User Sensitive Information Protection Scheme Based on Blockchain Technology

Sheng Luo

1School of Information and Statistics, Guangxi University of Finance and Economics, Nanning 530003, China
2Guangxi Key Laboratory of Cross-Border E-Commerce Intelligent Information Processing, Guangxi University of Finance and Economics, Nanning 530003, China

Correspondence should be addressed to Sheng Luo; 315412323@qq.com

Received 17 January 2022; Accepted 30 March 2022; Published 20 April 2022

Academic Editor: Ashish Bagwari

Copyright © 2022 Sheng Luo. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the continuous development of mobile applications and location technology, \(k\)-anonymity technology is usually used to protect the privacy and security of users in location-based services that are used by mobile users. Due to the self-interest of users, in the cooperative construction of a \(k\)-anonymity privacy protection scheme, it is difficult to guarantee the honest cooperation behavior of the requesting and cooperating users. To solve the above problems, this paper proposes a distributed \(k\)-anonymous location privacy protection scheme based on blockchain. In this paper, we record the requesting users, cooperative users, and their location information as evidence, and we punish the users with location leakage and deception. An anonymous zone cannot be constructed when the user is a requesting user. An interactive record mechanism is designed to constrain the self-interest behavior of the requesting and cooperating users in the process of anonymous region construction. Security analysis and experiments show that this scheme can effectively protect the user’s location privacy, promote the honest cooperation between the requesting user and the cooperative user, and encourage more users to participate in the construction of an anonymous zone.

1. Introduction

In recent years, with the rapid development of GPS equipment and mobile information technology, location-based services (LBS) have become one of the most developed potential services for mobile users [1]. LBS means that mobile services are more colorful according to the geographic location. LBS provides consumers with a series of location-based services and convenient experiences from social networks, navigation, takeout platforms, and so on. However, when people obtain location services through the network, they also expose their location information to LBS providers, which threatens the disclosure of the private information of users.

To prevent the leakage of privacy information, scholars have proposed many location privacy protection methods, including \(k\)-anonymity, differential privacies, location coordinate transformation, and cryptography-based methods [2–4]. Among them, \(k\)-anonymity is the most common method in LBS location privacy protection [5]. The basic idea of this method is that when sending an LBS query request, the user first obtains at least the real location of other \(k-1\) cooperative users, then constructs an anonymous area, and then submits the anonymous area instead of his real location, to effectively protect his personal location privacy. However, there are still two problems in \(k\)-anonymous location privacy protection. On the one hand, after the requesting user receives the real location provided by the cooperative user, the self-interested requesting user will disclose the location information to the third party to obtain additional benefits. Alternatively, the malicious attacker will disguise himself as a requesting user to obtain the real location of the collaborative user, which will lead to the disclosure of the location privacy of the collaborative user. On the other hand, after the cooperative user receives the collaboration request sent by the requesting user, even if some cooperative users are located in sensitive areas, they will still provide false
locations to the requesting users to improve their activity (or reputation) due to their self-interest, to enable them to construct anonymous regions efficiently when they are requesters. It can be seen that the existing distributed $k$-anonymous location privacy protection scheme cannot completely protect the user’s location privacy. Because blockchain technology has great advantages in information security protection, it has been widely used in AI and medical fields [6, 7]. To solve the above problems, this paper proposes a distributed $k$-anonymity location privacy protection scheme based on blockchain from the user’s self-interested behavior. According to the data, this scheme is the first to use blockchain to study LBS location privacy protection. The research results have certain practical significance and applications value.

2. Related Work

In recent years, there have been many research studies on the privacy protection of user location information, and some achievements have been made. This method was first proposed by Chow et al. and its basic idea is to make requests of users to obtain the real locations of at least $k-1$ other cooperative users by point-to-point communication to construct an anonymous area, for the purpose of making the LSP guess the real location of the requesting user from the anonymous area with a probability of no more than $1/k$ [8]. Ghinita et al. used the hibernate curve to map the location information of the requesting users and cooperative users from two-dimensional space to one-dimensional space, and they stored the one-dimensional location information of each user in the data node of a $B+tree$, which enables the requesting user to quickly obtain the real locations of the adjacent cooperative users in the constructed anonymous area [9, 10]. However, when there are many cooperative users, the requesting users must retrieve from the root node of the $B+tree$, which increases the computational cost of the requesting users. To solve this problem, reference [11] uses a ring structure instead of a $B+tree$ structure to store the one-dimensional locations of all of the users, which means that the requesting user can quickly find the adjacent users and construct the anonymous area. Chen et al. pointed out that the requesting user should combine with the actual road traffic network when constructing the anonymous area; otherwise, the LSP could identify the real location of some cooperative users from the anonymous area submitted by the requesting user according to the road traffic network and could even directly identify the real location of the requesting user [12]. They make LBS queries on each road for the requesting users and set different quality of service. On the premise of ensuring the quality of service, the generated anonymous area contains as many intersections as possible to improve the location privacy protection level of the requesting user.

In research on the location acquisition method of the collaborative users in a distributed environment, Chow et al. proposed to use the real location of historical cooperative users to construct an anonymous area for the requesting users [13, 14]. In their scheme, the requesting user stored the location information of the cooperative user after each LBS query. If the number of collaborative users obtained in the next LBS query did not meet the requirements of the location privacy protection, then the location information provided by the historical cooperative users could be directly used to construct the anonymous region. To reduce the storage cost of the requesting user, Kim et al. used the Hibert curve to reduce the dimension of the location information of the historical cooperative users, and they used the information entropy of the constructed anonymous area to measure the location privacy protection level of the requesting user; in addition, they proposed a distributed $K$-anonymous location privacy protection scheme based on a grid [15]. In addition to using the location information of historical cooperative users, some scholars have proposed two distributed $K$-anonymity location privacy protection schemes based on region awareness, combining them with the existing mobile communication infrastructure [16, 17]. In addition, Che et al. proposed a two-way active distributed $k$-anonymity privacy protection scheme by letting all of the users in the network send information tables of their real locations and the locations of their neighbors [18–20].

In research on incentive mechanisms in distributed $k$-anonymity, Yang et al. pointed out that the original distributed $k$-anonymity privacy protection schemes assume that the cooperative users are honest. They will provide their real location to the requesting user after receiving a request from the anonymous zone collaborative construction [21]. However, in the real world, users are self-interested. If the requesting users directly use these schemes to protect their location privacy in an LBS query, it will be difficult to obtain enough real locations of cooperative users to construct an anonymous area. They use a single round sealed double auction mechanism to allow multiple users to obtain the real location of the cooperative users by auction, thus encouraging all users in the network to participate in the construction of the anonymous area. In addition, Gong et al. pointed out that to better protect the location privacy of the requesting user, the requesting user and the cooperating user must use pseudonyms when participating in the anonymous region construction [22, 23]. Therefore, to encourage cooperative users to change their pseudonyms, they regard the requesting users and cooperative users as a special social group. Based on the social relationships among the group users, they use the maximum group income to encourage cooperative users to change their pseudonyms when they participate in the anonymous region construction.

