IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 18, 2020, accepted October 7, 2020, date of publication October 12, 2020, date of current version November 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3030241

DePET: A Decentralized Privacy-Preserving Energy Trading Scheme for Vehicular Energy Network via Blockchain and K - Anonymity

YANGYANG LONG[1,2], YULING CHEN[1,2], WEI REN[2,3], (Member, IEEE), HUI DOU[1,2], AND NEAL NAIXUE XIONG[4], (Senior Member, IEEE)

[1]College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
[2]State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
[3]School of Computer Science, China University of Geosciences, Wuhan 430074, China
[4]Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK 74464, USA

Corresponding author: Yuling Chen (ylchen3@gzu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61962009, in part by the Major Scientific and Technological Special Project of Guizhou Province under Grant 20183001, and in part by the Open Funding of Guizhou Provincial Key Laboratory of Public Big Data under Grant 2018BDKFJJ005 and Grant 2018BDKFJJ013.

ABSTRACT With the gradually opening of energy markets and popularization of Electric Vehicles (EVs), EVs can transmit, dispatch and recharge energy in different markets and domains dynamically. However, in Vehicular Energy Network, EVs may randomly enter and leave a market, it imposes a difficult problem in that how to schedule and distribute energy effectively. Additionally, the location of EV owners usually includes sensitive information such as home addresses, company names, hospital traces, and so on, which may be collected by attackers and may result in the privacy leakage about EV owners. In this article, we propose a decentralized blockchain-enabled energy trading scheme that can trade cross over various domains efficiently, which enables reliable transactions between EVs and energy nodes within short processing delay. It can also preserve the privacy of EV owners, by adopting the k-anonymity method in constructing a united request to hide the location information and creating a clocking area based on undirected graphs. Even though the server is maliciously attacked, the attacker cannot distinguish among EV owners, which breaks the linkage between real locations and identities to preserve EV owners' privacy. Finally, we conduct a comprehensive experimental evaluation to evaluate the trading performance and location privacy protection performance. The simulation results show that our proposed architecture outperforms over most state-of-the-art schemes in terms of processing delay and location privacy awareness.

INDEX TERMS Vehicular energy networks, energy trading, K-anonymity, location privacy, blockchain.

I. INTRODUCTION

Vehicular Energy Network (VEN) [1] is built upon the existing transportation networks, which deploys wireless charging and discharging energy storage equipment, and EVs can trade with energy nodes dynamically. It is regarded as a promising technology to improve energy efficiency and sustainable development [2], which has great potential to integrate renewable energy sources and electric vehicles (EVs).

The associate editor coordinating the review of this manuscript and approving it for publication was Bin Zhou.

However, a majority of current energy trading infrastructures [3], [4] are centralized, there is a possibility for the occurrence of single point of failure since allowed a third party to serve as a controller to manage or control all transaction information. The reason is that EV owners must rely on a central entity, which handles energy distribution and entity registration. Although it is convenient for trading energy in some cases, these centralized entities may not be completely credible. Once a central entity is attacked or data is unintentionally leaked, potential security issues will inevitably occur.

Recently, blockchain technology has emerged as a promising approach to remove the reliance on the central platform,

which records transactions in the decentralized network in a verifiable and immutable manner [5]. However, there are some challenges in leveraging blockchain technology to provide a transparent, immutable and auditable managing of transactions for P2P energy trading. On the one hand, owing to the high mobility, limited storage space and computational resources of EVs, EVs can arrive in and depart the market in a randomly feature, the network topology changes rapidly. On the other hand, when a transaction is initiated, the location information (e.g. home location, work location) of EVs can be collected by some untrusted nodes, or hijacked by some adversaries. With the obtained location information, the adversary could further infer the personally sensitive information (e.g. age, hobbies, heath conditions) of EVs by some certain algorithms (e.g. Data Aggregation [6], [7], semantic association [8]), which may pose serious threats to EV owners' privacy, even the EV owners' life security.

In recent years, location privacy has been a growing research area, with a number of research efforts devoted to the topic from a variety of perspectives. Representative privacy protection schemes include k-anonymity [9], [10], pseudonyms exchanges [11]–[13], obfuscation [14] and differential privacy [15]–[17], etc. Particularly, k-anonymity is one of the most popular strategies to protect location privacy [18], and has been widely used in numerous systems, including social network and electronic health records, among others. However, it cannot be directly applied in VEN, as the social features of EV users in VEN are not fully considered. Therefore, it is still an open and vital issue to design a secure location privacy-preserving energy trading scheme to improve the security and efficiency in energy trading in VEN.

To address the abovementioned problems, in this article, we propose a decentralized blockchain-enabled secure energy trading scheme named DePET for energy trading in VEN. First, we adopt consortium blockchain to build a network, which enables EV owners to trade with energy nodes directly, and allows EV owners and energy nodes to manage their resources and information in a decentralized, secure, trustful, transparent, anonymous and verifiable manner. Furthermore, a k-anonymity-based location privacy-preserving algorithm is designed to protect EV owners' location privacy. This algorithm adopts an undirected graph to construct anonymity sets for these participants who have different privacy requirements. Experimental evaluations show the effectiveness of the proposed DePET scheme by comparison with other schemes.

The contributions of our work in this article are shown as follow:

- We propose a decentralized energy trading scheme via a consortium blockchain, and EV owners can trade with energy nodes cross-domain and directly in a peer to peer manner, which removes the assumption of third trusted party.
- We adopt the k-anonymity to construct a united request deriving from an anonymity set based on an undirected graph to protect the EV owner's location privacy. In case the server is maliciously attacked, attackers still cannot distinguish among EV owners.

We will introduce the related work in Section II. The problem is stated formally in Section III. Section IV gives the details of our proposed scheme. Section V provides some experimental results and evaluation analysis. Finally, Section VI concludes the papers.

