International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol.10 No.6 July – August 2023

Evaluating The Efficacy Of A Novel Location Privacy-Preserving Approach Utilizing Blockchain Technology

Bhakti Chaudhari[1] & Dr. Shabnam Sharma[2]
[1]*Ph.D. Research Scholar, Department of Computer Science, Shri J.J.T. University, Rajasthan, India*
[2]*Professor & Research Guide, Department of Computer Science, Shri J.J.T. University, Rajasthan, India*
Corresponding Author - Bhakti Chaudhari

DOI - 10.5281/zenodo.10032565

Abstract:

Location-based services (also known as LBS) make people's life easier, but they also come with the risk of their private information being compromised. Numerous location privacy protection algorithms have been presented as a means of ensuring the confidentiality of LBS users' personal information. On the other hand, these algorithms often struggle to strike a healthy balance between the quality of the service and the privacy of the user. In this work, we first provide an overview of the drawbacks of the two current architectures and technologies for privacy protection, and then we offer a technique for location privacy protection that is based on blockchain. Because it adheres to the k-anonymity privacy protection principle, our approach does not need the assistance of reliable anonymousizing servers provided by a third party. The integration of many private blockchains has the potential to spread the transaction records of users. This has the potential to provide consumers enhanced security against location privacy intrusions while maintaining the same level of service quality. In addition, we suggest a reward system as a means of motivating user engagement. In the end, we show that our method is effective by implementing it in the Remix blockchain. This demonstrates the possibility for use in a distributed network setting, which further highlights the potential for the application.

Keywords: Location-Based Services; Location Privacy-Preserving; Blockchain; K-Anonymity

Introduction:

As a result of the fast development of communication technology, location-based services, often known as LBS, are finding widespread usage in a variety of industries [1–3], such as mobile social networking and health care. Users are provided with value-added services such as querying locations of interest using LBS [4,5], which is based on the location information and is supported by geographic information systems (GIS) and lightweight mobile devices. There are two different types of LBS queries: snapshot queries and continuous queries [6]. The user actively inputs query criteria to query as part of the snapshot inquiry. For example, the user may say, "query the gas stations that are nearest to me now." "query the gas stations nearest to me while

driving" is an example of a continuous inquiry, which indicates that the location service provider (LSP) is providing location services in accordance with the continual changes in the user's position. Numerous apps that are now being developed are based on various location services. The majority of apps fall into one of the following categories: map applications (like Google Maps), interest point query applications (like Meituan), location-aware services (like Foursquare), and so on [7]. When using these programmes, users are required to make their location data public. When users wish to "query which Meituan takeaways are near me," for instance, they are need to supply location data to the LSP. This is how the service works. Users have a greater chance of receiving improved location services via LBS in proportion to the amount of location information they give. The attacker's inference assault on the location data, on the other hand, may analyse sensitive information about the user, such as personal data, workplace, and health state [8,9]. Therefore, it has become an important challenge to determine how to strike a balance between the provision of location services via LBS and the leaking of users' private information [10–12].

Decentralized architecture and centralised architecture are the two broad categories that may be used to classify existing architectures for the protection of location privacy [13]. [14] The centralised design includes the implementation of a fully trusted third party (TTP) anonymizing server. After receiving the specific position of the user and the query information (as seen in Figure 1), the anonymizing servers utilise several technologies, such as spatial obfuscation, location perturbations, pseudonyms, and others, to safeguard the user's right to privacy about their location [15,16]. On the one hand, the anonymizing servers have access to all of the user's information; if they have been compromised, this information will constitute a bottleneck that introduces new security risks. On the other hand, it is challenging to strike a balance between the user's right to privacy and the quality of the location service when using privacy protection methods such as spatial obfuscation and location perturbations. The pseudonym technology has to depend on a reliable server hosted by a third party. In conclusion, anonymizing servers might quickly become the structure's performance bottleneck if they are subjected to intensive computational duties.

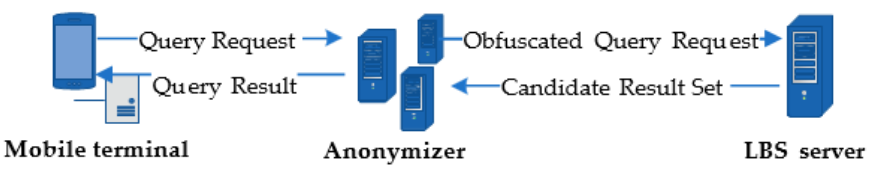


Figure 1. *The centralized architecture.*

The decentralised architecture, in contrast to the centralised design, does not need TTP anonymizing servers in order to function. In a decentralised design, the client connects directly with the LSP and employs encryption and user collaboration technologies on the client to safeguard user privacy. This kind of architecture is also known as a client-server architecture. However, these technologies that safeguard users' privacy still have a few holes in them. For instance, a client has to have powerful computation and processing skills in order to use a system that relies on encryption. The quality of location services would also be adversely affected by continual encryption and decryption processes in continuous query. User collaboration systems are incapable of weeding out malicious or even hostile users of the collaborative platform. As a result, there is the possibility that private information might be revealed. Due to the fact that there are not enough users willing to work together, it is often even difficult to properly establish an anonymous area. In a nutshell, our mission is to address the shortcomings of the current privacy protection architectures and privacy protection technologies in order to make them more capable of striking an optimal balance between the quality of location queries and the privacy of individual users.

Researchers are showing a significant amount of interest in a unique shared ledger technology called blockchain. Users conduct transactions on the blockchain network with the use of digital currency [17,18] and an asymmetric cryptographic algorithm to conceal their actual identities (ID). In addition, blockchain technology does not rely on any third parties and utilises a consensus process to achieve decentralisation of the system. The present blockchain infrastructure may be broken down into two distinct groups: public and permissioned [19]. Private blockchains and consortium blockchains are two categories that may be used to describe permissioned blockchains. On the public blockchain, everyone may participate in the process of reaching a consensus and receive services. Therefore, the process of transactions and blocks being propagated will take a significant amount of time. In contrast to the public blockchain, the private blockchain requires everyone to get a certificate before they can participate in the consensus process. However, a single private blockchain network cannot successfully safeguard user privacy in location services [20], despite the fact that transactions on private blockchains are quick and efficient.

