Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4036491, 13 pages
https://doi.org/10.1155/2022/4036491

Research Article

A Blockchain Based Privacy-Preserving Incentive Mechanism for Internet of Vehicles in Satellite-Terrestrial Crowdsensing

Zhuojia Ma,[1] **Yingqing Wang**,[1] **Jiawei Li**,[2] **and Yang Liu**[2]

[1]*International School, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Yang Liu; liu.yang@bupt.edu.cn

Received 6 October 2021; Revised 30 November 2021; Accepted 6 January 2022; Published 31 January 2022

Academic Editor: Changqing Luo

Crowdsensing has been a popular technology recently and has broad application prospects. The Internet of Vehicles (IoV) refers to the effective utilization of static and dynamic information on the network platform through electronic equipment loaded on vehicles and wireless technology, which means there are many devices generating a huge amount of worthy data. However, preserving the privacy of workers and incentivizing them should be concerned. To this end, we apply the satellite-terrestrial system to solve the communication limitation among vehicles. We propose to use blockchain to act as the channel that requesters and vehicles communicate in. Smart contracts are the main designable parts to do the interactions among the participants. Blockchain is tightly related to payment, so that we implement a total payment minimized auction algorithm on it. We carry out extensive simulations and run an experiment on blockchain to find the auction can be implemented as a smart contract and achieve privacy protection.

1. Introduction

Recently, with the increasing number of vehicles, road congestion and traffic accidents occur frequently. Vehicle operation state detection based on the Internet of Vehicles (IoV) has become the key to driving safety guarantee systems [1]. However, the traditional data acquisition technology of IoV has some defects, such as high construction cost, small coverage, insufficient data volume, and so on. Nowadays, because of the rapid development of mobile intelligent terminals, cameras, GPS, and other sensors are embedded in vehicles and other commonly used terminals. Therefore, the crowdsensing system, which depends on the mobile intelligent devices and vehicles to complete the perception task through conscious or unconscious cooperation, comes into being 2.

Implementing such a crowdsensing system still faces several challenges. First, privacy preserving problem is a severe obstacle. For example, one usual data type in crowdsensing is location, which is regarded as sensitive privacy by vehicles [3]. The location of vehicles is easy to expose the identity of them which is unacceptable. The privacy problem may even prevent vehicles from attending the crowdsensing tasks. Some mobile crowdsensing systems do not concern privacy at all, while most systems use algorithms to protect vehicles' privacy like differential privacy. But these mechanisms are too complex in one component, which is easy to fail. Second, since mobile crowdsensing systems use the devices owned by vehicles and crowdsensing platform needs participants to perform specific tasks, the system should have a mechanism to incentivize vehicles to participate. Designing a reasonable incentive mechanism can ensure the recruitment of enough participants and improve the enthusiasm of users to complete the sensing task. On the contrary, without the guarantee of incentive mechanism, users may be unwilling to participate because of resource consumption, privacy disclosure, and other losses [4]. Third, the existing infrastructure is usually used as the main endpoint for the data collection of the IoV, such as judging the current road condition information through the

camera collection equipment on the street [5]. The connection between smart phone and pavement is used to realize the mutual collection of data [6]. However, due to the limitations of the sensing ability of base stations, especially in remote areas lacking infrastructure, cars can not effectively transmit data to infrastructure, which brings difficulties to the implementation of the crowdsensing system.

In order to overcome the above challenges, we propose an incentive mechanism for crowdsensing with privacy protection based on blockchain since we find that blockchain has lots of characters that are preferable to combine with an incentive mechanism of crowdsensing. More specifically, we use satellite-terrestrial technology to solve the limitation of the existing infrastructure, which can make the satellite communicate directly with vehicles. We use blockchain as the communication channel for crowdsensing task requesters and vehicles to interact with each other. Secondly, we use Ethereum to deploy smart contracts because it is powerful and available for any application. Thirdly, we use an auction algorithm to decide the suitable payment to workers based on their bids and the requirements of tasks. Finally, we combine blockchain with total payment minimized by auction incentive mechanism in crowdsensing and carry out simulations to analyze its performance, and we also carry our smart contract deployment experiment on Ethereum.

The main contributions of this paper are as follows:

(i) We use satellite-terrestrial technology to make it possible for direct communication between vehicle and satellite. Satellite-terrestrial technology solves the problem of infrastructure limitations and realizes data transmission in any area without obstacles.

(ii) We propose to use blockchain as the communication channel for crowdsensing task requesters and vehicles to interact with each other. All sensitive information is through blockchain in an anonymous way with an additional mechanism so that vehicles' privacy is preserved. We use Ethereum to deploy smart contracts because it is powerful and available for any application.

(iii) We design an auction algorithm that is implemented as a smart contract on Ethereum. This auction algorithm decides the suitable payment to workers based on their bids and the requirements of tasks. Meanwhile, it minimizes the total payment of the platform. It satisfies several properties to keep the system working well.

(iv) We carry our extensive simulations to analyze our proposed mechanism's performance, and we also do smart contract deployment experiments on Ethereum.

The rest of this paper is organized as follows. Section 2 introduces the related work. Section 3 describes the system model. Section 4 presents problem formulation. Section 5 provides mechanism design. Section 6 performs the theoretical analysis. Section 7 carries out performance evaluation. Section 8 concludes the paper.

2. Related Work

2.1. Crowdsensing. The sensing services through the Internet of Things are called human-centric sensing by the researchers [7]. Human-centric sensing can be divided into two types, which are personal sensing and community sensing based on the specific object aiming at and the scale of sensing. Personal sensing serves the individual person, including step counting, heart beat monitoring for body health and appearance, transportation for a social character. Community sensing is serving a big set of people, city, or the society which needs to collect much data from many points for a large-scale mission like traffic status and air quality.

Recently, community sensing has been called crowdsensing by more scholars. Crowdsensing is usually divided into participatory sensing and opportunistic sensing as two types. The former needs users' initiative participation and the latter is running without users' awareness [8].

With the development of chip, sensor, integrated circuit, and wireless communication technology, there are more and more devices such as smart phones, smart watches, tablets, and car-equipment devices that integrated with many types of sensors can generate a huge amount of sensing data. They also have enough power, storage, and computing ability to link other small sensors for service links entering the superior network.

The crowdsensing that mainly uses mobile devices to sense data is usually called mobile crowdsensing [9]. Mobile crowdsensing has many advantages. The cost of a sensor network is lower because it does not need to own devices but only rents devices of users, and there are already many users who can also move and interact with others. The devices are often in good condition because their owner will maintain them. And the network can be easily scaled by adjusting the number of users to rent [10].

There have been many applications of mobile crowdsensing already. For environment monitoring, NoiseTube made a noise map by collecting the measurements of noise through smartphones' microphone. For smart transportation, CarTel uses the location from smartphones' sensors to track movement trajectory to advise navigation route. GigaSight can scan a huge number of videos and photos from mobile users to find lost children or crime suspects. Sensorly measure the cellular network signal quality by mobile phones to build the signal map, which can help the construction of the city's fundamental facilities.

