Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **6**, Number **3**, August **2021**

Location Privacy Protection Method Based on EMCS Model and Blockchain

Hui Wang, Wei Zhen, Kun Liu*, Zi-Hao Shen, Pei-Qian Liu, Yan-Peng Wang, Chuan-Han Zhu

College of Computer Science and Technology
Henan Polytechnic University
Jiaozuo 454000, China
786161871@qq.com , 88650698@qq.com , szh@hpu.edu.cn
liupeiqian@hpu.edu.cn , 979949553@qq.com , 1075987762@qq.com
*Corresponding Author: z3460821471@163.com

Received April 2021; revised July 2021

Abstract. *As location-based services facilitate our lives, they also raise many privacy leakage problems, such as users providing false location information or leaking other people's location information. Therefore, how to avoid these problems is still a current research problem. To reduce the participation of self-interested users in anonymous zone construction, this paper proposes a location privacy protection method based on the entropy method and credit system (EMCS) and blockchain technology. First, combined with the entropy method, the EMCS model can be constructed to calculate the Reputation Value of requesting users by obtaining the Credit Rating of users from different credit agencies. Second, collaborative users can quickly determine whether to participate in the construction of an anonymous area according to the Reputation Value of the requested user. Finally, blockchain technology is used to store and verify the information, such as the Reputation Value and reallocation of users. Once a user has acts of bad faith, a penalty bill will be generated for him. As a requester, he won't successfully construct an anonymous area. Experimental results show that this method can ensure the generation efficiency of anonymous area without increasing communication overhead and calculation delay, and provides better protection for the user's location privacy.*
Keywords: location-based services, location privacy protection, credit investigation, entropy method, blockchain

1. **Introduction.** With the continuous progress and development of 5G mobile networks and mobile positioning technology, location-based services (LBS) [1, 2] have been widely used in all areas of our lives, such as location-based navigation query, location-based travel information query, location-based life service query, etc. Meanwhile, with the help of Location-Based Service Provider (LSP), value-added additional services, including points of interest query, are also provided to users. The Swedish company Berg Insight released a forecast report, and the report predicted that beginning from 2014, the global LBS market would grow from 10.3 billion euros to 34.8 billion euros in 2020 at a compound annual growth rate (CAGR) of 22.5%. LBS applications will play a more important role in our daily lives [3]. However, there are a lot of privacy leakage problems while users enjoy the convenience provided by LBS [4, 5]. According to the survey, personal information (including phone numbers) of more than 267 million Facebook users was exposed to unprotected servers in 2019 [6]. Therefore, how to more effectively protect users' privacy and data security is gradually becoming a research hotspot.

The existing location privacy protection technology can be roughly divided into two structures: centralized structure and distributed structure. The centralized structure needs to add a trusted anonymous server between the LSP and the user. The role of the anonymous server is to save the user's private data and help request users to build an anonymous area. However, an anonymous server can easily become a performance bottleneck. Once an attacker successfully breaks the server, all location information of users will be exposed to the attacker, and it is difficult to find a completely trusted anonymous server in practical applications. In order to solve the problems of the centralized structure, experts and scholars have proposed a distributed structure of location privacy protection system. In the distributed structure, mobile users can communicate directly, and protect location privacy by using encryption technology and user collaboration technology on the mobile terminal. However, the existing distributed privacy protection technology has some shortcomings. And they can be improved greatly in how to judge the credibility of the requesting user, how to ensure that location information is not leaked, and how to balance query quality and query efficiency.

Based on the distributed privacy protection scheme, Credit Rating and Reputation Value are introduced to solute the difficulty problem of collaborative users quickly determining whether the requesting user is trustworthy. So that location leakage and location deception can be effectively prevented. Credit Rating is an numerical value used to judge the credit status of users. The numerical value is comprehensively derived from official credit institutions such as Ali Credit, JD IOU, and banks, based on user credit status and credit reports. However, considering that the credit reporting system of different credit agencies is different, it is difficult to make a horizontal comparison by directly using the credit score. Therefore, in order to quickly judge the creditworthiness of users, this paper proposes the concept of Reputation Value. The credibility value is based on the user's real-time credibility value, using the entropy method to process the credibility value, and transform it into a value that is uniform and can be horizontally compared. Using this value, the user's credibility can be accurately and quickly judged.

In summary, this paper uses the EMCS model to digitally measure the integrity of users. The user's Credit Rating obtain through the personal credit reporting system, and the requesting user's Reputation Value can be calculated by using the entropy method. The cooperative user can judge the integrity of the requesting user based on the Reputation Value, and further decides whether to participate in the construction of the anonymous zone. Users will use blockchain technology to save location information. Once one user is verified to have location leakage or location fraud, this user will be punished according to the data in the blockchain. The main contributions of this paper are as follows:

1. According to the requesting user's Credit Rating, the entropy method is used to comprehensively calculate the requesting user's Reputation Value. The collaborative user can quickly judge whether the requesting user is credible according to the Reputation Value, and this will reduce the computational burden of the collaborative user and improve the efficiency of anonymous area construction.
2. Blockchain technology can be used to save the user's real location in the public chain. And it can ensure that user information is not tampered during the construction of the anonymous area. Thus, it will enhance the security of the anonymity set. Once users are discovered to have location leakage and location fraud, they won't successfully construct an anonymous area as requesters. The result will improve the enthusiasm of users.

3. Experiments prove that communication overhead and calculation overhead between the requesting user and collaborative users are less in this method while the requesting user sends an anonymous area construction application. And the comprehensive response time of collaborative users is less. Anonymous regions can also be generated quickly.

2. **Related Work.** At present, as more and more users use location-based services and related value-added services. Therefore, scholars have paid much attention to how to protect the privacy of users. In this section, we mainly describe the related research of distributed structure and blockchain technology in protecting user privacy and security.

2.1. **Location privacy protection scheme under distributed structure.** The earliest distributed K anonymity technology was proposed by Chow [7] and others. It uses point-to-point communication to generate anonymity sets, avoiding third-party servers' problems but increasing network transmission delays.To solve the problem of time delay, Yiu et al. [8] proposed the SpaceTwist scheme, which randomly selects points of interest near the user's real location as anchor points and uses it to replace the user's real location to send a query to the LBS. Although this solution can protect the user's location privacy, it cannot satisfy K-anonymity. Zhang et al. [9] proposed a SCPPS scheme based on the concepts of information partition and user motivation. In this scheme, it is difficult for the cooperative user to obtain any information of the requesting user, and if other users do not collude with the user, the collusion will be difficult to form a query. At the same time, the scheme also proposes an incentive mechanism. Only the cooperative users who submit partition information first and get corresponding feedback can get incentive, which not only ensures the activity of anonymous users, but also has a good protection effect on the information of requesting users. Jin et al. [10] proposed a user centric location privacy transaction framework ULPT, and designed a heuristic algorithm with limited optimal gap, which reduced the budget on the basis of protecting the security of user location privacy.

It was aiming at the problem of K anonymous location privacy protection. Researchers from various countries have also proposed combining different methods to protect users' location privacy. Niu et al. [11] combined with background knowledge and selected points similar to the user's background information to generate an anonymous area. Zhang et al. [12] put forward an algorithm to resist association attacks, allowing users to select nodes that meet the threshold to generate anonymous regions. He et al. [13] used spatial diversity to divide users to achieve the construction of anonymous areas. Schlegel et al. [14] divided the user's query area into grids of equal size. The user sent the query information and grid information to the LBS. The LBS compared the interest points in the grid with the interest points of the requesting user. The matching results are returned to the requesting user. The user communication cost of this solution only depends on the number of relevant points of interest near the user, and at the same time, algorithms such as k-proximity query are used to ensure the efficiency of continuous query and the privacy of users.

Besides, some privacy protection technologies are based on encryption and incentive mechanisms. Yi et al. [15] used homomorphic encryption to protect the requesting user's content and reallocation information. However, encryption technology requires the mobile terminal to have relatively powerful computing capabilities, and ordinary mobile devices cannot meet this requirement. Simultaneously, the use of encryption technology cannot effectively balance the privacy protection of users and the quality of location services. Yang et al. [16] considered user's self-interest and introduced an incentive mechanism.

