sensors

MDPI

Article

A Blockchain-Based Location Privacy Protection Incentive Mechanism in Crowd Sensing Networks

Bing Jia [1,2], Tao Zhou [1,2], Wuyungerile Li [1,2], Zhenchang Liu [3,*] and Jiantao Zhang [4]

1 Inner Mongolia A.R. Key Laboratory of Wireless Networking and Mobile Computing, Hohhot 010021, China; jiabing@imu.edu.cn (B.J.); 31709071@mail.imu.edu.cn (T.Z.); gerile@imu.edu.cn (W.L.)
2 College of Computer Science, Inner Mongolia University, Hohhot 010021, China
3 Office of Informationization Construction and Management, Nankai University, Tianjin 300071, China
4 Human Resources Department, Nankai University, Tianjin 300071, China; zjt@nankai.edu.cn
* Correspondence: liuzc@nankai.edu.cn

Received: 17 September 2018; Accepted: 23 October 2018; Published: 12 November 2018

Abstract: Crowd sensing is a perception mode that recruits mobile device users to complete tasks such as data collection and cloud computing. For the cloud computing platform, crowd sensing can not only enable users to collaborate to complete large-scale awareness tasks but also provide users for types, social attributes, and other information for the cloud platform. In order to improve the effectiveness of crowd sensing, many incentive mechanisms have been proposed. Common incentives are monetary reward, entertainment & gamification, social relation, and virtual credit. However, there are rare incentives based on privacy protection basically. In this paper, we proposed a mixed incentive mechanism which combined privacy protection and virtual credit called a blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Its network structure can be divided into three parts which are intelligence crowd sensing networks, confusion mechanism, and blockchain. We conducted the experiments in the campus environment and the results shows that the incentive mechanism proposed in this paper has the efficacious effect in stimulating user participation.

Keywords: blockchain; incentive mechanism; crowd sensing network; Internet of Things; privacy protection; cloud computing

1. Introduction

Cloud computing has become a hot technology in research and application in the field of information technology, and it has gradually been applied to people's daily lives, bringing convenience to people. Crowd sensing networks are becoming common data sensing solutions. Longo Antonella et al. used crowd sensing in the field of teaching [1] and applied crowd sensing for environmental monitoring of several pollutants, such as noise, air, electromagnetic fields, and so on, in an urban area [2]. Alvear Oscar proposed that crowd sensing emerges as a powerful solution to address environmental monitoring, allowing one to control air pollution levels in crowded urban areas [3]. Corradi Antonio et al. used crowd sensing technology in community identification and cooperative task execution [4]. Habibzadeh Hadi et al. conducted a thorough study of both types of sensors and drew conclusions about which one becomes a favorable option based on a given application platform [5]. Panichpapiboon Sooksan et al. explored the possibility of using only the built-in sensors of off-the-shelf smartphones for traffic density estimation [6]. Cortellazzi Jacopo et al. presented an extension of the general-purpose ParticipAct platform, an MCS application developed by the University of Bologna, focused on the needs of people with impaired mobility. The goal is to specialize ParticipAct to enable a crowd sensing platform that guarantees a solid support for their lifetime allowing for reviewing and sharing opinions regarding public and private places and architectonic barriers of a city area [7].

Crowd sensing not only enables users to collaborate on large-scale awareness tasks but also provides users with the type of cloud platform, social attributes, and other information. Like personal relationships, the level of trust determines how we control privacy in the environment of IoT. As IoT devices become more connected, more data will be shared between people, companies, governments, and ecosystems. Sensors, devices, data, computers, and cloud connections rely heavily on established trust relationships. Connecting more types of IoT devices (equivalent to adding intrusion points) will increase the threat of established systems, increasing overall security risks. If there is no ability to limit privacy settings [8,9], it is difficult to establish a trust relationship with an IoT system or device. Many manufacturers want to accelerate the adoption of IoT products, but security is often the challenge they face. Many IoT devices will continue to face security risks without a security mechanism. Nowadays, mobile devices such as mobile phones and tablet computers have become part of life. This provides the conditions for the development of crowd sensing networks. Traditional sensors have high prices and are not portable. Crowd sensing networks use sensors carried by mobile phones to collect sensing data and can effectively save costs. However, the most important issue with the use of mobile phones to collect sensing data is privacy leakage. User engagement and correctness of information are two of the most important issues in crowd sensing networks. The problems caused by privacy leakage lead to low user involvement, or users intentionally upload false information in order to protect their privacy information. Most of the incentive mechanisms are based on user data quality to motivate users to participate. The higher the quality of data provided by users, the more rewards the server will return to users. Wen et al. proposed "Quality-Driven Auction-Based Incentive Mechanism for Mobile Crowd Sensing" [10], and Guo et al. proposed "TaskMe: Toward a Dynamic and Quality-Enhanced Incentive Mechanism for Mobile Crowd Sensing" [11] and "TaskMe: a cross-community, quality-enhanced incentive mechanism for mobile crowd sensing" [12]. In addition, some scholars have proposed other incentive mechanisms. Zhang et al. proposed an incentive mechanism with a moral hazard. They adopted the performance-related contract to incentivize users to turn on their sensors and allow data collecting for the principle [13]. Jiajun Sun proposed a behavior-based incentive mechanism for crowd sensing applications with budget constraints by applying sequential all-pay auctions in mobile social networks (MSNs) [14]. These incentives have certain effects, but the authors ignore the most fundamental issue: privacy protection. The blockchain [15,16] is a chained data structure that was designed by Nakamoto Sutoshi in 2008. It combines data blocks in a sequential manner in chronological order and ensures that information is not forged and modified through encryption technology. It has the characteristics of decentralization, openness, autonomy, information modification, and anonymity. Therefore, various industries have gradually applied blockchain technology to protect users' information security.