2.1.1. Privacy Preserving in Crowdsensing. Privacy preserving is a vitally important problem in mobile crowdsensing, which is not considered by old research. Mobile users are sensitive to their privacy, especially location [11]. Location data can expose many details based on the types of tasks. For example, if time and route of movements are required to submit, this data can expose sensitive locations of mobile users. Their identities can even be exposed by location-based attacks, even if they do not use real names. So, mobile users are very likely to hide their information like location to

preserve privacy, which may even prevent them from participating in the tasks.

Recent mobile crowdsensing research consider the privacy preserving problem. Lu et al. [12] design a blockchain empowered secure data sharing architecture for distributed multiple parties, which can maintain the privacy of data instead of revealing the actual data. Gai et al. [13] propose blockchain-based Internet of Edge model and establish a privacy-preserving mechanism while considering other constraints. Wang et al. [2] create a personalized privacy-preserving task allocation framework for mobile crowdsensing. These proposals use the architecture which is made of mobile applications to sensing data and servers to collect and analyze data. Some researchers proposed to use ISP to collect and process sensed data. For example, Andreoletti et al. [14] propose a Reinforcement-Learning-based algorithm to process data that the customer and ISPs cipher. However, the drawback of the algorithm is the high overhead of data that ISPs and the customer need to exchange with each other to execute it.

2.1.2. Incentive Mechanism of Crowdsensing. Since the importance of incentive users to participate in mobile crowdsensing tasks is realized by researchers, many kinds of incentive mechanisms have been developed recently. Game theory-based incentive mechanism is a very popular type among these mechanisms [15]. There exist many types within game theory-based type, including the auction model, which we are going to use and other models. These models satisfy game theory properties so that they can solve the incentive problem and also other potential problems like workers' selfish. Auction-based incentive mechanisms also have two design directions which are maximization of platform's profit or social welfare and minimization of platform's total payment or social total cost. Our proposal aims at minimization of platform's total payment.

An auction-based incentive mechanism is a better method to incentive mobile users to participate [16]. Cost optimal auction is a kind of auction mechanism which can minimize the total payment of the platform. The auction can also be divided into many types based on the number of items and units. Single-item-single-unit is the simplest condition of the auction, while multiple-items-multiple-units is a difficult problem to solve. Research community has designed auction mechanisms that fit all these four types. The more items and more units, the more complex the mechanism. Many related mechanisms add a lot of complex limitations and additional settings. It is obvious that the more parameters of a system, the more possible conditions may appear, the higher possibility of error and failure.

Our system is available to multiple items and multiple units. But to simplify the algorithm and avoid a potential failure, we determined to use single-item-multiple-units auction because we can distribute the pressure on topper level of our system so that we can run an auction for every single task to according set of mobile users [17].

Liu et al. [18] propose a robust optimization based method to implement a multi-item auction mechanism. Lin et al. [19] explore a method called Multiround Incentive Mechanism, but they do not consider some properties of tasks like the deadline of the tasks. Most of these proposals do not consider privacy preserving or only add a weak local privacy protection algorithm. With the further development of crowdsensing, Yang et al. [20] create a cost-effective crowdsensing system named CEDAR and design a mechanism based on the online auction to encourage involvement. Some researchers [21] design a scalable grouping based privacy-preserving participant selection scheme according to the classical VCG auction Blockchain.

Blockchain technology firstly appeared in Bitcoin: A Peer-to-peer Electronic Cash System by Satoshi Nakamoto as the fundamental bottom technology of Bitcoin. Blockchain described in this article is a data structure that links data blocks like linked list following time sequence. It also has distributed decentralized ledger, which is untamed and unforgeable which can store simple, time-related, and verifiable data [22].

The digital currency has two problems, which are the double payment problem and the Byzantine Generals problem. The double payment problem is using the same set of money more than one time which is easily prevented with physical currency but difficult with digital currency. Blockchain solves this problem with consensus mechanism and distributed ledger so that it is impossible unless the attacker controls more than half of the whole nodes [23]. Byzantine Generals problem is a real-world problem, and in blockchain, the abstract meaningful description is how nodes establish trust with each other without truthful central nodes like traditional centralized networks. Blockchain uses kinds of consensus mechanisms with encryption to build a truthful environment without the third party.

One core problem in the distributed system is how to gain consensus efficiently and properly. Similar to real society, centralization is likely to make a decision quickly, but dictatorship and autocracy are easy to appear, distribution has low efficiency to deciding, but decisions are more satisfied by the system. Any data sharing system based on the network can at most satisfy two of the following three items: consistency, availability, partition tolerance, which is known as CAP theorem. Blockchain, which is distributed system that satisfies partition tolerance, uses consensus mechanism to achieve consistency. There are many kinds of consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Activity (PoA), and several others and hybrid of them.

The smart contract is the core component of blockchain [24]. The smart contract is a computer program that is driven by event, stateful, running on reproducible shared blockchain data ledger and it implements data processing, receiving and storing and sending payment, controlling and managing all kinds of assets on the chain. Specifically, a smart contract is a set of programmatic rules and logic that responses to a specific scene. It is distributed, information shared program codes deployed on the blockchain. All parties that signed the contract agree on the content, then the contract is deployed on blockchain as a smart contract, which will automatically represent these parties without

relying on any central organization. Smart contract is distributed autonomically, which will run automatically after start-up without any effect from anyone.

The main advantage of blockchain is distribution and decentralization [25]. Due to consensus mechanism, encryption algorithm, tree structure, time stamp, and award mechanism, decentralized confidence is implemented so that nodes can interact with each other without a trusted third party. In Ethereum, a more completed, powerful smart contract system is implemented so that more complex and functional applications can be implemented. There are some distributed applications which are called DApp that have been published in lots of areas. Some more basic services based on blockchain technology like Inter-Planetary File System (IPFS) are approaching actual use.

Blockchain has been used in Intelligent Transportation systems to guarantee both safe and efficient transmissions. Some researchers construct a blockchain-enabled crowdsensing framework for distributed traffic management [26] to consider the data safety, utility, and system latency comprehensively. Some other researchers apply blockchain to assess the data quality of tasks reliably. An et al. [27] propose a lightweight blockchain-based model and expectation-maximization (EM) algorithm with multiverifiers to evaluate the performance of task participants.

2.2. Satellite-Terrestrial. Ground mobile communication network provides users with reliable and convenient services. However, in special and remote areas such as mountains, deserts, and seas that cannot be covered by the ground network, it is difficult to deploy base stations, so satellites have become a necessary tool for communication in these areas [28]. Compared with the ground mobile communication network, the satellite communication system mainly has the characteristics of large coverage area, strong broadcasting capacity, small terrain impact, convenient deployment, and so on. At present, there are hundreds of communication satellites in orbit, providing communication and broadcasting services to millions of users. The integration of ground mobile network and satellite network has also become a research hotspot.

In June 2017, SaT5G (satellite and terrestrial network for 5G) alliance was established. The alliance aims to find out the best scheme for seamless integration of satellite communication and 5G and try it out in Europe through a series of research, development, and experiments within 30 months. In the process of integration, the relationship between ground and satellite networks is not equal and cooperative. In this paper, the integrated network architecture should be based on the ground mobile communication network architecture and give due consideration to the special requirements of satellite transmission.

