Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6807257, 14 pages
https://doi.org/10.1155/2022/6807257

Research Article

Blockchain-Based Incentive Mechanism for Spectrum Sharing in IoV

Hongning Li,[1] Jingyi Li ,[2] Hongyang Zhao ,[3] Shunfan He,[4] and Tonghui Hu[2]

[1] *Xidian Guangzhou Institute of Technology, Guangzhou, Guangdong 511370, China*
[2] *Xidian University, Xi'an, Shaanxi 710071, China*
[3] *CEPREI, Guangzhou, Guangdong 511370, China*
[4] *South Central University for Nationalities, Wuhan, Hubei 430073, China*

Correspondence should be addressed to Hongyang Zhao; zhaohy@ceprei.com

Received 17 December 2021; Accepted 30 March 2022; Published 28 April 2022

Academic Editor: Celimuge Wu

In this paper, we design a blockchain-based incentive mechanism for the problem of low-level participation of primary users caused by location privacy leakage during spectrum data sharing in the Internet of Vehicles (IoV). First, we propose a K -anonymous location protection scheme for multiuser cooperation, which can protect the location privacy of primary users by generalizing their location information through the construction of anonymous areas. Then, we design an incentive mechanism, which performs reporting and adjudication strategy through the transaction stored in blockchain. Simulation results indicate that the proposed scheme can effectively prevent the privacy leakage of primary users' location and encourage them to actively participate in spectrum sharing in IoV.

1. Introduction

With the development of information technology, 6G will further realize the Internet of everything, establish multilevel and full-coverage seamless connection, and serve the key areas of multi-industry integration such as communication, transportation, and automobile. The vehicle networking system is being developed more quickly with the new generation of information and communication technology. 6G needs to support high-level security to meet the requirements of intelligent vehicle systems. The growing number of vehicles has significantly increased the consumption of spectrum resources. In fact, spectrum resources are divided into various frequency bands in a specific form given by government agencies, which are allocated to users with permission by issuing licenses. However, the existing spectrum management methods lead to some frequency bands being idle for most of the time, and the overall utilization rate of spectrum resources is very low. Take the USA as an example. A large number of investigations by the Federal Communication Commission show that the usage of spectrum resources is extremely unbalanced. Some authorized frequency bands are very crowded, while most of the others are idle [1]. Therefore, how to use spectrum effectively has become an urgent problem to be solved.

The 6G white paper points out that the full and efficient utilization of spectrum resources in different frequency bands can be realized through recultivation, aggregation, and sharing. It meets the spectrum needs of the 6G era. Most of the existing methods for obtaining free spectrum are based on the perception of secondary users, but the accuracy may be affected by malicious users. How to encourage primary users to actively participate in spectrum sharing and improve the accuracy of available spectrum information is an urgent problem to be solved.

Incentive mechanism can guarantee the needs of participating users through special forms of interest division, which is an effective way to stimulate users to participate in spectrum sharing. In spectrum sharing, to get benefits, primary users with permission can share the bands when they have no communication requirements. Other users that can use idle band shared by primary users are called secondary users. To get spectrum information, Feng et al. propose a monetary incentive mechanism based on reverse auction to encourage secondary users to participate in spectrum sensing [2]. Li et al. adopt a pricing mechanism based on maximizing expected utility to encourage users to participate in perception. Ying et al. [3] use cooperative spectrum sensing schemes based on the evolutionary game and Stenberg game model to improve detection performance [4]. However, most of the current research considers using spectrum sensing technology to obtain idle spectrum information and use idle bands for opportunities, while little research is done on the active sharing of primary users. Elnahas et al. [5] propose an auction mechanism with time-varying valuation information to maximize auction revenue to encourage primary users to join the market. Literature [6] proposes to increase auction revenue in a dynamic secondary market to improve spectrum utilization. In fact, the participation of primary users can effectively improve spectrum utilization efficiency.

The effective implementation of spectrum sharing in IoV depends on the active participation of all users in the network. How to encourage the primary users to actively participate in spectrum sharing is one of the important issues that need to be studied in IoV.

In addition, the primary users need to submit a certain range of location information to a third party (such as a spectrum distribution center) in spectrum sharing in IoV. The more precise the location provided, the more conducive to the allocation and use of free spectrum. Untrustworthy third parties can infer their personal sensitive information from the primary users' spectrum status and sharing license information, causing hidden dangers to user privacy and security [7], thereby reducing the primary users' enthusiasm for participating in spectrum sharing. Due to the lack of protection of the location information and effective incentive mechanism for primary users in IoV, primary users have no incentive to participate in spectrum sharing.

At present, there are many blockchain-based technologies and methods applied in privacy protection. In 2016, Yuan et al. used blockchain technology to build a secure and trusted distributed autonomous transportation system for the first time [8]. Benjamin et al. proposed a distributed storage-based vehicle networking system based on Ethereum to achieve secure communication between vehicles [9]. In the literature [10–12], to provide reliable reference and credible data for law enforcement agencies involved in information exchange or traffic accident evidence collection, a distributed data storage is constructed using blockchain technology. According to the literature [13–16], blockchain distributed storage can enhance the reliability of data, and users in the blockchain system use pseudonyms, which cuts off the connection between user names and their real identities and prevents malicious nodes from obtaining users' real identity. In [17], blockchain and in-vehicle IoT features and related research questions are discussed. Besides, in literature [18], a multichannel blockchain solution is applied to the blockchain. It can be seen that the current research uses the blockchain to solve the problem of privacy leakage. Therefore, the application of blockchain in the field of privacy protection can be used as an effective means to solve the problem of privacy leakage of main users in the spectrum sharing in IoV.

Therefore, the paper proposes an incentive mechanism based on location privacy protection (IMLPP), which uses the blockchain to protect primary users' location information and encourages them to actively participate in spectrum sharing. The incentive mechanism is designed to improve the utilization rate of the spectrum and further solve the problem of the shortage of spectrum resources. In the proposed mechanism, the distributed K-anonymous scheme based on blockchain is used to generalize the location information of primary users, which ensures that even if the opponents can obtain the spectrum allocation information, the real location of primary users cannot be inferred. The main contributions of the paper are as follows:

(1) We propose a privacy-preserving scheme based on blockchain to generalize primary users' location during spectrum sharing. In this scheme, users with a certain requirement can be selected to cooperate with primary users to construct anonymous areas. The information of construction of anonymous area is stored in blockchain as transaction, and it can be used as evidence of users' behavior

(2) We propose an incentive mechanism to encourage primary users to participate in spectrum sharing. The honesty degree is proposed to measure the integrity of users. Each user in the network has an initial honesty degree, which is updated according to the users' behavior. With deposit payment, honesty degree evaluation algorithm, and users' behavior constraint in the blockchain, the incentive mechanism can effectively encourage primary users to participate in spectrum sharing and constraint users' behavior

2. Spectrum Sharing Incentive Mechanism Based on Location Privacy Protection

2.1. System Model. This paper considers the spectrum sharing model of IoV as shown in Figure 1, which includes a fusion center and multiple vehicle users. Communication is enabled among users and between users and the fusion center. The fusion center issues spectrum sensing tasks, calculates spectrum data, and allocates idle spectrum to secondary users. Primary users share their idle spectrum and protect location information by issuing request for location information protection and constructing anonymous areas with the assistance of other users in the network.