We considered the issue of privacy protection and designed a blockchain-based incentive mechanism. We used the blockchain protection mechanism to protect the user's privacy information, giving certain incentives to motivate users to participate in sensing tasks. The rest of this paper is organized as follows. Section 2 introduces the blockchain-based incentive framework in crowd sensing networks. Section 3 describes the confusion mechanism and confusion mechanism algorithm (CMA). Section 4 reports the structure of the Merkle tree and motivation strategy. Finally, we conclude our work in Sections 5 and 6.

2. Blockchain-Based Incentive Framework in Crowd Sensing Networks

The extension of blockchain technology was born in Bitcoin. It is not just for Bitcoin. Since blockchain technology has unique timestamps, a chain structure, asymmetric encryption, etc., the data stored in the blockchain has the characteristics of being unforgeable and falsified. This non-tamperable characteristic has great significance in the fields of smart cities, intelligent transportation, Internet of Things, finance, finance, trade, trade, credit, etc. It marks the beginning of a truly trustworthy Internet [17].

As shown in Figure 1, the network structure of blockchains [18] can be divided into three parts: intelligence crowd sensing networks, confusion mechanisms, and blockchain. There are two types of nodes in crowd sensing networks. One is an ordinary user node carrying user information, and the other is a miner node. The miner node does not carry any information. Its main role is to mine the new block space. The main function of a server in a crowd sensing network is to publish task information and receive sensing data from the blockchain. The role of the confusion mechanism is to process the sensing data of the nodes in the crowd sensing network to achieve the effect of obfuscating the node data and to prevent the leakage of the node's privacy information. Blockchain includes characteristics of decentralization and transparent information. Using a blockchain structure can prevent user information from being tampered with and protect user information privacy. It can strengthen the privacy protection of information. After introducing the function of each parts, we describe the workflow of the framework. First, the server issues a sensing task. The nodes in the crowd sensing network accept the task. The node collects the sensing data and enters the confusion mechanism for information protection. Secondly, there are a certain number of miners which are red nodes, in Figure 1, responsible for opening up new block spaces. The confusion mechanism creates a group that includes 10 users and a miner. The group is used to handle the data of these users. After user data is stored in the blockchain, the blockchain will give the user the virtual coin as a reward. The more frequency with which the user participates in the task, the more reward coins there will be. The virtual coin can be exchanged for cash. Finally, the blockchain stores the information handled by the confusion mechanism, strengthens the protection on it, and sends the sensing data to the server.

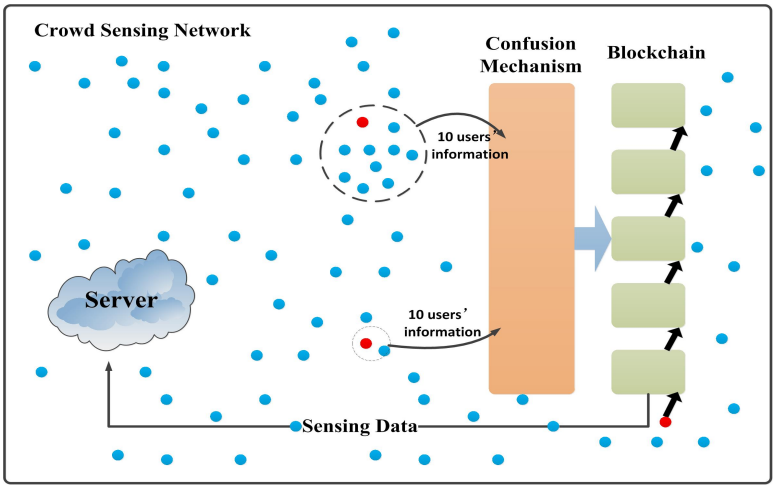

Figure 1. A blockchain-based incentive framework in a crowd sensing network.