The satellite-terrestrial network has become a promising paradigm of space telecommunication network in the future. Ruan et al. [29] investigate the energy effective power allocation of the satellite-terrestrial network to maximize the effective energy efficiency of secondary satellite communication while meeting the interference constraints of primary ground communication. Bai et al. [30] propose an atmosphere-informed predictive satellite channel model for satellite-terrestrial wireless communication systems at Q-band to model channel attenuation at any specific time. Similar to our thinking, Chen et al. [31] designed the algorithm called MCPR to match IIoT nodes with service sides, which achieve large-scale seamless connections by using a satellite-terrestrial network. Sharma et al. [32] consider an overlay satellite-terrestrial network (OSTN) where an opportunistically selected terrestrial internet-of-things (IoT) network assists the primary satellite communications.

To sum up, this article is more comprehensive than the article which have been submitted and further supplements the details [33]. In this article, not only the preliminary work is described at length, but the research results of crowdsensing and blockchain in recent years are listed. What's more, the article adds the interactions of the whole process.

3. System Model

3.1. Hardware Architecture. The architecture consists of three roles, crowdsensing service providers (CSP), Internet service providers (ISP), and vehicles (Vehs). CSP is the task requester that is the beginning of the whole procedure of the system. Anyone who wants to publish crowdsensing tasks can be CSP. ISP is the network infrastructure provider that allows the data transformation. Most physical devices which support the system belong to ISP. And in a mobile crowdsensing system, ISP is usually a cellular network operator. Veh is the worker who applies the tasks to complete and delivers the sensed data. Vehs own mobile devices like smart phones to perform tasks which can also easily submit results through ISP's network. At the same time, through the satellite-terrestrial system, Vehs can directly communicate with the satellite [34]. Satellite-terrestrial technology solves the problem of infrastructure limitations and realizes data transmission in any area without obstacles. At the same time, through the satellite-terrestrial system, Vehs send data to the satellite, and receive and process the signals sent by satellite through the antenna tower. [35]. The system architecture is shown in Figure 1.

3.2. Interaction Architecture. All interactions are among the three roles and some of them are through the satellite-terrestrial network and lower delay, while some of them are through blockchain based on smart contracts for privacy preserving [36].

When the crowdsensing task publisher publishes tasks, CSP will generate a request and send it to ISP, which we call REQ, which contains the details of the tasks, such as requirements. REQ will trigger ISP to generate a transaction, including the details of the request such as timestamp, deadline (D). This transaction will trigger the first smart contract that we call Request Registration (RR) which registers this current request in the blockchain. ISP will generate another smart contract named Data Access (DA), whose address is stored in RR. RR is then responsible for

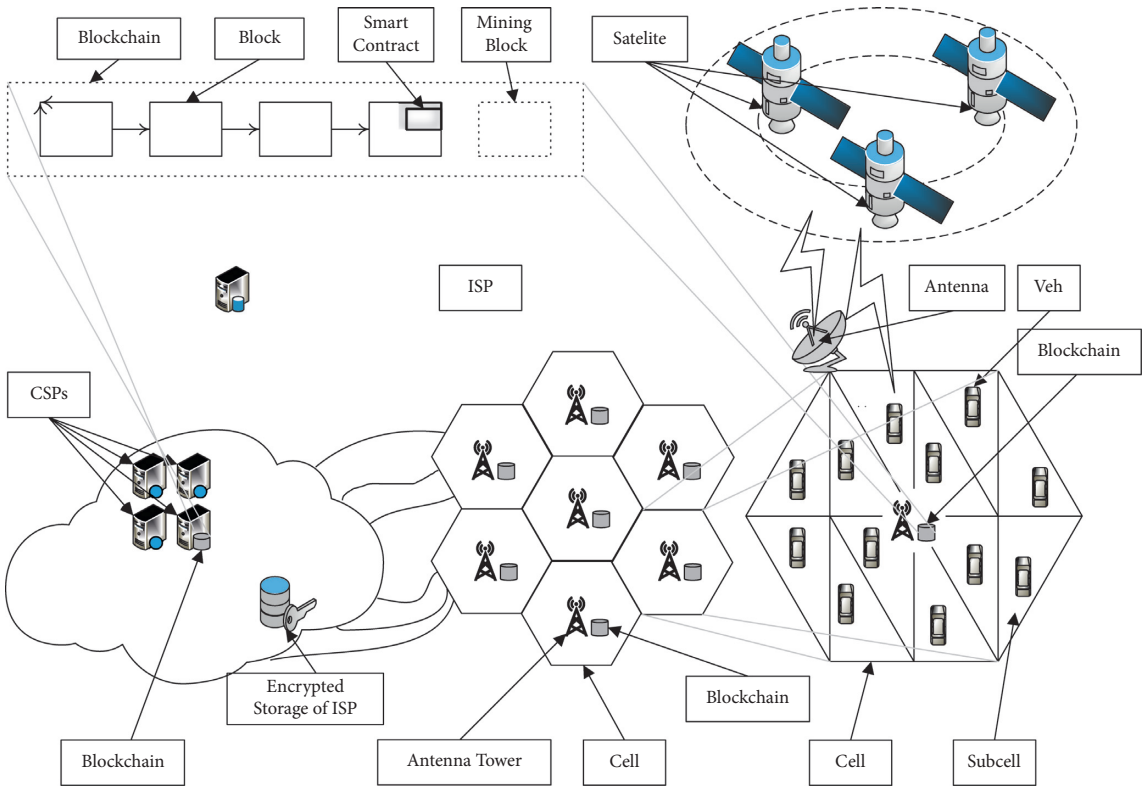

Figure 1: System architecture.

ensuring that CSP has to pay for ISP's work (PAY1) to get the address of DA (ADDR) to trigger it to access the sensed data. ISP will broadcast the set of tasks (T) to a specific set of vehicles based on some characters like their locations in the cellular network. Vehicles in different cells and subcells will receive different sets of tasks. ISP will assign temporary ID (Temp IDs), which will be different and unrelated in every auction for each vehicle so that they do not need a true identity to apply tasks to preserve privacy. Then vehicles will choose their interested tasks and bid for them. They send the bids to ISP and send a small payment which will trigger the smart contract of the auction to determine the auction results.

The smart contract of auction generates the winning vehicles and the payment prices for them. The winning vehicles will be informed to let them know and start their works. The small payment to trigger the auction of losing vehicles will be withdrawn. The payment prices are stored in another triggered smart contract called vehicle payment (VP) which will be triggered after the vehicles finish their works and submit valuable sensed data. When vehicles complete their work, they will send the sensed data to an external encrypted database owned by ISP using their temporary IDs. Then, ISP will inform CSP to the status of the completion of its requests.

CSP receives the information of requests' completion. Then, it will pay for vehicles (PAY2) at the auctioned payment prices, which will trigger the smart contract DA returned by RR at the beginning. DA will return the key of encrypted sensed data (KEY) in external storage to let CSP access it. Then, vehicles will send their own sensed data's hash to trigger smart contract VP to gain payment (PAY3). The last thing of this turn is the deadline D which is the symbol of the end. The step-by-step process of the mechanism is described in Figure 2.

Figure 3 describes the interactions within the system in a more physical and less abstract way.

