2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering

A Secure Private Charging Pile Sharing Scheme with Electric Vehicles in Energy Blockchain

Yuntao Wang[1], Zhou Su[1,2], and Kuan Zhang[3]
[1]MOE KLINNS Laboratory, School of Electronic and Information Engineering, Xi'an Jiaotong University, China
[2]School of Mechatronic Engineering and Automation, Shanghai University, China
[3]Electrical and Computer Engineering Department, University of Nebraska-Lincoln, USA
Corresponding author: zhousu@ieee.org

***Abstract*—With the rapid advance of electric vehicles (EVs) and the sparse public charging infrastructure, the private charging pile sharing networks (PCPSNs) hold the potential to improve the quality of experience (QoE) of using EVs by leveraging private charging piles (PCPs) as shared charging points to charge a group of distributed EVs. However, due to the potential security and privacy issues for EVs and PCPs caused by untrusted participants in decentralized energy market, it becomes a crucial challenge to optimally schedule the charging and sharing strategies of EVs and PCPs in PCPSNs. In this paper, we propose a secure and permissioned blockchain-based PCP sharing scheme for EVs in PCPSNs. Firstly, we present an energy blockchain-based PCPSN framework to enhance the security of distributed energy trading. Secondly, we develop a reputation-based secure PCP sharing protocol to efficiently reach consensus in the blockchain with the implement of BLS multi-signature. Thirdly, we investigate a distributed reputation model to evaluate the trustworthiness of participants and identify malicious users. In addition, based on the many-to-one matching game, the optimal strategies of EVs and PCPs are analyzed by searching the stable matching pairs. Finally, simulation results show that the proposed scheme can not only improve the QoE of users, but also protect the network from adversaries.**

***Index Terms*—Electric vehicles, sharing security, blockchain, reputation evaluation.**

I. Introduction

Electric vehicles (EVs) hold the promise to ease fossil fuel crisis and reduce gas emissions [1], have attracted worldwide attentions from academia and industry. EVs on the road will reach 140 million and constitute almost a third of new-car market by 2030 [2]. Due to the lack of public charging stations, the booming EV development has inevitably led to serious problems for EV charging, especially in remote areas. Besides, the utilization efficiency of private charging piles (PCPs) is low since they only serve for their owners and are left idle for a long time in a day [3]. Recently, the PCP sharing networks (PCPSNs) have been developed as a potential solution to facilitate the EV charging process and improve the PCP utilization efficiency by sharing PCPs, which are scattered throughout a city, with distributed foreign EVs [4].

PCPSNs basically consist of a group of publicly shared PCPs powered by community renewable energy (RE) generators and a fleet of moving EVs with charging desires. In PCPSNs, by publicly sharing PCPs, EVs users can attain a better quality of experience (QoE) and reduce charging costs, while PCP owners can earn extra profit by renting private charging facilities to EVs [5]. However, several challenges impede the current PCPSNs from being widely adopted.

On one hand, existing EV charging schemes [3]–[7] cannot be directly applied in PCPSNs to develop optimal charging strategies for connected EVs and PCPs, since the competition, cooperation and social features among users are not jointly considered in PCPSNs with practical constraints [8]. For instance, PCPs with limited renewable generation can cooperatively form coalitions with each other, and PCPs may be more interested in sharing their private charging facilities to EVs with higher social tie. Therefore, how to optimally schedule the EV charging and PCP sharing process in PCPSNs remains an issue of significance.

On the other hand, since PCP owners and EV users are commonly strangers without prior direct experience, there exist inherent risks and potential security and privacy issues caused by malicious users and the compromised central sharing platform during the PCP sharing process [9]. Recently, the blockchain technique offers a potential solution to reduce the reliance of the centralized sharing platform and defend against attackers to enhance the security in PCP sharing [10]. However, due to the high mobility and resource-constraint natures of EVs, it is still an open and vital issue to efficiently implement a blockchain network among PCPs and EVs in PCPSNs.