The k-anonymity technique is now the most widely used approach to protecting users' location privacy. It does this by disguising the user's actual location as one of k minus one other bogus places [21,22]. In contrast to previous ways, k-anonymity does not depend on the use of intricate cryptographic procedures. Because of this, the user's calculation overhead may be effectively reduced, and users may be able to take advantage of improved location service quality.

We will integrate k-anonymity with various private blockchain networks in order to overcome the challenges described above. This will be done on the basis of the structural features of the blockchain as well as the benefits offered by k-anonymity. In this piece, we provide a way for protecting the privacy of location data based on blockchain technology.

Related Work:

In this part of the article, we will discuss previous research that has been conducted on centralised design and decentralised architecture for the use of blockchain technology in LBS.

Existing Research On Two Architectures:

The architecture that is centralised. In the area of geographic obfuscation, Gruteser et al. [23] initially employed the k-anonymity technique to disguise the user's position inside the anonymizing servers. This was done in preparation for their work on spatial obfuscation. These strategies for generalising the user's location into a bigger region or adding more additional places [24] will result in a drop in the accuracy of the location query, which in turn will result in a reduction in the quality of location services. Location disturbances, which are very similar to spatial obfuscation, will similarly have the effect of lowering the quality of location services. For instance, Andrés et al. [25] were successful in developing a technique for geo-indistinguishability. The method employs a kind of controlled random noise to create confusion about the precise position of the user. Yin et al. [26] came up with a way to inject noise that would meet the differential privacy mechanism. Their technique included employing the Laplace mechanism. Even while these solutions take into account the quality of location services, they are not able to strike a perfect balance between the users' right to privacy and the quality of the location services. The pseudonymous method functions similarly to the anonymous attribute of the blockchain technology. This technique of altering the user's ID inside anonymizing servers in order to conceal their genuine identify [27] requires the assistance of a trustworthy third party.

Some academics have also suggested alternate methods in which various privacy protection systems might be combined. For instance, Zhang et al. [28] suggested a solution that combines order preserving symmetric encryption (OPSE) technology with k-anonymity. First, the users need to locate one or more dependable users in their immediate area. This method still calls for semi-TTP anonymizing servers, despite the fact that the performance constraint caused by third parties in the centralised design has been addressed. Han et al. [29] made use of multi-server architecture to sever the direct link that existed between the LSP and the user. They also made use of differential privacy mechanism to increase the level of security afforded to users' personal information. Even though this privacy protection architecture is capable

of achieving high service quality, the resources provided by social networks should not be trusted entirely. In addition, the differential privacy technique that has been presented would result in a decrease in the quality of the service.

The architecture that is decentralised. One example of a typical representation is distributed k-anonymity. For instance, Chow et al. [30] employed the point-to-point communication hop count approach to collect the position information that was supplied by cooperative users. This method will result in an increase in the amount of time it takes for the network to transmit data. In attempt to find a solution to this issue, Chow et al. [31] once again constructed anonymous zones based on the real locations of individuals who had participated in previous collaborations. Peng et al. [32] were able to discover the real locations of users who collaborated with them by submitting a fake request for collaboration and storing the results in a cache. The anonymous region may be generated for the subsequent LBS query by using the location information that is stored in the cache. Nevertheless, users of these technologies are required to give a substantial amount of storage space. Users may utilise the internet to acquire the true location of create an anonymous area, according to the strategy that was provided by Hwang et al. [33]. The purpose of the aforementioned is to build an anonymous place by locating individuals willing to collaborate. Because users who collaborate together might have bad intentions, the privacy of users cannot be completely ensured.

Dummies-based strategies have been presented by other researchers as a means to generate anonymous zones [34–36]. These algorithms establish anonymous zones based on the locations of the virtual users that they produce on the client. However, they will be limited by the real context in which they are operating. To find a solution to this issue, the research teams of Hara et al. [37] and Suzuki et al. [38] came up with a system that generates dummies everywhere around the user on the mobile terminal to conceal the user's actual position. However, assumptions about users of these algorithms are actually unworkable. One such assumption is that the user would constantly be moving.

In addition, there are a few technologies that safeguard users' privacy via the use of encryption. For instance, Yi et al. [39] made advantage of the technique of homomorphic encryption to safeguard both the query privacy and the location privacy of the user simultaneously. A high level of calculation processing capacity on the part of the client is necessary for the use of encryption technology, which often cannot properly balance the requirements of adequate privacy protection and adequate location service quality.

Application Of Blockchain:

The blockchain technology is being used extensively by the researchers in the LBS field because to the many advantages it offers. However, the purpose

of protecting users' location privacy in LBS is just a minor component. For instance, Jia et al. [40] presented a strategy to actively encourage users to actively engage in location services inside intelligence crowd sensing networks that was based on the preservation of users' privacy. This approach takes use of the immutability of the blockchain technology. The primary objective of this initiative is to encourage people to take part in location-based services. When it comes to location-based services, determining whether or not the location information provided by a user is genuine is another highly crucial problem. A proof-of-location system that is based on blockchain technology was developed by Amoretti et al. [41] as a reaction to the flaws that are present in centralised verification approaches that have been offered by researchers. This solution is implemented for the purpose of LBS in order to validate the presence of a user's designated geographical location. In the vehicular ad-hoc network (VANET), Luo et al. [42] advocated recording the credit of the car on the blockchain. This would help the vehicle avoid being tracked maliciously by other users in the network. The primary goal of these approaches is not to maintain the confidentiality of one's location while using LBS. To this aim, Yang et al. [43] presented a privacy-preservation crowdsensing system that is built on blockchain as a solution for the flaws caused by the centralised structure of the crowd perception system as well as the leaking of user location privacy. This method distributes user transaction data and protects user location privacy by combining a public blockchain network with numerous private blockchain networks. However, it solely addresses the use of blockchain technology in crowd sensing networks.