To summarize, the existing distributed $k$-anonymity location privacy protection schemes do not consider the privacy disclosure and deception behavior in the process of constructing the anonymous region. Therefore, this paper proposes a distributed $k$-anonymous location privacy protection scheme based on blockchain. In this paper, we record the requesting users, cooperative users, and their location information as evidence, and we punish the users who have location leakage and deception. The anonymous zone cannot be constructed when one of these users is the requesting user. An interactive record mechanism is designed to constrain the self-interest behavior of the requesting and
cooperating users in the process of anonymous region construction. Second, this paper uses the blockchain technology to effectively prevent the requesting users from disclosing the location information of the cooperative users, and at the same time, it can encourage the cooperative users to provide the real location to participate in the construction of the anonymous area. Finally, experiments show that when the requesting user uses this scheme to construct the anonymous area, the computational cost, communication cost, and storage cost of the cooperative user are less, and the anonymous area can be constructed efficiently. This finding shows that the scheme has good practicability.

3. Research Model

3.1. Blockchain Technology. The concept of blockchain was first proposed by a scholar whose pseudonym is "Nakamoto cong," blockchain was described as a distributed ledger based on a chain structure. In the ledger, data blocks are linked in the order of being generated over time. Cryptography and consensus algorithms are used to ensure the distribution consistency, tamper proof nature, and unforgeability of the account book data [24, 25]. The basic framework of blockchain can be divided into six layers: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer [26].

3.1.1. Data Layer. The main function of the data layer is to record and store the information on the chain and to ensure the unforgeability and traceability of the data through a Merkle tree, asymmetric encryption algorithm, hash function, time stamp, and other technologies.

3.1.2. Network Layer. The main function of the network layer is to transfer and verify the data through a point-to-point network.

3.1.3. Consensus Layer. The consensus layer mainly uses a consensus algorithm to achieve a stable consensus among the distributed nodes, to ensure the consistency and authenticity of the data.

3.1.4. Incentive Layer. In a blockchain, the data set is maintained by all of the nodes. To encourage nodes to actively participate in the maintenance of the blockchain, the incentive layer encapsulates the allocation rules and payment rules that are compatible with the incentive, to maximize the profits of each node while participating in the maintenance of the blockchain.

3.1.5. Contract Layer. The contract layer mainly provides the development environment of the smart contracts, including the sandbox environment of the blockchain platform and the corresponding programming language.

3.1.6. Application Layer. The application layer is used to realize the application of blockchain technology in various applications scenarios. According to the different applications scenarios, the development of blockchain technology is divided into three stages: programmable currency, programmable finance, and programmable society [27].

3.2. Model Description. In this paper, a point-to-point equality structure is adopted. It is composed of a requesting user, cooperative user, and LSP, and no third party is required. It is assumed that there are secure communications links between the requesting user and the cooperating user and between the requesting user and the LSP [22]. When the requesting user $P_0$ sends a query request to the LSP, the requesting user first sends a collaboration request to the surrounding users to obtain their real locations. After receiving the locations $Loc_{real}^0, Loc_{real}^1, \ldots, Loc_{real}^{K-1}$ provided by cooperative users $P_1, P_2, \ldots, P_{K-1}$, the requesting user constructs the anonymous area ACR and submits it to the LSP together with the query content.

After the LSP authenticates the identity of the requesting user $P_0$, it searches the database according to the anonymous area and query content submitted by the requesting user, and it returns all of the results to the requesting user $P_0$. After receiving the query results sent by the LSP, the requesting user $P_0$ filters them according to their real location $Loc_{real}^0$ to obtain accurate query results. Among them, $Loc_{real}^i$ represents the true location of the $i$th collaborative user $P_i$. For the anonymous zone, we have ACR $=$ Area$(Loc_{real}^0, Loc_{real}^1, Loc_{real}^2, \ldots, Loc_{real}^{K-1})$. Area$(\bullet)$ is the anonymous area constructor, and $K$ represents the privacy protection requirements of the requesting user $P_0$.

In addition, this paper assumes that both the requesting user and the cooperative user are rational; in other words, in the process of constructing the anonymous area, they always choose according to maximizing their own interests. For the rational requesting user $P_0$, he first expects to obtain the real location provided by the cooperative user to generate the anonymous area ACR. Second, when the anonymous area is constructed successfully, it will disclose the real location of the cooperative users to obtain more additional benefits. Therefore, in the process of constructing the anonymous area, the rational requesting user’s preference satisfaction is the following: Among them, $U^+ > U > \bar{U} > \bar{U}$,

where

1. $U^+$ represents the profit when the user $P_0$ successfully constructs the anonymous area and discloses the real location of the cooperative user $P_i$
2. $U$ represents the profit when the user $P_0$ successfully constructs the anonymous area without disclosing the real location of the cooperative user $P_i$
3. $\bar{U}$ represents the profit when the user $P_0$ fails to successfully construct the anonymous area and discloses the real location of the cooperative user $P_i$
4. $\bar{U}$ represents the profit when the user $P_0$ fails to successfully construct the anonymous area and does not disclose the real location of the cooperative user $P_i$

For the rational cooperative user $P_i$, he first hopes to protect his location privacy; second, he can effectively protect his location privacy and, at the same time, provide collaborative help for the requesting user. Therefore, in the
process of constructing the anonymous region, the preference of the rational cooperative user \( P_i \) satisfies the following requirements: \( W^+ > W > W > W^f > W \).

1. \( W^+ \) is the profit when the cooperative user \( P_i \) provides the false location \( \text{Loc}_{\text{fake}} \) to the requesting user \( P_0 \), and the requesting user \( P_0 \) uses the false location to construct the anonymous area.
2. \( W \) is the profit when the cooperative user \( P_i \) provides the real location \( \text{Loc}_{\text{real}} \) to the requesting user \( P_0 \), and the requesting user \( P_0 \) did not disclose the location.
3. \( W \) is the profit when the cooperative user \( P_i \) does not provide the location information to cooperate with user \( P_0 \) to construct the anonymous area.
4. \( W^f \) is the profit when the cooperative user \( P_i \) provides the false location \( \text{Loc}_{\text{fake}} \) to the requesting user \( P_0 \), but the requesting user identifies it correctly and does not use the location to construct the anonymous area.
5. \( W \) represents the profit when the cooperative user \( P_i \) provides his/her real location \( \text{Loc}_{\text{real}} \) to the requesting user \( P_0 \) but requests that user \( P_0 \) disclose his/her real location.

3.3. Model Security Definition. In this paper, the requesting user and the surrounding cooperative user are regarded as attackers. In the process of constructing a distributed anonymous area, self-interest request-users are to disclose the location information provided by cooperative users to a third party to obtain additional benefits. However, after receiving the anonymous region construction request sent by the requesting user, the self-interest cooperative user might provide false location information to the requesting user, which makes the anonymous area constructed by the requesting user unable to meet the privacy protection requirements, and it even enables the LSP to directly infer the personal privacy of the requesting user.

To clearly define the security of the distributed anonymous zone construction, this paper regards the cooperative construction of the anonymous zone as a two-party game between the requesting user \( P_0 \) and the cooperative user \( P_i \). First, the cooperative construction game of the anonymous zone is formally described.