4. Problem Formulation

We let $x_{ij} \in \{0, 1\}$ to indicates user i's task assignment, $x_{ij} = 0$ means user i will not do task j, and $x_{ij} = 1$ means user i will do the task j. Then, for the given bid matrix b and user information θ_i, the utility user i gains is as follows:

$$u_i(b, \theta_i) = p_i(b) - \sum_{j=1}^{|T_i|} x_{ij} c_{ij}, \tag{1}$$

where $p_i(b)$ is the payment price for user i when he makes bid b, c_{ij} is the cost when user i performs task j. We define that user i has data collection level η_{ij} to task j, which satisfies $\eta_{ij} = \mathbb{E}[|D_{ij} - d_j^*|] \in \{0, 1\}$, in which D_{ij} means the data that user i collects, d_j^* means real data. We design a data collection mechanism to make $\Pr[|D_j - d_j^*| \geq \alpha_j] \leq \beta_j$, in which α_j is the data accuracy budget of task j and β_j is the error tolerance of task j. The total number of vehicles that participate in a specific task should satisfy $N \geq (\sqrt{2}\,\gamma/\alpha\sqrt{1-\delta})\sqrt{\sum_{i=1}^{M}(1/\varepsilon_i^2)}$ to satisfy the data accuracy limitation [37], in which α is the aggregation error, γ is

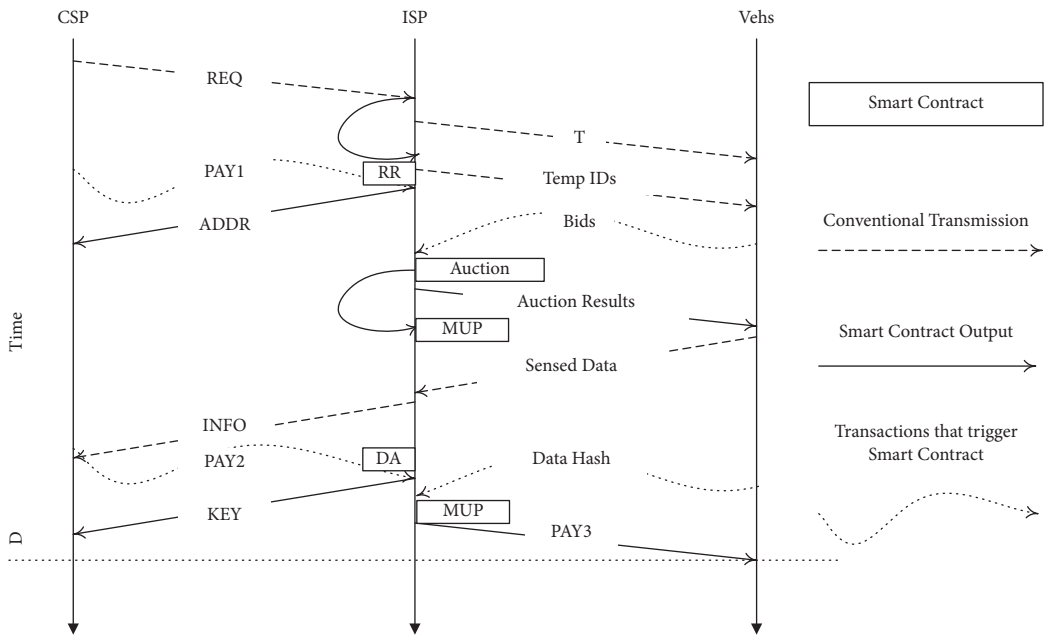

Figure 2: Interactions among the roles.

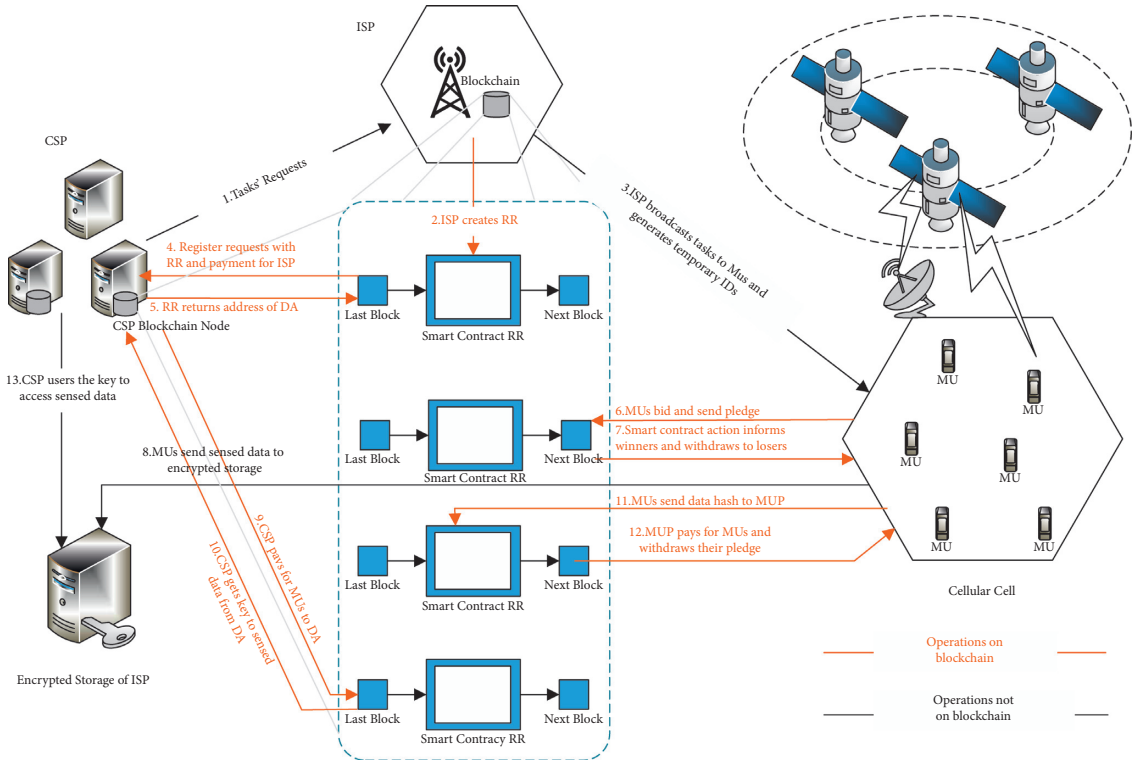

Figure 3: Interactions of the whole process.

worker's data range, δ is fusion center's confidence level of the aggregation error, ε_i is worker i's privacy preserving level, and M is the total number of all vehicles.

We use vector $\mathbf{p} = [p_1, p_2, \ldots, p_M]$ to denote the payment prices for all vehicles on a specific task, and vector $\mathbf{x} = [x_1, x_2, \ldots, x_M]$ in which $x_i \in \{0, 1\}$ denotes

participation or not for all vehicles on a specific task. And we aim to minimize the total payment (MTP), i.e.,

$$\min \sum_{j \in \mathcal{T}} \mathbf{px}$$

$$\text{s.t.} \sum_{i \in \mathcal{M}} x_i \geq \frac{\sqrt{2}\gamma}{\alpha\sqrt{1-\delta}} \sqrt{\sum_{i=1}^{M} \frac{1}{\varepsilon_i^2}}, \tag{2}$$

$$x_i \in \{0, 1\}, \quad \forall i \in \mathcal{M}.$$

5. Mechanism Design

To approach the aim of total payment minimization and satisfy the accuracy limitation as well, we design an auction algorithm.