In this paper, the primary users who participate in spectrum sharing and need to protect their location information are called the requesting user, and users that provide encrypted location information to help the requesting user construct an anonymous area are called cooperative users. Requesting users use the location information provided by cooperative users to construct anonymous areas to meet the needs of privacy protection.

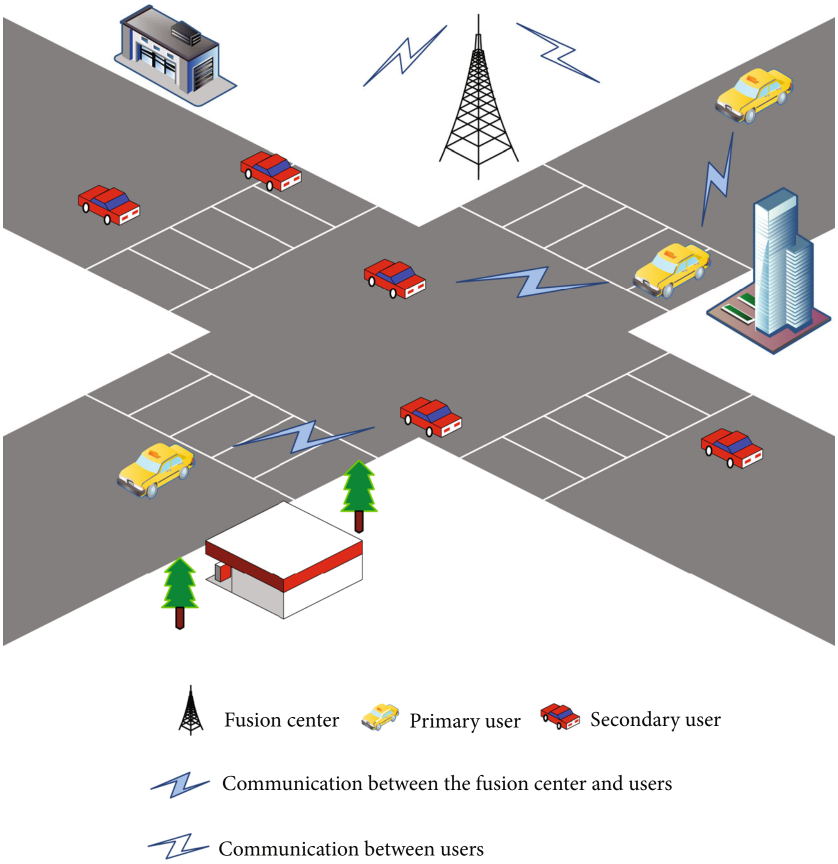
Fusion center
Primary user
Secondary user
Communication between the fusion center and users
Communication between users

Figure 1: System model.

To construct a reliable anonymous area, cooperative users' behavior should be constrained. In this paper, we define two types of illegal behaviors, one is requesting users who disclose the location information of cooperative users, and the other one is cooperative users who provide false locations. The process of assisting a requesting user to construct anonymous area is regarded as a transaction. The requesting user ID, the cooperative user ID, and the location information of the cooperative user are taken as transaction bill information and then encrypted and recorded in the blockchain (the blockchain is a private chain in IoV). This process will generate a certain amount of virtual currency (called mining) in the blockchain system.

2.2. Incentive Mechanism Based on Location Privacy Protection. In this section, an incentive mechanism based on location privacy protection (IMLPP) is proposed, which is shown in Figure 2. The mechanism uses K-anonymous scheme based on blockchain with cooperative users to generalize primary users' location information. In this mechanism, an honesty degree evaluation mechanism is designed to provide a basis for selecting between requesting users and cooperative users. By paying the deposit, reporting and adjudicating with the transaction bill as the evidence, users' location information can be protected. On this basis, the honesty degree and virtual currency in the blockchain are taken as incentives for the primary users to participate in spectrum sharing.

IMLPP scheme is divided into four sections, honesty degree mechanism, anonymous area construction, report and adjudication strategy, and incentive mechanism.

2.2.1. Honesty Degree Mechanism. In the honesty degree mechanism, honesty degree is used to measure the credibility of users, as the basis for mutual choice in the transaction, to meet the user's personalized security requirements for location privacy, and as the reference basis for the fusion center to allocate spectrum. Specifically, requesting users want the cooperative users with high honesty degree to participate in anonymous area construction to ensure the accuracy of the location provided by cooperative users. Cooperative users also tend to cooperate with requesting users with high honesty degree to ensure that location information is not disclosed. Secondary users with high honesty degree will be allocated spectrum with high probability.

The honesty degree evaluation algorithm is the basis of honesty degree update. Assuming that m_0 and m_1 are constant coefficients, m_0 and m_1 can be any positive number, and the value of m_0 and m_1 has no effect on the results of this experiment. We consider $m_0 = 20$, $m_1 = 20$ in this paper. B is a Boolean variable, and if the user has illegal behavior, $B = 0$, and on the contrary, $B = 1$. The initial honesty degree H_0 of all users is 60, and the upper limit of the honesty degree is 200. We assume that the current honesty degree of user U_i is H_i, and the honesty degree evaluation algorithm is shown in Algorithm 1.