We propose a novel technique for the preservation of location privacy by drawing inspiration from Han et al. [29] and the debate that has taken place so far. The goal of our method is to investigate k-anonymity privacy protection from the point of view of blockchain.

Blockchain:

Satoshi Nakamoto is credited with the invention of the blockchain in the year 2008 [44]. Blockchain is a novel application platform that combines a number of different technologies [45,46]. These technologies include distributed storage, consensus mechanism, asymmetric cryptographic algorithm, and smart contract. The shared ledger is responsible for keeping a record of all user transactions that take place inside the blockchain network. Because of the consensus process, it is necessary for all nodes in the blockchain to come to an agreement before transactions can be recorded. It protects the integrity of the data by preventing unauthorised changes. A user's identification may be processed in a way that is completely anonymous thanks to the blockchain, which employs an asymmetric cryptographic method. Because the user's genuine identity is hidden behind the public key that serves as their account address, it is very difficult

for other people to establish the user's true identity. The smart contract is a little executable programme that is capable of running on its own upon the fulfilment of specific requirements in the blockchain. It makes it possible for P2P networks of any kind to carry out trustworthy transactions and come to mutually acceptable agreements.

The administration of blockchain nodes is the responsibility of every piece of computer hardware (including mobile phones, servers, and so on) that is a part of the blockchain. These pieces of hardware will collectively be referred to as "blockchain nodes" throughout this piece. Each node in the blockchain is linked to every other node in the network.

k-Anonymity:

k-anonymity ensures the privacy of the data at the expense of accuracy by simplifying and concealing a number of characteristics [21]. The greater the value of k, the less readily available the data will be, but the greater the degree to which the user's privacy will be protected. In the context of location privacy protection, k-anonymity conceals the user's precise position by shuffling it across k-1 fake locations while maintaining the integrity of the query content. The higher the value of k, the smaller the likelihood that the user's private information would be disclosed; however, this comes at the expense of a diminishing level of service.

Notations Definition and System Model:

Notations:

Let's say that the set of requesters is denoted by U=, where U1, U2, U3,..., Un, and that the set of incentives for an agent to upload a job is denoted by A=, where a1, a2, a3,..., ak. Let T= "T1, T2,..., Tk," which stands for the collection of tasks, often known as k query requests. The requester determines the value of t, which is the maximum amount of time that should be allowed for the agent to finish Tk. The requester is responsible for setting Tr, which indicates the amount of time that must pass before the agent may do the task. T. The query request is being made at the coordinates (Xi, Yi). The content of the question is denoted by qc. The result of the query is denoted by qr.

Modeling the System

Figure 2 illustrates the fundamental components that make up our location privacy protection technique.

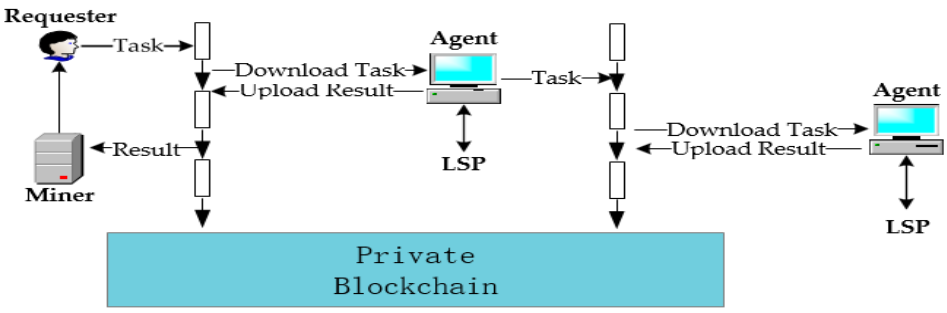


Figure 2. *Framework of the proposed location privacy protection.*

The following three parties are involved in the proposed framework:

- The user who is in need of location services is referred to as the requester. The requester will first release tasks to the private blockchain in order to launch a transaction, and then they will utilise the smart contract included inside the private blockchain to receive adequate location services. Requesters may include the person who created the private blockchain as well as other nodes that are part of the private blockchain.
- The agent acts on behalf of the requester to submit query requests to the LSP and then provides the user with the results of the queries that were submitted. They have the option of participating in activities on the private blockchain depending on their own individual concerns about privacy. The reward distribution method states that the most amount of awards are given to the first node that successfully completes the job, while the lowest amount of rewards are given to the node that successfully completes the work last.
- It is the responsibility of the miner to validate the service results that have been uploaded by the agent and to record the new transaction in the distributed ledger. If miners successfully record new transactions, they are eligible to receive transaction fees as well as incentives. A miner may also act as a requester who releases a job or an agent who conducts a task. Both of these roles are known as "mining." In the system that is being suggested, the requester is the one who hands over the work to the private blockchain. The agent retrieves the assignment from the private blockchain, begins working on it, and finishes it within the allotted amount of time in order to earn incentives.

Attacker and Attack Strategy:

We are operating on the assumption that none of the members in the blockchain network can be trusted. Any participating node in the blockchain has the potential to act as the attacker. The following provides a summary of attack tactics as well as three categories of jobs that may pose a risk to our system. They are suitable adversaries according to the Honest-But-Curious (HBC) paradigm [47].

- The creator of a private blockchain is both the requester and the requester's requester; yet, the creator may also act as an attacker. The inventor of the blockchain has the ability to store the transaction records of the nodes on his or her own network.
- Agent: The agent is able to collect the transaction records of other requesters that are stored on the participating private blockchain. The

agent then stores the transaction records that it has downloaded into the network. The membership control mechanism of the private blockchain unfortunately makes it impossible for the agent to join all of the private blockchain networks. Therefore, it is not possible for the attacker to access all of the transaction data associated with the same requester.