3. Confusion Mechanism

3.1. Information Coding Definition

There are many algorithms for handling user privacy protection. The classical privacy protection algorithm is the K-anonymity algorithm [19]. These algorithms have one commonality: fuzzing user information. When the server is attacked by a malicious attacker, the attacker can find many users that meet the conditions, such that the attacker cannot distinguish the target user and ensure the security of the user. In this paper, we use coded methods to protect user information [20]. Each part of the user information is encoded, and the obtained coding information is combined using a plurality of coding methods to form a final user code. Since the privacy of the location information is mainly considered in this paper, the ID of the user and the perceptual information of the user are not encoded. We will then introduce the coding method of each part [21–23].

1. Longitude coding method: Change the longitude to a 9-digit number (remove the extra part after the decimal point) and change the number to a vector $\vec{Lo}$. The calculation is as shown

in Equations (1) and (2). Converting $\vec{Lo}'$ into a number is the encoding of longitude. Similarly, as shown in Equation (3), when decoding $\vec{Lo}'$, simply multiply by Q^{-1} to obtain the original vector $\vec{Lo}$ [24,25].

$$Q = \begin{bmatrix} Q_{1,1} & Q_{1,2} & \cdots & Q_{1,9} \\ Q_{2,1} & Q_{2,2} & \cdots & Q_{2,9} \\ \vdots & \vdots & \ddots & \vdots \\ Q_{9,1} & Q_{9,2} & \cdots & Q_{9,9} \end{bmatrix} \tag{1}$$

$$\vec{Lo} \times Q = \vec{Lo}' \tag{2}$$

$$\vec{Lo}' \times Q^{-1} = \vec{Lo}. \tag{3}$$

2. Latitude coding method: Latitude code and longitude code are the same. Change the latitude to an 8-digit number (remove the extra part after the decimal point) and change the number to a vector $\vec{La}$. The calculation is as shown in Equations (4) and (5). Converting $\vec{La}'$ into a number is the encoding of longitude. Similarly, as shown in Equation (6), when decoding $\vec{La}'$, simply multiply by P^{-1} to obtain the original vector $\vec{La}$.

$$P = \begin{bmatrix} P_{1,1} & P_{1,2} & \cdots & P_{1,8} \\ P_{2,1} & P_{2,2} & \cdots & P_{2,8} \\ \vdots & \vdots & \ddots & \vdots \\ P_{8,1} & P_{8,2} & \cdots & P_{8,8} \end{bmatrix} \tag{4}$$

$$\vec{La} \times P = \vec{La}' \tag{5}$$

$$\vec{La}' \times P^{-1} = \vec{La}. \tag{6}$$

3. Age information coding: The age information is encoded as shown in Equation (7). $Key_a = (\alpha, \beta)$ and $\hat{age}$ is the age code. The decoding method is as shown in Equation (8) [26].

$$\hat{age} = age \times \alpha + \beta \tag{7}$$

$$age = (\hat{age} - \beta) \div \alpha. \tag{8}$$

4. Gender information coding: Gender information is relatively simple. We directly define its encoding. Male is encoded as 01 and female is encoded as 02.
5. Hobby information coding: As shown in Equation (9), we use an affine cipher algorithm [27,28] to encode hobby messages in Equation (9). The key is $Key_h = (\mu, \nu)$. $fun(hobby)$ is used to convert an alphabet letter to a corresponding number. Its decoding is shown as Equation (10).

$$\widehat{f}(hobby) = [fun(hobby) \times \mu + \nu] mod(26) \tag{9}$$

$$\begin{gathered} fun(hobby) = \lambda \times (\widehat{f}(hobby) - \nu) mod(26) \\ \lambda = \mu^{-1} mod(26). \end{gathered} \tag{10}$$

6. Occupation information coding: Occupation information coding is the same with hobby information coding in Equation (11). The key is $Key_o = (\mu^{'}, \nu^{'})$. $fun(occupation)$ is used to convert an alphabet letter to a corresponding number. Its decoding is shown as Equation (12).

$$\widehat{f}(occupation) = [fun(occupation) \times \mu^{'} + \nu^{'}] mod(26) \tag{11}$$

$$fun(occupation) = \gamma \times (\widehat{f}(occupation) - \nu^{'}) mod(26) \tag{12}$$

$$\gamma = \mu^{'-1} mod(26).$$

3.2. Coding And Decoding Algorithm

Based on the above, we summarize two algorithms: the Confusion Mechanism Encode Algorithm (CMA-E) and the Confusion Mechanism Decode Algorithm (CMA-D). The order of the user information is as shown in Figure 2. Algorithm 1 is an encoding algorithm that encodes the information obtained by the user, and the coding of each part is spliced to form a code carrying all the user information. Algorithm 2 is a decoding algorithm that decodes the encoded information formed by the user and restores the user information [29].

ID	Sex	Age	Hobby	Occupation	Latitude	Longitude	Time	Sensing Data

Figure 2. The order of the user information.