In this algorithm which we call MTP auction, the inputs are the user set which is denoted by U and the bid information vector, denoted by b. The outputs are the winner set of vehicles for the current task, which is denoted by S and the payment price vector for the winner vehicles denoted by p.

The algorithm includes two subalgorithms, winner selection and payment determination. Winner selection is to select a set of vehicles that win this auction to be chosen to do the current task. Payment determination is to compute the appropriate price for every user in the winner set, which satisfies some game theory properties. The algorithm is shown in Algorithm 1.

Line 2 calculates the least number of workers that is needed to satisfy the limitation of data accuracy requirement. In the formula, N is the least number, and α is the aggregation error, γ is worker's data range, δ is fusion center's confidence level of the aggregation error, ε_i is worker i's privacy preserving level, and M is still the total number of all users. Line 3 initializes the winner to be empty at the beginning. Lines 4–8 are a loop to choose N winners who exit when the number of winners reaches N or all users have been selected out. Line 5 is one of the most important lines in the algorithm, which selects a user with the smallest bid price among the remain users. $b(S)$ not only represents the summation of all bids in set S, but b_j denotes the bid price of user j. It is obvious that $b_j = b(S \cup \{j\}) - b(S)$ so that $b(S) + b_j$ represents the total bids after this time of selection. Since payment price has to be equal to or larger than user's bid price to make the deal established, we can choose the minimum bid price as the payment price, which achieve the total payment minimization goal. Line 6 adds the chosen user to winner set and Line 7 calculates the set of remain users.

Line 11 initializes payment prices of all users to zero at the begging of payment determination. Lines 9–19 are an outer loop to determine the payment prices of every winner user, whose exit condition is the payment prices of all users has been determined. Line 10 constructs a set of users from all users except the current user i. Line 11 initializes a temporary selection set to be empty. Lines 13–25 are an inner loop which actually do winner selection on the set except current user i. We explain in detai. Line 17 selects a user with the smallest bid price in the remain users. Line 18 chooses the larger one from the current payment price and the bid price of the user in Line 17 selected. Line 19 adds this user into the temporary set and Line 20 calculates the new remaining users' set. The exit condition described by Line 21 of the inner loop is also the number of selected users reaches N or all users have been selected out. Line 23 compares the price outputted by the inner loop above to the bid price of the current user i and chooses the larger one as the final payment price of user i, because i is possible to be the N th smaller one in the winner set by coincidence.

```
(1) //Winner Selection
(2) N = (√2 γ/α√(1−δ)) √(Σ_{i=1}^{M} (1/ε_i^2));
(3) S←∅;
(4) while |S| < N and U′ ≠ ∅ do
(5)     i←argmin_{j∈U′} (b(S) + b_j);
(6)     S←S ∪ {i};
(7)     U′←U\S;
(8) end while
(9) //Payment Determination
(10) for all i ∈ U do
(11)     p_i←0;
(12) end for
(13) for all i ∈ S do
(14)     U′ ← U\{i};
(15)     T ← ∅;
(16)     repeat
(17)         i_j ← argmin_{j∈U′} (b(T) + b_j);
(18)         p_i ← max{p_i, b_{i_j}};
(19)         T ← T ∪ {i_j};
(20)         U′ ← U′\T;
(21)     until |T| ≥ N or U′ = ∅
(22)     if |T| < N then
(23)         p_i ← max{p_i, b_i};
(24)     end if
(25) end for
(26) return (S, p);
```

Algorithm 1: MTP Auction.

Line 26 returns the outputs including the winner set S that contains all users won in the auction and the payment prices vector p of each one in the winner set.

6. Theoretical Analysis

Theorem 1. *The MTP problem is NP-hard.*

Proof. The MTP problem's target is $\min \sum_{j \in \mathcal{T}} px$, in which p and x are both vectors containing various numbers, but in fact, for any real condition, all values in p are equal to each other because there will certainly exist enough users who bid the same price based on our constraints. Thus in this proof, we can regard p as a constant, then the computational complexity of the MTP problem is the same as the modified MTP problem whose aim is $\min \sum_{j \in \mathcal{T}} x$ with the original constraints, which means minimizing the total number of

workers for all tasks in the task set $\mathcal{T}$. The NP-hardness of the modified MTP problem is the same as the original one so we can prove it instead.

Minimum weighted set cover problem is a well-known problem, which is similar to the modified MTP problem and is proved NP-hard. We consider a set with X elements $P = \{\tau_1, \tau_2, \ldots, \tau_X\}$ and a set of sets with Y sets $Q = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_Y\}$. The objective of the minimum weighted set cover problem is finding a subset of Q with a minimum number of cardinalities and the union of the sets in this subset contains all elements in set P. In our proof, set P is regarded as the set of all tasks, and set Q is regarded as the set of mobile users' bidding tasks' sets. Based on these representations, we can build the representations of our modified MTP problem. For every bidding user i's bidding tasks set, Γ_i we build set Γ_i' whose elements $\tau_j \in \Gamma_i$. Then we get a set $Q' = \{\Gamma_1', \Gamma_2', \ldots, \Gamma_Y'\}$ which represents the winning tasks' sets of every bidding user. And Q' is required to cover all tasks $\tau_j \in P$ at least N_j times because of our constraints of the error bound. If we use $R = \{N_1, N_2, \ldots, N_X\}$ to denote the minimum number constraints, P, Q', and R construct the representations of our modified MTP problem. The modified MTP problem then can be essentially regarded as a minimum weighted set cover problem which is proved to be NP-hard, which is hard to find a result in polynomial time. The modified MTP problem is then NP-hard. And our MTP problem is proved to be NP-hard.

Since the problem is NP-hard, in the design level of the auction algorithm, we determine to run an auction for every single task in the task set. We split and reorganize the bids of users to compose bids based on each task, and then the algorithm is simpler to implement and find results. □

Lemma 1. *MTP Auction is computationally efficient.*

Proof. Computationally efficient means the results of the whole auction have to be calculated in polynomial time. When computing the computational complexity, we consider the condition that the algorithm runs the greatest number of iterations. The winner selection part of the algorithm takes $O(NM)$ time, where finding the minimum value of $b(S) + b_j$ costs $O(M)$ time and the loop iterates for N times costs $O(N)$ time. When it comes to the payment determination, the process of the inner loop of this part which is from Line 12 to 17 is similar to the winner selection part. It also costs $O(NM)$ time to run. The payment determination part also has an outer loop that iterates for each user in the winner set with the number of N, so it takes $O(N)$ time to execute. Hence, the payment determination part takes $O(N^2M)$ time. The total time of this auction is $O(NM) + O(N^2M)$. Hence the execution time of the whole auction algorithm is dominated by the payment determination part, which is bounded by $O(N^2M)$. □

Lemma 2. *MTP Auction is individually rational.*

Proof. Individually rational means the vehicles that participate in the auction are not willing to gain negative utility. We let i_i denote the user who replaces the position of user i in the sorting of $U\backslash\{i\}$ which is the whole user set except user i in one iteration of the payment determination part of the auction algorithm. User i_i is at i th position because of the outside of user i. It will not be here if user i is considered, so $b(S) + b_i \le b(S) + b_{i_i}$. Hence, we have $b_i \le b_{i_i}$ and based on the selection method, they will replace each other in the sorting at N th position. If we use $b_i(U)$ to represent every bidding price of all vehicles in U, we get $b_i \le b_{i_i} \le b_i(U\backslash\{i\})$. And since we choose the maximum one of b_{i_i} and b_i as the payment price of the user i which is p_i, we have $b_i \le b_{i_i} \le p_i$, according to Line 18. Besides, the bidding price of the user i is to make itself earn positive utility because it will not submit a price lower than its own cost.