- The malicious agent gains the advantage by giving the creator with information on the user's location, which is a type of collusion between the agent and the developer.
- The attacker will determine the user's true location by following the transaction records of the same account. This is the method behind the attack.

Our Location Privacy Protection Method:

In this part, we provide the suggested blockchain-based decentralised technique for protecting location privacy. This method is based on blockchain technology. During the process of submitting query requests and getting query service responses, the suggested system lowers the likelihood that sensitive location information may become publicly known.

Overview:

We propose a location privacy protection system that makes use of the typical benefits offered by blockchain technology, namely anonymization, independence, and decentralisation. The blockchain network eliminates the need for anonymizing servers hosted by third parties and is able to compensate for the shortcomings of such servers. To be more specific, users have the option of creating an unlimited number of private blockchains or joining existing private blockchains to participate in the distribution of their transaction records via the use of query queries. The query request that was submitted by the user may be downloaded by the nodes that are part of the private blockchain, which then transmits the query request to the LSP. In the end, the nodes will provide the user the query response that was given to them by the LSP so that they may get their reward. These nodes terminate the connection that was previously maintained directly between the LSP and the user. An adversary will have a difficult time gathering all of the transaction information in order to deduce the real ID of the user. Even if the attackers have some prior knowledge, it is still difficult to retrieve important information from the user. The actual query request made by the user is concealed inside the query text that is delivered by the node. This allows the LBS server to offer the most accurate location services while still protecting the privacy of the user.

Figure 3 depicts the whole procedure that will be followed by the blockchain-based system that has been presented.

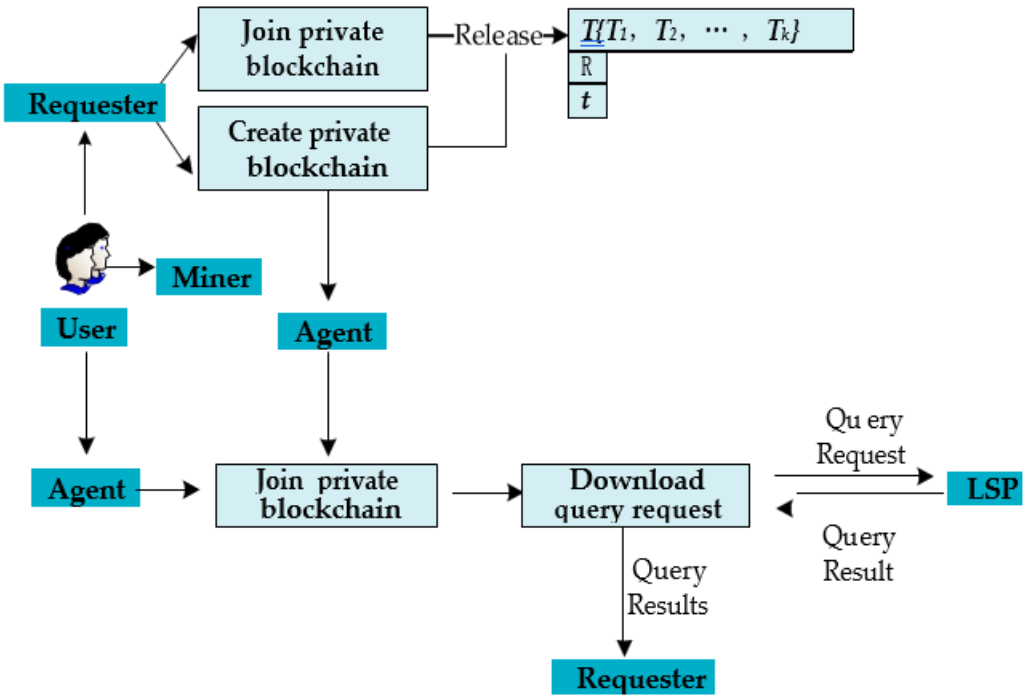


Figure 3. *The general process of the proposed framework.*

Users have the option of creating their own private blockchain network or joining one that was developed by another user. Alternatively, users may choose to participate in a private blockchain network that was built by another user. They are able to distribute tasks as requesters regardless of whether or not they are creators or other nodes on the blockchain.

- Users who wish to acquire location services as requesters may construct their own private blockchains in order to do so when they utilise the Create Private Blockchain option. The user then either becomes an agent to do the work that has been provided by other requesters on the blockchain or releases the task to the blockchain so that it may be used to start a transaction.
- When users want to obtain location services as a requester, they can also apply to join others' private blockchain release task to initiate a transaction or as an agent to undertake the task released by other requesters on the blockchain. This is done through the process of joining a private blockchain. Joining a private blockchain also allows users to obtain location services.
- Release query request: The

requester is responsible for releasing a query request to the blockchain and determining the reward for the agent depending on the amount of resources used by the query request.

- In order to carry out a query request, the agent first downloads the job from the blockchain and then, after a certain amount of time, uploads the query results to the blockchain. All data that meets the requirements will be accepted and recorded, and the agents who provided them will be rewarded. If it is determined that the data does not qualify, the agent will forfeit their deposit.

Implementation Of The Proposed System:

A smart contract is created by the requester as part of the procedure described above to guarantee that all transactions are conducted fairly. The components of the smart contract are shown in Figure 4.

The requester ID identifies the person who is responsible for the job. The node identified by the Agent ID is the one that has agreed to do the job. The amount of bitcoin that an agent is rewarded with after completing a task is represented by the reward. The requester is required to make a deposit, which will later have that amount automatically taken out of their account via the smart contract. Agents are also required to pay a deposit, which is intended to prevent a malevolent agent from completing a job but refusing to provide relevant data. This is accomplished by requiring agents to pay the deposit. The representative is responsible for submitting the service outcomes. The evaluation function is used to determine if the results provided by the location service are suitable, and the miner is responsible for determining whether or not the results are qualified.