Algorithm 1 Confusion Mechanism Encode Algorithm (CMA-E)

Require: User information
Ensure: Encoded user information
$\vec{Lo} \leftarrow$longitude;
$\vec{La} \leftarrow$latitude;
$Key_a = (\alpha, \beta)$;
$Key_h = (\mu, \nu)$;
$Key_o = (\mu^{'}, \nu^{'})$;
Matrix P and matrix Q;
if sex=man **then**
  $sex^{'} \leftarrow$01;
else
  $sex^{'} \leftarrow$02;
end if
$\vec{Lo}' \leftarrow \vec{Lo} \times Q$;
$\vec{La}' \leftarrow \vec{La} \times P$;
$\hat{age} \leftarrow age \times \alpha + \beta$;
$fun(hobby) \leftarrow \lambda \times (\widehat{f}(hobby) - \nu) mod(26)$;
$fun(occupation) = \gamma \times (\widehat{f}(occupation) - \nu^{'}) mod(26)$;
Combine coding information in order
which as $ID, sex^{'}, \hat{age}, \widehat{f}(hobby), \widehat{f}(occupation), Lo^{'}, La^{'}, sensingdata, Time$

Algorithm 2 Confusion Mechanism Decode Algorithm (CMA-D)

Require: Encoded user information
Ensure: User information
Split coding information in order, which as $ID, sex^{'}$,
$a\hat{g}e, \widehat{f}(hobby), \widehat{f}(occupation), Lo^{'}, La^{'}, sensingdata, Time$
$Key_a = (\alpha, \beta)$;
$Key_h = (\mu, \nu)$;
$Key_o = (\mu^{'}, \nu^{'})$;
Matrix P^{-1} and matrix Q^{-1};
if $sex^{'} = 01$ **then**
sex←man;
else
Data does not exist;
end if
if $sex^{'} = 02$ **then**
sex←woman;
else
Data does not exist;
end if
$\vec{Lo} = \vec{Lo'} \times Q^{-1}$,$\vec{La} = \vec{La'} \times P^{-1}$;
$age \leftarrow (a\hat{g}e - \beta) \div \alpha$;
$fun(hobby) = \lambda \times (\widehat{f}(hobby) - \nu) mod(26)$;
$fun(occupation) = \gamma \times (\widehat{f}(occupation) - \nu^{'}) mod(26)$;

4. The Application of Blockchain in Crowd Sensing Networks

Blockchain has the following characteristics:

1. Decentralization: Due to the use of distributed accounting and storage, there is no centralized hardware or management organization. The rights and obligations of any node are equal.
2. Openness: The system is open. In addition to the private information of the parties to the transaction being encrypted, the data of the blockchain is open to everyone. Anyone can query the blockchain data and develop related applications through the open interface. The entire system information is highly transparent.
3. Autonomy: Blockchain adopts consensus-based specifications and protocols (such as a set of transparent and transparent algorithms) to enable all nodes in the entire system to exchange data freely and securely in a trusted environment, so that the trust of "people" can be changed. Become a trust in the machine, and any human intervention does not work.
4. Information cannot be tampered with: Once the information is verified and added to the blockchain, it is stored permanently. Unless more than 51% of the nodes in the system can be controlled at the same time, the modification of the database on a single node is invalid, so the data stability and reliability of the chain is extremely high.
5. Anonymity: Since the exchange between nodes follows a fixed algorithm, the data interaction does not need to be trusted (the program rules in the blockchain will judge whether the activity is valid), so the counterparty does not need to open the identity to let the other party generate itself. Trust is very helpful for the accumulation of credit.

In this paper, we have changed the structure of the blockchain. It is shown as Figure 3. After the confusion mechanism handles the information. The information of users was put to the blockchain structure for storage. The blockchain is linked by a hash value. Each block is composed of a block

header and a block body. The block header includes the hash value of the previous block, the timestamp, and the root hash value of the Merkle tree. The block body consists of a Merkle tree and a table which stores user location and sensing data. The reasons for using the blockchain structure after the confusion mechanism are as follows: Firstly, the main function of the confusion mechanism is to encode the user's information, but it cannot guarantee that the user's information is not falsified. The blockchain has the function of tamper-proof, so the blockchain technology is an effective method to protect a user's information. Secondly, blockchain is a distributed database. We use blockchain to store data information because it can retain the characteristics of the blockchain itself, such as decentralization, openness, self-control, information that cannot be tampered with, and anonymity.