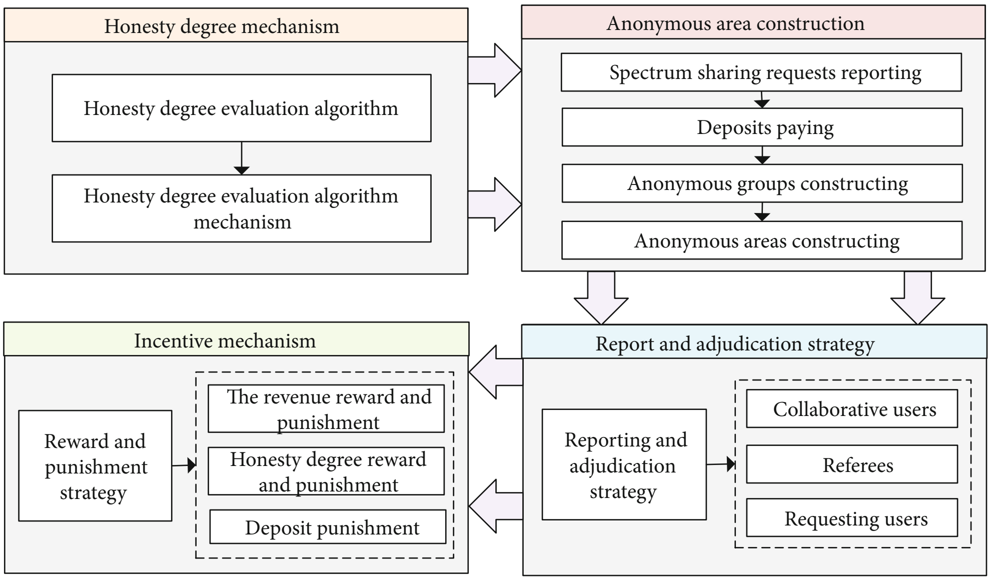
Honesty degree mechanism
Honesty degree evaluation algorithm
Honesty degree evaluation algorithm mechanism
Anonymous area construction
Spectrum sharing requests reporting
Deposits paying
Anonymous groups constructing
Anonymous areas constructing
Incentive mechanism
Reward and punishment strategy
The revenue reward and punishment
Honesty degree reward and punishment
Deposit punishment
Report and adjudication strategy
Reporting and adjudication strategy
Collaborative users
Referees
Requesting users

Figure 2: IMLPP.

According to the honesty degree evaluation algorithm, if the user's honesty degree is higher, the more honesty degree will be deducted when the user commits illegal acts, and the more slowly of the user's honesty degree increases.

2.2.2. Anonymous Area Construction. This section gives the detail of anonymous area construction, which uses distributed K-anonymous scheme to protect primary users' location information. It contains spectrum sharing requests, deposits paying, anonymous groups constructing, and anonymous areas constructing. Among them, the anonymous group is a set of users who are willing to participate in the construction of the anonymous area and meet the requirements.

To illustrate, we take a primary user PU_i as an example. PU_i sends a request to the smart contract:

$$\text{request} = \left\{ID_{PU_i}, H_{PU_i}, H_U, (K-1)\right\}, \tag{1}$$

where ID_{PU_i} is the only identifier of PU_i in the blockchain system. H_{PU_i} is PU_i's honesty degree. H_U is the lower limit of the honesty degree of cooperative users. $(K-1)$ is the number of cooperative users to meet different requirements of different requesting users for location privacy.

After receiving the request, the smart contract determines whether to assist in constructing the anonymous area according to PU_i's honesty degree H_{PU_i}:

(1) When $\mathrm{H_{PU_i}} < 40$, the request is rejected.

Then, the smart contract calculates and returns the deposit that PU_i has to pay:

$$D_{PU_i} = \frac{m_2}{H_{PU_i}}, \tag{2}$$

where m_2 is the income to be generated from this mining. It can be seen from Formula (2) that the higher the honesty degree, the lower the deposit PU_i need to pay.

After paying the deposit, PU_i's location protection request is broadcasted in the network, and other users in the network choose whether to participate in the anonymous area construction according to PU_i's honesty degree H_{PU_i}. In order to guarantee the construction of anonymous area, this paper introduces willingness list wish $= \{U_1 : H_{U_1}, U_2 : H_{U_2}, \cdots, U_i : H_{U_i}\}$, which includes users' honesty degree and their serial numbers.

When the user U_i is willing to participate in the anonymous area construction, it sends a request to the smart contract. Then, the smart contract will put U_i into the willingness list. If U_i's honesty degree $H_{U_i} \geq H_U$, the smart contract returns the deposit D_{U_i}, and U_i will join the anonymous group after paying the deposit D_{U_i}, which meets the following requirements:

$$D_{U_i} = \frac{m_2}{K * H_{U_i}}. \tag{3}$$

If K-1 cooperative users join the anonymous group, the anonymous group is successfully constructed. If the anonymous group construction fails because K or H_U value is too high, the smart contract will send the wish list to PU_i. PU_i adjusts H_U and K according to the wish list and sends to the smart contract to reconstruct the anonymous group.

After the anonymous group is successfully constructed, all cooperative users $U_i (i = 1, 2, \cdots, K-1)$ in the group send PU_0 location information bills $Bill_{LOC_{U_i}}$, which meets the following requirements:

$$Bill_{LOC_{P_i}} = \left\{ID_{U_i}, P_{PU_i}\left(E_{U_i}\left(Loc_{U_i}\right)\right)\right\}, \tag{4}$$

where ID_{U_i} is the cooperative user U_i's identity, Loc_{U_i} is U_i's

```
Input: Current honesty degree $H_i$;
Output: Updated honesty degree $H_{i'}$.
For each $H_i$ do:
    if $B$=0:
            //The user has illegal behavior
        $H_{i'}=H_i - H_i/m_1$
    else if $B=1$ and $H_i < 200$:
            //The user is honest and the current honesty degree level is not up to the upper limit
        $H_{i'} = H_i + m_0/H_i$
        if $H_{i'} > 200$:
                //Updated fidelity exceeds the upper limit
            $H_{i'} = 200$
    else:
            //The user is honest and the honesty degree reaches the upper limit
            $H_{i'} = 200$
```

Algorithm 1: Honesty degree evaluation algorithm.

location information, and $E_{U_i}(Loc_{U_i})$ is the encrypted ciphertext of location information using the U_i's SU1 private key and PU_i's public key.

PU_i uses his private key and U_i's public key to decrypt the ciphertext $E_{U_i}(Loc_{U_i})$ and obtain U_i's location information Loc_{U_i}, which is used to construct the location anonymous area.

We assume PU_i's identity is ID_{PU_i}, and the location information is Loc_{PU_i}. Before using the location privacy protection scheme, PU_i submits location information that is shown in Table 1, and the fusion center can directly obtain PU_i's location information.

With the location privacy protection scheme, a multilocation information anonymous area is submitted to the fusion center by PU_0. As shown in Table 2, the probability that the fusion center can correctly analyze the location information of the primary user is only *1/K*.

After the anonymous area is constructed, PU_i submits the anonymous area together with the spectrum sharing license to the fusion center. Then, $P_{PU_i}(E_{U_i}(Loc_{U_i}))$, ID_{PU_i}, and ID_{U_i} are written into the transaction bill by PU_i for broadcasting throughout the network, which is shown in Table 3. The users with honesty degree greater than 60 in IoV jointly participate in the calculation competition to write the transaction bill on the block and add the block to the blockchain.