This scheme proposes that cooperative users will get some benefits by providing help to requesting users, thereby encouraging users to participate in anonymous areas actively. Li et al. [17] proposed a K anonymity protection scheme based on a reputation mechanism. This scheme determines a Reputation Value for the requesting user. Only users who meet this value can successfully construct an anonymous area, and users who participate multiple times will increase their Reputation Value. Nevertheless, this solution needs to upload user information to a semi-trusted cloud server. Although the cloud server can reduce the problem of performance bottlenecks, once an attacker breaches it, all user's private information will be exposed.

2.2. **Location privacy protection scheme combined with blockchain technology.** As blockchain technology has many beneficial properties, researchers have proposed some new location privacy protection schemes based on blockchain characteristics. Amoretti et al. [18] proposed a location verification scheme based on blockchain technology to help LBS verify the user's real geographic location information. However, in location-based services and the authenticity of the user's location information, the trust issue between the user and the LSP is also an essential factor affecting location privacy and security. For this reason, Fan et al. [19] used the decentralization and non-tampering of blockchain technology to ensure access control and privacy of LSPs, to realize mutual trust between users and LSPs in 5G mobile networks. Jia et al. [20] proposed using blockchain technology's immutability in the intelligent crowd perception network. Encourage users to actively participate in the anonymous area's construction so that the anonymous area meets K anonymity needs to ensure user's privacy. Qiu et al. [21] constructed multiple private blockchains to establish communication between mobile users and LBS servers. In user transactions, smart contracts are used to ensure transactions' fairness. Luo et al. [22] designed a trust management method based on Dirichlet distribution in the vehicle-mounted ad hoc network VANET. Using blockchain technology, the credibility of the vehicle is recorded on the public chain in time so that any vehicle can access the historical trust information of the transaction object when necessary. The centralized crowd perception system is vulnerable to attack, intrusion, and manipulation to solve the problem. Yang et al. [23] introduce a private blockchain to distribute user transaction records and use the immutability and decentralization of blockchain technology to hide and protect users' accurate identity information.

Most of the above distributed anonymous construction schemes only consider avoiding LSPs from leaking user location information. It did not analyze in detail the situation where real location information was leaked and users provided false locations. To make up for the shortcomings of the above schemes, this article combines blockchain technology with a distributed structure. They utilized blockchain technology's immutability and decentralization to protect users' location information from tampering and leakage. However, although the existing blockchain technology guarantees the security of location privacy, it cannot avoid location fraud. It has not proposed a better solution for how collaborative users judge whether the requesting user is trustworthy. In summary, this article combines the requesting user's credit rating with the entropy method, and proposes the EMCS model to calculate the requesting user's Reputation Value. Then, using the blockchain and distributed anonymous area constructor, without increasing the calculation delay and communication overhead, location leakage and location spoofing can be avoided with significant probability, and the user's location privacy can be effectively protected.

3. **Related Knowledge.**

3.1. **System structure.** This paper uses a distributed structure, consisting of three parts: requesting user R, cooperating user S, and LSP. When R initiates a query request, it sends a broadcast request for assistance to surrounding users. After S receives the request, it decides whether to participate in the construction of the anonymous area according to the Reputation Value of R. When R receives the real location provided by S, it mixes the location of the requesting user with the real locations of $K-1$ cooperating users to construct an anonymous set, and sends the anonymous set to LBS for query. The system structure is shown in Figure 1:

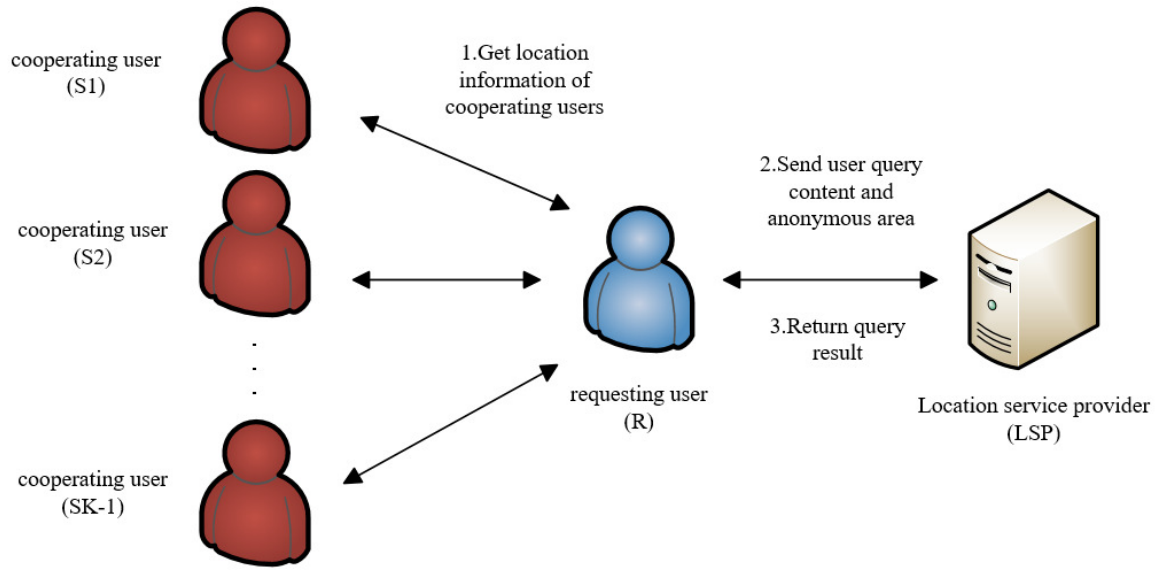

FIGURE 1. System structure

3.2. **Blockchain.** In 2008, Satoshi Nakamoto proposed the concept of Bitcoin [24], and blockchain, as the underlying core of cryptocurrencies such as Bitcoin, has become a research hotspot in various industries [25]. Blockchain is a data structure based on cryptography technology to organize and maintain large amounts of data in a decentralized or multi-centralized manner. In other words, the blockchain is a decentralized or multi-centralized, public distributed ledger. The nodes participating in the system may not belong to the same organization and do not trust each other. Blockchain data is jointly maintained by all nodes, and each node participating in the maintenance can get a copy of the complete record. The key technologies of blockchain are consensus protocol, cryptography and economic game. The main function of the consensus protocol is distributed consistency, resistance to multiple payments, and independence from trusted institutions [26]. The main role of cryptography is to ensure that data cannot be tampered with, undeniable, and privacy protection. The role of economic games is to provide incentives or punishment mechanisms and economic growth logic. The core characteristics of the blockchain have the following three aspects: 1. Decentralization [27] 2. Immutability of data [28] 3. Smart contracts [29].

This article makes full use of the key technologies of the blockchain, and uses the decentralization of the core characteristics of the blockchain and the immutability of data to ensure the security of user location information. The basic structure of the blockchain is shown in Figure 2:

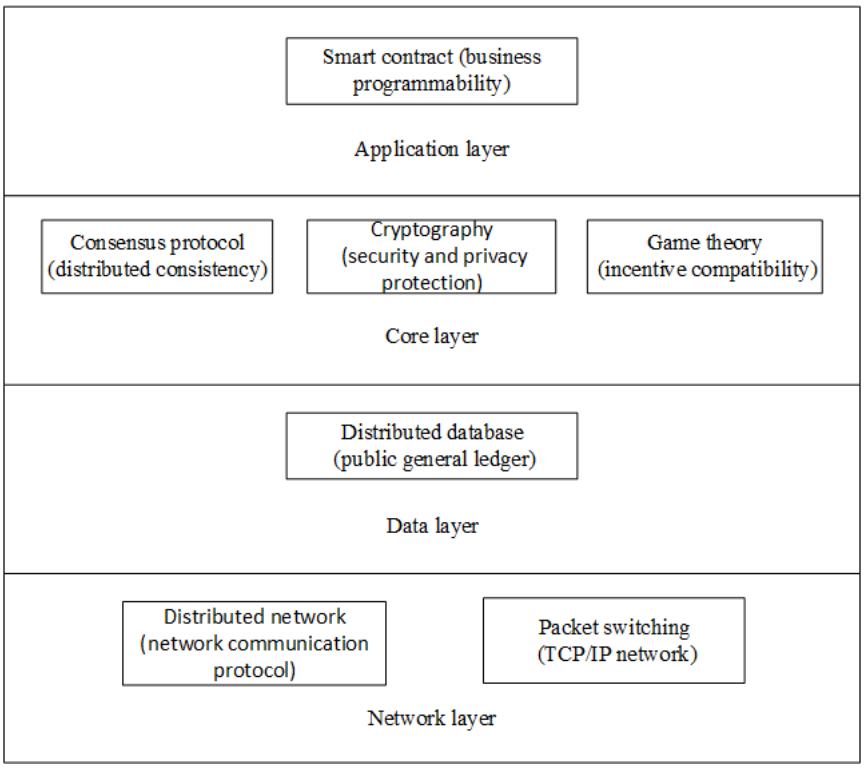

FIGURE 2. The basic structure of the blockchain

3.3. **Symbols and definitions.** This article defines the requesting user set is $R = \{R_i \mid i = 1, 2, \ldots, n\}$, where R_i represents the requesting user. the collaborative user set is $S = \{S_j \mid j = 1, 2, \ldots, m\}$, S_j represents the collaborative user. The process of requesting the user to obtain the location information of the collaborative user is called a transaction. After the transaction is completed, the record generated in the blockchain is called the transaction bill. More symbol definitions are shown in Table 1:

4. **Location Privacy Protection Method Based on EMCS Model and Blockchain.** In order to study whether the requesting user is credible, this paper introduces the user's credit rating c_i of different credit agencies as initial parameters. Regarding how collaborative users can quickly determine whether the requesting user is credible, the Reputation Value cv_i is introduced to help collaborative users make judgments. The credit rating c_i of the requesting user R is converted into the Reputation Value cv_i through the EMCS model. cv_i serves as the proof of R's own reputation in the process of issuing and querying. Then R sends a query request and to the collaborative user S.After receiving the query request, S judges whether to participate in the construction of the anonymous area through cv_i.S willing to participate will send his real location to R, and R will verify it in the blockchain after receiving the message. After verification, mix its own location with the locations of $K-1$ collaborative users, and at the same time, constructs an anonymous area. After the anonymous zone is constructed, it sends a query request to the LBS. The specific method flow of this article is shown in Figure 3:

4.1. **Use EMCS model to generate Reputation Value.** Based on the credit information system and entropy method, this paper proposes an EMCS model to calculate the Reputation Value of the requesting user R.

Step1. Request the user to send a credit inquiry request to the credit agency

Table 1. Notations

Notation	Description
R	Request user
S	Collaborative users
c_i	Request user's credit rating
c_i'	User credit rating after normalization
cv_i	The Reputation Value of the requesting user
P	A collection of users participating in the competition for bookkeeping rights
P'	A collection of users who have obtained the right to bookkeeping
$(PK_R,\ SK_R)$	The public key and private key of the user in the credit value acquisition
$PK{-}ID, SK{-}ID$	The public and private keys of the user during the blockchain transaction
K	User-defined privacy protection requirements
μ	The number of successful anonymous zones as a collaborative user
λ	Threshold for collaborative users to judge Reputation Value

The credit rating of requesting users under different credit institutions is different. This article sends a query request to major financial credit institutions to query the credit rating of the requesting user. The query request Qre is as follows:

$$Qre = \{RO_{\text{name}}, NID_i, T_Q, SK_R\} \tag{1}$$

Among them, RO_{name} represents the credit rating agency from which the credit rating comes. Credit agencies include bank credit, Alibaba credit, Tencent credit, etc. NID_i refers to the user's identity, used to determine the user's identity information. The meaning of T_Q is the timestamp when the credit inquiry is issued. SK_R indicates the private key, which signs the user's identity information, timestamp and credit value to prevent user information from being tampered with.

Step2. Get the credit rating of the requesting user

After receiving the query request from the requesting user, the reputation agency encrypts the credit rating and sends it to the requesting user. After the requesting user receives the return information, it verifies the credit rating with the public key. The return request $Gre$is as follows:

$$Gre = \{NID_i, c_i, T_G, PK_R\} \tag{2}$$

Among them, the meaning of NID_i is the user's identity, which is used to verify the user's identity information. $c_i = \{c_1, c_2, \ldots, c_n\}$ represents the credit rating of different credit agencies of the requesting user. T_G means the timestamp when the credit agency sends a return request to the requesting user. PK_R represents the public key, request The user uses the public key to verify the return request.

Step3. normalize the credit rating of the requesting user.

For the credit rating of positive correlation:

$$c_i' = \frac{c_i - \min(c_1, c_2, \ldots, c_n)}{\max(c_1, c_2, \ldots, c_n) - \min(c_1, c_2, \ldots, c_n)} \tag{3}$$

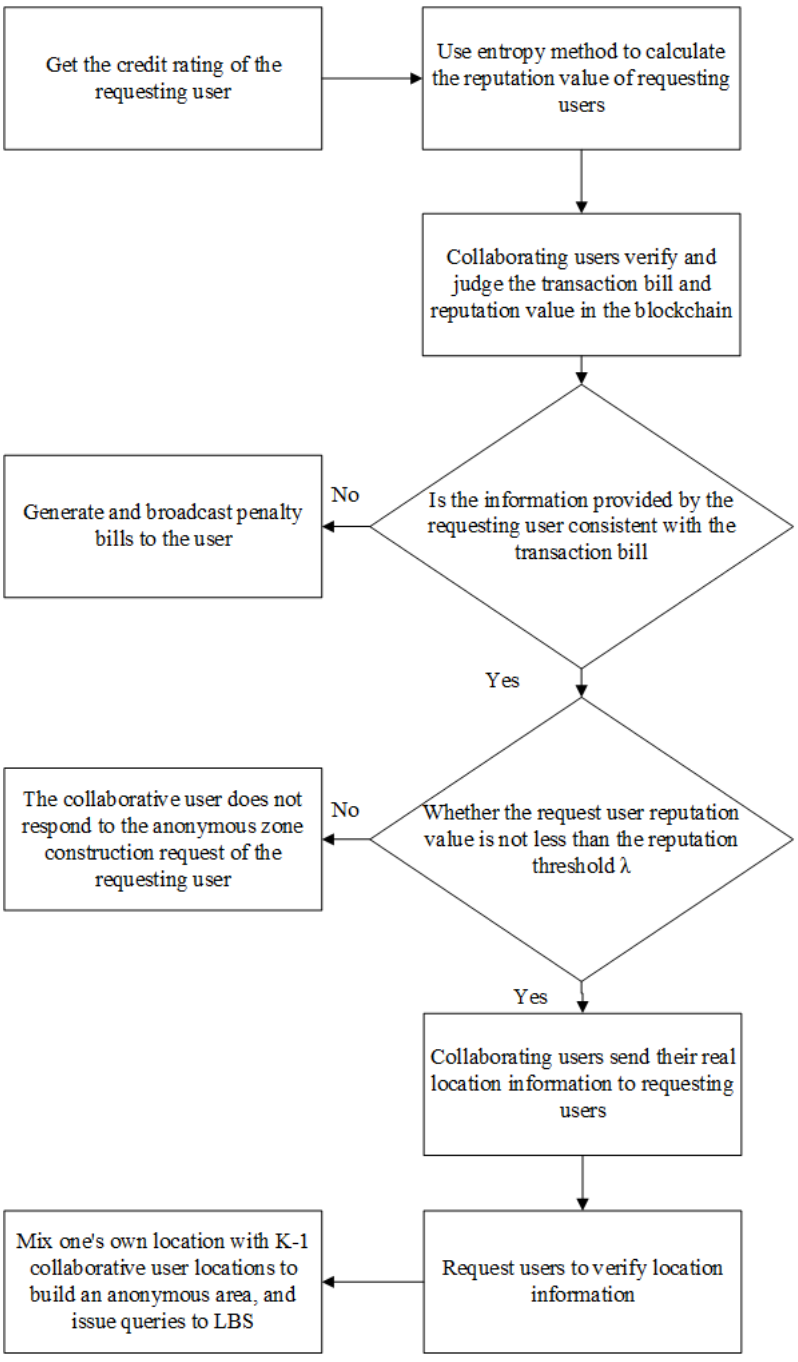

FIGURE 3. Method flow

For the credit rating that is negatively related to features:

$$c_i' = \frac{\max(c_1, c_2, \ldots, c_n) - c_i}{\max(c_1, c_2, \ldots, c_n) - \min(c_1, c_2, \ldots, c_n)} \tag{4}$$

The meaning of c_i' is to request the user's credit rating of the $-ith$ credit agency after normalization, and the value range of i is $1, 2, \ldots, n$. The meaning of max is to select the largest credit rating in the user's credit rating set. Similarly, the meaning of min is to select the smallest credit rating. Its purpose is to normalize the credit information of different attributes, so that these credit information can be converted into similar attributes, which can be calculated by entropy method and converted into reputation value.