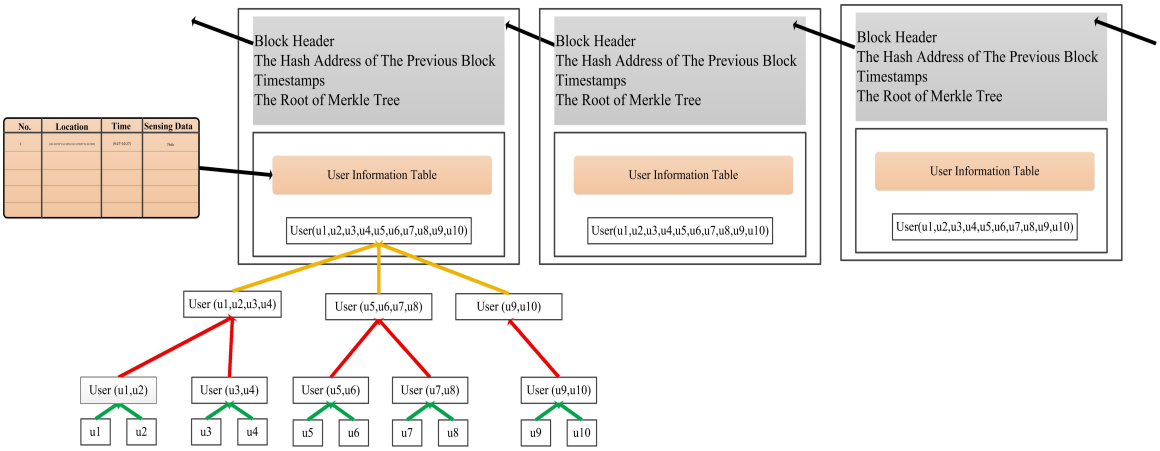

Figure 3. The application of blockchain in a crowd sensing network.

4.1. The Structure of the Merkle Tree and Motivation Strategy

The Merkle tree [30,31] is built from the bottom up. We hash the user information and store the hash in the corresponding leaf node shown in Figure 3. In this paper, we use the double-SHA256 encryption hash algorithm to hash the user information. The formula is as follows:

$$H \sim u_i = SHA256(SHA256(Information_{ui}). \quad (13)$$

By concatenating the hash values of adjacent leaf nodes and hash it, the two leaf nodes are concatenated as a parent node, and that is repeated until one node remains at the top, which is the root of the Merkle tree. Thus, through the Merkle tree, all of the information of the nodes in the group is concatenated into a DataGroup, which is verified by blockchain. If the verification is successful, it will generate the block into the blockchain. Each block has 10 virtual currencies. After the verification is successful, the block distributes the 10 virtual currencies equally to 10 users in order to motivate them to participate more in the task [32,33]. The above description can be summarized as Algorithm 3.

Algorithm 3 Building the Merkle Tree and Currency Allocation

Require: 9 encoded user information and a minner ($u_1, u_2 ... u_9$ and miner)
Ensure: Merkle tree and currency allocation

repeat
Continue to find new block;
until miner find the new block
$u_{10} \leftarrow miner$
for $i = 1; i <= 10; i++$ **do**
$H(u_i) \leftarrow SHA256(SHA256(Information_{ui})$
end for
for $i = 1; i <= 9; i + 2$ **do**
$H(u_i, u_{i+1}) \leftarrow SHA256(H(u_i), H(u_{i+1)})$
end for
for $i = 1; i <= 9; i + 4$ **do**
if $i <= 8$ **then**
$H(u_i, u_{i+1}, u_{i+2}, u_{i+3}) \leftarrow SHA256(H(u_i, u_{i+1}), H(u_{i+2}, u_{i+3}))$
else
$H(u_i, u_{i+1}) \leftarrow SHA256(SHA256(H(u_i), H(u_{i+1)}))$
end if
end for
$H(u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, u_9, u_{10}) \leftarrow SHA256(H(u_1, u_2, u_3, u_4), H(u_5, u_6, u_7, u_8), H(u_9, u_{10}))$
if $H(u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, u_9, u_{10})$ is legal **then**
$Reward \leftarrow 10$
for $j = 1; j <= 10; j++$ **do**
$Reward_{u_j} \leftarrow 1$
end for
else
Reassemble data;
end if

4.2. User Information Table

The main function of the user information table is to send the user's perception information to the server to complete the sensing task [34]. As shown in Figure 4, in the user information table, we only store the user's number, location information, sensing data, and acquisition time. In order to ensure the security of the user's information, the user's location information and the user's acquisition time are the information processed by the confusion mechanism. When the block meets the verification of the blockchain, the blockchain sends this table to the server. Because the user information recorded in the blockchain is not modifiable, when the server finds that there is a problem with the user, the validity of the user information can be verified through the blockchain, thereby removing malicious users.

ID	Time	Longitude	Latitude	Sensing Data
446deb1a-c0e2-469f-b8c2-4f440c0f17f6	2018-06-10 07:23:11	478625143	68276450	48. 10dB
239a0c55-6c99-4ad2-8003-34adeb7013ad	2018-06-11 07:46:46	374859751	36475871	37. 27dB

Figure 4. User information table.

5. Experiment and Result

5.1. Set up

The task of this experiment is to collect noise information in the environment. The experiment employed Android Studio and Eclipse as the experimental environment. We use Android Studio [35] to write the app because it is convenient for users to carry and collect environmental information. The environmental information collected in this experiment mainly includes collection time, GPS information, noise information, and basic user information. The collection method is divided into two kinds for comparison. One is the traditional mode which collects and transmits the data directly to the server without encryption protection and the other is the proposed mode, where the data is encrypted by the CMA algorithm and stored. Parameters are shown in Table 1. Encrypted data forming blocks were added to the blockchain to prevent tampering.