Since the size of the anonymous area is much larger than the moving distance of vehicles during the time when the anonymous area is constructed, the error caused by the vehicle movement is ignored in this paper.

2.2.3. Report and Adjudication Strategy. For the possible users' illegal behaviors in this scheme, this paper proposes a strategy for judging and punishing illegal behaviors, which is called report and adjudication strategy. In addition, we give the concept of referees to refer to those users who participate in adjudicating illegal behavior. Firstly, the reporting and adjudication strategy of requesting users and cooperative users are defined as follows.

(1) Definition I (Reporting and Adjudication Strategy).

(i) In the reporting and adjudication strategy a_1, we define the reporting and adjudication strategy of cooperative users. When U_i discovers that his location information is leaked by PU_i, U_i sends the smart contract a request to report PU_i, and provides evidence of PU_i 's illegal behavior. Then the request is broadcasted in the network. The first 50 users (referees) in the network to respond carry out verification and adjudication. Referees retrieve transaction bills in the blockchain, verify the report information according to the transaction bills, and determine whether support the reporting based on the evidence

(ii) In the adjudication strategy a_2, we define the reporting and adjudication strategy of the requesting users. When PU_i finds that the security of the constructed anonymous area is reduced due to the provision of false location information by U_i, PU_i uses his private key to decrypt $P_{PU_i}(E_{U_i}(Loc_{U_i}))$ in the transaction bill, and obtain $E_{U_i}(Loc_{U_i})$. Then, $E_{U_i}(Loc_{U_i})$ and related evidence (such as the location is no man's land, etc.) are sent to the smart contract for reporting, which is broadcasted in the network. After verifying the report information, the referees use U_i 's public key to decrypt the ciphertext $E_{U_i}(Loc_{U_i})$ to get the location information Loc_{U_i}. Finally, referees determine whether support the report based on Loc_{U_i} and the evidence

According to reporting and adjudication strategy, after the user initiates a report, if there are more than 25 referees who support the report, it will be determined that the

Table 1: Position table before generalization.

User	Location information
ID_{PU_i}	Loc_{PU_i}

Table 2: Anonymous area.

User	Location information
ID_{PU_i}	$Loc_{U_1}, Loc_{U_2}, Loc_{U_3}, \ldots, Loc_{PU_i}, \ldots, Loc_{U_{k-1}}$

Table 3: Transaction bill.

User	Location information
ID_{PU_0}	–
ID_{U_1}	$P_{PU_i}\left(E_{U_1}\left(Loc_{U_1}\right)\right)$
ID_{U_2}	$P_{PU_i}\left(E_{U_2}\left(Loc_{U_2}\right)\right)$
…	…
$ID_{U_{K-1}}$	$P_{PU_i}\left(E_{U_{K-1}}\left(Loc_{U_{K-1}}\right)\right)$

reported user has illegal behavior; otherwise, the report will be invalid.

Considering that the referee may make an adjudication without verification, which will affect the report result, this paper puts forward the adjudication strategies for the referee's illegal behaviors.

For the referee J_i, if the adjudication is wrong for T consecutive times, J_i would be adjudicated as an illegal user, and the T value meets

$$T = \left[H_{J_i}{}^{m_4}\right] + m_5, \tag{5}$$

where H_{J_i} is J_i's honesty degree. The value range of m_4 is between 0 and 1, and m_5 can be other positive numbers. In subsequent simulation experiments, we consider m_4= 0.5, m_5=2.

From Formula (5), the value of T is related to the honesty degree of the user. The higher the honesty degree of the user, the better the inclusiveness to the user, and the more times the error can be decided.

2.2.4. Incentive Mechanism. To encourage the primary user to participate in spectrum sharing, all users in the network to participate in anonymous area construction and adjudication and restrict users' behavior; this paper proposes reward and punishment mechanisms in different scenarios.

(1) Definition II (Responsivity). The ratio of the number of users responding to a primary user's request for anonymous area construction information to the total number of users in the network is called the response rate.

For the primary users, the higher the honesty degree, the higher the response rate. Only by improving the honesty degree can the higher response rate be obtained. For secondary users, only by improving honesty degree can they have higher priority in spectrum allocation. Therefore, in addition to the virtual currency in the blockchain, honesty degree is also used as an incentive for users. In this scheme, we propose a reward and punishment mechanism to reward users and punish users who have illegal behavior, which consists of reward and punishment strategies in three aspects, namely income, deposit, and honesty degree.

(2) Definition III (Reward and Punishment Strategy).

(i) In the reward and punishment strategy b_1, the revenue reward and punishment are defined. Users who participate in anonymous area construction or spectrum sharing will get virtual currency rewards, and users who have illegal behaviors have lower income in the penalty round (we set the penalty round to 10 rounds).

After the transaction bill is linked up, the miners look for whether there is a penalty transaction bill for PU_i's and U_i's illegal behaviors in the blockchain. Assume that m_2 is the virtual currency generated by the miner through mining, and the miner obtains virtual currency is $m_2/3$:

(1) If no penalty transaction bill for PU_i's illegal behavior is found in the blockchain, the miner will assign PU_i virtual currency C_{PU_i}, which meets the following requirements:

$$C_{PU_i=}\frac{m_2}{3}. \tag{6}$$

(2) If no penalty transaction bill for U_i's illegal behavior is found in the blockchain, the miner will assign U_i virtual currency C_{U_i}, which meets the following requirements:

$$C_{U_i=}\frac{m_2}{3K}. \tag{7}$$

(3) When PU_i's illegal behavior is found and it exists in the lth block $block_l$, assume that N is the current number of blocks, C_i is the income when the user has no illegal behavior, and C_i' is the actual income of the user this time:

(a) If $N - L \leq 10$, then the miner assigns virtual currency to the user:

Table 4: Simulation parameter table.

Parameters	Meaning	Default
N	Number of users	10000
A	Proportion of primary users	30%
B	Proportion of secondary users	50
C	Percentage of attackers	20%
Cycle	Number of simulations	0 ~ 200
Block	Current block length	100
M	Number of transactions stored per block	100
K	Number of users participating in anonymous area construction	2 ~ 37

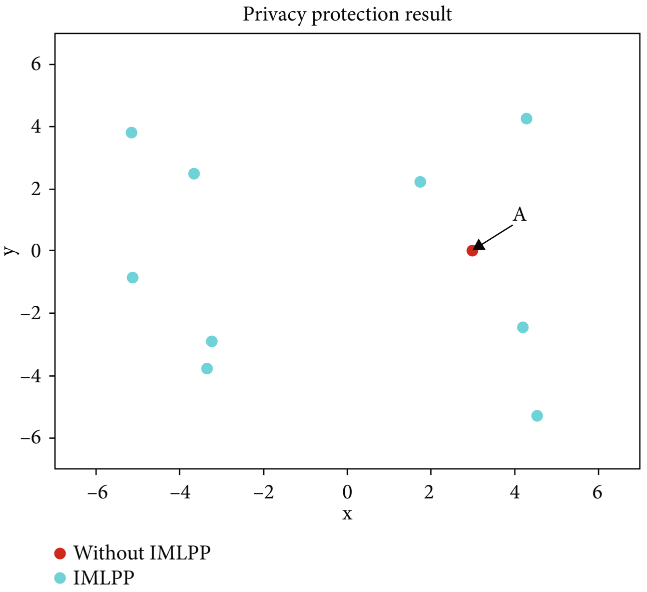

Figure 3: Anonymous region of $K = 10$.