**Definition 1** (Anonymous zone cooperative construction game). The anonymous region cooperative construction game is a five-tuple \( G_{\text{ACR}} = \{ P, A, H, F, U \} \). Among them are the following:

(i) \( P = \{ P_0, P_i \} \) is the rational user set; \( P_0 \) is the requesting user; \( P_i \) is the cooperative user.
(ii) \( A = \{ A_0, A_i \} \) is the policy set of participants, where \( A_0 = \{ a_{0}^{(1)}, a_{0}^{(2)} \} \) is the policy set of the requesting user \( P_0 \). Here, \( a_{0}^{(1)} \) means that the requesting user \( P_0 \) will not disclose the location \( \text{Loc}_0 \) to the third party after receiving it, and \( a_{0}^{(2)} \) means that the requesting user \( P_0 \) will disclose the location \( \text{Loc}_0 \) provided by cooperative user \( P_i \) to a third party after receiving it. \( A_i = \{ a_{i}^{(1)}, a_{i}^{(2)}, a_{i}^{(3)} \} \) is the policy set of the cooperative user \( P_i \); \( a_{i}^{(1)} \) means that the cooperative user \( P_i \) provides its own real location \( \text{Loc}_{\text{real}} \) to the requesting user \( P_0 \) after receiving the collaboration request, \( a_{i}^{(2)} \) means that the collaborative user \( P_i \) does not provide location information to the requesting user \( P_0 \) after receiving the collaboration request, and \( a_{i}^{(3)} \) indicates that the cooperative user \( P_i \) provides a false location \( \text{Loc}_{\text{fake}} \) to the requesting user \( P_0 \) after receiving the cooperation request. Moreover, in the anonymous zone cooperative construction game \( G_{\text{ACR}} \), the requesting user and the cooperative user each choose a strategy form vector \( a = (a_0, a_i) \) as the rational user’s strategy combination. Among them, \( a_0 \in A_0 ; a_i \in A_i \).

(iii) \( H \) is the set of histories. Any history \( h \in H \) represents the combination of policies selected by rational users at the corresponding time. Obviously, the null character \( \tau \in H \) represents the beginning of the cooperative construction game of the anonymous area. For any history \( h \in H \), all policy combinations that can appear after it are recorded as \( A(h) = \{ a(h, a) \in H \} \). If there is \( h' \in H \) such that \( A(h') = \emptyset \), then the history \( h' \) is said to be terminated. The set \( Z \) represents the set of all termination histories.

(iv) \( F : (H \setminus Z) \rightarrow P \) is the user assignment function, which specifies the user who will make the next policy selection for the history \( h \in H \setminus Z \) without termination. In the anonymous area cooperative construction game, rational cooperative user \( P_i \) takes the lead in policy selection, and thus, \( F(\tau) = P_i \).

(v) \( U = \{ u_0, u_i \} \) is the revenue set of rational users. Among them, \( u_0 \in \{ U^+, U, \bar{U}, \bar{U} \} \) is the revenue function of the rational requesting user \( P_0 \) and \( u_i \in \{ W^+ , W, W^f, W \} \) is the revenue function of the rational cooperative user \( P_i \).

Based on the formal description of the anonymity zone cooperative construction game model, the security definition of distributed \( k \)-anonymity is given below.

**Definition 2** (Security of distributed \( k \)-anonymous location privacy protection). Suppose that \( P_0 \) is a rational requesting user and \( P_1, P_2, \cdots, P_{K-1} \) is \( K-1 \) rational cooperative users. When the rational user \( P_0 \) uses the distributed \( k \)-anonymous privacy protection scheme to send a cooperative anonymous area request to \( P_1, P_2, \cdots, P_{K-1} \), and there is successful construction of the anonymous area \( ACR \), the following conditions are true:
Then, the distributed $k$-anonymous location privacy protection scheme is called secure. Here, $K$ represents the location privacy protection requirement of the requesting user $P_0$ when sending the current LBS query. Here, $1 \leq i \leq k - 1$. $P_{\text{LSP}}[\text{Loc}^\text{real}_i | \text{ACR}]$ represents the probability that LSP can correctly identify its real location $\text{Loc}^\text{real}_i$ from the anonymous area ACR submitted by the requesting user $P_0$.

In the above definitions, formula (1) defines the security of the distributed $k$-anonymous location privacy protection from the perspective of anonymous region construction. Formula (1) indicates that the requesting user $P_0$ will not disclose the location of the cooperative user during the construction of the anonymous area. Formula (1) indicates that during the construction of the anonymous area, cooperative user $P_i$ provides its own real location $\text{Loc}^\text{real}_i$ to the requesting user $P_0$. Formula (1) defines the security of the distributed $k$-anonymous location privacy protection from the perspective of the LBS query.

4. Research Design

To prevent the requesting users from divulging the locations of cooperative users and providing false locations to cheat the requesting users during the construction of a distributed anonymous area, in this paper, encryption and signature techniques are used to prevent other users from illegally obtaining the location information provided by cooperative users and from participating in anonymous area construction that deny users who have location deception or disclosure behavior. Blockchain is used for distributed storage, and both sides of the game involved in the construction of the anonymity zone and the location information provided by them are used as evidence; hence, a distributed $k$-anonymous location privacy protection scheme is designed.

4.1. Consensus Mechanism. To prevent the requesting users from divulging the location information of cooperative users and providing false locations to cheat the requesting users during the construction of a distributed anonymous area, this section first designs a collaboration request recording mechanism to constrain the self-interest behavior of the requesting user and the cooperative user and also proposes a blockchain accounting competition mechanism to encourage all users in the network to participate in the maintenance of the blockchain.

Suppose that in any $q$-th anonymous region cooperative construction game, policy $a_i^{q,(1)}$ means that the requesting user $P_0$ will not disclose the location $\text{Loc}^\text{a}_i$ provided by cooperative user $P_i$ to the third party after receiving it. Policy $a_i^{q,(2)}$ means that the requesting user $P_0$ will disclose the location $\text{Loc}^\text{a}_i$ provided by the cooperative user $P_i$ to the third party after receiving it.

Policy $a_i^{q,(1)}$ means that the cooperative user $P_i$ provides the real location $\text{Loc}^\text{real}_i$ to the requesting user $P_0$ after receiving the collaboration request. Policy $a_i^{q,(2)}$ means that the cooperative user $P_i$ does not provide any location information to the requesting user $P_0$ after receiving the collaboration request. Policy $a_i^{q,(3)}$ indicates that the cooperative user $P_i$ provides a false location $\text{Loc}^\text{false}_i$ to the requesting user $P_0$ after receiving the cooperation request. Let $u_i^{q,0}$ and $u_i^{q,1}$ represent the profits of the requesting user $P_0$ and the cooperating user $P_i$ at the end of the $q$-th anonymous region cooperative construction game, respectively. Moreover, the strategy $a_i^{q,0}$ represents the strategy chosen by the requester $P_0$ of the $q$-th anonymous zone cooperative construction game when he is still the requester in the $j$-th game. The strategy $a_i^{q,j}$ represents the strategy chosen by the cooperative user $P_i$, who participates in the $q$-th anonymous zone cooperative construction game as the requester in the $j$-th game. Then, the collaboration request recording mechanism proposed in this paper is as follows:

**Definition 3** (Consensus mechanism I-interactive recording mechanism). The interactive record mechanism $M_R = (a_i, p^{[q+m]})$ is a two-tuple. Among them, we have the following:

(i) $a_i = (a_i^{0}, a_i^{q})$ is a combination of strategies ($a_i^{0}$ and $a_i^{q}$ ) selected by the requesting user $P_0$ and the cooperating user $P_i$ in the $q$-th anonymous region cooperative construction game