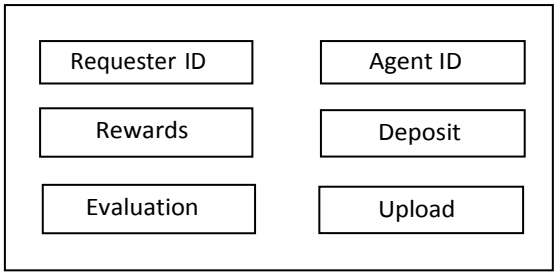


Figure 4. *The components of smart contract.*

To be more specific, users send their requests for membership in the private blockchain network to the person who first created the private blockchain to

signal that they are interested in joining the network. If the user is properly authenticated, then the request ought to be granted permission. The authentication procedure is broken down into its component parts in Algorithm 1. The appearance of bulleted lists is as follows:

Algorithm 1. Authentication process in joining private blockchain
Require: *Utype*
Ensure: *pk*, *sk*, U_{id}, permit 1: permit = false;
2: {*pk*, *sk*} ←KeyGenerator ();3: ID_u ←pk;
4: *Utype* ∈ {Requester, agent};
5: **if** ID_u *been cleared three times or Blockchain is full* **then**
6: **return** permit
7: **else if** $ID_u \in Pool_u$ **then**
8: permit = true;
9: **else if** $Pool_u \leftarrow Pool_u \cup \{ID_u\}$ **then**
permit = true;
10: **end if**
11: **return** permit

Algorithm 1 demonstrates that the value of the variable permit may be used to determine whether or not authentication was successful. The generation of a pair of secret keys takes place in step 2. In the third phase, the user's ID is derived from the public key. The value of utype tells you what kind of registered user you are dealing with, which might be a requester or an agent. Steps 5 and 6 demonstrate that the verification process is unsuccessful if the user account ID has been cleared three times on the chain or if the node has surpassed the maximum allowed capacity. In the event that none of these requirements is satisfied, the algorithm will go directly to step 7 and check to see whether the account ID is already in the user pool. In such case, the verification is successful. In the event that this is not the case, the algorithm provides the user with a pair of keys and stores those keys in the user pool (steps 8 and 9).

Release Query Request:

The requester must first deposit a certain quantity of bitcoin into the blockchain before sending any query queries. The maximum number of query requests that may be sent is k. The quantity of bitcoin that will be sent to the agent will be determined by the requester and deducted by the smart contract in accordance with that amount.

- Tasks associated with initialization include the requester providing the system with k values, R values, and the transaction Tr. The amount of bitcoin that must be removed from the deposit of the requester by the smart contract is determined by the values of k and R.
- Create a request for information by: Requester will build k query requests on the mobile terminal, which will result in the task set T being equal to [(Xi,Yi), qc]. In

order to cut down on the amount of resources that are used by users, the range of k has been chosen to be between 5 and 10. On the mobile terminal, the user must input k different tasks.

- Request to release the query: The requester is the one who submits a task to the blockchain in order to begin the transaction. The structure of the assignment is outlined as "Ti, R, t." The agent is able to make task choices determined by how much R there is. As a result, the accomplishment of the mission is also contingent on the amount of compensation that the requester is prepared to give to the agent.

Following the completion of the agent's participation in the blockchain, he will be required to provide an initial deposit of a certain quantity of bitcoin. The requester then broadcasts the job to the distributed ledger. The agent selects a job and downloads the query request based on the payment (R) offered by the requester, the amount of time (t) that has been indicated by the requester, and the agent's own need for privacy. The assignment will be forced revoked by the requester if the agent downloads the task but does not submit the outcome within the allotted amount of time; the deposit will be deducted as a penalty for the agent's failure to comply.

Performance Analysis:

On the Ubuntu operating system, we construct smart contracts by using remix, and the version of solidity that is built is 0.5.1. This serves both to explain and test the suggested technique. While the users will release query queries and acquire service responses on web pages, we will communicate with smart contracts using the tool web3.js. On the platform in the top image, we carried out simulation tests. After that, we will evaluate the effectiveness of the suggested system by considering its performance in relation to the following criteria: the effectiveness of the blockchain, the success rate, the reaction time, and the effectiveness of the mechanism for reward distribution. At the conclusion, the suggested technique is evaluated in light of the current privacy protection structures as well as the baseline method presented in Han et al. [29].

Efficiency Of The Blockchain:

We evaluate the effectiveness of the systems that make use of the blockchain as well as those that do not make use of the blockchain, and based on our findings, we describe the following characteristics:

- Because of its decentralised nature, the blockchain does not need the use of an intermediary server, which may result in significant reductions in the amount of server overhead required.
- Transactions on the blockchain, which employ bitcoin, are conducted anonymously. There is no need for the identification information of each node to be revealed or validated, and

anonymous information transmission may take place. The untrustworthy vulnerability of collaborative users in user-collaboration technology is eliminated as a result of blockchain technology's capacity to enable people to work together on a wide scale without the need of mutual confidence.

- Contracts that are "smart" have the ability to guarantee the integrity and fairness of any transactions that take place on the blockchain. The interactions between users in the proposed system are improved as a direct result of this factor.
- Every transaction on the blockchain network is required to be validated by a consensus process, and a timestamp will be recorded for each transaction in each block [50]. Through the use of the access block, users are able to quickly check and see past transactions.

The construction of a new block in the blockchain network is subject to a rigorous verification procedure [44], which will cause a delay in the confirmation time. As a direct consequence of this, the efficiency of applications that use blockchain to get services is diminished. The requester is responsible for discreetly determining the amount of the reward, while the agent is responsible for privately obtaining location services. As a result, there is no labor-intensive calculating work performed on the blockchain. The efficiency of the system that has been presented is adequate.