Hence, we prove that the payment price of the user i is equal to or larger than its bidding price for sure. Since the user i bids at this price so that it will not get negative utility at its own bidding price, and it will not be even at a higher price. Hence, the users will not get negative utility for sure, which means the auction is individually rational. □

Lemma 3. *MTP auction is profitable.*

Proof. Profitable means the platform that runs the auction among buyers and sellers will gain utility by serving the auction. In our design, the auction algorithm does not act as a usual auction that the platform receives payment from buyers, leaves some utility for itself, and then sends payment to sellers. The auction that runs in our system and acts as the smart contract on blockchain on devices of ISP only chooses winners and determines the payment prices of them, but it does not directly deal with money. As introduced above, the payment prices will be stored into other smart contracts and crowdsensing providers who request tasks will directly pay for vehicles via blockchain to execute these smart contracts to get sensed data. So the platform will not earn money from the auction or will not lose money either. However, the auction algorithm is implemented as a smart contract which requests a crowdsensing task requester to pay for its work to execute. This payment is the profit of the auction platform. The determination of this fee to execute the auction smart contract is not the problem our proposal will discuss, but it is easy to consider that it can be related to the amount of workload of the platform. Hence, we can say the MTP auction is profitable. □

Lemma 4. *MTP auction is systematically efficient.*

Proof. Systematically efficient means the auction not only makes the platform earn utility but also earns more utilities. In our system, a crowdsensing task requester will pay for selected vehicles no matter how high prices are determined to ensure the tasks are completed as the constraints, so crowdsensing providers may have a high cost to gain the data. If the auction algorithm selects the mobile user with the lowest bid that can complete the task to minimize the total payment, the cost of the crowdsensing provider is reduced. This will make the crowdsensing task requesters more willing to choose this platform to save costs. Then the platform will have more opportunities to execute auctions

and gain more utilities from the running of the auction, which means the platform tends to earn more utilities. Hence, we prove the MTP auction is systematically efficient. □

Lemma 5. *MTP auction is truthful.*

Proof. Truthful means the best strategy of the participants is to bid with truthful values, and they cannot gain more utilities by bidding with fake prices. A theorem has been proved that an auction mechanism is truthful if and only if the selection rule is monotone and each winner is paid the critical value. A selection rule is monotone means if a user i wins in the auction with a bidding price b_i, it will also win by bidding a lower price $b_i' \leq b_i$. The payment prices of winners are critical means if user i bids a price higher than this critical value, it will not win in the auction. Based on this theorem, we can prove our auction is truthful by proving the winner selection is monotone and payment determination is critical meanwhile. □

Theorem 2. *MTP auction is computationally efficient, individually rational, profitable, systematically efficient, and truthful.*

Proof. From Lemmas 1–5, Theorem 2 is proved. Thus, the MTP auction satisfies these five properties. □

7. Performance Evaluation

We carry out extensive simulations to verify the proposed algorithm.

7.1. Ethereum Smart Contract Experiment. We designed an experiment to find our auction algorithm can be deployed on the blockchain. We are determined to use Ethereum because its support to the development of smart contracts is easier and more powerful. All parts of our system can be implemented on it. The programming language of Ethereum smart contract development is Solidity, which we use to implement the auction. The complier version we use is 0.5.8 + commit.23d335f2.Emscripten.clang. The environment we use is Remix, whose version is v0.7.6. It is a web page opened in the browser and it will generate the blockchain environment which is called a private test chain within the browser using JavaScript Virtual Machine. Running smart contracts, creating accounts and payments are easy to do in this environment.

We first observe the influence of the aggregation error α to the total payment of the auction. A smaller aggregation error means more participants are required to complete the task. And in the simulation, we set the total number of vehicles M as 100, the privacy preserving levels ε_i of vehicles are randomly generated in the range from 0.2 to 1, workers' data range γ is 1, the fusion center's confidence level of the aggregation error δ is 0.5. The bidding prices of vehicles are randomly generated, satisfying Gauss distribution with mean of 10 and variance of 5. We consider the aggregation error α varies from 0.1 to 2, and we calculate each step with 0.1.

As shown in Figure 4, when aggregation error is small, we can see the total payment is high and nearly does not vary. The reason is when aggregation error is too small, the required number of participants N will be very large. If it is larger than the total number of vehicles M, all vehicles will be selected as winners and be paid. This leads to high total payment and since all vehicles have to be winners, the selection rule will not affect the results of the auction. This results in the total payment of the auctions being the same as each other. It can be seen that the data of them are not completed because in our simulations, we generate random bidding price for vehicles and run it for some time to take average values to reflect common conditions, so the total payment of them may not be the same. When aggregation error is larger we can see our MTP auction actually has a lower total payment than baseline and TASC [38].

In the second part, we simulate the influence of the user number. The more users are willing to bid, the more choices the auction has. Therefore, it can lead to a lower payment. In this simulation, we set the total number of users M as 100. The privacy preserving levels ε_i of users are randomly generated in the range from 0.2 to 1, workers' data range γ is 1, the fusion center's confidence level of the aggregation error δ is 0.5. The bidding prices of users are randomly generated, satisfying Gauss distribution with a mean of 10 and variance of 5. We also set the aggregation error α to 2, which can make the results easy to observe. The number of users bidding for the current task ranges from 30 to 100. And we calculate the results and total payment with 5 users of each step, which displays in x-axis in the output figure. Figure 5 is the diagram drawn according to the simulation results.

We can see in Figure 5, with the increase of the number of people willing to participate in the current task, the total payment decreases. The total payment at some points increases while the number of people willing to participate increases because the bidding prices of vehicles are randomly generated by Gauss distribution which may cause total payment increase by coincidence. Our MTP auction produces less total payment than the baseline and TASC. Figure 6 shows the time efficiency of our proposed mechanism, which verifies Lemma 1.

7.2. Blockchain Smart Contract Experiment. We use Remix to compile and run the auction implemented as a smart contract. Since Solidity does not provide functions like print () to show the results in a terminal, we add event variables and output the information to logs. The smart contract running result is shown in Table 1.