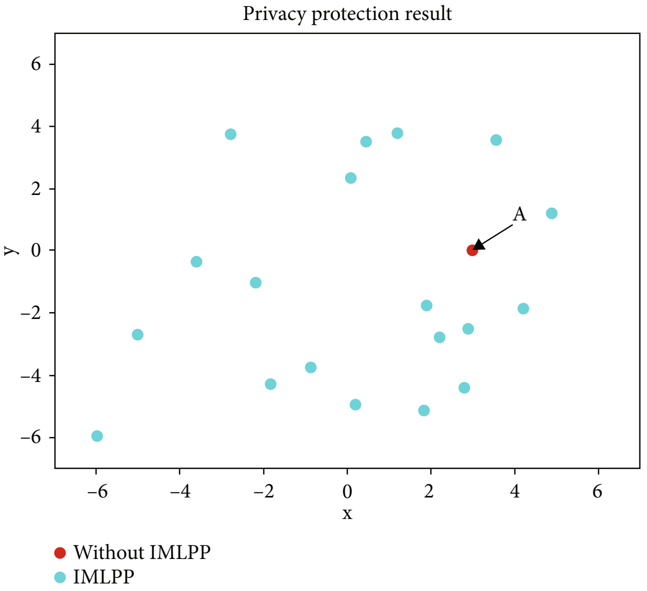

Figure 4: Anonymous region of $K = 20$.

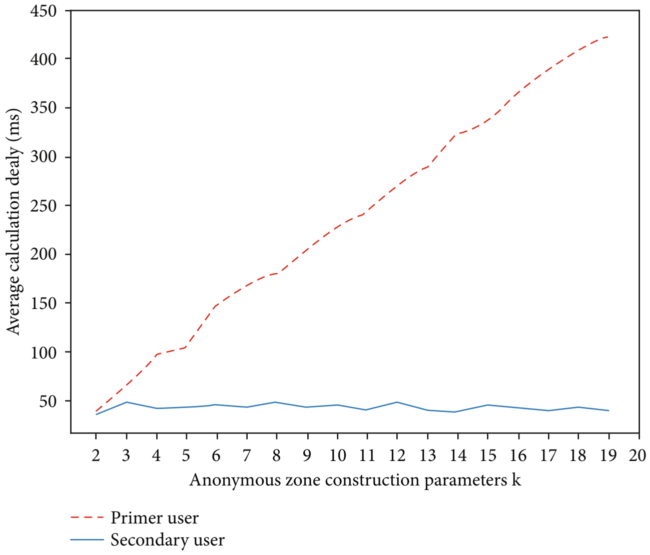

Figure 5: Average calculation delay.

$$C_i{}' = \frac{C_i}{2}. \tag{8}$$

(b) If $N - L < 10$, then the miner assigns virtual currency to the user:

$$C_i{}' = C_i. \tag{9}$$

(ii) In the reward and punishment strategy b_2, honesty degree reward and punishment and deposit punishment are defined. The honesty degree is updated according to the honesty degree evaluation algorithm. If users participate in anonymous area construction, share spectrum, or have illegal behavior, their honesty degree will be updated. Besides, the deposit paid by illegal users will be used as compensation for privacy victims

After the transaction bill is linked, PU_i's and U_i's honesty degree H_i will be updated as follows according to the honesty degree evaluation algorithm:

$$H_i = H_i + \frac{20}{H_i}. \tag{10}$$

If there is a user who has illegal behavior during the construction of the anonymous area, the penalty transaction bill will be broadcast and the user will be punished:

(1) If U_i is adjudicated to have illegal behavior, the deposit paid by U_i will be used as PU_i's compensation, and U_i's honesty degree H_{U_i}will be updated as follows according to the honesty degree evaluation algorithm:

$$H_{U_i} = H_{U_i} - \frac{H_{U_i}}{20}. \tag{11}$$

(2) If PU_i is adjudicated to have illegal behavior, the deposit paid by PU_iwill be used as compensation, and PU_i's honesty degree H_{PU_i}will be updated according to the honesty degree evaluation algorithm:

$$H_{PU_i} = H_{PU_i} - \frac{H_{PU_i}}{20}. \tag{12}$$

The following is an introduction to the reward and punishment mechanism of referees.

Assume that a referee J_i's honesty degree is H_i:

(1) If after J_i participating in the ruling, J_i is not determined to be user who has illegal behavior, and J_i's honesty degree will increase to

$$H_{J_i} = \left(H_{J_i} + \frac{20}{H_{J_i}} \right). \tag{13}$$

(2) If J_i's adjudicated to be an illegal user after participating in the ruling, J_i's honesty degree will be reduced to

$$H_{J_i} = \left(H_{J_i} - \frac{H_{J_i}}{20} \right). \tag{14}$$

The reward and punishment mechanisms reward the primary users who participate in spectrum sharing, the cooperative users who participate in the construction of anonymous areas, and the referees who participate in the adjudication, and punish the illegal users, which not only play an incentive role, but also can effectively restrain the user behavior.

3. Simulation Experiment and Analysis

3.1. Simulation Environment. In this section, we conduct a simulation analysis on the proposed IMLPP scheme to verify its impact on location privacy protection and spectrum sharing incentives in spectrum sharing in IoV. The parameter settings of simulation environment are shown in Table 4.

3.2. Simulation Analysis and Results of Location Privacy Protection. In this paper, a distributed K-anonymous

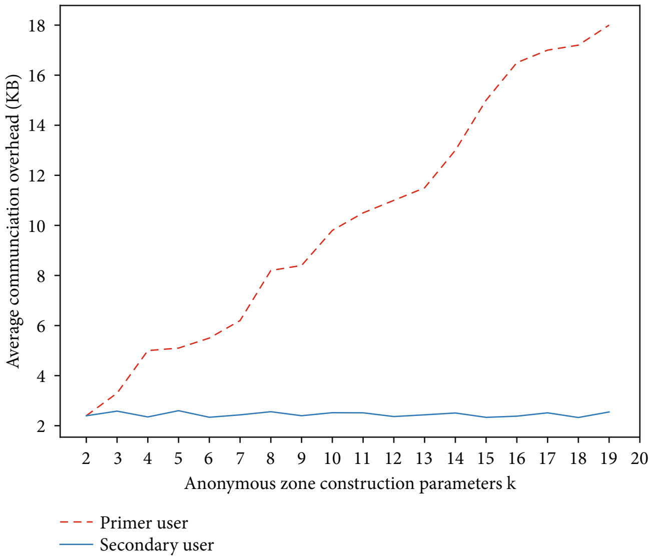

Figure 6: Average communication overhead.