In this paper, we propose a novel permissioned blockchain-based PCP sharing scheme for EVs in PCPSNs. Firstly, a decentralized blockchain-based PCPSN framework is developed, where EVs and PCPs can publicly share energy transactions. Secondly, with the implement of BLS multi-signature [11], a novel reputation-based secure PCP sharing protocol with lower signature size is developed to improve the efficiency to reach consensus. For each consensus node, the difficulty of proof-of-work (PoW) is adaptive according to its reputation value. Thirdly, a reputation model is presented to assess the trustworthiness of various nodes in PCPSNs and identify malicious nodes based on ratings recorded in blockchain while users' social features are considered. In addition, we develop a many-to-one matching game to model the interactions among EVs and PCP coalitions. The stable matching pairs are derived for both sides to select the best candidate to connect. Finally, simulation results prove that the proposal outperforms other conventional schemes in terms of security and efficiency.

The remainder of the work is organized as follows. Related

2324-9013/19/$31.00 ©2019 IEEE
DOI 10.1109/TrustCom/BigDataSE.2019.00092

work is reviewed in Section II. The system model is introduced in Section III. The proposed scheme is presented in Section IV. Performance evaluations are shown in Section V. Conclusion and the future work are given in Section VI.

II. Related Work

A. EV Charging Scheduling

Recently, a number of EV charging scheduling methods have been proposed to improve the performance of energy management in the vehicular networks and the smart grid. Luo *et al*. [6] studied the multi-objective optimization framework for EV charging stations integrated with RE sources and designed a stochastic dynamic programming algorithm to derive the optimal pricing and energy management policy. Cao *et al*. [7] investigated a public charging station selection scheme in distributed energy scheduling systems to minimize EVs' trip duration, where EVs' parking duration, charging reservations and mobility uncertainty are taken into consideration.

Zhang *et al*. [12] presented a three-party network architecture including the main grid, EVs and smart communities in the smart grid and proposed a novel schedule-upon-request energy scheduling framework to achieve flexiable and effective energy management. To minimize the energy cost and charging cost of substations with eased computational difficulty, Song *et al*. [13] developed an optimal EV charging station scheduling model in distributed power systems via convex relaxation techniques. However, the security in the charging process of EVs and the social features of EV users and PCP owners are still not discussed sufficiently in most of the existing works.

B. Energy Blockchain

Recently, there have been an increasing number of studies to improve the security of energy trading using the promising blockchain technology. Silvestre *et al*. [14] reviewed different blockchain paradigms in microgrids and proposed a blockchain-based real-time energy loss tracking and attribution scheme for distributed energy transactions without reliance on trusted intermediaries. To enhance transaction security and privacy preservation in decentralized energy trading context, Aitzhan *et al*. [15] developed a blockchain technology based prototype named PriWatt by using anonymous encrypted message propagation and multi-signature approaches.

Kang *et al*. [16] presented a local peer-to-peer energy exchanging model among plug-in hybrid EVs with decentralized permissioned blockchain technique to improve the privacy preservation and transaction security. Based on smart contracts and lightning network in energy blockchain ecosystem, Huang *et al*. [17] proposed a novel secure charging scheme for EVs and charging piles in the Internet of energy to meet the security requirements during energy trading process. However, due to the resource constraints of EVs and PCPs and the existence of multiple PCP coalitions, the above blockchain systems cannot be directly applied in PCPSNs.

In contrast to the existing works, we investigate the secure and incentive mechanism for EVs and PCPs in PCPSNs based on the blockchain technology, reputation model, and game theoretic model with the consideration of user's competition, cooperation, and social features.