Step4. Calculate the proportion of requesting users under the $-ith$ credit agency in the credit investigation:

$$P_i = \frac{c_i'}{\sum_{i=1}^{n} c_i'}, \quad i = 1, 2, \ldots, n \tag{5}$$

Step5. Calculate the entropy of the $-ith$ credit agency:

$$e_i = -k * \sum_{i=1}^{n} P_i * \ln(P_i) \tag{6}$$

The constant k is related to the number of samples $n, k > 0$ and $k = \frac{1}{\ln(n)}, e_i \geq 0$

Step6. Calculate the difference coefficient of the $-ith$ credit agency credit:

$$cod_i = 1 - e_i \tag{7}$$

For the credit of the $-ith$ credit agency, the greater the difference in credit value c_i, the greater the effect on program evaluation, and the smaller the entropy value. That is, the larger cod_i is, the more important the feature is.

Step7. Calculate the credit weight of each credit agency:

$$W_i = \frac{cod_i}{\sum_{i=1}^{n} cod_i}, i = 1, 2, \ldots, n \tag{8}$$

Step8. Calculate the Reputation Value cv_i of the requesting user:

$$cv_i = \sum_{i=1}^{n} W_i * c_i', \quad i = 1, 2, \ldots, n \tag{9}$$

The specific implementation is shown in Algorithm 1:

Algorithm 1 Calculate the Reputation Value of the requesting user

Input: Request user's Credit Rating c_i
Output: The Reputation Value of the requesting user cv_i

Obtain the credit rating of the user's various institutions c_i
If the user credit c_i value is positively correlated
$c_i' = c_i.apply(lambda\ c_i : ((c_i - \min)/(\max - \min)))$
else
$c_i' = c_i.apply(lambda\ c_i : ((\max - c_i)/(\max - \min)))$
end if
$rows = \{c_i.index.size\}$
$cols = \{c_i.columns.size\}$
$k = 1.0/math.log(rows)$ // Calculate the constant k
$P_i = [[None]^* cols\ for\ i\ in\ range(rows)]$
$P_i = array(P_i)$ // Calculate specific gravity
$for\ i\ in\ range(0, rows)$
if $c_i = 0$
$e_i = 0$
else
$e_i = math.log(P_i) * sum(P_i) * (-k)$
end if //Calculate entropy
$for\ i\ in\ range(0, cols)$
$W_i = cod_i/sum(cod_i)$
$cv_i = sum(W_i)^* c_i'$
print cv_i

4.2. **Privacy protection process combined with blockchain.** In order to avoid self-interested behavior of requesting user R and cooperating user S. This article uses blockchain technology in the construction of distributed anonymous zones. Prevent R from leaking S's location and S providing the false location to deceive R. In order to improve user enthusiasm, a competition incentive mechanism for bookkeeping rights is proposed. Encourage all users in the network to actively participate in the maintenance and construction of the blockchain.

4.3. **Competitive incentive mechanism for bookkeeping rights.** This paper proposes a competition incentive mechanism for bookkeeping rights $C = (N, E)$ to encourage users to participate in the construction of the blockchain. The set of users participating in this bookkeeping right competition incentive mechanism is $P = \{P_i | i = 1, 2, \ldots, n\}$. The main function of the bookkeeping right competition incentive mechanism is to select a user to update the blockchain. The right to bookkeeping is determined based on the Reputation Value of P and the number of successful anonymous areas as a collaborative user. The user with the most successful constructions and whose Reputation Value is greater than the participant's average reputation cv can obtain the right to bookkeeping. The specific meaning of N and E are as follows:

$$N = (\tilde{\mu}, \tilde{cv}) \tag{10}$$

N means that when a new block is generated. The set of the number of times $\tilde{\mu} = \{\tilde{\mu}_i \mid i = 1, 2, \ldots, n\}$ of the anonymous area successfully constructed by the user P participating in the competition and its Reputation Value $\tilde{cv} = \{\tilde{cv}_i | i = 1, 2, \ldots, n\}$.

$$E = argmax|\sin x| + 1 \tag{11}$$

E represents the income of user P' who has the right to bookkeeping when generating a new block. This article considers that users who have a high Reputation Value and have successfully constructed the most anonymous areas may have always been in control of the update authority of the block, which makes the blockchain present a certain security risk. In order to solve the problem of the distribution of accounting rights, this paper introduces the $argmax|\sin x|$ function so that accounting rights can be distributed to more users, reducing the risk of location privacy information leakage.

In addition, to encourage more users to participate in the maintenance and update of the blockchain, this article regards the users who have obtained the new block's accounting rights and have no bad records as successfully constructing an anonymous area. For any user in the network, the more times that the requesting user R successfully constructs an anonymous area, then when he is the requester of the location privacy query service, the more collaborative users S willing to send real location information, the higher the efficiency of constructing the anonymous area and the greater the benefit.

In this article's solution, the user will generate a transaction bill in real-time during the transaction.The bill's record contains the identity of R and S, the timestamp of the transaction, and the reallocation provided by S. The bill is then stored in the public chain. When S provides false location information, or R leaks the real location information provided by S, the transaction bill in the public chain can be used as evidence to punish the user in question. When the user in question sends a query request to the location server, the user will not obtain the collaborative user's location information and cannot construct an anonymous zone.

4.4. **The construction process of anonymous zone combined with blockchain.** Step1. requests user R to send an anonymous area construction request to collaboration

user S.

$$Req = \{\ CID_R, T_{R-i}, \mu, cv_i,\ TID_R, sign_{SK-ID_R}\,(T_{R-i}, cv_i)\ \} \tag{12}$$

Among them, CID_R represents the unique identity identifier of R, which is used to replace the real identity information of the requesting user. T_{R-i} represents the timestamp when R sends a query request to S. μ represents the number of times that R successfully constructed an anonymous area as a collaborative user. cv_i represents the Reputation Value of R. TID_R represents the transaction ID of R in the blockchain, which is used as a proof of transaction and to ensure the timeliness of the transaction. $sign_{SK-ID_R}\,(T_{R-i}, cv_i)$ means that in the blockchain, R uses the private key $SK - ID_R$ to sign the timestamp and Reputation Value.

Step2. After receiving the anonymous area construction request Req from the requesting user R, the collaborative user S uses R's public key $SK - ID_R$ in the blockchain to verify the transaction bill, and verify whether CID_R, μ, and TID_R provided by R are consistent with the data stored in the blockchain.

When the information provided by R is consistent with the information of the transaction bill in the blockchain, S will judge cv_i according to the reputation threshold λ, where λ is the reputation threshold based on fuzzy logic.

1. If $cv_i < \lambda$, then S does not respond to R's anonymous area construction request.
2. If $cv_i \geq \lambda$, then S encrypts its own location information and sends the encrypted information to R.

$$Res = \ \{CID_S, T_{s-i}, Enc_{PK-ID_R}\,(T_{s-i}, Loc_i)\ \ sign_{SK-ID_S}\,(Enc_{PK-ID_R}\,(T_{s-i}, Loc_i))\} \tag{13}$$

Among them, CID_s represents the unique identifier of S, which is used to replace the real identity information of the collaborative user. T_{s-i} represents the timestamp when S sends the real position to R. $Enc_{PK-ID_R}(T_{s-i}, Loc_i)$ means that in the blockchain, S uses R's public key $PK - ID_R$ to encrypt the timestamp and real location information to obtain the ciphertext. $sign_{SK-ID_R}\,(Enc_{PK-ID_R}\,(T_{s-i}, Loc_i))$ means that S uses the private key $SK - ID_S$ to sign the sent ciphertext.

When the information provided by R is inconsistent with the information of the transaction bill in the blockchain, S does not respond to R's request for constructing an anonymous area, generates and broadcasts a penalty bill.

$$Pen = \ \{\ T_{p-i}, Penalize, sign_{SK-ID_s}, (T_{p-i}, Penalize),\ CID_R, T_{R-i}, \mu, sign_{SK-ID_R}(T_{R-i}, cv_i)\} \tag{14}$$

Among them, T_{p-i} is the time stamp for generating the penalty bill. $Penalize$ is the identifier of the penalty bill. $sign_{SK-ID_R}(T_{p-i}, Penalize)$ means that S uses its private key $SK - ID_S$ to sign the time stamp and the penalty bill identifier.