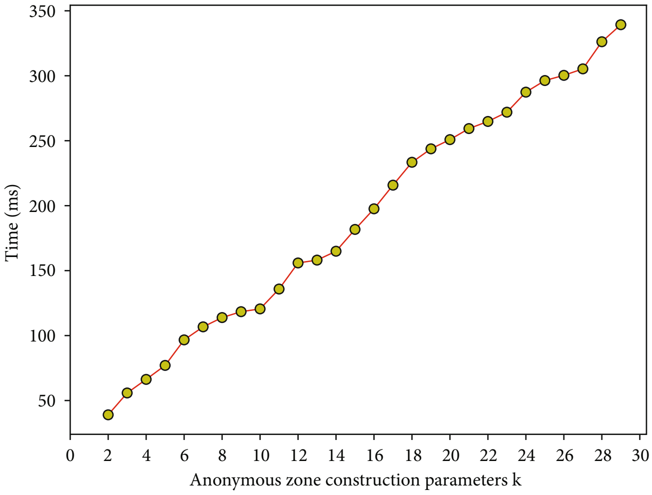

Figure 7: Time consumption for different K values.

algorithm is designed by using blockchain technology, which protects the location privacy security of the primary user in the spectrum sharing of the vehicle network and solves the privacy security threat of the primary user caused by spectrum sharing.

3.2.1. Privacy Protection of Constructing Anonymous Areas. This part of the experiment analyzes the privacy protection effect of the privacy protection scheme on the primary user. The vehicle user running in the vehicle network is regarded as a point moving in a two-dimensional plane coordinate system, and the coordinates of the point represent the position of the user. As shown in Figure 3, before using IMLPP scheme, the user's position is red point A, which can be directly obtained by attackers. After using this scheme, when $K = 10$, the user's position A (3, 0) is generalized to an anonymous area composed of 10 points, and the probability that the attacker can correctly analyze the position of point A is only 1/10. When $K = 20$, as shown in Figure 4, the probability that the attacker gets the location of A is 1/20. The larger the K value, the safer the user's location privacy. We use Java to perform simulation experiments and use Python to plot and analyze the experimental result data.

3.2.2. Influence of Parameter K on Average Computing Delay and Communication Overhead. In this part, the calculation delay and communication overhead of users in the process of anonymous area construction are analyzed experimentally.

We select different K values for simulation experiments; the value of K ranges from 2 to 19 and obtains the user's computing delay and communication overhead, as shown in Figures 5 and 6. It can be seen from the figure that the K value will affect the computational delay and communication overhead required by the requesting users, and the cooperative users will not be affected by it.

This is because when the requesting user receives the location bill of the cooperative user, the requesting user

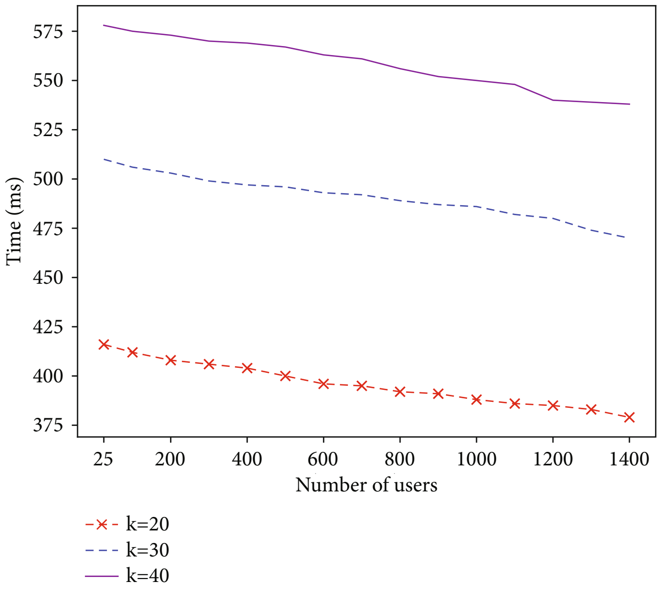

Figure 8: Time consumption when the number of users in the network varies.

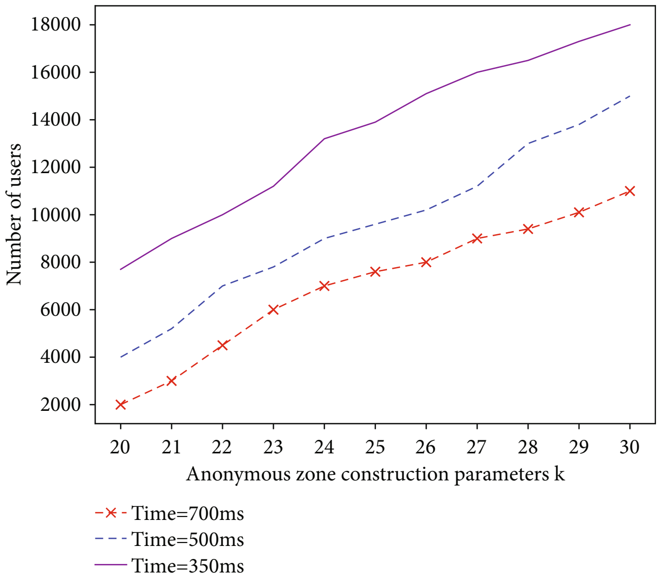

Figure 9: Relationship between users and K value in the network at a limited time.

needs to decrypt the location information using the public key of the cooperative user, while the cooperative user only needs to send the location bill to the requesting user. Therefore, with the increase of K value, the calculation delay required by the requesting user increases, and the cooperative user will not be affected by it, as shown in Figure 5.

In addition, during anonymous area construction, as the number of cooperative users participating in the anonymous area construction increases, the number of location information bills that the requesting user needs to receive increases, and the amount of information that needs to be processed increases, while the cooperative user is not affected. Therefore, as shown in Figure 6, the communication overhead of the requesting user increases with the value of K, while the communication overhead of the cooperative user is not affected by the change of the value of K.