Success Rate and Response Time:

The amount of time that a requester spends using the proposed system in order to get location services is the response time. The process of obtaining location services begins with the initialization of tasks, followed by the construction of k query requests by the requester, the downloading of tasks by agents, the obtaining of location services privately by agents, followed by the uploading of service results, and finally, the obtaining of service results by requesters. The amount of time that is necessary for the user to generate k query requests on the mobile terminal is contingent upon the circumstances that are unique to the requester. Because the requester determines the amount of time needed for a single task, the requester also decides how much time the agent has to obtain the location service in private and upload the service results. The maximum amount of time the agent has to complete these two tasks is also up to the requester. In conclusion, during the course of the experiment, the only thing that needs to be recorded is the amount of time it took to complete the initialization task, the amount of time it took to complete the agent download task, and the amount of time it took for the requester to obtain the service results. We determined the task success rate and the average reaction time needed of the user in order to operate the suggested system by simulating a number

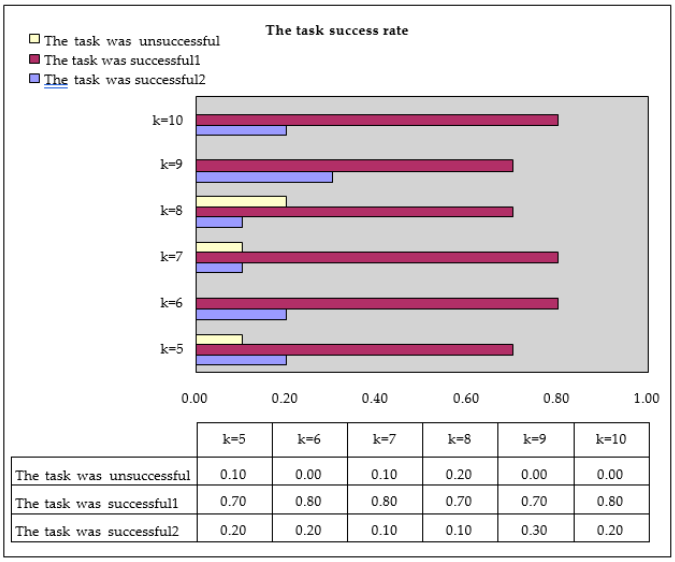
of different tests and analysing the results.

The amount of time required to respond is measured in seconds. We shall maintain t = 25 seconds and Tr = 120 seconds regardless of the value of k. We keep the value of k constant and simultaneously post 10 different job sets on the website in a random order. In the last step, we do the necessary calculations on the acquired service outcomes.

When k equals 5, the circumstances surrounding the acquisition of service results are detailed in Table 1. "None" indicates that the service could not be obtained. The results of task set 6 are shown in the table, and they show that it was unsuccessful. The remaining nine task sets were able to effectively receive all service results in one minute and twenty seconds. The percentage of successful completion of each individual job is shown in Figure 5, which provides an overview of the current situation. As can be seen in Figure 5, when k equals 5, out of the total of 10 task sets that have been issued, there are nine successful task sets, of which two correspond to the second category of task success. The table clearly demonstrates that the percentage of successful completion of the assigned work is quite near to one hundred.

Table 1. The total time required to obtain service results when *k* = 5.

	Task Sets									
***k* = 5**		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	Tr	110s	95s	102s	89s	101s	None	100s	111s	114s	101s



	k=5	k=6	k=7	k=8	k=9	k=10
The task was unsuccessful	0.10	0.00	0.10	0.20	0.00	0.00
The task was successful1	0.70	0.80	0.80	0.70	0.70	0.80
The task was successful2	0.20	0.20	0.10	0.10	0.30	0.20

Figure 5. *The task success rate.*

Figure 6 depicts the average amount of time needed to provide a response in the two instances when the job was completed successfully. Milliseconds

are used for all of the response time measurements in the figure. It is clear from the chart that the typical amount of time required to respond is not more than 5 seconds at any point in time. It is clear that the user will not suffer a significant loss even if an agent fails to upload the service results in accordance with the requirements, as shown by the needed response time.

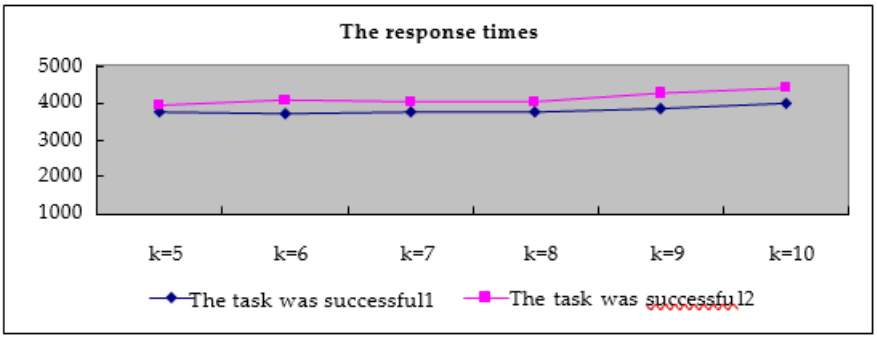


Figure 6. *The response times.*

Efficiency Of The Reward Distribution Mechanism:

We will refer to the reward system as an average distribution mechanism and a differential distribution mechanism in the event that k and the task set do not change. The amount of emphasis placed on response time reflects how well the reward unequal distribution mechanism is being carried out. When k is less than seven, it is clear from looking at Figure 7 that the reaction time needed by the differential distribution mechanism is noticeably less than the response time needed by the average distribution method. When k is greater than seven, the response time of the differential mechanism is greater than the response time of the average mechanism. This is due to the fact that the calculation amount required by the differential distribution mechanism is greater than that required by the average distribution mechanism. However, if we look at the figure, we can see that when k is more than seven, the time difference does not go beyond one second at the very most. The statistics shown in the accompanying figure demonstrate that the differential distribution mechanism is capable of motivating agents to download data preferentially and to finish tasks in a more expedient manner in comparison to the average distribution incentives.