Step3. After requesting user R receives the transaction bill sent by collaboration user S. Use the public key $PK - ID_s$ in the blockchain to verify the real location information sent by S.

When the verification is successful, R uses its private key $SK-ID_R$ to decrypt Enc_{PK-ID_R} (T_{s-i}, Loc_i) to obtain S's real location information. After that, S uses its own public key $PK - ID_s$ to encrypt the timestamp and real location information to generate ciphertext $Enc_{PK-ID_S}(T_{s-i}, Loc_i)$. R uses its private key $SK - ID_R$ to sign the ciphertext $Enc_{PK-ID_S}(T_{s-i}, Loc_i)$. Then record the ciphertext and signature in the transaction bill and broadcast it.

When the verification fails, R does not use the real location of S to construct an anonymous area, and broadcasts the penalty bill.

$$Pen = \begin{array}{l}\{T_{p-i}, Penalize, sign_{SK-ID_S}(T_{p-i}, Penalize), \\ Enc_{PK-ID_R}(T_{s-i}, Loc_i), sign_{SK-ID_S}(Enc_{PK-ID_R}(T_{s-i}, Loc_i))\}\end{array} \tag{15}$$

Step4. After receiving the transaction bill sent by the broadcast, the user on the network verifies its authenticity, and stores the real bill in the blockchain. The block is updated by the decentralized accounting algorithm.

Step5. When R receives the real location information of S, it mixes its real location with $K-1$ S locations to construct an anonymous area, and then sends the anonymous area to the LSP for query. After the query is over, the LSP returns the query result to R, and R filters the query result according to its real location. When using the method in this article to query, if R performs multiple queries at the same location, R does not need to send a query request to S, and only needs to obtain the true location of S at the time of historical query based on the transaction bill stored in the blockchain; When R continuously performs LBS queries, it can quickly obtain the information of the collaborative users who participated in the construction of the anonymous zone last time based on the transaction bills stored in the blockchain, and can directly send query requests to these users. Under the method in this article, the user's location spoofing and location leakage behaviors are avoided. On the basis of protecting the user's location privacy and security, an anonymous area can be quickly constructed to improve the quality and efficiency of the query.

5. **Security Analysis.** This article uses a distributed architecture, which is mainly composed of three parts: requesting users, cooperating users and LBS server. Introduce blockchain technology in the interaction between R and S. Using the decentralization and immutability of blockchain technology, based on ensuring the efficiency of the generation of anonymous areas, the user's real location information is protected being leaked. Simultaneously, when users upload their information to the blockchain, they cannot make changes. Once the user is found to provide false location information, a penalty bill will be generated. The situation where users provide false location information is much avoided.

In order to solve the problems of location deception and whether the requesting user is honest, this paper introduces the concept of credit rating. Use the existing credit reporting system of large-scale official credit agencies, such as Tencent, Alipay, JD IOU, and banks, to obtain the credit status and real-time credit rating of users of these institutions. Then, use the entropy method to calculate the user's real-time credit rating and convert it into a Reputation Value. Collaborating users can quickly judge whether the requesting user is credible through the Reputation Value, and can also participate in the construction of anonymous areas safely and efficiently, which greatly reduces the probability of the real location of the collaborative user being leaked.

This article also comprehensively considers user enthusiasm and other issues, and proposes a special incentive mechanism to encourage users to actively participate in the construction and maintenance of anonymous areas. Their Reputation Value will be increased for actively participating users when they apply to construct an anonymous zone. In the continuous query, it can be guaranteed that the user's anonymous area always contains the real location information of K-1 collaborative users. In summary, this article combines the relatively novel location privacy protection methods in recent years to optimize and improve the existing distributed anonymous construction methods. The algorithm security, information authenticity and communication efficiency have been improved. It

helps to learn and master the new algorithm, and then propose a safer and more efficient location privacy protection method.

5.1. **Time complexity analysis.** This article uses entropy method and Credit Rating to calculate the user's reputation. During the execution of this algorithm, the user's Credit Rating needs to be standardized, and different calculation methods are adopted for the Credit Rating of different attributes. The Credit Rating and difference coefficient can be directly calculated according to the algorithm. However, in the process of calculating entropy and weight, it is necessary to carry out cyclic processing.

In summary, the time complexity of the algorithm in this article is $O(n)$. On the basis of ensuring the efficiency of the algorithm, the Credit Rating of the user's different credit institutions has been optimized.

5.2. **Privacy security analysis.** This article assumes that all requesting users R are rational users, and the benefit of successfully constructing an anonymous area is greater than the benefit of leaking the location information of the collaborative user S. The return under the R corresponding strategy from high to low is:

U_R^{++}: R completes the construction of the anonymous area and also leaks the location information of S.

U_R^{+}: R completed the construction of the anonymous zone, but did not disclose the location information of S.

U_R^{-}: R has not completed the construction of the anonymous area, but leaked the location information of S.

U_R^{--}: R has not completed the construction of the anonymous area, and has not leaked the location information of S.

Similarly, for a rational S, the returns from high to low for different strategies are as follows:

U_S^{++}: S participates in the construction of the anonymous zone with a fake location, and is not recognized by R.

U_S^{+}: S participates in the construction of the anonymous zone with its real location, and its location information has not been leaked.

U_S^{-}: S participated in the construction of the anonymous zone with a fake location, but was identified by R and broadcasted a penalty bill.

U_S^{--}: S participated in the construction of the anonymous zone with its real location, but it was leaked by R.

Theorem 5.1. *Suppose that when the requesting user R sends an anonymous area construction request, at least $K-1$ cooperative users S provide their real location information. If and only if the following conditions are met:*

$$\begin{cases} U_R = U_R^{+} \\ U_S = U_S^{+} \\ LA = \dfrac{1}{K} \end{cases} \tag{16}$$

When satisfied, the method in this article is safe and effective. Where $U_R$is the income of R, $U_S$is the income of S, and LA represents the probability that the LSP correctly recognizes the true position of R.

Proof: When using the method in this paper, $U_R = U_R^{+}$ means that R has not disclosed the income of S's real location information after successfully constructing an anonymous area, and maximizes the income of R on the premise of protecting the real location

of S. $U_S = U_S^+$ means that S provides real location information to participate in the construction of the anonymous area to ensure the authenticity of the location information inside the anonymous area.When the above two conditions are met, the meaning of $LA = \frac{1}{K}$ is to request the user R to replace the K anonymous area to initiate a query to the LSP, and the probability that the LSP can correctly analyze the location information of R is $\frac{1}{K}$.Therefore, from the perspective of the authenticity and security of the anonymous area, the method in this paper is safe and efficient.

5.3. **Security analysis of Reputation Value.**

Theorem 5.2. *Suppose that the probability that S finds that R leaks its true location information is δ, and the probability that R finds that S provides false location information is η. When there are $K-1$ S provides location information to participate in the construction of the anonymous area. This article defines the number of penalty rounds as Pr, which means that every time a user receives a broadcast penalty bill pen, it is recorded as one round. If Prsatisfies:*

$$Pr \geq max\left\{\frac{U_R^{++} - U_R^+}{\delta(U_R^+ - U_R^{--})}, \frac{(1-\eta)(U_S^{++} - U_S^+)}{\eta(U_R^+ - U_R^{--})}\right\} \tag{17}$$

This method can prevent R from leaking the location information of S, and at the same time ensure that S provides real location information when participating in the anonymous area construction process.

Proof: Suppose that R chooses the strategy of leaking the position information of S after constructing the anonymous region for the nth time, then its profit in this construction game is U_R^{++}.When S discovers that R has leaked its location information at time t, the verification process of its blockchain will not be passed, and a penalty bill will be generated and broadcasted to reduce R's cv_i. At this time, R's revenue will be regarded as incomplete An anonymous area is constructed, and the location information of S is leaked, and the income is U_R^{--}. After that, R will not be able to successfully construct an anonymous area, and no S is willing to provide its own location information to participate in the construction of the anonymous area. Therefore, from the perspective of revenue, R's revenue at this time is U_R^{--}. In summary, R's total income obtained in the $i+1$ round of anonymous region construction M_{R1}:

$$M_{R1} = \delta[U_R^{++} + i \times U_R^{--}] + (1-\delta)[U_R^{++} + i \times U_R^+] \tag{18}$$

In the same way, in the process of constructing the game for the nth time, if R does not disclose the location information of S after constructing the anonymous area, its profit will be U_R^+. After that, the two parties will carry out a virtuous circle. From the perspective of comprehensive income, R's income is U_R^+. In summary, R's total income obtained in the $i+1$ round of anonymous region construction M_{R2}:

$$M_{R2} = (i+1)U_R^+ \tag{19}$$

From the perspective of game theory, when $M_{R1} \leq M_{R2}$, R will choose to leak S's location information, so let's get $M_{R1} \leq M_{R2}$:

$$Pr \geq \frac{U_R^{++} - U_R^+}{\delta(U_R^+ - U_R^{--})} \tag{20}$$

In summary, when $Pr \geq \frac{U_R^{++} - U_R^+}{\delta(U_R^+ - U_R^{--})}$, R can establish an anonymous area in good faith.