(ii) $p^{[q+m]} = \{p_0^{[q+m]}, p_i^{[q+m]}\}$ is the interactive record mechanism $M_{R^j}$ according to the strategy chosen by the requesting user $P_0$ and the cooperative user $P_i$ in the $q$-th anonymous area cooperative construction game, and it gives them the payment income from the $q$-th anonymous area collaborative construction game to the $(q + m)$-th anonymous area collaborative construction game $G_{ACR}^{q+m}$. For any $j \in [q, q + m]$, it satisfies the following:

\[
\begin{align*}
p_0 & = \left\{ u_0^{q,0}(a_0^{0,0} , a_0^{q,1}), a_0^{0} = a_0^{q,1} \right\}, \\
& \quad u_0^{q,0}(a_0^{0,0} , a_0^{q,2}), a_0^{0} = a_0^{q,2}, \\
& \quad \cdots \\
& \quad u_0^{q,q-1}(a_0^{0,0} , a_0^{q,1}), a_0^{0} = a_0^{q,1}, \\
& \quad u_0^{q,q}(a_0^{0,0} , a_0^{q,2}), a_0^{0} = a_0^{q,2}, \\
& \quad \cdots \\
& \quad u_0^{q+1,q-1}(a_0^{0,0} , a_0^{q,1}), a_0^{0} = a_0^{q,1}, \\
& \quad u_0^{q+1,q}(a_0^{0,0} , a_0^{q,2}), a_0^{0} = a_0^{q,2}. \\
p_i & = \left\{ u_i^{q,0}(a_i^{0,0} , a_i^{q,1}), a_i^{0} = a_i^{q,1} \right\}, \\
& \quad u_i^{q,0}(a_i^{0,0} , a_i^{q,2}), a_i^{0} = a_i^{q,2}, \\
& \quad \cdots \\
& \quad u_i^{q,q-1}(a_i^{0,0} , a_i^{q,1}), a_i^{0} = a_i^{q,1}, \\
& \quad u_i^{q,q}(a_i^{0,0} , a_i^{q,2}), a_i^{0} = a_i^{q,2}, \\
& \quad \cdots \\
& \quad u_i^{q+1,q-1}(a_i^{0,0} , a_i^{q,1}), a_i^{0} = a_i^{q,1}, \\
& \quad u_i^{q+1,q}(a_i^{0,0} , a_i^{q,2}), a_i^{0} = a_i^{q,2}. \end{align*}
\]

Among them, $m$ is the number of penalty rounds, $a_i^{j}$ represents the cooperative user $P_i$ selection strategy in the anonymous zone cooperative construction game $G_{ACR}^{j}$, $\lambda_{i-0}$ is the number of times that the cooperative users $P_i$ who participate in the anonymous zone cooperative construction game $G_{ACR}^{j}$ assist other users in constructing the
anonymous area when they participate in game $G_{ACR}^j$, and $\delta_i$ is the judgment threshold of cooperative users $P_i$ in the anonymous zone cooperative construction game $G_{ACR}^j$. When $\lambda_i \equiv \delta_i, a_i^{(j)}(\lambda_i \equiv \delta_i) = a_i^{(j)(2)}$; otherwise, $a_i^{(j)}(\lambda_i \equiv \delta_i) = a_i^{(j)(1)}$. Interactive recording mechanism $M_R$ refers to using the requesting users, cooperative users, and location information provided by them to restrict their self-interest behavior. In other words, in the anonymous region collaborative construction game $G_{ACR}^j$, once it is found that the requesting user $P_0$ divulges the location information of the cooperative user, and then there will be no user to help him construct an anonymous area in the subsequent $m$-times service queries. Similarly, in the anonymous region collaborative construction game $G_{ACR}^j$, if the cooperative user $P_i$ provides a false location, then the cooperative user will not have other users to help him construct the anonymous area in the subsequent $m$-times of service queries.

In the scheme proposed in this paper, the researcher uses blockchain distributed storage, with the requesting user, collaborative user, and location information, as evidence. Therefore, to encourage all users in the network to participate in the maintenance of the blockchain, this paper also proposes a block chain accounting rights competition mechanism.

**Definition 4** (Consensus mechanism II-accounting rights competition mechanism). Accounting rights competition mechanism $M_C = (\bar{\lambda}, \bar{\rho})$ is a two-tuple. Among them, we have the following:

(i) $\bar{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ is the set of times $\lambda_1, \lambda_2, \ldots, \lambda_n$ that users $P_1, P_2, \ldots, P_n$ who participate in the competition to obtain accounting rights help other users to construct an anonymous area in the competitive production of the new block $block_M$. Here, $\lambda_i$ is the number of times that the $i$-th users $P_i$ history, which participates in the generation of accounting rights in the new block, and helps other users to construct anonymous zones.

(ii) $\bar{\rho} = \{p_{i}^1, p_{i}^2, \ldots, p_{i}^m\}$ is the revenue when the new block is generated (users $P_1, P_2, \ldots, P_n$ who participate in the competition of the new block generation bookkeeping rights help other users to construct anonymous areas in history). For any $p_i \in \bar{\rho}$, the following conditions are satisfied:

$$P_i = \begin{cases} 0, \text{other} \\ \lambda_i + 1, \lambda_i = \arg \max \{\lambda_i \mod \Lambda_{\max}^{-1}\} \end{cases} \tag{3}$$

Among them, $\Lambda_{\max}^{-1}$ represents the number of times $i^{\prime} \in [1, 2, \ldots, n]$ that the user who has obtained the accounting rights of the generated block $block_{M-1}$ has helped other users to construct an anonymous zone at that time.

In short, the basic idea of the new block accounting rights competition mechanism $M_C$ proposed in this paper is to allow the users who participate in the anonymous zone construction for the largest number of times obtain the accounting rights. However, to prevent the users who participate in the anonymous zone construction for the largest number of times from always obtaining the accounting permission, and thus have the opportunity to forge the distributed anonymous area collaborative construction blockchain, this paper uses $\lambda_i = \arg \max \{\lambda_i \mod \Lambda_{\max}^{-1}\}$ to make the accounting rights of the blockchain disperse to each user in the network. In addition, to encourage all users in the network to participate in the updating of the blockchain, this paper regards the accounting rights of generating new blocks as a special way to participate in the construction of an anonymous area. Obviously, for any user $P_i$ in the network, the larger that $\lambda_i$ is, the more help to other users in constructing anonymous areas. Then, when $P_i$ as a requester sends an anonymous area collaborative construction request, the larger the number of users who provide their location information to him is, and the greater the probability that RR can successfully construct an anonymous area. This approach can also prevent users from using new cid frequently in the blockchain system to a certain extent.

It is worthwhile to note that in the accounting rights, competition mechanism proposed in this paper, any user in the network, including the requesting user who sends the anonymous zone collaborative construction request, the collaborative user who provides the location information, and the other users who receive the anonymous zone collaborative construction request without providing the location information, can participate in the competition of generating the new block accounting rights.