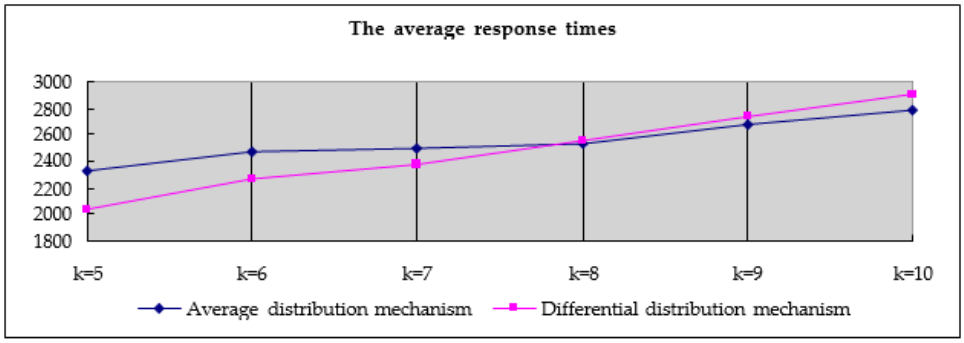


Figure 7. *Efficiency comparison of two reward distribution mechanisms.*

Conclusions:

In this research work, we presented a unique architecture for the preservation of location privacy. We employ numerous private blockchains to secure location privacy without the assistance of a third party, and we use the nodes on the private blockchain to cut off direct interaction between the user and the LSP. This allows us to do away with the need for a third party. It is no longer possible for untrusted LBS servers or any other kind of attacker to directly obtain the location information of the user. We use the k-anonymity principle to maximise the level of privacy protection afforded to users' locations while simultaneously ensuring that users have access to the most precise location services possible. The differential distribution technique that was presented in this research increases not only the effectiveness of the functioning of the system but also the experience that the user has. Transactions are guaranteed to be fair and enforceable because to the use of smart contracts. We validated that the approach does not need the employment of any sophisticated algorithms and is able to deliver the most accurate location services while also strengthening location privacy protection using a combination of theoretical analysis and a series of simulated exercises.

On the other hand, our approach is more suited for snapshot query. In subsequent work, we are going to modify our system such that it is more effective when it is used in conjunction with a continuous query. In addition to that, we will also apply our methodology to several real-world scenarios.

References:

[1].Zhang, S.; Li, X.; Tan, Z.; Peng, T.; Wang, G. A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services. Futur. Gener. Comput. Syst. 2019, 94, 40–50. [CrossRef]

[2].Bettini, C.; Freni, D.; Jensen, C.S. Location-Related Privacy in Geo-Social Networks. *IEEE Internet Comput.* **2011**, *15*, 20–27.

[3].Gao, H.; Liu, H. Data Analysis on Location-Based Social Networks. In

Mobile Social Networking; Springer: New York, NY, USA, 2014; pp. 165–194.

[4]. Roza, T.D.; Bilchev, G. An overview of location-based services. *BT Technol. J.* **2003**, *21*, 20–27. [CrossRef]

[5]. Jiang, B.; Yao, X. Location-based services and GIS in perspective. *Comput. Environ. Urban Syst.* **2006**, *30*,712–725. [CrossRef]

[6]. Schiller, J.H.; Voisard, A. Location-Based Services; Morgan Kaufmann Publishers Inc.: San Francisco, CA, USA, 2004.

[7]. Tefera, M.K.; Yang, X.; Sun, Q.T. A Survey of System Architectures, Privacy Preservation, and Main Research Challenges on Location-Based Services. KSII Trans. Internet Inf. Syst. 2019, 13, 3199–3218. [CrossRef]

[8]. Sun, Y.; Chen, M.; Hu, L.; Qian, Y.; Hassan, M.M. ASA: Against statistical attacks for privacy-aware users in Location Based Service. Futur. Gener. Comput. Syst. 2017, 70, 48–58. [CrossRef]

[9]. Sung, K.; Levine, B.; Zheleva, M. ZipPhone: Protecting user location privacy from cellular service providers.

[10]. *arXiv* **2020**, arXiv:2002.04731.

[11]. Fung, E.; Kellaris, G.; Papadias, D. Combining Differential Privacy and PIR for Efficient Strong Location Privacy. In *Proceedings of the Claramunt C. et al. (eds) Advances in Spatial and Temporal Databases*; Springer: Cham, Switzerland; Hong Kong, China, 2015; Volume 9239, pp. 295–312.

[12]. Yang, B.; Sato, I.; Nakagawa, H. Bayesian Differential Privacy on Correlated Data. In Proceedings of the Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data—SIGMOD ’15; ACM Press: New York, NY, USA, 2015; Volume 2015, pp. 747–762.

[13]. Ji, Y.; Gui, R.; Gui, X.; Liao, D.; Lin, X. Location Privacy Protection in Online Query based-on Privacy Region Replacement. 2020 10th Annu. Comput. Commun. Work. Conf. 2020, 0742–0747. [CrossRef]

[14]. Zhang, S.; Wang, G.; Liu, Q.; Wen, X.; Liao, J. A Trajectory Privacy-Preserving Scheme Based on Dual-K Mechanism for Continuous Location-Based Services. *Inf. Sci. (Ny).* **2020**, *527*, 406–419. [CrossRef]

[15]. Gedik, B.; Liu, L. Protecting location privacy with personalized k-anonymity: Architecture and algorithms.

[16]. *IEEE Trans. Mob. Comput.* **2008**, *7*, 1–18. [CrossRef]

[17]. Serjantov, A.; Danezis, G. Towards an information theoretic metric for anonymity. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 2003, 2482, 41–53. [CrossRef]

[18]. Machanavajjhala, A.; Kifer, D.; Gehrke, J.; Venkitasubramaniam, M. L-Diversity: Privacy Beyond k-Anonymity.