For S, when participating in the construction of the anonymous area for the nth time, choosing to provide a fake location and not being identified by R, then S's revenue is U_S^{++}, and the user's profit when making a build request as the requesting user afterwards

is U_S^+. If S provides a false position but is identified by R, its return during the game will be reduced to U_S^-. At the same time, the dishonest behavior of the user will be broadcast to other users in the network. If S wants to restore its own Reputation Value, it needs to make multiple requests as the requesting user. At this time, S's revenue is U_S^-. In summary, the total revenue S obtained in the $i+1$ round of anonymous region construction M_{S1}:

$$M_{S1} = \eta[U_S^- + i \times U_R^{--}] + (1-\eta)[U_S^{++} + i \times U_R^+] \tag{21}$$

In the same way, in the game process of the nth anonymous region construction, if S provides real location information and is not leaked by R, then its profit during the nth construction of the game is U_S^+. After that, the two parties will carry out a virtuous circle. From the perspective of comprehensive income, S's income is U_R^+. To sum up, the total income obtained by S in the $i+1$ round of anonymous area construction M_{S2}:

$$M_{S2} = U_S^+ + i \times U_R^+ \tag{22}$$

From the perspective of game theory, when $M_{S1} \leq M_{S2}$, users who meet the reputation threshold will send their real location to participate in the construction of an anonymous area. So that $M_{S1} \leq M_{S2}$ can be obtained:

$$Pr \geq \frac{(1-\eta)(U_S^{++} - U_S^+)}{\eta(U_R^+ - U_R^{--})} - \frac{U_S^+ - U_S^-}{U_R^+ - U_R^{--}} \tag{23}$$

We take $Pr \geq \frac{(1-\eta)(U_S^{++}-U_S^+)}{\eta(U_R^+-U_R^{--})}$, which obviously satisfies the above formula. Therefore, when $Pr \geq \frac{(1-\eta)(U_S^{++}-U_S^+)}{\eta(U_R^+-U_R^{--})}$, S can honestly participate in the construction of the anonymous area.

So when $Pr \geq max\left\{\frac{U_R^{++}-U_R^+}{\delta(U_R^+-U_R^{--})}, \frac{(1-\eta)(U_S^{++}-U_S^+)}{\eta(U_R^+-U_R^{--})}\right\}$, the method in this paper can effectively avoid dishonest behavior of R and S, and ensure the authenticity and availability of the anonymous area.

6. **Experiment and Analysis.** This experiment was carried out on Intel(R)Core(TM) i7-9750H processor, Windows10 64-bit operating system with 16G memory. In order to verify the security and feasibility of the scheme, the experiment uses Ethereum 1.8.1 version to build a blockchain platform in the Ubuntu system and write smart contracts. The Ubuntu system version used is 17.10. Ethereum is an open-source and public blockchain platform with smart contract functions.

Taking into account the experimental environment and other factors, the experimental settings in this article request the user's privacy protection requirement K value to vary from 2 to 30. The reason is that if there is only one user in the network, it will be meaningless to construct an anonymous area. Therefore, the minimum K value of the privacy protection requirement of the requesting user is set to 2; When the number of users in the network continues to increase, the success rate of the anonymous area construction continues to increase, but as the K value increases, the success rate of the construction will gradually stabilize. An excessive K value is less helpful to the experiment, so Set the maximum value of K to 30. In the built blockchain platform, the bookkeeping right competition incentive mechanism proposed in this article is used to select the bookkeeper of the new block.

Compared with the existing location privacy protection scheme, this paper uses the entropy method combined with the user's credit rating to ensure that the requesting user is completely credible.In the process of private information transmission, blockchain technology is used to ensure that location leakage and location fraud will not occur, and

the broadcast efficiency is increased.Using smart contracts and encryption technology to ensure the privacy of all users in the anonymous area.This method has a greater improvement than existing solutions in terms of algorithm execution efficiency and privacy security.

The experiment is compared with the scheme [19], scheme [20] and scheme [21] under different privacy protection requirements K of requesting users. Among them, the scheme [19] uses blockchain technology to ensure LSP access control and protect user privacy as much as possible, and promote mutual trust between LSP and users. Scheme [20] proposes to mix privacy protection technology with virtual credit to generate a special incentive mechanism to encourage users to actively participate in the construction of anonymous areas. The scheme [21] proposes to use multiple private blockchains to cut off the direct connection between users and LSPs, so that LSPs cannot directly obtain the user's location information, and at the same time use smart contracts to ensure the security and fairness of transactions. This paper compares the response time of cooperative users, calculation delay and communication overhead, and proves the efficiency and feasibility of this method. By comparing the user's location privacy leakage probability, it proves that this method can protect the user's location privacy. Safety plays an effective protective role.

6.1. **Cooperative user response time.** It can be seen from Figure 4 that with the increase of user privacy protection requirements K, the response time of collaborative users of the following four schemes is increasing. This is because with the continuous increase of K, the number of broadcasts continues to increase, and the number of users required to construct an anonymous area is also increasing.

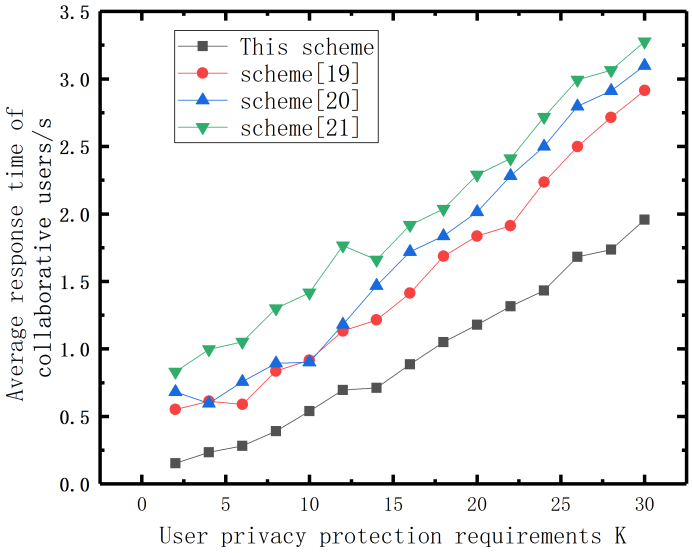

FIGURE 4. Average response time of collaborative users

Scheme [19] needs to select bookkeepers from participating users to be responsible for updating the blockchain each time. Compared with the method in this paper, this paper uses a special bookkeeping right competition incentive mechanism to select bookkeeping users, which greatly reduces Response time. Scheme [20] proposes a hybrid incentive mechanism whose purpose is to increase user participation, but this scheme needs to combine the obfuscation mechanism with blockchain technology to increase the response time. This article uses the user's Reputation Value and bookkeeping rights competition incentive mechanism to encourage more users to actively participate in the construction of

the anonymous zone while ensuring a low response time. The scheme [21] and the scheme in this paper both store the user's data in the blockchain, but scheme [21] uses multiple private blockchains to connect users, and the response process of the collaborative users is more complicated, so the collaborative users of this plan the longest response time. The solution in this article only needs to judge the Reputation Value, which greatly reduces the computational burden of the collaborative users, and at the same time guarantees the security of the data. Therefore, the comprehensive response time of the collaborative users in this solution is the shortest.

6.2. **Average calculation delay.** It can be seen from Figure 5 that with the increase of user privacy protection demand K, the calculation delay of the following four schemes is also increasing. This is because when user privacy protection K increases, the number of collaborative users required Increasingly, these four programs all use blockchain technology in the process of information exchange, which enables their calculation delay to rise relatively smoothly.