II. RELATED WORK

Some research studies [19]–[25] utilize blockchain technology to decentralize the complex energy market's networks and peer-to-peer (P2P) energy trading.

The authors in Reference [19] proposed a localized P2P electricity trading model for locally buying and selling electricity among plug-in hybrid electric vehicles (PHEVs), which achieves demand response by providing incentives to discharging PHEVs to balance local electricity demand out of their own self-interests. Motivated by the pricing mechanism, the authors in Reference [20] proposed a blockchain-based secure incentive scheme to stimulate EVs to cooperatively deliver renewable energy to various areas with different electricity loads while maximizing EVs' utilities. Similarly, the authors in Reference [21] combined additive homomorphic encryption and consortium blockchain to provide privacy and trust, proposed a dynamic energy pricing model including demurrage fees, which is a monetary penalty imposed on a prosumer, if it failed to deliver energy within the agreed duration.

The authors in Reference [22] proposed a blockchain-based Local Energy Market (LEM) model, which introduces a Home Energy Management (HEM) system and demurrage mechanism. The model allows both the prosumers and consumers to optimize their energy consumption, minimize electricity costs and shift their load to off-peak hours. The authors in Reference [23] proposed a consortium blockchain-based scheme (BETS) to tackle the privacy leakage problem in a smart grid, which provides a noise-based privacy-preserving method to hide the trading distribution tendency. The authors in Reference [24] proposed a P2P energy trading system on public blockchain where all bids are encrypted and peer matching is performed on the encrypted bids by a functional encryption-based smart contract.

Generally, according to the literature discussed above, most of the research do not emphasize how to resolve the privacy and security issues during P2P energy trading. Thus, there is urgently need to design a location privacy-preserving energy trading scheme.

III. PROBLEM FORMULATION

In this section, we introduce the main four components in the system model. Then, we explain the threat model of proposed scheme, and give some reasonable assumptions and design goals.

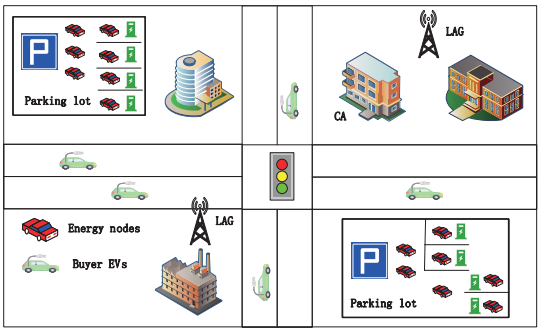

FIGURE 1. Overall architecture of our DePET scheme.

A. SYSTEM MODEL

The proposed scheme DePET mainly includes four different components: EVs, local aggregators (LAGs), parking lots and certificate authority (CA), which is shown in Fig. 1.

- **EVs.** The EVs play different roles in proposed scheme: charging EVs and discharging EVs. Each EV chooses its own role according to current energy state and driving plan. And each EV is equipped with a smart meter for recording energy trading volume in real time. The payments of energy trading are based on these records in smart meter.
- **LAGs.** LAGs work as energy brokers to provide access points of electricity and wireless communication services for EVs. Each EV owner sends a request about electricity demand to the nearest LAG. The LAG does a statistics of local electricity demand and announces this demand to energy nodes.
- **Parking lots.** The parking lots work as the place for energy trading between EV owners and energy nodes.
- **CA.** CA works as the credible authority, which enables security and certificate-related services, is mainly responsible for supervision of transaction data and register of participants, such as LAGs, energy nodes and EVs owners.

B. THREAT MODEL

In the energy trading process, LAGs match energy nodes and provide location-based services for EV owners. We assume that the communication associated with the location is not secure enough, then attackers can get the accurate location of target EV owner through these services. Because EV owners' location information contains sensitive information, such as home, company, hospitals, etc. once obtained by the attacker, the EV owners' privacy will be leaked, even the personal safety will be threatened. For example, the attacker can analyze the hobby or health status of target EV owner, and send a request to the target LAG for profit.

We divide the attackers that want to get the location information of EV owners into two categories: external attackers and internal attackers. The external attacker can get EV owners' location information from the transaction data recorded on blockchain, and the internal attacker is an internal malicious node in our proposed scheme, which can collect user data information. We assume that the LAG can be an internal attacker, and collect EV owners' accurate location information during the trading process.

C. ASSUMPTIONS

To make the scheme more easily understood, reasonable assumptions is needed. The assumptions are as follows: First, the energy node is located in the designated parking lots, and cannot moving while bidding with a certain EV owner. The EV owners without such a restriction, can be located in different places, and the location also couldn't be changed while starting the transaction with the bidding energy node; Second, all the EV owners are rational, and will not misreport the arriving time and current location. Once the EV finished trading operation, the EV owner drive away from the parking lot immediately; Finally, the proposed scheme contains multiple parking lots, and all available for EV owners.

D. DESIGN GOALS

In this article, there are three main objectives to be achieved: one is adoptable efficiency and another is k-anonymity-based location privacy preservation.

1) AUTHENTICATION

The real identity of an EV owner, which uploads data to the blockchain, should be authenticated to rule out illegal entities.

2) ADOPTABLE EFFICIENCY

This goal implies that our scheme should avoid a long latency time to make it adoptable in practice. The vital part of this aspect is that the time of reach a consensus should be limited in an acceptable period. This is because that the storage capacity of EVs in VEN is vulnerable, and it is not enough to have the backup of data of blockchain network or participate in the consensus, which will make it unadoptable in practice. Therefore, we adopt consortium blockchain to reduce the time cost in consensus process.