Table 1. The simulation parameters.

No.	Parameter	Value
1	$Key_a = (\alpha, \beta)$	$Key_a = (2, 3)$
2	$Key_h = (\mu, \nu)$	$Key_h = (3, 5)$
3	$Key_o = (\mu^{'}, \nu^{'})$	$Key_o = (6, 2)$
4	Q	$Q = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 9 \end{bmatrix}$
5	P	$P = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 3 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 2n-1 \end{bmatrix}$
6	Q^{-1}	$Q = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1/2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1/9 \end{bmatrix}$
7	P^{-1}	$P = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1/3 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1/(2n-1) \end{bmatrix}$
8	α	2
9	β	5

This experiment used Eclipse to write the server responsible for processing the collection data (the construction of data blocks, user data storage, etc.). The participants participated in the acquisition of noise information in the environment using their Android mobile phone, and the collected data was uploaded to the server. We conducted a total of 10 acquisitions. Each time, the user voluntarily selected the acquisition mode (proposed or traditional mode), collecting only one piece of data per person at a time.

5.2. Result and Analysis

In the experiment, we collected a total of 100 pieces of data. The data that we collected is shown in Figure 5. The results are shown in Figure 6. The x-axis indicates that we randomly selected 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 from all data. The participation rate represents the ratio in each set. There are obviously more people who chose the proposed than those who chose the traditional mode. People who chose the proposed are stableat 80%. The male-to-female ratio of the two methods is shown in Figure 7. Women are the majority in the traditional method, and males account for the majority in the proposed method. This shows that men are more concerned about the importance of privacy protection. Experimental results show that the method proposed in this paper has a certain incentive effect. Algorithm 3, building the Merkle tree and currency allocation, and the Algorithm 3 has three parallel loops, so its time complexity is $Tn = O(3n)$. The time complexity of the blockchain is $Tn = O(1)$. Therefore, the time complexity of the proposed mode is $O(n)$, which is less time-complex compared with the other method.

```
ID:446deb1a-c0e2-469f-b8c2-4f440c0f17f6
Date:2018-06-10 07:23:11
Age:20~30
Sex:man
Profession:graduate student
Hobby:sporting
Noise:58.20dB
GPS:
latitude: 40.81026613712311
longitude: 111.68137907981873
```

Figure 5. The data collected by the traditional mode.

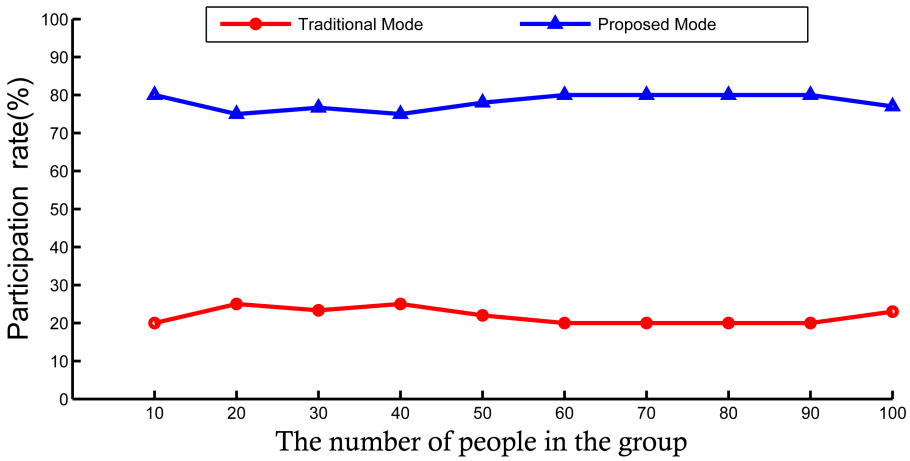

Figure 6. Participation rate.

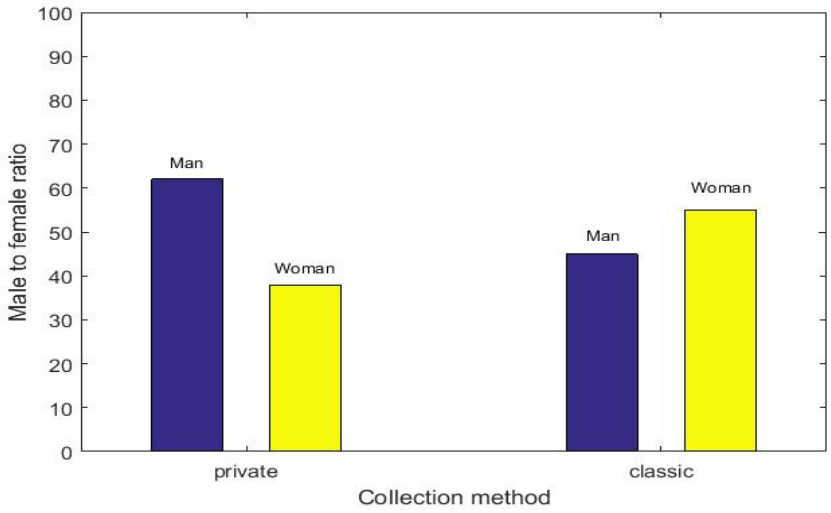

Figure 7. Male-to-female ratio.