[19]. ACM Trans. Knowl. Discov. Data 2007, 1, 3. [CrossRef]

[20]. Currency—Dash, D.O.W.C. Available online: www.dash.org (accessed on 3 April 2020).

[21]. Litecoin, Litecoin-Open Source P2P Digital Currency. 2013. Available online: https://litecoin.org/ (accessed on 3 April 2020).

[22]. Wang, H.; Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352. [CrossRef]

[23]. Shahid, A.R.; Pissinou, N.; Njilla, L.; Alemany, S.; Imteaj, A.; Makki, K.; Aguilar, E. Quantifying location privacy in permissioned blockchain-based internet of things (IoT). In *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*; ACM Press: New York, NY, USA, 2019; pp. 116–125.

[24]. Bayardo, R.J.; Agrawal, R. Data Privacy through Optimal k-Anonymization. In Proceedings of the 21st International Conference on Data Engineering (ICDE'05), Tokoyo, Japan, 5–8 April 2005; pp. 217–228.

[25]. Gkoulalas-Divanis, A.; Kalnis, P.; Verykios, V.S. Providing K-Anonymity in location based services.

[26]. *ACM SIGKDD Explor. Newsl.* **2010**, *12*, 3–10. [CrossRef]

[27]. Gruteser, M.; Grunwald, D. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In Proceedings of the 1st International Conference on Mobile Systems, Applications and Services—MobiSys '03, San Francisco, CA, USA, 5–8 May 2003; ACM Press: New York, NY, USA, 2003; pp. 31–42.

[28]. Li, F.; Chen, Y.; Niu, B.; He, Y.; Geng, K.; Cao, J. Achieving Personalized k-Anonymity against Long-Term Observation in Location-Based Services. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 9–13 December 2018; pp. 1–6.

[29]. Andrés, M.E.; Bordenabe, N.E.; Chatzikokolakis, K.; Palamidessi, C. Geo-indistinguishability: Differential privacy for location-based systems. In Proceedings of the Proceedings of the ACM Conference on Computer and Communications Security, Berlin, Germany, 4–8 November 2013; ACM Press: New York, NY, USA, 2013; pp. 901–914.

[30]. Yin, C.; Xi, J.; Sun, R.; Wang, J. Location privacy protection based on differential privacy strategy for big data in industrial internet of things. IEEE Trans. Ind. Informatics 2018, 14, 3628–3636. [CrossRef]

[31]. Boualouache, A.; Senouci, S.-M.; Moussaoui, S. PRIVANET: An Efficient Pseudonym Changing and Management Framework for Vehicular Ad-Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2019**, *PP*, 1–10. [CrossRef]

[32]. Zhang, S.; Choo, K.-K.R.; Liu, Q.; Wang, G. Enhancing privacy through uniform grid and caching in location-based services. *Futur. Gener. Comput. Syst.* **2018**, *86*, 881–892. [CrossRef]

[33]. Han, M.; Li, L.; Xie, Y.; Wang, J.; Duan, Z.; Li, J.; Yan, M. Cognitive Approach for Location Privacy Protection.

[34]. *IEEE Access* **2018**, *6*, 13466–13477. [CrossRef]

[35]. Chow, C.Y.; Mokbel, M.F.; Liu, X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service. *GIS Proc. ACM Int. Symp. Adv. Geogr. Inf. Syst.* **2006**, 171–178. [CrossRef]

[36]. Chow, C.Y.; Mokbel, M.F.; Liu, X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *Geoinformatica* **2011**, *15*, 351–380. [CrossRef]

[37]. Peng, T.; Liu, Q.; Meng, D.; Wang, G. Collaborative trajectory privacy preserving scheme in location-based services. *Inf. Sci. (Ny).* **2017**, *387*, 165–179. [CrossRef]

[38]. Hwang, R.H.; Hsueh, Y.L.; Wu, J.J.; Huang, F.H. SocialHide: A generic distributed framework for location privacy protection. *J. Netw. Comput. Appl.* **2016**, *76*, 87–100. [CrossRef]

[39]. Kido, H.; Yanagisawa, Y.; Satoh, T. An anonymous communication technique using dummies for location-based services. *Proc. Int. Conf. Pervasive Serv. ICPS'05* **2005**, *2005*, 88–97. [CrossRef]

[40]. Lu, H.; Jensen, C.S.; Yiu, M.L. PAD: Privacy-Area Aware, Dummy-Based Location Privacy in Mobile Services. In Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access—MobiDE '08, Vancouver, BC, Canada, 13 June 2008; ACM Press: New York, NY, USA, 2008; p. 16.

[41]. Yanagisawa, Y.; Kido, H.; Satoh, T. Location Privacy of Users in Location-based Services tGraduate. In Proceedings of the 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, San Jose, CA, USA, 17–21 July 2006; pp. 1–4.

[42]. Hara, T.; Suzuki, A.; Iwata, M.; Arase, Y.; Xie, X. Dummy-Based User Location Anonymization under Real-World Constraints. *IEEE Access* **2016**, *4*, 673–687. [CrossRef]

[43]. Suzuki, A.; Iwata, M.; Arase, Y.; Hara, T.; Xie, X.; Nishio, S. A user location anonymization method for location based services in a real environment. In Proceedings of the Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems—GIS '10, San Jose, CA, USA, 2–5 November 2010; ACM Press: New York, NY, USA, 2010; p. 398.

[44]. Yi, X.; Paulet, R.; Bertino, E.; Varadharajan, V. Practical Approximate k Nearest Neighbor Queries with Location and Query Privacy. *IEEE Trans. Knowl. Data Eng.* **2016**, *28*, 1546–1559. [CrossRef]

[45]. Jia, B.; Zhou, T.; Li, W.; Liu, Z.; Zhang, J. A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Sensors 2018, 18, 3894. [CrossRef]

[46]. Amoretti, M.; Brambilla, G.; Medioli, F.; Zanichelli, F. Blockchain-Based Proof of Location. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16-20 July 2018; pp. 146–153.