as a Reviewer of the IEEE COMMUNICATIONS LETTER, the *IEEE Communications Magazine*, and the IEEE INTERNET OF THINGS JOURNAL. He achieved the title of Outstanding Young Teacher of Beijing City in 2010, because of high-quality teaching, inspiring research papers and professional patents. He is currently hosting one National Key R & D Program of China, as well as one General Program of Science and Technology Development Project of Beijing.

CHAO WANG received the Ph.D. degree from the Beijing Institute of Technology. He has published six research articles in refereed international conferences and premier journals. His research interests include security and privacy in cyber-physical systems and Internet of Vehicles.