3) K-ANONYMITY

Constructing an anonymous set to achieve k-anonymity, which ensures that the attacker cannot distinguish an individual with a probability higher than 1/k, is the primary goal of our scheme. To achieve k-anonymity, there must be at least k EVs, which cannot be identified in an anonymously configured set, we define as clocking area.

Existing anonymity-based schemes can be divided into two groups: identifier anonymity [24] and location anonymity. The identifier anonymity-based strategy hides the EV owners' real identifier with a set of pseudonyms. In this way, the adversary cannot distinguish the relationship between specific pseudonym and k EVs. Nonetheless, there must be a trusted third party to hide the EV owner's real identifier and sometime the trust third party is hard to realize in real-world practice. And the adversary could also utilize the open information recorded in blockchain and obtain privacy from linking the identifiers of users with information.

Unlike identifier anonymity, the location anonymity-based strategy hides the exact location of the target EV owner in a geographic area, which includes at least k-1 other EV owners. Even if the malicious attacker obtains the location through historical transaction records in blockchain, the attacker can only obtain the approximate location of the target EV, instead of the exact location. In this article, and utilize a graph-based strategy to achieve k-anonymity and protect the location privacy of EV owners.

IV. THE PROPOSED SCHEME - DePET

A. BLOCKCHAIN-BASED NETWORKING DESIGN

In VEN, the storage capacity of EVs is vulnerable, which is not enough to store all transactions. If we adopt the public blockchain, all nodes should participate in the consensus and have the backup of data of blockchain network, which will slow down the transaction speed, and cannot meet the needs of high-frequency energy trading. Therefore, to make the energy trading information more transparent and more reliable, we adopt consortium blockchain to build a blockchain network.

In our proposed scheme, the LAGs, EVs, and energy nodes act as nodes, and not all of them necessarily store the whole blockchain and participate in the consensus protocol. The LAGs are full nodes with read and write permissions on blockchain network, which means that they should participate in the consensus protocol and have the backup of data of blockchain network. And the EVs are light nodes only save their identity information and with read permission, which means that they need to send a read request to LAG through some protocols to confirm whether the submitted transactions are successfully written to blockchain, such as Simple Payment Verification [25]. This can guarantee transaction data will not to be tampered and manipulated by malicious EV attackers due to the EVs only hold reading permission. Also, these interactions with the smart contracts between EVs and LAGs are made through transactions, which are signed with the private key part of the respective addresses. To send transactions, EVs should connect to a LAG that broadcasts their demands on the blockchain network. To be specifically, while starting a transaction with the bidding energy node, the EVs need to access the nearest LAG, upload its account to the LAG, download the latest transaction data from the LAG, and synchronize the block header of transaction data. This is because that all the LAGs have the complete backup of data of blockchain network, the transaction's hash value is stored in block header, no matter how large the transaction data, all the EVs only need to synchronize data of block header. This can guarantee that the size of data is always 80 bytes, which greatly reduces the storage pressure of EVs and proves the system response time.

B. CONSENSUS PROCESS

Consensus process is an essential part during P2P energy trading in VEN. In our proposed DePET scheme, we adopt a three-phase consensus mechanism to efficiently reduce the confirmation delay of transactions and energy consumption for reaching consensus.

The first stage is the leader selection. All LAGs collect transaction records within certain periods, and then encrypt these transaction records with its signature. Similar to Bitcoin, the LAGs try to find a hash value that satisfies a certain difficulty for data audit. A LAG calculates the hash value of its block based on the random number x, the hash value of the previous block, timestamp, transactions' merkle root, etc. denoted as *data*. As shown in formula (1):

$$Hash(x + data) < Difficulty \tag{1}$$

Here, *Difficulty* is an integer controlled by the system, mainly used to adjust the search speed of random numbers, and the fastest LAG finds the random number is the leader node of current consensus process, denoted as *dm*.

In the second stage, for the ease of mutual verification and supervision, dm broadcasts the block data, random number x, timestamp to other LAGs, and these LAGs will audit the block data and broadcast the verification results with signature to other LAGs. Each verification result comprises of (audit result, verification result, signature, reply). The LAGs audit whether their own data has been tampered and verify whether illegal data are included in this block and reply to other LAGs with their signatures. Once all LAGs receive the unmistakable audit messages from others, they will send commit messages to *dm*.

In the third stage, *dm* performs mathematical statistical analysis on the received feedback, if all LAGs agree with the block data, *dm* will broadcast the verification results with signature to other LAGs for storage. Then the consensus process completed, the block data is written into the blockchain by *dm* in an orderly manner, and *dm* receives the rewarded Tokens. If some LAGs do not agree the block data, *dm* will analyze the verification result and send the block data to these LAGs again for audit. In such a consensus protocol, each verification result holds a signature, which is easy to count and located.

C. IN-STU ENERGY TRADING PROTOCOL DESIGN

In our proposed scheme, each LAG consists of a Transaction Server (TS) and a Memory Pool (MP). TS is responsible for collecting energy trading requests and matching energy nodes for EV owners. MP stores the backup of data of blockchain network. Token is similar to NRG coin [26], and has no effect on transaction efficiency and security. Also, each LAG can communicate with any EV owners in its range. The interaction of system is presented in Fig. 2. Here, we explain three mainly interactions between the different components in VEBN.