4.2. Specific Scheme. In this paper, the process of requesting users to obtain the real location of collaborative users is regarded as a special kind of transaction. The ID of both parties and the location information provided by cooperative users are recorded in the transaction bill, and the bill is stored in the public chain. When the requesting user indicates that the cooperative user provides a false location or the cooperative user indicates that the requesting user discloses his location, the transaction bill can be used as a voucher for arbitration. Once the location disclosure or spoofing behavior is confirmed, the user who has the above behavior will not be helped by other users when they are the requester, which makes them unable to construct an anonymous area successfully. In addition, to encourage network users to participate in the maintenance of the blockchain, users who generate blocks each time are regarded as helping users to construct anonymous zones. The specific scheme is as follows:

**Step 1.** The requesting user sends an anonymous zone construction collaboration request to the cooperative user.

$$\text{Req} = \{T_{i\rightarrow}, \text{cid}_0, A_0, N(\text{Tran}_1), N(\text{Tran}_2), \ldots, N(\text{Tran}_n), \text{sign}_{\text{sk}_{\text{CID}}}(\text{cid}_0 || T_{i\rightarrow})\} \tag{4}$$
Among them, $T_{i-1}$ represents the timestamp when the requesting user $P_i$ sends an anonymous zone construction collaboration request. Additionally, $cID_0$ is the pseudonym used by the requesting user $P_0$ in the blockchain system, and $\lambda_0$ represents the number of times that the requesting user has participated in the anonymous zone construction when he is a cooperative user. $N(\text{Tran}_0)$ represents the bill number of the transaction bill $\text{Tran}_0$, which stores the request of user $P_0$ to cooperate with other users to construct the anonymous zone. Here, $1 \leq k \leq \lambda_0$, $SK - cID_0$, is the private key of the requesting user in the blockchain system. $\text{sign}_{SK - cID_0}(\lambda_0\|T_{i-1})$ means signing $\lambda_0\|T_{i-1}$ with private key $SK - cID_0$ and “||” is the connection symbol.

**Step 2.** After receiving the anonymous area construction request sent by the requesting user, the cooperative user $P_i$ (i ≠ 0) first counts the number of times $\lambda'_0$ that the requesting user has participated in the anonymous area construction in the distributed anonymous area collaborative construction blockchain $\text{Blockchain} = \{\text{Block}_1, \text{Block}_2, \cdots, \text{Block}_{M-1}\}$ and determines whether there is a penalty transaction bill recording the cheating behavior of the requesting user $P_0$ in the blockchain.

1. When $\lambda'_0 = \lambda_0$ and no penalty transaction bill is found to record the cheating behavior of the current requesting user $P_0$, the cooperative user $P_i$ decides whether to send his real location $\text{Loc}_{i}^{\text{real}}$ to the requesting user according to the threshold value $\delta_i$.

   (i) If $\lambda_0 < \delta_i$, the collaboration user $P_i$ does not respond to the collaboration request of the requesting user $P_0$

   (ii) If $\lambda_0 \leq \delta_i$, the cooperative user $P_i$ sends the transaction bill to the requesting user $P_0$

   \[
   \text{Tran} = \{T_{i-0}, cID_0, \text{Enc}_{PK - cID_0}(\text{Loc}_{i}^{\text{real}}\|T_{i-0}), \text{sign}_{SK - cID_0}(\text{Enc}_{PK - cID_0}(\text{Loc}_{i}^{\text{real}}\|T_{i-0}))\}. \tag{5}
   \]

2. When $\lambda'_0 = \lambda_0$, but the penalty transaction bill recording the cheating behavior of the current requesting user $P_0$ is found in the block $\text{Block}_{i'}$, the cooperative user $P_i$ judges whether the requesting user $P_0$ is still in the penalty period according to the number of current blocks.

   (i) If $M - 1 - i' \leq m$, in other words, the requesting user $P_0$ is still in the penalty period, the cooperative user $P_i$ does not respond to the request of the requesting user $P_0$, and the penalty transaction bill is broadcast:

   \[
   \text{Tran}_{\text{pun}} = \{T_{i-0}, cID_0, \text{Punishment}, \text{sign}_{SK - cID_0}(\text{punishment}\|T_{i-0})\}. \tag{6}
   \]

   (ii) If $M - 1 - i' > m$, in other words, the requesting user $P_0$ has been punished, and the cooperative user $P_i$ will send the transaction bill $\text{Tran}$ to the requesting user $P_0$

   \[
   \text{Tran} = \{T_{i-0}, cID_0, \text{Punishment}, \text{sign}_{SK - cID_0}(\text{punishment}\|T_{i-0})\}. \tag{7}
   \]

$M$ represents the number of blocks in the distributed anonymous zone collaborative construction blockchain when the requesting user $P_0$ sends the cooperation request. Here, $\lambda'_0$ represents the block number of the recorded requesting user $P_0'$'s spoofing behavior, which satisfies $1 \leq \lambda_0' \leq M - 1$. $T_{i-0}$ represents the timestamp that generated the transaction bill and is the penalty threshold. $PK - cID_0$ is the public key of the requesting user $P_0$ in the blockchain system. $SK - cID_0$ is the private key of the cooperative users $P_i$ in the blockchain system. Punish – ment is the identifier of the penalty transaction bill. $\text{Enc}_{PK - cID_0}(\text{Loc}_{i}^{\text{real}}\|T_{i-0})$ represents the ciphertext obtained by encrypting $\text{Loc}_{i}^{\text{real}}\|T_{i-0}$ with the public key $PK - cID_0$ of the requesting user $P_0$ in the blockchain system.

**Step 3.** After receiving the transaction bill $\text{Tran}$ sent by the cooperative user $P_i$, requesting user $P_0$ uses the public key $PK - cID_0$ of the cooperative user $P_i$ in the blockchain system to verify the correctness of the signature information.

\[
\text{sign}_{SK - cID_0}(\text{Enc}_{PK - cID_0}(\text{Loc}_{i}^{\text{real}}\|T_{i-0})). \tag{8}
\]

1. If the verification is successful, then requesting user $P_0$ decrypts $\text{Enc}_{PK - cID_0}(\text{Loc}_{i}^{\text{real}}\|T_{i-0})$ with his private key $SK - cID_0$ to obtain the real location $\text{Loc}_{i}^{\text{real}}$ of the cooperative user $P_i$. Then, $\text{Enc}_{PK - cID_0}(\text{Loc}_{i}^{\text{real}}\|T_{i-0})$ and $\text{sign}_{SK - cID_0}(\text{Enc}_{PK - cID_0}(\text{Loc}_{i}^{\text{real}}\|T_{i-0}))$ are calculated and written into the transaction bill $\text{Tran}$ for broadcasting.

2. If the verification fails, then $\text{Loc}_{i}^{\text{real}}$ is not used to construct the anonymous area $ACR$, and the penalty transaction bill is broadcast.
The anonymous region can be constructed successfully when the requesting user obtains the real location provided by no less than $K - 1$ cooperative users.

**Step 4.** All of the users in the network verify their authenticity after receiving the transaction bill sent by the broadcast. If the verification fails, then new penalty transaction bills are generated and broadcast. If the verification is passed, the transaction bill is saved to generate a new block $B_k$. When the distributed anonymous zone is to be updated in practical applications, we can introduce a sliding window mechanism in the above scheme to reduce the number of blocks that store transaction bills in the blockchain.

Moreover, if the location privacy data update frequency is much higher than the transaction speed in the public chain network when using the scheme in practice, the scheme can be optimized by using methods such as region division and alliance chain technology.

### 4.3. Scheme Analysis

#### 4.3.1. Security Certification

This paper assumes that there are at least $K - 1$ users $P_1(1 \leq i \leq K - 1)$ with the threshold $\delta_i < \lambda_0$ in the network. The requesting user $P_0$ can successfully construct an anonymous area $ACR$ that contains the location provided by the other $K - 1$ cooperative users.

Moreover, it is also assumed that if the requesting user $P_0$ receives the real locations $Loc_{real}^0$, $Loc_{real}^1$, $\ldots$, $Loc_{real}^{K-1}$ provided by the $K - 1$ users, the anonymous area construction method $Area(\cdot)$ adopted by the user is secure; in other words, equation (12) holds.

$$\Pr_{\lambda_{SP}} \left[ \frac{\lambda_{real}^0 \cdot \lambda_{real}^1 \cdot \lambda_{real}^{K-1}}{\lambda_{real}^0 \cdot \lambda_{real}^1 \cdot \lambda_{real}^{K-1}} \right] \leq \frac{1}{K}. \tag{12}$$

Therefore, this paper proves only that the scheme is secure from the perspective of anonymous region construction.