III. System Model

A. Network Model

As shown in Fig. 1, the energy blockchain-based PCPSN consists of the following entities:

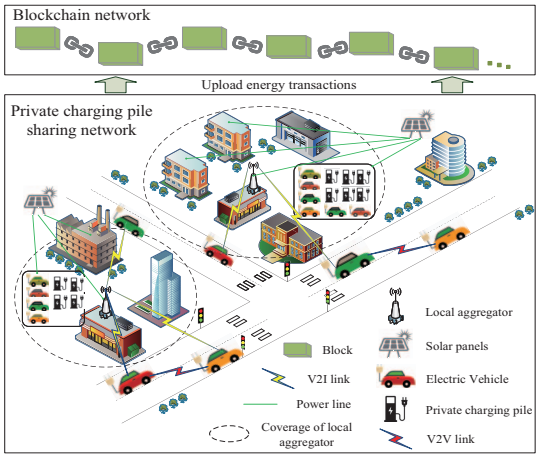

Fig. 1. System model of energy blockchain-based PCPSNs.

Electric Vehicles (EVs). The set of EVs with charging request is denoted as $\mathcal{I} = \{1, \cdots, i, \cdots, I\}$. To facilitate the charging operations of EVs, each EV user i can send its charging request with the desired energy demand to nearby PCPs when its remaining state of charge (SoC) is low. Let SoC_i denote the SoC of EV i, which is constrained by $SoC_i^{min} \leq SoC_i \leq 1$, where SoC_i^{min} is the minimum SoC of EV i to prolong its battery life [18].

Private Charging Piles (PCPs). There are M communities located in a given investigated area. The set of PCPs in each community $m \in \mathcal{M}$ is denoted as $\mathcal{J}_m = \{1, \cdots, j, \cdots, J_m\}$. Each PCP $j \in \mathcal{J}_m$ is privately owned and managed by its owner and equipped with a charging outlet for EV charging. Multiple solar panels are installed on the rooftop of community buildings to provide clean energy supply for local PCPs. Let $E_j^{PV}(t)$ be the clean energy supply for PCP j at time slot $t \in \mathcal{T} = \{1, \cdots, t, \cdots, T\}$. Furthermore, a group of PCP owners in the same community with social relationships can form social coalitions to exchange and share their limited solar energy resources with each other to earn profit. The set of PCP coalitions in community m is defined as $\Pi_m = \{\Phi_1, \cdots, \Phi_n, \cdots, \Phi_{N_m}\}$, where $\Phi_n \cap \Phi_{n'} = \emptyset, \forall n \neq n'$, and $\bigcup_{n=1}^{N_m} \Phi_n = \mathcal{J}_m$.

Local Aggregators (LAGs). Each community m is equipped with a LAG $m \in \mathcal{M} = \{1, \cdots, m, \cdots, M\}$ which can provide both energy exchange and wireless communication services for EVs and PCPs in its coverage area [19]. Specifically, LAG m receives charging requests from multiple EVs and obtains the latest information of local shared PCPs, e.g., location, residual solar energy, charging state (i.e., busy or idle), etc. In the blockchain, LAGs are performed as full nodes which store all the blockchain data and can participate in the consensus process for global ledger management. Due to resource constraints, EVs and PCPs are light nodes which only

store the metadata of blocks (i.e., the block header) and can send, relay and accept ledger data in the blockchain [20].

B. Adversary Model

In the network, potential attacks will threaten user's security and privacy. We define the following kinds of adversaries:

Honest but curious EVs and PCPs. A EV or PCP may be honest but curious by stealing the other's privacy (e.g., identity, occupation, habits, etc) during energy charging process.

Malicious EVs and PCPs. A malicious EV may pretend that it has not received any charging service from the corresponding PCP and refuses to pay. A malicious PCP may advertise fraudulent charging services to nearby EVs. Malicious EVs and PCPs may conduct the bad mouth attack by conducting multiple small energy transactions and generating multiple untruthful ratings to illegally increase or decrease the reputation value of participants in PCPSNs.

Malicious LAGs. A malicious LAG may forge or tamper with the data stored in it (e.g., local energy transactions) and disclosure user's privacy for profit.

Malicious sharing platform. Since all energy transactions are stored in the sharing platform in traditional centralized PCPSNs, a malicious sharing platform may conduct transaction falsification attacks by modifying or forging transactions to tamper with users' account balances for self-interest.