1) REGISTER OF EVs

If an EV owner wants to join the vehicular energy blockchain network, the EV first submits its identity information (name, age, ID number, etc.) for initiating a registration request to

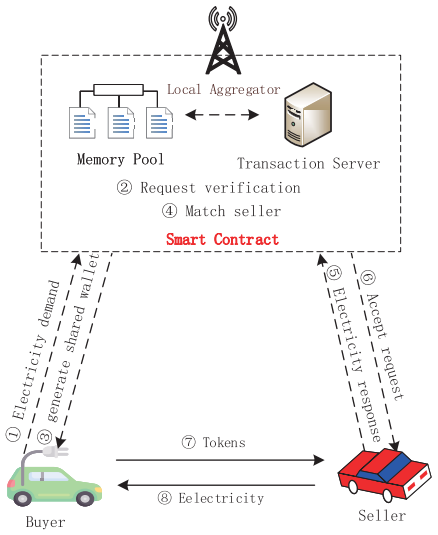

FIGURE 2. The interaction of energy trading protocol.

the CA server. Then the CA server utilizes an asymmetric encryption algorithm to generate a set of public key PK_i and private key SK_i for the EV owner, and uses its private key SK_{CA} to encrypt the EV owner's public key PK_i to form a digital signature SIGN(PK_i,SK_{CA}), and finally return (PK_i, SK_i, $SIGN(PK_i, SK_{CA})$) to the EV owner. After that, the EV owner is to be a legal node. The others can use the CA's public key PK_{CA} to verify the legality of the EV owner.

2) BUYING AND SELLING ENERGY

The EV owner initiates an energy trading request in the form of smart contract to the nearest LAG. When the LAG received the request, TS will verify its validity, if success, then packages the request and broadcasts it to all other LAGs for matching an energy node. If matched successfully, the EV owner receives the contract submitted by the energy node from the LAG, and generates a new contract to negotiate the price with the seller. If the agreement is reached, the EV owner will pay tokens to the energy node through its own wallet, and generates transaction records and sends it to the energy node. The energy node confirms and uses its private key to form a digital signature for the transaction record, and finally uploads the transaction record to LAG for carrying out consensus process.

3) CARRY OUT CONSENSUS PROCESS

Owning to all the LAGs are registered in CA server, we the three-phase consensus mechanism abovementioned to proceed. When the consensus process is completed, transactions are successfully written into blockchain network and stored in a transparent and immutable manner.

D. LOCATION PRIVACY-PRESERVING ALGORITHM DESIGN

The proposal of the decentralized energy trading model requires the protection of EV owners' location privacy while energy trading operations need to be efficient, transparent and reliable. In this work, we adopt the k-anonymity technology to construct a united request to protect the EV owner's location privacy.

When an EV owner wants to trading with other energy nodes, the EV owner collects and integrates the location l, request content c, identity id and other information of other k-1 EVs, and sends a united request to LAG. The format of an united request is shown in Table 1. LAG only holds a set of location coordinates, which can obscure the connection between the EV owner and its location. Although the attacker can get the location coordinate (x,y) of an EV in the clocking area, but it is hard to distinguish which EV the coordinate belongs to.

TABLE 1. The format of an united request.

An united request	
id	$id_1, id_2, ..., id_k$
l	$l_1, l_2, ..., l_k$
c	$c_1, c_2, ..., c_k$

A first-come, first-served method is usually adopted to connect with other k-1 EVs while constructing such a clocking area, but it is hard to judge whether this connection is reasonable. Therefore, we transform the optimal resource allocation problem into a linear programming problem. For ease of description, we put the underlying physical network as an undirected graph. Based on the physical network, the undirected graph can be constructed. As for the connection between EVs, we can utilize two indicators in an undirected graph to measure the effectiveness of clocking area: connectivity Δ and weight w.

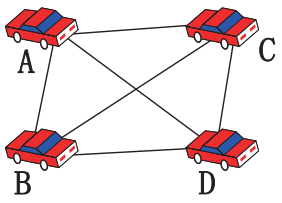

FIGURE 3. The united EVs construct a complete graph.

1) AVERAGE CONNECTIVITY $\bar{\Delta}$

If each request contains the same information, the request is invalid. As shown in Fig. 3, we suppose that k is 4 and the connected EVs are $\{A, B, C, D\}$. Because all nodes $\{A, B, C, D\}$ are interconnected, the request sent by each EV is the same, as shown in Table 2.

Suppose that an EV as a node of graph. If two EVs are connected together, there is an edge between the corresponding nodes, and the distance between nodes is the weight of the edge. As shown in Fig. 3, the undirected graph cannot be a complete graph, otherwise the requests sent by all EVs in the clocking area are the same. Therefore, the number of

TABLE 2. The same request of each EV.

Each united request	
id	id_A, id_B, id_C, id_D
l	l_A, l_B, l_C, l_D
c	c_A, c_B, c_C, c_D

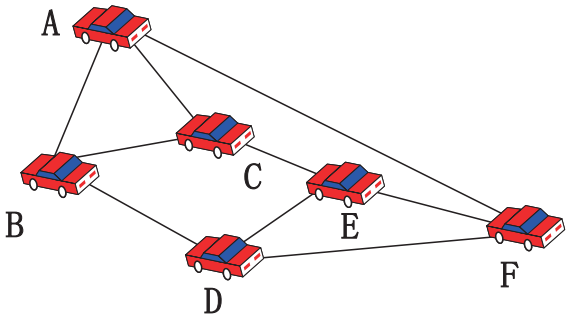

FIGURE 4. The united EVs construct a uncomplete graph.

connected EVs must be greater than k to ensure that the constructed undirected graph is not a complete graph, as shown in Fig. 4. We assume that $k = 4$, EV is $\{A, B, C, D, E, F\}$, and the number of EVs is $n = 6$ (and $n > k$). In the clocking area constructed in Fig.4, the requests submitted by EVs are different. Table 3 shows the requests submitted by EVs $\{A, B, C, D, E, F\}$ in the clocking area.

TABLE 3. The different united request of each EV.