**Lemma 5.** Let $\alpha$ denote the probability that the cooperative user $P_i$ can correctly identify the location disclosure behavior of the requesting user $P_0$ and let $\beta$ represent the probability that the requesting user $P_0$ identifies the false location provided by the cooperative user $P_i$. When the threshold $\delta_i < \lambda_0$ of $K - 1$ users exists in the network, if $m > \max \left( \left\{ \frac{U - U/a}{(U - U)}, \left(1 - \beta\right) \cdot \left(W + W\right)/\beta \cdot U - U \right\} \right)$, then the scheme is able to not only prevent the requesting users $P_0$ from disclosing the location information of the cooperative users $P_i(1 \leq i \leq K - 1)$ but also ensure that the cooperative users $P_i$ provide the real locations $Loc_{real}^i$ when participating in the distributed anonymous construction.

**Proof.** Proof by contradiction. Suppose that when the threshold value of rational user $P_i$ is $\delta_i < \lambda_0$ and $m > \max \left( \left\{ \frac{U - U/a}{(U - U)}, \left(1 - \beta\right) \cdot \left(W + W\right)/\beta \cdot U - U \right\} \right)$, the requesting user $P_0$ will disclose the real location $Loc_{real}^i$ to the third party after receiving the rational user $P_i$’s real location in any $q$-th anonymous area cooperative construction game, in other words, the selection strategy $a_{0,2}^{q-2}$. At this time, for the requesting user $P_0$, his profit in the game $G_{ACR}$ is as follows:
\[ u_0\left( a_0^{q_2-2}\right) = U^+. \]  

When the rational cooperative user \( P_i \) confirms that \( P_0 \) has ever disclosed his real location \( \text{Loc}_i^{\text{real}} \), \( P_0 \) still acts as the requester in the \( a_i^{(2)} \) anonymous area cooperative construction game \( G_{\text{ACR}}^{q}, G_{\text{ACR}}^{q+1}, \ldots, G_{\text{ACR}}^{q+m} \) after that time, and the revenue satisfies the following:

\[ u_{0}^{j+i} \left( a_0^{j+i} \right) | a_0^{q_2-2}) = U, \]

for \( 1 \leq j \leq m \). Therefore, the total revenue of rational user \( P_0 \) for the selection strategy \( a_0^{q_2-2} \) in the \((m+1)\)-time game \( G_{\text{ACR}}^{q}, G_{\text{ACR}}^{q+1}, \ldots, G_{\text{ACR}}^{q+m} \) is as follows:

\[
\bar{u}_0 \left( a_0^{q_2-2} \right) = \alpha \cdot u_0 \left( a_0^{q_2-2} \right) + \left( 1 - \alpha \right) \cdot \left[ u_0 \left( a_0^{q_2-2} \right) \right] + u_0 \left( a_0^{q_2-2} \right) + \cdots + u_0 \left( a_0^{q_2-2} \right) = U + mU + \alpha \cdot m \cdot \left( U - U \right)
\]

However, if the requesting user \( P_0 \) does not disclose the real location to the third party after receiving the real location \( G_{\text{ACR}}^{q}, G_{\text{ACR}}^{q+1}, \ldots, G_{\text{ACR}}^{q+m} \) in the \( a_i^{q_2-2} \)-th anonymous area cooperative construction game, in other words, when selecting the strategy \( a_0^{q_2-1} \), the overall revenue of the user in the anonymous area cooperative construction game \( G_{\text{ACR}}^{q}, G_{\text{ACR}}^{q+1}, \ldots, G_{\text{ACR}}^{q+m} \) is as follows:

\[
\bar{u}_0 \left( a_0^{q_2-1} \right) = \alpha \cdot u_0 \left( a_0^{q_2-1} \right) + u_0 \left( a_0^{q_2-1} \right) + \cdots + u_0 \left( a_0^{q_2-1} \right) = U + mU + \alpha \cdot U
\]

According to the hypothesis, if and only if \( u_0 \left( a_0^{q_2-1} \right) \leq \bar{u}_0 \left( a_0^{q_2-2} \right) \), the requesting user will disclose the location information provided by the cooperative user. More specifically, the following holds:

\[
U + mU \leq U^+ + mU + \alpha \cdot m \cdot \left( U - U \right)
\]

the rational cooperative user \( P_i \) provides a false location \( \text{Loc}_i^{\text{false}} \) to the requesting user \( P_0 \), and the probability of correct identification of the requesting user \( P_0 \) is \( \beta \). Therefore, after the cooperative user is proven to provide a false location in the current game \( G_{\text{ACR}}^{q} \), the total revenue of the cooperative users participating in the \( a_i^{(2)} \)-th anonymous zone cooperative construction game \( G_{\text{ACR}}^{q}, G_{\text{ACR}}^{q+1}, \ldots, G_{\text{ACR}}^{q+m} \) is as follows:

\[
\bar{u}_i \left( a_i^{q_2-3} \right) = \beta \cdot u_i \left( a_i^{q_2-3} \right) + \left( 1 - \beta \right) \cdot \left[ u_{i-0} \left( a_i^{q_2-3} \right) \right] + u_{i-0} \left( a_i^{q_2-3} | a_i^{q_2-3} \right) + \cdots + u_{i-0} \left( a_i^{q_2-3} | a_i^{q_2-3} \right) = (1 - \beta) \cdot W^+ + \beta \cdot W^+ + \beta \cdot m \cdot \left( U - U \right)
\]

Among them, in the anonymous area collaborative construction game \( G_{\text{ACR}}^{q}, \bar{u}_{i-0} \left( a_i^{q_2-3} \right) \) represents the revenue function of the cooperative users as requesters in the subsequent collaborative construction game. When the cooperative user \( P_i \) decides to help the requesting user construct the anonymous area and provide the real location \( \text{Loc}_i^{\text{real}} \), in other words, to choose the strategy \( a_i^{q_2-1} \), the total revenue in the game \( G_{\text{ACR}}^{q}, G_{\text{ACR}}^{q+1}, \ldots, G_{\text{ACR}}^{q+m} \) is as follows:

\[
\bar{u}_i \left( a_i^{q_2-1} \right) = u_i \left( a_i^{q_i-1} \right) + u_{i-0} \left( a_i^{q_i-1} \right) + u_{i-0} \left( a_i^{q_i-1} \right) + \cdots + u_{i-0} \left( a_i^{q_i-1} \right) = W + mU
\]

According to the hypothesis, if and only if \( \bar{u}_i \left( a_i^{q_2-1} \right) \leq \bar{u}_i \left( a_i^{q_2-3} \right) \), the cooperative user \( P_i \) will provide a false location to the requesting user. In other words, \( W + mU \leq \left( 1 - \beta \right) \cdot W^+ + \beta \cdot W^+ + \beta \cdot m \cdot \left( U - U \right) \) holds. Then, \( m < (\alpha \cdot (U^+ - U))/\beta \left( U - U \right) \) contradicts the known \( m > \alpha \cdot (U^+ - U)/\beta \left( U - U \right) \). Therefore, for rational requesting users \( P_0 \), it will not reveal the real location of the collaborative users \( P_i \). In the same way, suppose that in any \( q \)-th anonymous cooperative construction game, when \( m > \max \left\{ \left[ (U^+ - U)/\alpha \cdot (U - U) \right], \left[ (1 - \beta) \cdot (W^+ + W)/\beta \cdot (U - U) \right] \right\} \) and the cooperative user \( P_i (1 \leq i \leq K - 1) \) decides to help the requesting user construct the anonymous area, the cooperative user \( P_i \) provides a false location \( \text{Loc}_i^{\text{false}} \), in other words, the selection strategy \( a_i^{q_2-3} \). At this time, the proof is complete.