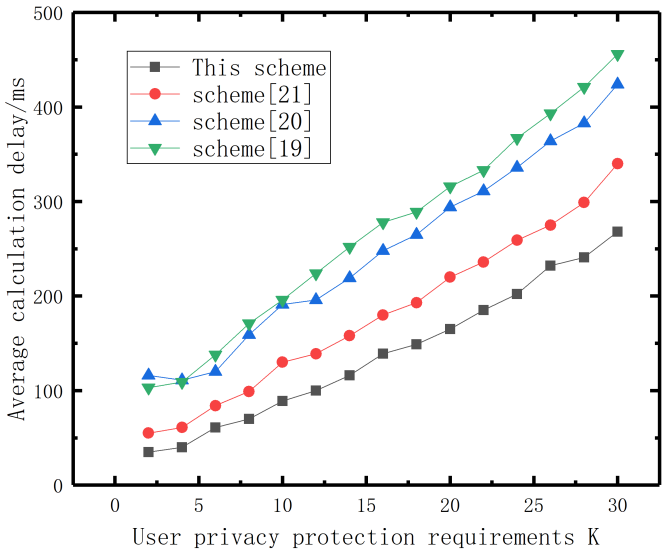

FIGURE 5. Average calculation delay

Among them, the scheme [19] uses blockchain technology to achieve mutual trust between LSPs and users in order to solve the privacy and security issues in 5G networks, but for users who have obtained the right to keep accounts, additional calculation delays need to be provided to achieve this. Green communication, so the average calculation delay of this scheme is relatively large. Scheme [20] proposes an obfuscation mechanism for privacy protection technology, which requires a combination of virtual credit and some privacy protection technologies, so the calculation delay is relatively large compared with this paper. Scheme [21] uses multiple private blockchains to disperse the user's transaction records, using private blockchain nodes instead of users to send the real location. Collaborating users need to communicate with each private blockchain, and requesting users can only use private blockchains to communicate with each private blockchain. Obtaining location information in the blockchain increases the calculation delay while ensuring the security of user information. The solution in this paper is to request users and cooperating users to send encrypted information to each other, and verify and decrypt them through the public and private keys in the blockchain, which not only guarantees the security of the information, but also reduces the calculation delay.

6.3. **Average communication overhead.** For the average communication overhead, the experimental results are shown in Figure 6:

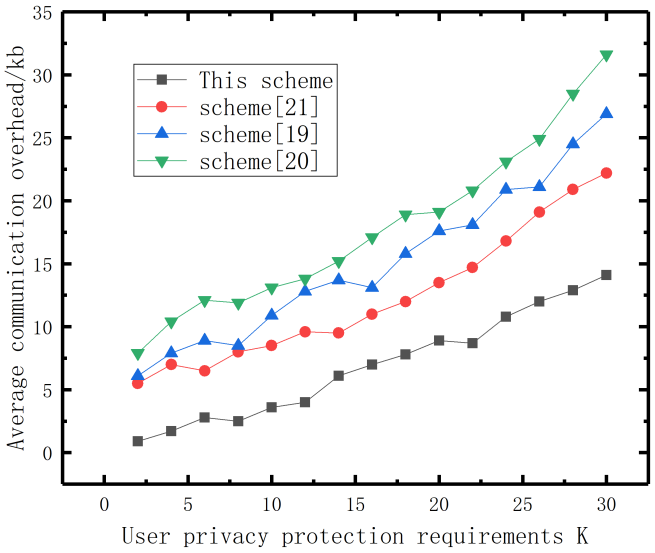

FIGURE 6. Average communication overhead

Scheme [19] provides a green channel for users who have the right to keep accounts, reducing part of the communication overhead and network delay. Scheme [20] divides the network structure into three parts: perception network, obfuscation mechanism and blockchain. Each part needs to communicate with each other, so the average cost of this scheme is the largest. Scheme [21] uses multiple private blockchains to achieve decentralization, cutting off the direct contact between users and location service providers. Although the user's location privacy is protected, users can only communicate through private blockchains. Increase the communication overhead between users. The solution in this paper is to directly communicate between the collaborative user and the requesting user. All user information is stored in the blockchain. This prevents users from leaking location privacy and providing false location information while keeping the communication overhead to a minimum.

6.4. **The influence of Reputation Value on the construction of anonymous zone.** Through a comprehensive analysis of the number of users in the network and the Reputation Value of requesting users, this paper's method is used to construct an anonymous zone, and the success rate of anonymous zone construction under different data is recorded. Under different K values, calculate the corresponding average Reputation Value of users, and users who are greater than the average Reputation Value can successfully construct an anonymous area. This article sets the privacy protection requirements K of the requesting user as 10, 20, and 30. Repeat the experiment for different K values, and the specific experimental results are shown in Figure 7:

The experimental results show that when the number of users in the network continues to increase, the number of collaborative users who are willing to participate in the construction of anonymous areas continues to increase, that is, the number of users satisfying $cv_i \geq \lambda$ continues to increase. Therefore, when the requesting user's Reputation Value does not change, the larger the K value, the higher the success rate of anonymous area construction. However, if the Reputation Value of the requesting user is too low, the collaborative user will be regarded as an extremely dishonest user. When it sends a query

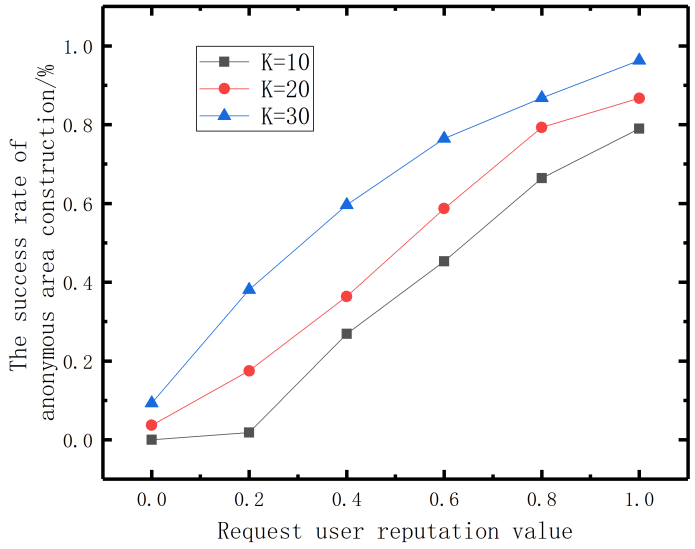

FIGURE 7. The success rate of anonymous area construction

request, even if the K value continues to increase, the success rate of its anonymous area construction is still very low.

6.5. **Probability of user's location privacy leakage.** Scheme [19] uses the openness and immutability of blockchain technology to ensure access control and privacy security of LSPs, and establish a trust relationship between users and LSPs. At the same time, users who have the right to keep accounts are given special treatment for green communications. However, the average calculation delay of this scheme is large, and it is difficult to avoid the location deception in the process of anonymous area construction. Therefore, the user's location privacy leakage probability of this scheme fluctuates greatly under different K values.

The scheme [20] proposes an obfuscation mechanism for users' social relations, virtual credit and other attributes, which combines this mechanism with blockchain technology to encourage users to actively participate in the construction of anonymous areas. However, this solution only considers how to improve the construction efficiency of the anonymous zone, and cannot effectively guarantee that the user's location information will not be tampered with. Therefore, under this solution, the user's location privacy is likely to be leaked.The experimental results are shown in Figure 8:

Scheme [21] uses multiple private blockchains to avoid direct communication between users and LSPs. Although it protects the user's location information to a certain extent, it cannot be completely in the information exchange process of each private blockchain. To avoid the possibility of user location information being stolen, and each individual block has to select the appropriate bookkeeper, the use of multiple blockchains increases the calculation delay and communication overhead. At the same time, compared with the solution in this paper, the scheme [19] has a higher probability of user location privacy leakage.