	EV_A	EV_B	EV_C
id	id_A, id_B, id_C, id_F	id_A, id_B, id_C, id_D	id_A, id_B, id_C, id_E
l	l_A, l_B, l_C, l_F	l_A, l_B, l_C, l_D	l_A, l_B, l_C, l_E
c	c_A, c_B, c_C, c_F	c_A, c_B, c_C, c_D	c_A, c_B, c_C, c_E
	EV_D	EV_E	EV_F
id	id_B, id_D, id_E, id_F	id_C, id_D, id_E, id_F	id_A, id_D, id_E, id_F
l	l_B, l_D, l_E, l_F	l_C, l_D, l_E, l_F	l_A, l_D, l_E, l_F
c	c_B, c_D, c_E, c_F	c_C, c_D, c_E, c_F	c_A, c_D, c_E, c_F

This article utilizes Δ to measure the connectivity of the constructed undirected graph.

$$\Delta = \frac{(num.(EV))}{n} \geq \frac{k}{n} \tag{2}$$

Here, n represents the total number of EVs in the graph, $num.(EV)$ represents the number of EVs connected to the target EV and is more than k. If the constructed graph is not connected, the segmentation sub-graph must be incomplete, otherwise there will be many EVs submitting the same request. If the constructed graph is connected, part of nodes can form a sub-complete graph. For example, if B and E are connected in Fig. 4, $\{A, B, C\}$,$\{B, C, E\}$,$\{B, D, E\}$,$\{D, E, F\}$ can all constitute sub-complete graphs with different connectivity of EV, as shown in Fig. 5.

The connectivity of EV_A and EV_B can be calculated as formula (3), (4).

$$\Delta_A = \frac{(num.(EV_A))}{n} = \frac{4}{6} \tag{3}$$

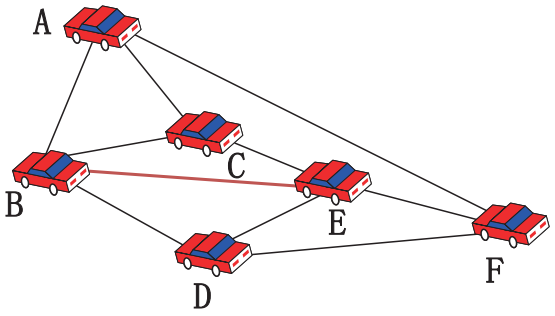

FIGURE 5. Certain EVs construct a sub-complete graph.

$$\Delta_B = \frac{(num.(EV_B))}{n} = \frac{5}{6} \tag{4}$$

Therefore, the connectivity of EV_B is greater than connectivity of EV_A.

In an undirected graph, the connectivity includes all the EVs', the greater the connectivity, the greater the similarity of requests. Therefore, the higher connectivity of the graph, the better the privacy protection. In this article, the average connectivity of EVs is used to measure the privacy protection standard. The average connectivity $\bar{\Delta}$ is:

$$\bar{\Delta} = \frac{(\Delta_1 + \Delta_2 + \ldots + \Delta_n)}{n} \leq 1 \tag{5}$$

When the graph constructed by connected EVs is a complete graph, the average connectivity $\bar{\Delta}$ is the maximum value 1.

2) AVERAGE WEIGHTS $\bar{w}$

To protect location privacy of the target EV, when the location of connected EVs is adjacent or even the same, the connection is invalid. In this article, the location of the EV is represented by (x,y), where x and y are the horizontal and vertical coordinates, respectively. The average weight between EVs in the undirected is defined as follows:

$$\bar{w} = \frac{\sum_{i \neq j} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2)}}{C_n^2} \tag{6}$$

(x_i, y_i) and (x_j, y_j) represent the location coordinates of any two EVs in the graph. For n nodes in an undirected graph, there exists an edge between any 2 connected EVs, if the graph is a complete graph, there are $\frac{1}{2}n(n-1)$ edges. We denote that the weight of edge between any 2 connected EVs is represented by w, and $\bar{w}$ is the average weight of all edges. The more the average weight between EVs, the better the location privacy protection, and the higher effectiveness of k-anonymous unity. To prevent EVs from being adjacent or being in the same position, this article sets a threshold δ. When $\bar{w} \leq \delta$, the connection is valid.

E. K-ANONIMITY CLOCKING AREA GENERATION

The undirected graph is generated based on the speed, location, and direction of the target EV, and is a static representation of the EV range within a given time, as shown

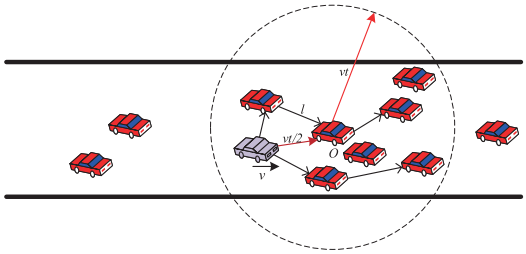

FIGURE 6. The range and generative process of clocking area.

in Fig. 6. The generation process can be divided into three phases:

We first initialize the range $A(O, vt)$ of the clocking area based on the location and velocity of the target EV. Where O is the center of the circle and vt is the radius. This can prevent an attacker from guessing that the target EV is in the center of range A, and ensure that the target EV is in range A within time t, as shown in Fig. 6.

Then we count the number of EVs in the range A, denoted as $num.(A)$, when $num.(A) > 2r$, an undirected graph G is generated, and r is the number of connected EVs. We initialize G and set the initial vertex as the target EV, and use an array $nodes[]$ to store these vertexes in G, and add the target EV to the array, and denote as EV_i. Notice that the length of $nodes$ is r. If a new vertex EV_j connected with EV_i, EV_j will be pushed into the array, then we traversing each vertex in the array until no new vertex can be added to the array. Finally, based on the array $nodes$, an undirected graph G is constructed. If G is not a complete graph, then the average connectivity of G is calculated. If G is a complete graph (we define as CP), modify the radius of range A from vt to $2vt$.