**Lemma 6.** Let \( \alpha \) denote the probability that the cooperative user can correctly identify the location leakage behavior of the requesting user \( P_0 \). Here, \( \beta \) represents the probability that the requesting user \( P_0 \) identifies the false location provided by the cooperative user.

Let \( \alpha \) denote the probability that the cooperative user can correctly identify the location leakage behavior of the requesting user \( P_0 \). Here, \( \beta \) represents the probability that the requesting user \( P_0 \) identifies the false location provided by
the cooperative user. It is assumed that rational users $P_0$ adopt this scheme to protect their location privacy during an LBS query, and there is a threshold $\delta_i = \lambda_i$ of $K - 1$ other rational users $P_i$ $(1 \leq i \leq K - 1)$ in the network. Here, $\lambda_i$ represents the number of times in the history that rational requesting users $P_i$ help other users to construct anonymous zones. If $m > \max \{(U^+ - U/\alpha \cdot (U - U)), \{(1 - \beta) \cdot (W^+ - W) / \beta \cdot (U - U)\}\}$, the scheme is safe. In other words, this scheme is able to not only promote the cooperative users $P_i$ $(1 \leq i \leq K - 1)$ to provide their real locations to the requesting users $P_0$ but also prevent the requesting users $P_0$ from divulging these locations. At the same time, the accuracy rate of the LSP in identifying the real location from the anonymous area submitted by the requesting user $P_0$ is not higher than that of $1/K$.

4.3.2. Computational Complexity. This scheme involves encryption, decryption, and a signature operation. In this paper, the signature operation is regarded as a special encryption operation. Because the decryption operation is the inverse of the encryption operation, $O(\text{Enc})$ is used to represent the computational complexity of the encryption, decryption, and signature operations.

In this scheme, when each cooperative user $P_i$ receives the anonymous region construction request sent by the requesting user $P_0$, it first calculates according to the requesting user $P_i$’s public key $PK - cID_0$, and it verifies the correctness of the signature data $\text{sign}_{\text{SK} - cID_0}(\lambda_0 || T_0 - \omega)$. At this time, the required computational complexity is $O(\text{Enc})$. If the correctness is verified, then the cooperative user $P_i$ will query the transaction bill stored in the blockchain $\text{Blockchain} = \{\text{Block}_1, \text{Block}_2, \ldots, \text{Block}_{M-1}\}$, determine the authenticity of the number of times $\lambda_0$ that requesting user $P_0$ helped other users construct an anonymous area, and determine whether there is a penalty transaction bill from recording $P_0$ cheating in the blockchain. When it is found that the requesting user $P_0$ sends a false $\lambda_0$ or it is still in the penalty period, the penalty transaction bill is broadcast after calculating the $\text{sign}_{\text{SK} - cID_0}(\text{Punishment} || T_i - \omega)$. In this case, the computational complexity of is

$$O(M) + O(\text{Enc}) = O(\text{Enc}).$$  \hspace{1cm} (20)

When $\lambda_0$ is verified to be correct and no penalty transaction bill is found to record the cheating behavior of the requesting user $P_0$, then the cooperative user $P_i$ decides whether to provide his own location to the requesting user $P_0$ according to the threshold value $\delta_i$. If $\lambda_i < \delta_i$, then it does not respond to the anonymous area construction request sent by the requesting user, and the computational cost is $O(1)$. If $\lambda_i \geq \delta_i$, then after calculating the $\text{Enc}_{\text{PK} - cID_0}(\text{Loc}_{i - \omega} \parallel T_i - \omega)$ and the corresponding signature $\text{sign}_{\text{SK} - cID_0}(\text{Enc}_{\text{PK} - cID_0}(\text{Loc}_{i - \omega} \parallel T_i - \omega))$, the transaction bill is sent to the requesting user $P_0$, and the computational complexity of the cooperative user $P_i$ is

$$O(1) + O(\text{Enc}) + O(\text{Enc}) = O(\text{Enc}).$$  \hspace{1cm} (21)

Therefore, when an anonymous construction request is received, the upper limit of the computational complexity required by the cooperative user $P_i$ is as follows:

$$O(\text{Enc}) + O(\text{Enc}) + O(\text{Enc}) = O(\text{Enc}).$$  \hspace{1cm} (22)

In the same way, after receiving the transaction bill sent by the cooperative user $P_i$, the computational complexity required by the requesting user is $O(\text{Enc})$. When a new block is generated, the computational complexity of the users participating in the new block $\text{Block}_{k+1}$ generation is $O(\text{Enc})$.

To summarize, if the user successfully obtains the real location provided by $r \leq K - 1$ cooperative users, the computational complexity of each user in the network is as follows:

1. For the requesting user, the calculation complexity is as follows:

$$r \cdot O(\text{Enc}) + O(\text{Enc}) = O(\text{Enc}).$$  \hspace{1cm} (23)

2. For users who provide their own real location to construct the anonymous area, the computational complexity is as follows:

$$O(\text{Enc}) + O(\text{Enc}) + O(\text{Enc}) = O(\text{Enc}).$$  \hspace{1cm} (24)

3. For the users who do not respond to the anonymous region cooperative construction request, the computational complexity is as follows:

$$O(\text{Enc}) + O(1) + O(\text{Enc}) = O(\text{Enc}).$$  \hspace{1cm} (25)

5. Experiment

To test the effectiveness of the proposed scheme, the computational cost and communication overhead are examined. The experimental environment configuration is shown in Table 1.

In the blockchain network, there are 25 network nodes: one is the requesting user $P_0$ node, and the other 24 are the cooperative user $P_1, P_2, \ldots, P_{24}$ nodes. By generating random numbers, the number of times $\lambda_i$ that the requesting user’s $P_0$ node has participated in the construction of an anonymous area and the thresholds $\delta_1, \delta_2, \ldots, \delta_{24}$ of the cooperative user nodes are generated in such a way that there are at least $K - 1$ cooperative users $P_1, P_2, \ldots, P_{k-1}$ with thresholds $\delta_1, \delta_2, \ldots, \delta_{k-1} \leq \lambda_0$. In other words, after sending an anonymous region to construct a cooperative request, the requesting user can obtain at least cooperative users’ location information to construct the anonymous region. In addition, in the established blockchain network.
platform, the “Consensus mechanism — competition mechanism of bookkeeping rights” proposed in this paper is used to determine which user in the network obtains the generation rights to the new block. Moreover, in the blockchain network platform, each block is set to store 100 historical transaction bills. Each transaction bill is used to record the ciphertext and signature data of the requesting user and the cooperative user about the location information provided by the cooperative user during the construction of the anonymous area. We set the current blockchain length to |Blockchain| = 100; in other words, there are 100 × 100 = 10000 historical transaction bills. In this experiment, the user’s privacy protection requirement K value changes from 2 to 20, and the algorithm is repeated 100 times for different K values.