The test results show that compared with the above three schemes, this paper greatly reduces the probability of users' location privacy leakage on the basis of ensuring the efficiency of anonymous area construction. The use of entropy method and blockchain technology can prevent users' location deception and location leakage, and use the bookkeeping rights competition incentive mechanism to efficiently select suitable bookkeepers,

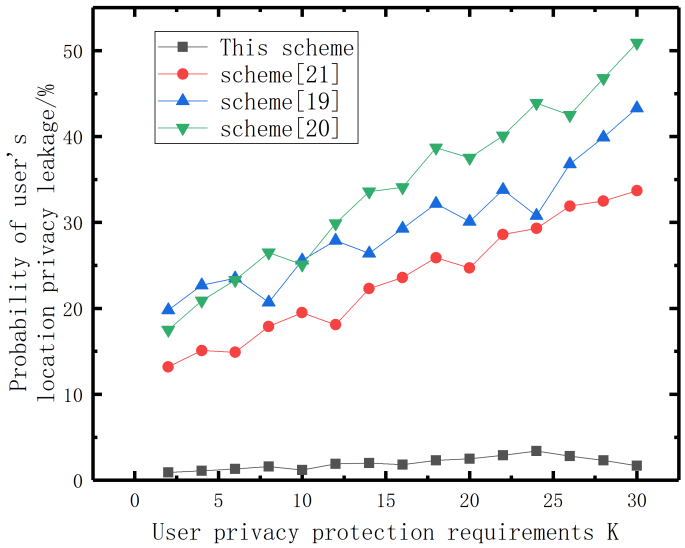

FIGURE 8. Probability of user's location privacy leakage

thereby improving the efficiency of users in constructing anonymous areas and ensuring users' Location privacy and security.

7. **Conclusions.** This article proposes a relatively novel location privacy protection structure based on a distributed structure. Regarding the user's credit rating, the entropy method is used to calculate the user's credit rating of different credibility agencies, and the user's Reputation Value is comprehensively obtained. The collaborative user decides whether to participate in constructing an anonymous area based on the Reputation Value. We use blockchain to store user information without a third party's help. Location service providers or any other organization cannot directly obtain the user's real-location information. The security and fairness of transactions are guaranteed through the blockchain. For users who leak location information or provide false location information, a penalty bill will be generated. An anonymous area cannot be successfully constructed when they are the requesting user. Through theoretical analysis and a series of simulation experiments, this method's usability is verified. On the basis of not requiring complex calculations, it can provide users with secure and reliable location services and enhance location privacy protection. However, there is a lot of room for improvement in all aspects of the algorithm in this paper, and further research is needed on how to apply it to actual scenarios.

Acknowledgement. This work was supported by the National Natural Science Foundation of China (61300216).

REFERENCES

[1] Z. W Hu and Jing Y, Trajectory privacy protection based on location semantic perception, *International Journal of Cooperative Information Systems,*, vol. 28, no. 3, pp. 317-322, 2019.

[2] S. B. Zhang, X. Li, X. Y. Tan, T. Peng, and G. J. Wang, A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services, *Future Generation Computer Systems*, vol. 94, pp. 40-50, 2019.

[3] LBS revenue to grow to 34.8 billion in 2020. Berg Insight., Mar. 08, 2015. [Online]. Available: www.gps-businessnews.com /Berg-Insight-LBS-Revenue-to- Grow-to-34-8-billion-in-2020-a5627.html.

[4] C. S. H. Eoma, C. C. Lee, W. Leea, and C. K. Leung, Effective privacy preserving data publishing by vectorization, *Information Sciences*, vol. 527, pp. 311-328, 2019.
[5] Y. X. Liu, A. F. Liu, X. Liu, and X. D. Huang, A statistical approach to participant selection in location-based social networks for offline event marketing, *Information Sciences*, vol. 480, pp. 90-108, 2019.
[6] Security researchers say the data of 267 million Facebook users has been compromised [Online] Available: https://www.cnbeta.com/ articles/tech/923591.html, Accessed on: Feb. 01, 2021
[7] C. Y. Chow, M. F. Mokbel, and X. Liu, A peer-to-peer spatial cloaking algorithm for anonymous location-based services, *roceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems(GIS 2006)*, Arlington, USA, 2006, pp. 171-178.
[8] M. L. Yiu, C. S. Jensen, J, Mller, and H. Lu, Design and analysis of a ranking approach to private location-based services, *ACM Transactions on Database Systems*, vol. 36, no. 2, pp. 1-42, 2011.
[9] L. Zhang, D. Liu, M. Chen, H. Li, C. Wang, Y. Zhang, and Y. Du, A user collaboration privacy protection scheme with threshold scheme and smart contract, *Information Sciences*, vol. 560, pp. 183-201, 2021.
[10] W. Jin, M. Xiao, and L. Guo, ULPT: A User-Centric Location Privacy Trading Framework for Mobile Crowd Sensing, *IEEE Transactions on Mobile Computing*, 2021, https://doi.org/10.1109/TMC.2021.3058181.
[11] B. Niu, Q. H. Li, X. Y. Zhu, G. H. Gao, and H. Li, Achieving k-anonymity in privacy-aware location-based services, *IEEE Infocom*, pp. 754-762, 2014.
[12] Z. Lei, L. Y. Yu, J. Li, and F. B. Meng, Location privacy protection algorithm based on correlation coefficient, *Proceedings of the 4th International Conference on Control, Automation and Robotics (ICCAR)*, pp. 332-335, 2018.
[13] X. F. He, R. C. Jin, and H. Y. Dai, Leveraging spatial diversity for privacy-aware location-based services in mobile networks, *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1524-1534, 2018.
[14] R. Schlegel, C. Y. Chow, Q. Huang, and D. S. Wong, User-defined privacy grid system for continuous location-based services, *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2158-2172, 2015.
[15] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, Practical approximate k nearest neighbor queries with location and query privacy, *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 6, pp. 1546-1559, 2016.
[16] D. J. Yang, X. Fang, and G. L. Xue, Truthful incentive mechanisms for K-anonymity location privacy, *roceedings of the 32nd IEEE International Conference on Computer Communications(INFOCOM 2013)*, pp. 2994-3002, 2013.
[17] X. H. Li, M. X. Miao, H. Liu, J. F. Ma, and K. C. Li, An incentive mechanism for K-anonymity in LBS privacy protection based on credit mechanism, *Soft Computing*, vol. 21, no. 14, pp. 3907-3917, 2017.
[18] M. Amoretti, G. Brambilla, F. Medioli, and F. Zanichelli, Blockchain-Based Proof of Location, *In Proceedings of the 2018 IEEE International Conference on Software Quality*, pp. 146-153, 2018.
[19] K. Fan, Y. H. Ren, Y. Wang, H. Li, and Y. Yang, Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G, *IET Communications*, vol. 12, no. 5, pp. 527-532, 2018.
[20] B. Jia, T. Zhou, W. Y. Li, Z. C. Liu, and J. T. Zhang, A blockchain-based location privacy protection incentive mechanism in crowd sensing networks, *Sensors*, vol. 18, no. 11, 2018.
[21] Y. Qiu, Y. Liu, X. Li, and J. H. Chen, A novel location privacy-preserving approach based on Blockchain, *Sensors*, vol. 20, no. 23, 3519, 2020.
[22] B. Luo, X. H. Li, J. Weng, J. J. Guo, and J. F. Ma, Blockchain enabled trust-based location privacy protection scheme in VANET, *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2034-2048, 2020.
[23] M. M. Yang, T. Q. Zhu, K. T. Liang, W. L. Zhou, and R. H. Deng, A blockchai'n-based location privacy-preserving crowdsensing system, *Future Generation Computer Systems*, vol. 94, pp. 408-418, 2019.
[24] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, *Consulted*, 2008.
[25] S Shamshad, K Mahmood, S Kumari, CM Chen, A secure blockchain-based e-health records storage and sharing scheme - ScienceDirect, *Journal of Information Security and Applications*, vol. 55, no. 102590, 2020.

[26] C.M. Chen, X, Deng, W. Gan, J. Chen, S.K.H. Islam, A secure blockchain-based group key agreement protocol for IoT, *The Journal of Supercomputing*,vol. 77, pp. 9046–9068, 2021.

[27] J. M. -T. Wu, Z. Li, G. Srivastava, J. Frnda, V. G. Diaz and J. C. -W. Lin, A CNN- based Stock Price Trend Prediction with Futures and Historical Price," *2020 International Conference on Pervasive Artificial Intelligence (ICPAI)*, pp. 134-139, 2020.

[28] J. M. T. Wu, Z. Li, N. Herencsar, B. Vo, J. C. W. Lin, A graph-based CNN-LSTM stock price prediction algorithm with leading indicators, *Multimedia Systems*, 2021, https://doi.org/10.1007/s00530-021-00758-w.

[29] E.K. Wang, R.P. Sun, C.M. Chen, Z. Liang, S. Kumari, M.K. Khan, Proof of X-repute blockchain consensus protocol for IoT systems, *Computers & Security*, vol. 95, 101871, 2020.