Finally, we find k connected EVs from set M. The average weight of EVs in G must be greater than the threshold to prevent EVs from being too close or even the same. First, suppose that the target EV receives $r-1$ location coordinates of other EVs in the clocking area, and stores these coordinates in the set D. Then we initialize the set M, select k EVs from the set D, including the target EV, and store the k EVs in M, and calculate the weight w between every two EVs in the set M, storing them in ascending order, and calculate the average weight w. If $\bar{w} \geq \delta$, the k matching cars can be found. Otherwise, select the two EVs closest to the target EV to replace. If the target EV belongs to $\{EV_i, EV_j\}$, that is, the target EV=EV_i, select another EV from the set D to replace EV_j. If the target EV does not belong to $\{EV_i, EV_j\}$, select two EVs from D to replace $\{EV_i, EV_j\}$. Then update the set M and continue to calculate the average weight until k matching EVs are found.

After above preparations, Algorithm 1 is proposed as follows:

Algorithm 1 Location Privacy-Preserving Algorithm

Input: input parameters k, t, r, v.
Output: M that is k matching EVs

```
A.radius = vt;
while t&A.radius do
    G ⇐ getGraph(nodes);
    if G typeof CP then
        A ⇐ 2vt;
    else
        Δ ⇐ getAvgCon(G);
    end if
    D ⇐ nodes;
    M ⇐ D.randomK().sort();
    for i = 0 to k do
        for d in M[i].degree() do
            sw+ = d;
        end for
        w̄ ⇐ sw / G.numberOfNodes();
        if w̄ > δ then
            return M;
        else
            if EV == M[i]||EV == M[j] then
                M[j] ⇐ D.randomOneNotSelect();
            else
                M[i], M[j] ⇐ D.randomTwoNotSelect();
            end if
            return newM;
        end if
    end for
end while
```

V. EXPERIMENT RESULTS AND ANALYSIS

In this section, we firstly introduce the security of our proposed DePET scheme. Then, the simulation environment requirements are given. Finally, we give the experimental results of the proposed DePET scheme and the comparison results with different architecture.

A. SECURITY ANALYSIS

There are three essential goals in our designed DePET scheme that need to be presented and described here, including authentication, adoptable efficiency and k-anonymity. We will describe these goals in detail as follow:

Authentication: In DePET, all the transaction records hold digital signatures of LAG, if a malicious LAG to modified a transaction, then can be easily counted and located by CA. After the CA verifies, the malicious LAG cannot execute any transaction-related behaviors. CA is auditable so that the change will be discovered.

Adoptable efficiency: With the help of consortium blockchain, EVs can trade energy with energy nodes directly without a third party to make system robust and scalable. In addition, EVs should not participate in the consensus protocol and have the backup of data of blockchain network like a public chain.

K-anonymity: To explain this, let us assume that an attacker knows the current united request of the target EV.

Once the attacker observes the request body, it cannot continue to track this EV. Let k represent the number of buyers in a single clocking area. If the attacker gets the location of an EV, the probability that the EV's accurate location cannot be distinguished is more than 1/k. Therefore, our proposed scheme satisfies k-anonymity.

To be specifically, we use an example to illustrate how our proposed scheme ensures the privacy protection of k-anonymous EVs location. Assuming that 30 EVs submit requests in the same clocking area. For these EVs, LAG holds a set of location coordinates, not their accurate location coordinates. Although the attacker can obtain the location coordinates of an EV in the clocking area, it is hard to distinguish which EV the location belongs to. Then, if an attacker breaks into the system, only 30 EVs are known to be in this area. In other words, the attacker cannot distinguish where the EV is located at a probability more than 1/30. This will make the linking attack harder to succeed. Hence, the attacker cannot continue to link the location of target EV.

B. SIMULATION SETTING

Our proposed DePET scheme can be divided into two parts: EV network and blockchain network. The blockchain network is responsible for the transaction record, and the EV network mainly do that EVs construct a clocking area based undirected graph and upload the united requests. We use Hyperledger Fabric and Python to simulate the blockchain network and EV network, the experiment was carried out on a computer with 3.20 GHz Inter(R) Core (TM) i5-6500 CPU and GeForce GT 730 graphics card. Hyperledger Fabric is a blockchain- based platform, which provides the power of chain codes and consensus process. Notice that smart contract is also called chaincode. Thus, in our experiment, we use Hyperledger Fabric platform to write rules (e.g. authentication rule, k-anonymity rule, transaction rule) into chaincodes. For blockchain network, using the abovementioned three-phase consensus to verify the new data block.

For EV network, the experiment mainly uses two indicators (average connectivity $\bar{\Delta}$ and average weight $\bar{w}$) to verify the location privacy protection performance. The experiment collected 10 positions of the target EV on its trajectories $\{l_1, l_2, \ldots, l_{10}\}$, and generated an undirected graph for each location. Thus, there exists 10 undirected graphs $\{l_1, l_2, \ldots, l_{10}\}$, and generated an undirected graph for each location. Thus, there exists 10 undirected graphs $\{G_1, G_2, \ldots, G_{10}\}$. As shown in Fig. 7, the target EV generated 10 undirected graphs on these locations.

C. RESULTS AND DISCUSSION

The trading performance mainly depends on the blockchain processing time. The blockchain processing time refers to the time when a LAG completes the consensus process of an energy trading between energy nodes and EV owners. For the purpose of illustration, we simulate the performance among 100 LAGs nodes within 4 hours based on the abovementioned three-phase consensus. Similar to that in Bitcoin,

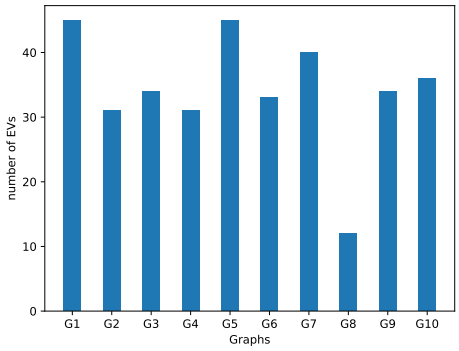

FIGURE 7. The number of EVs in different graph.

the verification time takes 60 minutes, whereas that of our proposed DePET scheme is set to be 10 minutes as an example [27]. In our experiment, 40 LAGs are randomly selected from these 100 LAGs to join the consensus process, and the transaction delay (transaction times) per hour takes values from set {1, 2, 3, 4, 5} with equal probability for EV owners and energy nodes.