5.1. Experiment-1. This experiment is to construct an anonymous region. In experiment 1, suppose that the requesting user has provided his real location and participated in the construction of an anonymous area 100 times, in other words, λ_n = 100. When the requesting user receives more than K − 1 cooperative users’ location information, K − 1 locations are randomly selected to construct the anonymous area. The average computation delay and communication cost required by the cooperative user and the requesting user in the anonymous region construction process are shown in Figure 1, respectively.

When the user uses this scheme to protect its location privacy in an LBS query, the average computing delay required for the successful construction of the anonymous area increases when K increases. For cooperative users, the average computing delay is independent of the privacy protection requirements K value of the requesting user, as shown in Figure 1(a). The reason for the above phenomenon is that with an increasing K value, the requesting user must verify the correctness of the signature data sent by the cooperative user, and the number of times to decrypt and obtain the real location of the cooperative user also increases. However, for cooperative users P_i (1 ≤ i ≤ K − 1), when they receive the cooperation request of constructing the anonymous area sent by the requesting user P_0 and δ_i < λ_n, it is only required to encrypt its real location with the public key of the requesting user and send the encrypted ciphertext to the requesting user. Therefore, the average computing delay required by the requesting user is independent of the K value.

In addition, in the process of constructing the anonymous area, the average communication cost of the requesting user increases with the increase in the K value of the privacy protection requirement of the requesting user. The reason is that with an increase in the K value, the requesting user must receive more location information provided by cooperative users to construct the anonymous area, which increases the average communication cost of the requesting users. However, for the cooperative users, the point-to-point communication is used to provide their real location to the requesting users. Therefore, the average communication cost required by the cooperative users does not change with the K value of the privacy protection requirement of the requesting users, as shown in Figure 1(b).

Through the above experiments, it can also be found that when the requesting user successfully generates the anonymous area by using this scheme, the computation delay and communication cost required by the requesting user and the cooperative user are also very limited. For example, when K = 20, the average computing delay of the requesting user is 311.924 ms, and the average communication cost is 17.206 kb; additionally, the average computing delay of the cooperative user is 32.985 ms, and the average computational communication cost is 1.241 kb. This finding shows that the scheme has good usability and can efficiently generate an anonymous area for the requesting user.

5.2. Experiment-2. This experiment is to update the blockchain. Next, we analyze the average computing cost and storage cost of a block chain update. In experiment 2, we set the number of transaction bills included in the new block generation to 100. When updating the blockchain, regardless of whether the requesting user has the permission to update the blockchain or not, the calculation delay decreases with the increase in the privacy protection demand K value. The reason is that when the K value increases, the amount of verified signature data sent by the cooperative users increases when the requesting users construct the anonymous zone, which reduces the amount of verified signature data sent by cooperative users in the process of updating the blockchain. Figure 2(a) shows this relationship. For example, when the K value changes from 2 to 20, if the

| Table 1: The configuration of the experimental environment. |
|----------------|-------------------|------------------|
| Name            | Parameter         | Remarks          |
| CPU             | Intel(R) CoreTM i5-2400 @ 3.10 GHZ |                   |
| Memory          | DDR3 1333/1600 MHz,4G | 8Mcache(I/O)Read |
| Harddisk        | 256 GB PCIe × 4 NVMe SSD | -ing speed 2 M    |
| Network         | Guangxi telecom   |                  |
| Operating-system | Ubuntu 17.10      |                  |
| Blockchain-platform | Ethereum 1.5.5 |                  |
| Encryption-mode | OpenSSL-1.0.0c,256Bit, ECC | Nothing          |
| Programe-linguage | JAVA              |                  |
For collaborative users, when updating the blockchain, regardless of whether the requesting user has permission to update the blockchain or not, it must verify the correctness of all transaction bills sent by the requesting user. Therefore, the computing delay required by the cooperative user is not affected by the $K$ value of the requesting user, as shown in Figure 2(b).

Moreover, since the cooperative user is only required to verify the correctness of the signature data about the real location of the cooperative user in each transaction bill, in the process of updating the blockchain, the computing time delay required by the cooperative users is much less than that of the requesting users.

5.3. Experiment-3. This experiment is used to analyze when the blockchain is updated, to assess the impact of the number of transaction bills on the communication cost, calculation delay, and block size. We set the number of transaction bills from 100 to 1000 when the new block is generated. In this scheme, the transaction bills stored in the blockchain are finally broadcasted by the requesting users, which enables all of the users in the network to verify the correctness of these transaction bills. Therefore, the communication cost of the requesting users in the process of the blockchain update increases with an increase in the number of transaction bills, as shown in Figure 3. Moreover, with an increase in the number of transaction bills, when the new block is generated, the number of transaction bills to be stored and the computing delay of the Merkle tree root node to calculate these bills will also increase. As a result, the calculation delay and the size of the new block will increase with an increase in the number of transaction bills, as shown in Figure 4, respectively.
Figure 2: Average computing delay required by the requesting user and collaboration user in the blockchain update.

Figure 3: The number of transaction bills and communication costs of the requesting user.
According to the above analysis, when a new block is generated, when there is an increase in the number of transaction bills, the computing delay, communication cost, and storage cost of each user in the network will also increase. However, for the requesting user, when it obtains the generation rights of the new block, it can construct the anonymous area first and then generate the new block. It can be seen from Figure 1(a) and Figure 1(b) that the computation delay and communication cost required by both the requesting user and the cooperative user are very limited when the anonymous area is generated by this scheme. This finding shows that the scheme can generate an anonymous region efficiently and has good practicability.

In addition, in practical applications, the number of transaction bills used to generate a new block can be reduced by adjusting the frequency of generating new blocks, and the computing delay, communication cost, and storage cost of each user in the network can be reduced when the blockchain is updated, to further improve the usability of the scheme.

6. Summary and Prospects

The existing distributed $k$-anonymity privacy protection schemes cannot effectively protect the users’ location privacy. The reason for this problem is that these schemes do not consider privacy disclosure and deception during the construction of an anonymous area, which makes a self-interested requesting user disclose the real location of the cooperative users to a third party to obtain additional benefits. However, the self-interested cooperative users will provide false locations to the requesting user, which results in the constructed anonymous area not meeting the location privacy protection requirements of the requesting user. To solve this problem, this paper first describes the game of constructing a distributed anonymous area, and it then analyzes the policy choices and benefits of the requesting and cooperating users. The security definition of distributed $k$-anonymous location privacy protection is given. Then, the blockchain distributed storage is used to take the requesting users, cooperative users, and location information provided by the cooperative users as evidence. When punishing the users who have location leakage and spoofing behavior, they cannot construct an anonymous area successfully when sending anonymous area collaborative construction requests in the future, which will restrict the self-interest behavior of the requesting users and the cooperative users. Based on the above discussion, this paper proposes a distributed $k$-anonymous location privacy protection scheme based on blockchain. Security analysis and experiments show that this scheme can not only effectively prevent the requesting users from divulging the location information of the cooperative users but also urge the cooperative users to provide the real location, to construct the anonymous area efficiently. In addition, this scheme can not only protect the location privacy of the user in a sparse crowd scene but also protect the location privacy of the continuous queries.

Data Availability

The data used to support the findings of this study are included within this article.

Conflicts of Interest

The authors declare there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research work was supported by the Central Government Guides the Local Science and Technology Development Fund Project Subsidization (Guike AD20238072) and
Middle-Age and Young Teachers’ Basic Ability Promotion Project of Guangxi under Grant (2019KY0659).

References