6. Conclusions

In this paper, we propose a mixed incentive mechanism that considers privacy protection and virtual credit. The data processed by the confusion mechanism can be prevented from being attacked. In addition, the addition of blockchain ensures that data is not tampered with by others. Compared with the traditional model, the proposed model in this paper can significantly stimulate user participation. However, due to the small scope of the experiment and the small number of samples, the experimental results obtained may be one-sided. Therefore, our future work will expand the scope of the experiments and the experimental data for a more complete judgment. We will also continue to improve the experimental algorithm and achieve the best protection effect.

Author Contributions: Conceptualization, B.J.; Methodology, B.J.; Software, T.Z.; Validation, T.Z. and W.L.; Formal Analysis, T.Z.; Investigation, B.J.; Resources, B.J.; Data Curation, T.Z.; Writing—Original Draft Preparation, W.L.; Writing—Review & Editing, T.Z., W.L., Z.L. and J.Z.; Visualization, Z.L. and J.Z.; Supervision, B.J.; Project Administration, B.J.; Funding Acquisition, B.J.

Funding: This work was supported by the National Natural Science Foundation of China under Grants 41761086, 61461037, 61761035, and 61661041, the National Science and Technology Major Project of the Ministry of Science and Technology of China under Grant No.2016YFB0502102, the Natural Science Foundation of Inner Mongolia Autonomous Region of China under Grant 2017JQ09, and the "Grassland Elite" Project of the Inner Mongolia Autonomous Region under Grant CYYC5016.

Acknowledgments: The authors wish to thank the anonymous reviewers for their helpful comments in reviewing this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Longo, A.; Zappatore, M.; Bochicchio, M.A. Collaborative learning from Mobile Crowd Sensing: A case study in electromagnetic monitoring. In Proceedings of the 2015 IEEE Global Engineering Education Conference (EDUCON), Tallinn, Estonia, 18–20 March 2015; pp. 742–750.
2. Longo, A.; Zappatore, M.; Bochicchio, M.A.; Navathe, S.B. Crowd-Sourced Data Collection for Urban Monitoring via Mobile Sensors. *ACM Trans. Internet Technol.* **2017**, *18*, 1–21. [CrossRef]
3. Alvear, O.; Calafate, C.; Cano, J.C.; Manzoni, P. Crowdsensing in Smart Cities: Overview, Platforms, and Environment Sensing Issues. *Sensors* **2018**, *18*, 460. [CrossRef] [PubMed]
4. Corradi, A.; Foschini, L.; Gioia, L.; Ianniello, R. Leveraging Communities to Boost Participation and Data Collection in Mobile Crowd Sensing. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6.