Due to the limitation of JavaScript VM and Solidity, in this experiment, we set the total number of users M as 10, the privacy preserving levels ε_i of users are all 1, workers' data range γ is 1, the fusion center's confidence level of the aggregation error δ is 0.5. The bidding prices of users are randomly generated from 5 to 15. We also set the aggregation error α to 2. If a smart contract is executing, the

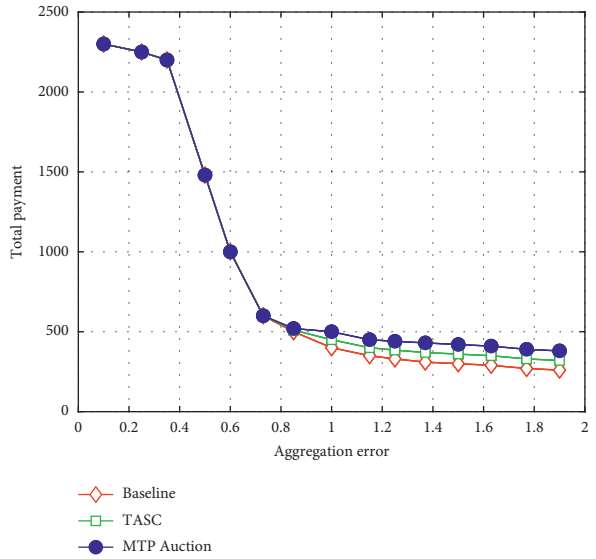

Figure 4: Influence of aggregation error.

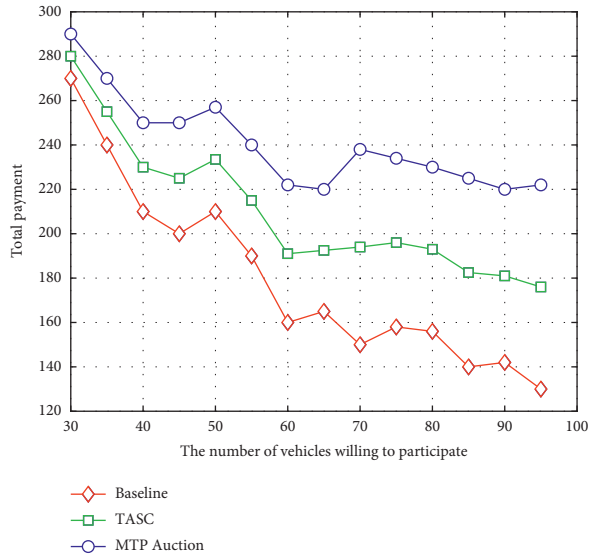

Figure 5: Influence of the number of bidding vehicles.

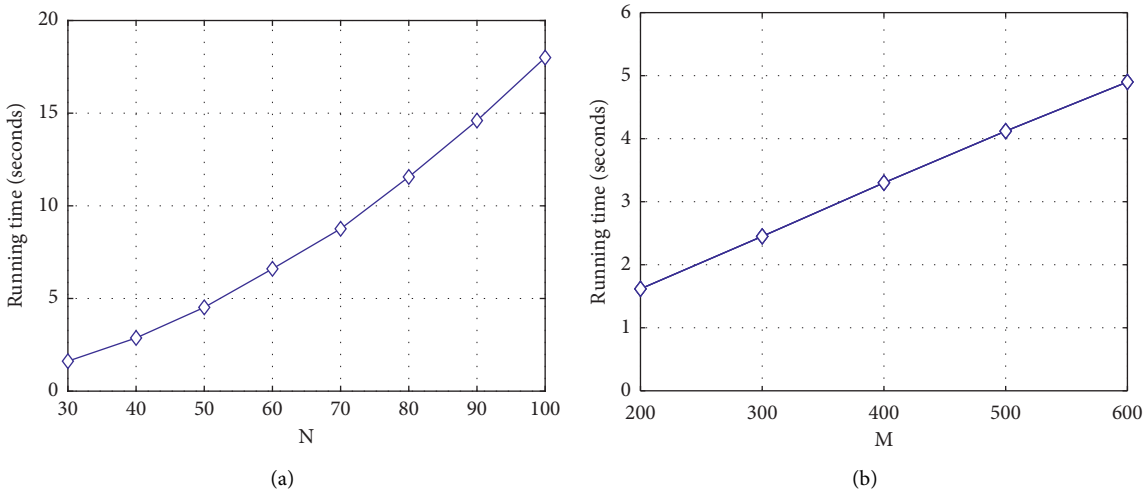

Figure 6: The time efficiency of the proposed mechanism. (a) The number of vehicles willing to participate. (b) The number of vehicles.

Table 1: Smart contract running result.

status	0 ×1 Transaction mined and execution succeed
transaction hash	0 × dc95c1be5d36bd4876167e454ecb1dd5a80752aef4fde1899beba8544c37c53d
from	0 × ca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Auction.run() 0 × 692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	99999999999999999999 gas
transaction cost	1887509 gas
execution cost	3133437 gas
hash	0 × dc95c1be5d36bd4876167e454ecb1dd5a80752aef4fde1899beba8544c37c53d
import	0 × c04. . .06226
decoded input	{}
decoded output	{}
logs	[{”from”: ”0x692a70d2e424a56d2c6c27aa97d1a86395877b3a,” ”topic”: ”0 × 223049034c7b838b932cc4017be9fe8a14c35c24f08efe5ff82f515a576fa903,” ”event”: ”logUintArray,” ”args”: {”0”: ”winners,” ”1”: [”9”,”1”,”4”,”10”], ”length”: 2}}, [{”from”: ”0x692a70d2e424a56d2c6c27aa97d1a86395877b3a,” ”topic”: ”0 × 223049034c7b838b932cc4017be9fe8a14c35c24f08efe5ff82f515a576fa903,” ”event”: ”logUintArray,” ”args”: {”0”: ”payments,” ”1”: [”12”,”12”,”12”,”12”],” length”: 2}}]

pending status will be displayed in the terminal, like the first line in Table 1. After execution of it, the information of this execution will be displayed as a table in the terminal, like the table in Table 1. To execute a smart contract, an account must be chosen and some amount of gas that is larger than the transaction and execution need have to be left. In Table 1, the value of “from” ended with 733c is the account address that triggered the execution. The value of “to” is the address of the current smart contract. The value of “gas” is the gas limit that the account that triggers the execution allows using, which we set to multiple 9 s in the experiment. And the values of “transaction cost” and “execution cost” are the actual cost of gas of this execution. This means CSP has to pay for ISP’s work to execute the auction in our system. If we set the gas limit to zero which means CSP does not pay for ISP, the smart contract will not be executed. The value of “logs” in Table 1 is what we let the smart contract log which are the winners and their payments. In the first part of the log, we can see the winners’ IDs are 9, 11, 4, and 10. These IDs we assigned for easier understanding by human in this experiment, which are temporary account addresses like the value of “from” assigned to users in interactions before the auction in real system. And in the second part we can see the payments of them are all 12 in this time of simulation. Through this experiment, we ensure that our ideas of privacy protection and payment to incentive vehicles can be done based on blockchain.

8. Conclusion

In this paper, we propose a new system architecture of mobile crowdsensing which not only can preserve the privacy of vehicles but also efficiently incentivize them to participate in the tasks. We apply the satellite-terrestrial system to solve the communication limitation among vehicles. This system is deployed on devices of ISP and based on blockchain and uses smart contracts to deal with the interactions among the roles in the system. Four smart contracts are implemented to do tasks requesting, running an auction to select appropriate vehicles, payment operating, and sensed data accessing. This structure preserves the privacy of vehicles because crowdsensing providers cannot know their identities and sensitive information. We design an auction algorithm that aims to minimize the total payment and ensure the completion of the tasks with given aggregation accuracy constraints. We discuss the NP-hardness and mathematical proofs of the five properties of this auction. We implement the auction algorithm in Ethereum as a smart contract.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by Research Innovation Fund for College Students of Beijing University of Posts and Telecommunications.