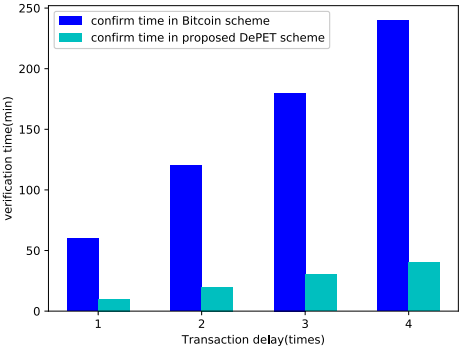

FIGURE 8. The confirm delays.

As shown in Fig. 8, when the transaction delay increases, the verification time required in Bitcoin is more than our proposed DePET scheme. This is due to the fact that our proposed DePET scheme only carries out the consensus process by LAGs, and it takes less time, instead of all nodes in Bitcoin. In addition, the verification time takes 60 minutes in Bitcoin, whereas that of our proposed DePET scheme only needs 10 minutes. Therefore, compared with Bitcoin, the energy nodes of our proposed scheme will take less time to continue energy trading on the blockchain. Experimental results show that our proposed DePET scheme has a lower comfirm delays, and supports fast P2P energy trading.

Fig. 9 describes the average weight $\bar{w}$ in the case of road congestion and unblocked conditions. The average weight $\bar{w}$ in a congested road condition is about $750m$, and the average weight is about $650m$ in an unblocked road condition, which is less than $\bar{w}$ in a congested road condition about $100m$. This is because EVs are denser when the road is congested, and the construction of the clocking area will be faster, there are fewer EVs when the road is clear. From Fig. 9, we can find that the

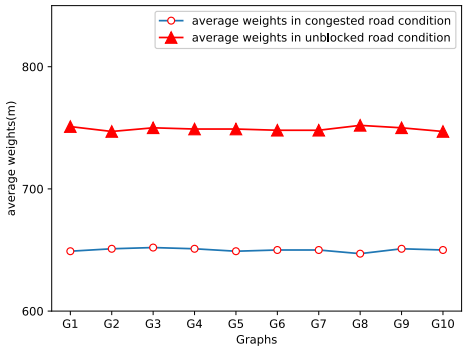

FIGURE 9. The average weights in different scenario.

change of the average weight $\bar{w}$ is stable. Experimental results show that and our proposed DePET scheme is stable enough whether it is when the road is congested or clear.

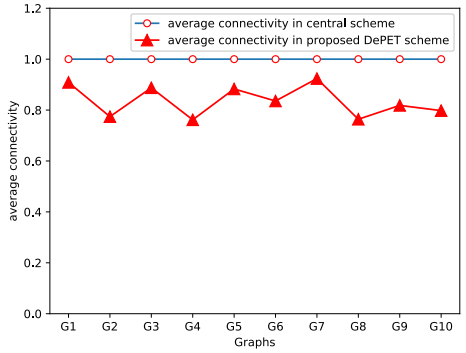

FIGURE 10. The average connectivity in different scenario.

In addition, the experiment uses average connectivity to verify the performance of privacy protection, as shown in Fig. 10. When $\Delta = 1$, the undirected graph is a complete graph, which is not conducive to identity privacy protection. When it is not equal to 1, the more the average connectivity is, the better the privacy protection is. Compared with the centralized architecture [11], the average connectivity of the proposed scheme is lower, about 0.83. This is because each node holds a request, and the request contains its sensitive information, such as identity, location etc. and then the connectivity and the risk of privacy leakage is equal to 1 in reference [11]. Therefore, the privacy protection performance of our proposed scheme is higher than the centralized architecture.

VI. CONCLUSION

In this article we propose DePET scheme to address two critical limitations in current centralized vehicular energy networks - cross-domain energy trading and location privacy protection. Our scheme employs consortium blockchain to enable cross-domain trading and P2P trading, which also make the energy trading transparently and reliably. DePET further preserves the location privacy of EV owners, by proposed location privacy-preserving algorithm. We utilize a clocking area based on undirected graph to generate a united request, which can satisfy k-anonymity to hide the real location for EV owners. The experimental results justified that the performance is manageable, e.g., energy trading delay is short. Moreover, the security performance such as privacy protection is also guaranteed.

REFERENCES

[1] T. Fu, C. Wang, and N. Cheng, "Deep-learning-based joint optimization of renewable energy storage and routing in vehicular energy network," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6229–6241, Jul. 2020.

[2] K. Wang, J. Yu, Y. Yu, Y. Qian, D. Zeng, S. Guo, Y. Xiang, and J. Wu, "A survey on energy Internet: Architecture, approach, and emerging technologies," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2403–2416, Sep. 2018.

[3] M. Xiong, F. Gao, K. Liu, S. Chen, and J. Dong, "Optimal real-time scheduling for hybrid energy storage systems and wind farms based on model predictive control," *Energies*, vol. 8, no. 8, pp. 8020–8051, Aug. 2015.

[4] D. Li, Q. Yang, D. An, W. Yu, X. Yang, and X. Fu, "On location privacy-preserving online double auction for electric vehicles in microgrids," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5902–5915, Aug. 2019.