In addition, we control the number of users in the network to be 10,000 and select different K values for simulation experiments. The K value ranges from 2 to 30, and the generation time of the anonymous area is obtained, as shown in Figure 7. The figure shows, when the number of users in the network is fixed, the time for constructing the anonymous area will increase with the increase of the K value, but the larger the K value, the better the location privacy of the primary user can be protected. In addition, when the value of K is fixed, as shown in Figure 8, the number of users in the network is inversely proportional to the time for constructing the anonymous area, and the more users in the

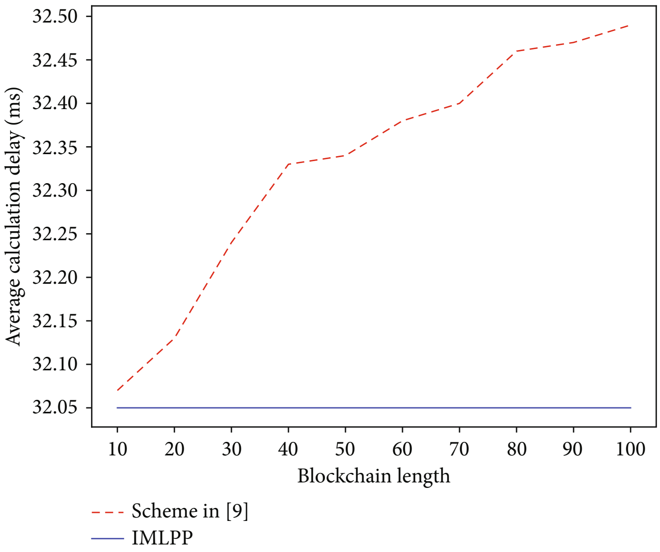

Figure 10: The effect of blockchain length on unauthorized users.

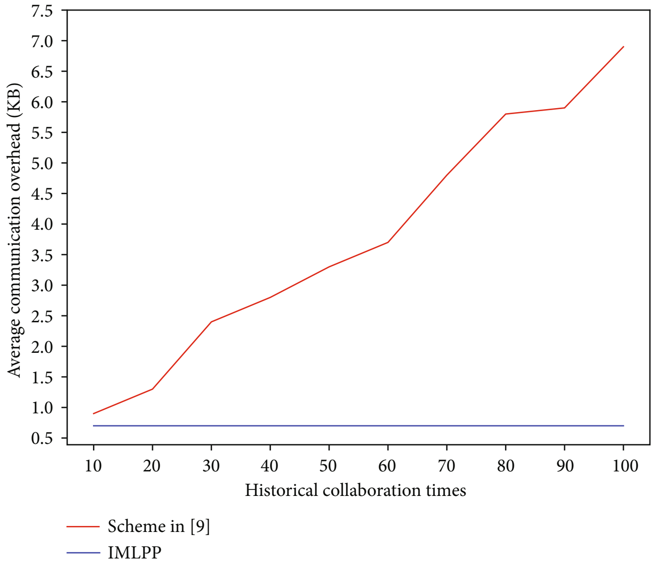

Figure 11: The impact of historical collaboration times on the communication overhead required by requesting users.

network, the less time it takes to construct the anonymous area. However, within a limited time, as shown in Figure 9, the larger the K value required by the primary user, the higher the number of users in the network.

3.2.3. The Influence of Blockchain Length. In this scheme, after receiving an anonymous area construction request sent by an authorized user, it is only necessary to choose whether to participate in its spectrum sharing according to its integrity, and the length of the blockchain will not affect unauthorized users, while in the scheme [19], in order to verify whether there is location privacy leakage or fraudulent behavior in the history of the requesting user, the collaborating user needs to download and query the transaction bills stored in the entire blockchain. Therefore, as shown in Figure 10 in the scheme [19], with the increase in the length of the distributed anonymous area cooperative construction blockchain, the computing delay required by users in the anonymous area construction process is also increasing, and the length of the blockchain will not affect this scheme. Therefore, this scheme can reduce the computational experiment well.

3.2.4. The Impact of Historical Collaboration Times. In scheme [19], the user's ID will be used as an index to retrieve all historical transaction bills containing the ID in the blockchain system, so that each user in the network can trace the historical behavior of requesting users and cooperative users. As shown in Figure 11, as the number of times that the requesting user participates in the construction of the anonymous area as a collaborator increases, the number of transaction bill numbers that the requesting user needs to provide also increases, resulting in the requesting user needing to construct the anonymous area. The communication

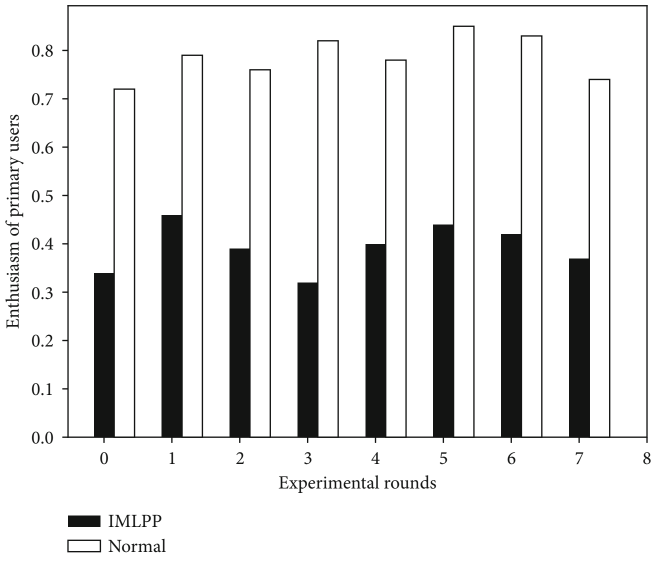

Figure 12: Enthusiasm of primary users to participate in spectrum sharing.

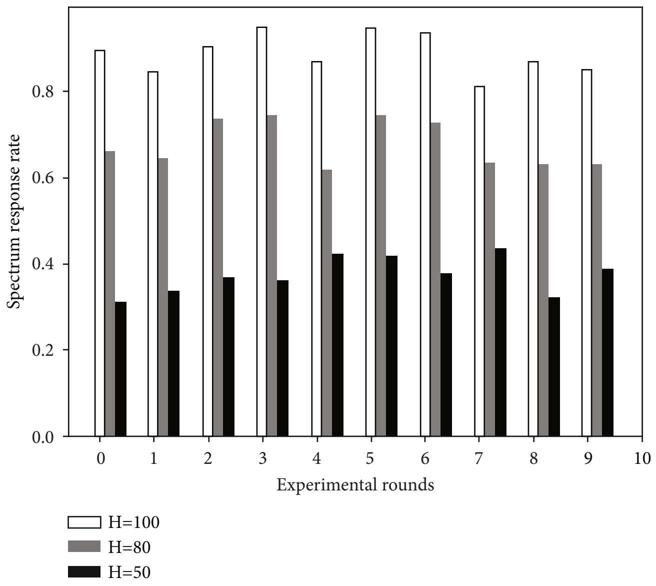

Figure 13: Response rates of primary users with different honesty degree.

overhead also increases, and the integrity evaluation algorithm used in this paper makes the user do not need to provide the transaction bill number, so the number of historical cooperation will not affect the communication overhead required in the construction of the user's anonymous area. This scheme can reduce the communication overhead very well.