References

[1] H. Yang, X. Xie, and M. Kadoch, “Intelligent resource management based on reinforcement learning for ultra-reliable and low-latency iov communication networks,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4157–4169, 2019.

[2] Z. Wang, J. Hu, R. Lv et al., “Personalized privacy-preserving task allocation for mobile crowdsensing,” *IEEE Transactions on Mobile Computing*, vol. 18, no. 6, pp. 1330–1341, 2019.

[3] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, “Privacy-preserving energy trading using consortium blockchain in smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.

[4] L. Shi, L. Zhao, G. Zheng, Z. Han, and Y. Ye, “Incentive design for cache-enabled d2d underlaid cellular networks using stackelberg game,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 765–779, 2019.

[5] A. H. Sodhro, J. J. P. C. Rodrigues, S. Pirbhulal, N. Zahid, A. R. L. de Macedo, and V. H. C. de Albuquerque, "Link optimization in software defined iov driven autonomous transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3511–3520, 2021.

[6] F. Amato, G. Cozzolino, F. Moscato, V. Moscato, and F. Xhafa, "A model for verification and validation of law compliance of smart contracts in iot environment," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7752–7759, 2021.

[7] E. Wang, M. Zhang, X. Cheng et al., "Deep learning-enabled sparse industrial crowdsensing and prediction," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 6170–6181, 2021.

[8] L. Wang, Z. Yu, D. Zhang, B. Guo, and C. H. Liu, "Heterogeneous multi-task assignment in mobile crowdsensing using spatiotemporal correlation," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 84–97, 2019.

[9] F. Campioni, S. Choudhury, K. Salomaa, and S. G. Akl, "Improved recruitment algorithms for vehicular crowdsensing networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1198–1207, 2019.

[10] Y. Qu, S. Tang, C. Dong et al., "Posted pricing for chance constrained robust crowdsensing," *IEEE Transactions on Mobile Computing*, vol. 19, no. 1, pp. 188–199, 2020.

[11] Y. Li, L. Zhu, H. Wang, F. R. Yu, and S. Liu, "A cross-layer defense scheme for edge intelligence-enabled cbtc systems against mitm attacks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, 2021.

[12] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[13] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156–4165, 2020.

[14] D. Andreoletti, T. Velichkova, G. Verticale, M. Tornatore, and S. Giordano, "A privacy-preserving reinforcement learning algorithm for multi-domain virtual network embedding," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2291–2304, 2020.

[15] L. Zhu, Y. Li, F. R. Yu, B. Ning, T. Tang, and X. Wang, "Cross-layer defense methods for jamming-resistant cbtc systems," *Transactions on Intelligent Transportation Systems*, vol. 22, no. 11, 2021.

[16] A. Asheralieva, D. Niyato, and Z. Xiong, "Auction-and-learning based lagrange coded computing model for privacy-preserving, secure, and resilient mobile edge computing," *IEEE Transactions on Mobile Computing*, no. 1–1, 2021.

[17] M. Xiao, W. Jin, M. Li, L. Yang, A. Thapa, and P. Li, "Collusion-resistant worker recruitment in crowdsourcing systems," *IEEE Transactions on Mobile Computing*, no. 1–1, 2021.

[18] D. Liu, A. Hafid, and L. Khoukhi, "Multi-item auction based mechanism for mobile data offloading: a robust optimization approach," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4155–4168, 2020.

[19] Y. Lin, Z. Cai, X. Wang, F. Hao, L. Wang, and A. M. V. V. Sai, "Multi-round incentive mechanism for cold start-enabled mobile crowdsensing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 993–1007, 2021.

[20] G. Yang, X. Shi, L. Feng, S. He, Z. Shi, and J. Chen, "Cedar: a cost-effective crowdsensing system for detecting and localizing drones," *IEEE Transactions on Mobile Computing*, vol. 19, no. 9, pp. 2028–2043, 2020.

[21] T. Li, T. Jung, Z. Qiu, H. Li, L. Cao, and Y. Wang, "Scalable privacy-preserving participant selection for mobile crowdsensing systems: participant grouping and secure group bidding," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 855–868, 2020.

[22] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in v2g network," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5799–5812, 2020.

[23] L. Zhu, H. Liang, H. Wang, B. Ning, and T. Tang, "Joint security and train control design in blockchain empowered cbtc system," *IEEE Internet of Things Journal*, 2021.

[24] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4197–4205, 2019.

[25] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11169–11185, 2019.

[26] Z. Ning, S. Sun, X. Wang et al., "Blockchain-enabled intelligent transportation systems: a distributed crowdsensing framework," *IEEE Transactions on Mobile Computing*, no. 1–1, 2021.

[27] J. An, J. Cheng, X. Gui et al., "A lightweight blockchain-based model for data quality assessment in crowdsensing," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 1, pp. 84–97, 2020.

[28] A. Guidotti, "Beam size design for new radio satellite communications systems," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11379–11383, 2019.

[29] Y. Ruan, Y. Li, C.-X. Wang, R. Zhang, and H. Zhang, "Energy efficient power allocation for delay constrained cognitive satellite terrestrial networks under interference constraints," *IEEE Transactions on Wireless Communications*, vol. 18, no. 10, pp. 4957–4969, 2019.

[30] L. Bai, Q. Xu, S. Wu, S. Ventouras, and G. Goussetis, "A novel atmosphere-informed data-driven predictive channel modeling for b5g/6g satellite-terrestrial wireless communication systems at q-band," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14225–14237, 2020.

[31] D. Chen, C. Yang, P. Gong et al., "Resource cube: multi-virtual resource management for integrated satellite-terrestrial industrial iot networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11963–11974, 2020.

[32] P. K. Sharma, B. Yogesh, D. Gupta, and D. I. Kim, "Performance analysis of iot-based overlay satellite-terrestrial networks under the interference," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 3, 2021.

[33] Z. Ma, Y. Wang, J. Li, and Y. Liu, "A blockchain based privacy-preserving incentive mechanism for internet of vehicles in satellite-terrestrial crowdsensing," in *Proceedings of the 2021 IEEE 7th International Conference on Computer and Communications (ICCC)*, Chengdu, China, December 2021.

[34] B. Di, H. Zhang, L. Song, Y. Li, and G. Y. Li, "Ultra-dense LEO: integrating terrestrial-satellite networks into 5G and beyond for data offloading," *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 47–62, 2019.

[35] C. Qiu, H. Yao, F. R. Yu, F. Xu, and C. Zhao, "Deep Q-learning aided networking, caching, and computing resources

allocation in software-defined satellite-terrestrial networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5871–5883, 2019.

[36] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and demonstration of blockchain applicability framework," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1142–1156, 2020.

[37] Z. Zhang, S. He, J. Chen, and J. Zhang, "REAP: an efficient incentive mechanism for reconciling aggregation accuracy and individual privacy in crowdsensing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 2995–3007, 2018.

[38] D. Yang, X. Fang, and G. Xue, "Truthful auction for cooperative communications," in *Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 1–9, Paris, France, May 2011.