[5] R. Xu, S. Y. Nikouei, Y. Chen, E. Blasch, and A. Aved, "BlendMAS: A blockchain-enabled decentralized microservices architecture for smart public safety," in *Proc. IEEE Int. Conf. Blockchain*, Jul. 2019, pp. 564–571.

[6] H. Zheng, W. Guo, and N. Xiong, "A kernel-based compressive sensing approach for mobile data gathering in wireless sensor network systems," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 12, pp. 2315–2327, Dec. 2017.

[7] Y. Yang, N. Xiong, and N. Y. Chong, "A decentralized and adaptive flocking algorithm for autonomous mobile robots," in *Proc. 3rd Int. Conf. Grid Pervas. Comput. Workshops*, May 2008, pp. 262–268.

[8] R. He, N. Xiong, L. T. Yang, and J. H. Park, "Using multi-modal semantic association rules to fuse keywords and visual features automatically for Web image retrieval," *Inf. Fusion*, vol. 12, no. 3, pp. 223–230, Jul. 2011.

[9] W. Guo, N. Xiong, A. V. Vasilakos, G. Chen, and C. Yu, "Distributed k-connected fault-tolerant topology control algorithms with pso in future autonomic sensor systems," *Int. J. Sensor Netw.*, vol. 12, no. 1, pp. 53–62, 2012.

[10] B. Ying and A. Nayak, "A distributed social-aware location protection method in untrusted vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 6114–6124, Jun. 2019.

[11] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 93–105, Jan. 2016.

[12] P. K. Singh, S. N. Gowtham, T. S, and S. Nandi, "CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100183.

[13] L. Benarous, B. Kadri, and S. Boudjit, "Alloyed pseudonym change strategy for location privacy in VANETs," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–6.

[14] P. Corcoran, P. Mooney, and A. Gagarin, "A distributed location obfuscation method for online route planning," *Comput. Secur.*, vol. 95, Aug. 2020, Art. no. 101850.

[15] Y. Sang, H. Shen, Y. Tan, and N. Xiong, "Efficient protocols for privacy preserving matching against distributed datasets," in *Information Communication Security*, P. Ning, S. Qing, and N. Li, Eds. Berlin, Germany: Springer, 2006, pp. 210–227.

[16] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets VANET: An architecture for identity and location privacy protection in VANET," *Peer Peer Netw. Appl.*, vol. 12, no. 5, pp. 1178–1193, Sep. 2019.

[17] I. Rasheed, L. Zhang, and F. Hu, "A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing," *Comput. Netw.*, vol. 176, Jul. 2020, Art. no. 107283.

[18] B. S. Kumar, T. Daniya, N. Sathya, and R. Cristin, "Investigation on privacy preserving using K-Anonymity techniques," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2020, pp. 1–7.

[19] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized Peer-to-Peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[20] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3620–3631, Jun. 2019.
[21] O. Samuel and N. Javaid, "A secure blockchain based demurrage mechanism for energy trading in smart communities," *Int. J. Energy Res.*, pp. 1–19, Apr. 2020.
[22] A. S. Yahaya, N. Javaid, F. A. Alzahrani, A. Rehman, I. Ullah, A. Shahid, and M. Shafiq, "Blockchain based sustainable local energy trading considering home energy management and demurrage mechanism," *Sustainability*, vol. 12, no. 8, p. 3385, Apr. 2020.
[23] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.
[24] Y.-B. Son, J.-H. Im, H.-Y. Kwon, S.-Y. Jeon, and M.-K. Lee, "Privacy-preserving Peer-to-Peer energy trading in blockchain-enabled smart grids using functional encryption," *Energies*, vol. 13, no. 6, p. 1321, Mar. 2020.
[25] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6564–6574, Oct. 2020.
[26] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowé, "NRGcoin: Virtual currency for trading of renewable energy in smart grids," in *Proc. 11th Int. Conf. Eur. Energy Market (EEM14)*, Kraków, Poland, 2014, pp. 1–6, doi: 10.1109/EEM.2014.6861213.
[27] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

YANGYANG LONG is currently a Graduate Student with the College of Computer Science and Technology, Guizhou University. His research interests include blockchain, privacy protection, cryptography, and information security.

YULING CHEN received the B.S. degree from Taishan University, Tai'an, China, in 2006, and the M.S. degree from Guizhou University, Guiyang, China, in 2009. She is currently an Associate Professor with the Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University. Her recent research interests include cryptography and information security.

WEI REN (Member, IEEE) received the Ph.D. degree in computer science from the Huazhong University of Science and Technology, China. He was with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, USA, in 2007 and 2008; the School of Computer Science, University of Nevada, Las Vegas, USA, in 2006 and 2007; and the Department of Computer Science, The Hong Kong University of Science and Technology, in 2004 and 2005. He is currently a Full Professor with the School of Computer Science, China University of Geosciences, Wuhan, China. He has published more than 70 refereed articles, one monograph, and four textbooks. He obtained ten patents and five innovation awards. He is also a Distinguished Member of the China Computer Federation.

HUI DOU is currently a Graduate Student with the College of Computer Science and Technology, Guizhou University. Her research interests include data security and privacy protection, cryptography and information security, and wireless sensor networks.

NEAL NAIXUE XIONG (Senior Member, IEEE) received the dual Ph.D. degrees in sensor system engineering and in dependable communication networks from Wuhan University and the Japan Advanced Institute of Science and Technology, in 2007 and 2008, respectively. He is currently an Associate Professor (fifth year) with the Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK, USA. Before he attended Northeastern State University, he worked with Georgia State University, the Wentworth Institute of Technology, and Colorado Technical University (a Full Professor for about five years) for about ten years. His research interests include cloud computing, security and dependability, parallel and distributed computing, networks, and optimization theory.