3.3. Simulation Results and Analysis of Spectrum Sharing Excitation. This part of the experiment analyzes the incentive effect of incentive mechanism on primary users. In an environment without incentive mechanism, primary users are divided into three types: (1) always actively share their idle spectrum, (2) sometimes share their free spectrum, and (3) do not participate in spectrum sharing. Set the initial proportion of class I users with idle spectrum to 20%, class II users to 60%, and class III users to 20%. Assuming that all primary users in the current network have idle spectrum, the proportion of primary users willing to participate in spectrum sharing to the total number of primary users in the network is taken as the positive rate of spectrum sharing. As shown in Figure 12, in the absence of incentives, only the first and second types of primary users will participate in spectrum sharing, and due to the low enthusiasm of the second type of primary users, the positive rate of spectrum sharing is between 0.3 and 0.5. Under the environment of incentive mechanism, the second and third types of primary users will also actively participate in spectrum sharing to obtain virtual currency rewards and improve honesty degree, so the positive rate of spectrum sharing is between 0.7 and 0.9.

As shown in Figure 13, in the histogram, from left to right are the response rates of the primary users with honesty degree of 100, 80, and 50 in the location privacy protection scheme. The higher the honesty degree of the primary users, the higher the response rate. This is because the higher the honesty degree, the more credible the users are, and the more users are willing to participate in their location privacy protection.

4. Concluding Remarks

This paper proposes an incentive mechanism called IMLPP, which uses a blockchain-based K-anonymity scheme to construct a K-anonymity area that meets the needs of the primary user to protect their location information in spectrum sharing. On this basis, honesty degree and virtual currency are used to motivate users. The proposed scheme can effectively generalize primary users' location information, meet their personalized privacy protection needs, and encourage them to actively participate in spectrum sharing. In addition, both requesting users and cooperative users need to pay deposit, which restricts the user's behavior.

Data Availability

The data of secure computation protocols and algorithms used to support the findings of this study are available from the corresponding author upon request.

Additional Points

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is partly supported by the National Key Research and Development Program of China under Grant 2021YFB2700600 and 2019YFC0118800, the National Natural Science Foundation of China under Grant 62132013 and 61903384, the Key Research and Development Programs of Shaanxi under Grant 2021ZDLGY06-03, and High-Level Innovation Research Institute Project under Grant 2021B0909050008.

References

[1] M. Rajendran and M. Duraisamy, "Distributed coalition formation game for enhancing cooperative spectrum sensing in cognitive radio ad hoc networks," *IET Networks*, vol. 9, no. 1, pp. 12–22, 2020.

[2] F. Jingyu, Y. Jinwen, Z. Ruitong, and Z. Wenbo, "Internet of things spectrum sharing incentive mechanism against location privacy leakage," *Computer Research and Development*, vol. 57, no. 10, pp. 2209–2220, 2020.

[3] L. Xiaohui, Z. Qi, and W. Xianbin, "Privacy-aware crowdsourced spectrum sensing and multi-user sharing mechanism in dynamic spectrum access networks," *IEEE Access*, vol. 7, pp. 32971–32988, 2019.

[4] Y. Xuhang, S. Roy, and R. Poovendran, "Pricing mechanisms for crown-sensed spatial-statistics-based radio mapping," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 2, pp. 242–254, 2017.

[5] O. Elnahas, M. Elsabroute, O. Muta, and H. Furukawa, "Game theoretic approaches for cooperative spectrum sensing in energy-harvesting cognitive radio networks," *IEEE Access*, vol. 6, pp. 11086–11100, 2018.

[6] Y. Changyan, J. Cai, and G. Zhang, "Spectrum auction for differential secondary wireless service provision with time-dependent evaluation information," *IEEE Transactionson Wireless Communications*, vol. 16, no. 1, pp. 206–220, 2017.

[7] X. Dong, T. Zhang, D. Lu, G. Li, Y. Shen, and J. Ma, "Preserving geo-distinguishability of the primary user in dynamic spectrum sharing," *IEEE Transactions on Veterinary Technology*, vol. 68, no. 9, pp. 8881–8892, 2019.

[8] Y. Yuan and F. Y. Wang, "Towards blockchain based intelligent transportation systems," in *2016 IEEE 19th international conference on intelligent transportation systems (ITSC)*, pp. 2663–2668, Rio de Janeiro, Brazil, 2016.

[9] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain based vehicular ad-hoc networks," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pp. 137–140, Heidelberg, Germany, 2016.

[10] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.

[11] M. Cebe, E. Ergin, K. Akkaya, H. Aksu, and S. Uluagac, "Block 4forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50–57, 2018.

[12] M. Li, L. Zhu, and X. Lin, "Efficient and privacy preserving carpooling using blockchain assisted vehicular fog computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4573–4584, 2019.

[13] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, and A. Taherkordi, "Mobility-Aware Multi-Hop Task Offloading for Autonomous Driving in Vehicular Edge Computing and Networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–14, 2022.

[14] C. Tan, X. Li, T. H. Luan, B. Gu, Y. Qu, and L. Gao, "Digital twin based remote resource sharing in internet of vehicles using consortium blockchain," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, pp. 1–6, Norman, OK, USA, 2021.

[15] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in industry 4.0 networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2964–2973, 2021.

[16] L. Liu, J. Feng, Q. Pei et al., "Blockchain-enabled secure data sharing scheme in mobile-edge computing: an asynchronous advantage actor–critic learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2342–2353, 2021.

[17] C. Peng, C. Wu, L. Gao, J. Zhang, K. L. Alvin Yau, and Y. Ji, "Blockchain for vehicular internet of things: recent advances and open issues," *Sensors*, vol. 20, no. 18, p. 5079, 2020.

[18] L. Gao, C. Wu, T. Yoshinaga, X. Chen, and Y. Ji, *Multi-channel blockchain scheme for internet of vehicles*, 2021.

[19] L. Hai, L. Xinghua, L. Bin et al., "A distributed K-anonymous location privacy protection scheme based on blockchain," *Journal of Computer Science*, vol. 42, no. 5, pp. 942–960, 2019.