5. Habibzadeh, H.; Zhou, Q.; Soyata, T.; Kantarci, B. Large Scale Distributed Dedicated- and Non-Dedicated Smart City Sensing Systems. *IEEE Sens. J.* **2017**, *17*, 7649–7658. [CrossRef]
6. Panichpapiboon, S.; Leakkaw, P. Traffic Density Estimation: A Mobile Sensing Approach. *IEEE Commun. Mag.* **2017**, *55*, 126–131. [CrossRef]
7. Cortellazzi, J.; Foschini, L.; Rolt, C.R.D.; Corradi, A.; Neto, C.A.A.; Alperstedt, G.D. Crowdsensing and proximity services for impaired mobility. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–30 June 2016; pp. 44–49.
8. Knijnenburg, B.P.; Kobsa, A.; Jin, H. Dimensionality of information disclosure behavior. *Int. J. Hum. Comput. Stud.* **2013**, *71*, 1144–1162. [CrossRef]
9. Li, H.; Sarathy, R.; Xu, H. Understanding Situational Online Information Disclosure as a Privacy Calculus. *J. Comput. Inf. Syst.* **2010**, *51*, 62–71.
10. Wen, Y.; Shi, J.; Zhang, Q.; Tian, X.; Huang, Z.; Yu, H.; Cheng, Y.; Shen, X. Quality-Driven Auction-Based Incentive Mechanism for Mobile Crowd Sensing. *IEEE Trans. Veh. Technol.* **2015**, *64*, 4203–4214. [CrossRef]
11. Guo, B.; Chen, H.; Yu, Z.; Nan, W.; Xie, X.; Zhang, D.; Zhou, X. TaskMe: Toward a Dynamic and Quality-Enhanced Incentive Mechanism for Mobile Crowd Sensing. *Int. J. Hum. Comput. Stud.* **2016**. [CrossRef]
12. Guo, B.; Nan, W.; Yu, Z.; Xie, X.; Chen, H.; Zhou, X. TaskMe: A cross-community, quality-enhanced incentive mechanism for mobile crowd sensing. In Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Osaka, Japan, 7 September 2015; pp. 49–52.
13. Zhang, Y.; Gu, Y.; Liu, L.; Pan, M.; Dawy, Z.; Han, Z. Incentive mechanism in crowdsourcing with moral hazard. In Proceedings of the 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, 9–12 March 2015; pp. 2085–2090.
14. Sun, J. Behavior-Based online Incentive Mechanism for Crowd Sensing with Budget Constraints. *arXiv* **2013**, arXiv:1310.5485.
15. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP) (2016), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
16. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
17. Chatzopoulos, D.; Gujar, S.; Faltings, B.; Hui, P. Privacy Preserving and Cost Optimal Mobile Crowdsensing using Smart Contracts on Blockchain. *arXiv* **2018**, arXiv:1808.04056.
18. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
19. Meyerson, A.; Williams, R. On the complexity of optimal K-anonymity. In Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, Paris, France, 13–18 June 2004; pp. 223–228.
20. Li, J.; Huang, X.; Li, J.; Chen, X.; Xiang, Y. Securely Outsourcing Attribute-Based Encryption with Checkability. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 2201–2210. [CrossRef]
21. Wang, J.; Ren, P.; Zhenqiang, W.U.; Yanping, L.I. Anonymous communication mechanism based on coding-confusion. *Comput. Eng. Appl.* **2014**.
22. Liu, Z.; Li, T.; Li, P.; Jia, C.; Li, J. Verifiable searchable encryption with aggregate keys for data sharing system. *Future Gener. Comput. Syst.* **2017**, *78*. [CrossRef]
23. Li, T.; Chen, W.; Tang, Y.; Yan, H. A Homomorphic Network Coding Signature Scheme for Multiple Sources and its Application in IoT. *Secur. Commun. Netw.* **2018**. [CrossRef]
24. Kumar, M.K.; Azam, S.M.; Rasool, S. Efficient Digital Encryption Algorithm Based on Matrix Scrambling Technique. *Int. J. Netw. Secur. Appl.* **2010**, *2*.
25. Obimbo, C.; Salami, B. A Parallel Algorithm for determining the inverse of a matrix for use in blockcipher encryption/decryption. *J. Supercomput.* **2007**, *39*, 113–130. [CrossRef]
26. Merkle, R.C. A Digital Signature Based on a Conventional Encryption Function. In Proceedings of the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, London, UK, 16–20 August 1987; Springer: Berlin/Heidelberg, Germany, 1987; pp. 369–378.
27. Liang, X.U.; Tong, W.Q. Image Scrambling Algorithm based on Affine Cipher and Stream Cipher. *Mod. Comput.* **2006**, *48*, 099101.

28. Wahyuni, D. The Research Design Maze: Understanding Paradigms, Cases, Methods and Methodologies. *J. Appl. Mang. Acc. Res.* **2012**, *10*, 69–80.
29. Peng, T.; Liu, Q.; Meng, D.; Wang, G. Collaborative Trajectory Privacy Preserving Scheme in Location-based Services. *Inf. Sci. An Int. J.* **2017**, *387*, 165–179. [CrossRef]
30. Buchmann, J.; Dahmen, E.; Schneider, M. Post-Quantum Cryptography. In Proceedings of the Second International Workshop, PQCrypto 2008, Cincinnati, OH, USA, 17–19 October 2008; pp. 63–78.
31. Meng, W.; Tischhauser, E.W.; Wang, Q.; Wang, Y.; Han, J. When Intrusion Detection Meets Blockchain Technology: A Review. *IEEE Access* **2018**, *6*, 10179–10188. [CrossRef]
32. Wang, J.; Li, M.; He, Y.; Li, H.; Xiao, K.; Wang, C. A Blockchain based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. *IEEE Access* **2018**, *6*, 17545–17556. [CrossRef]
33. Zhu, Y.; Zhang, Y.; Li, X.; Yan, H.; Li, J. Improved collusion-resisting secure nearest neighbor query over encrypted data in cloud. *Concurr. Comp.-Pract. E* **2018**. [CrossRef]
34. Chen, X.; Li, J.; Weng, J.; Ma, J.; Lou, W. Verifiable Computation over Large Database with Incremental Updates. *IEEE Trans. Comput.* **2016**, *65*, 3184–3195. [CrossRef]
35. Khaled, R.; Lishan Ke, R. RoughDroid: Operative Scheme for Functional Android Malware Detection. *Secur. Commun. Netw.* **2018**. [CrossRef]