IV. The Proposed Scheme

In this section, the energy blockchain is first introduced followed with the reputation model. Then, we analyse the optimal strategies of users by the matching game model.

A. Energy Blockchain

To secure the PCP sharing process, we propose a reputation-based PCP sharing protocol in permissioned blockchain-based PCPSNs, which contains the following steps:

1) Entity Registration: For system initialization, registration authority (RA) selects a bilinear pairing $e : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ in groups $\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_2$ of prime order q, where g_0 and g_1 are the generators of $\mathbb{G}_0, \mathbb{G}_1$, respectively. Two hash functions are selected, i.e., $H_0 : \{0,1\}^* \rightarrow \mathbb{G}_2$ and $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q$. Each node k becomes authorized in the network after registration with RA by using its real identity. Then, each authorized node k gets V public/private key pairs $\{y_k^v, x_k^v\}_{v=1}^V$, certificates $\{Cer_k^v\}_{v=1}^V$, and wallet addresses $\{w_k^v\}_{v=1}^V$, where $x_k \xleftarrow{S} \mathbb{Z}_q$, $y_k = g_1^{x_k}$, and $\xleftarrow{S}$ means randomly sampling.

2) BLS Multi-signature for PCP Coalition: Compared with other digital signature schemes, BLS signatures [11] are far shorter in the signature size. The security of BLS multi-signature scheme relies on the standard computational co-Diffie-Hellman (co-CDH) assumption. Each PCP j in PCP coalition $\Phi_n \in \Pi_m$ signs message Msg and generates its signature $\sigma_j = H_0(Msg)^{\alpha_j \cdot x_j}$, where $\alpha_j = H_1(y_j, \{y_1, \cdots, y_{|\Phi_n|}\})$. By computing the aggregated public key $apk = \prod_{j=1}^{|\Phi_n|} y_j^{\alpha_j}$, the BLS multi-signature is generated as $\sigma = \prod_{j=1}^{|\Phi_n|} \sigma_j$. Given (Msg, apk, σ), if $e(\sigma, g_1^{-1}) \cdot e(H_0(Msg), apk) = 1_{\mathbb{G}_2}$, the verification passes.

3) Energy Transaction: After PCP $l \in \Phi_n$ offers charging service for EV i, an energy transaction tx_1 is generated as

$$tx_1 = \left\{ \begin{array}{r} tx_{ID}^1 || w_i^v || w_n || \{s_j\}_{j=1}^{|\Phi_n|} || rating || coin \\ || time || Sig_i || MulSig_n \end{array} \right\}, \quad (1)$$

where tx_{ID}^1 is the hash of transaction tx_1, w_i^v is the v^{th} wallet address of EV i, w_n is the wallet address of coalition Φ_n, s_j is the contribution of PCP j in coalition Φ_n defined in Section IV-C. The tuple $rating = \{ra_{i,l} || ra_{l,i} || ra_{i,m} || ra_{l,m}\}$ consists of the rating $ra_{i,l}$ that EV i gives to PCP l, the rating $ra_{l,i}$ that PCP l gives to EV i, the rating $ra_{i,m}$ that EV i gives to LAG m, and the rating $ra_{l,m}$ that PCP l gives to LAG m, where 1 means absolutely positive and 0 means totally negative. $coin$ is the energy coin that EV i should pay to coalition Φ_n, $time$ is the timestamp for transaction generation, $Sig_i = \sigma_i$ is the signature of tx_{ID}^1 using EV i's private key x_i^v, and $MulSig_n = (apk, \sigma)$ is the BLS multi-signature of tx_{ID}^1 signed by all members in coalition Φ_n. Then, each PCP j in PCP coalition Φ_n can redeem its reward $coin_j$ in coalition Φ_n's wallet address w_n by sending a redeem transaction tx_2, where the reward is allocated based on its contribution in the coalition, i.e., $coin_j = s_j \cdot coin$. Here, the transaction tx_2 is

$$tx_2 = \{tx_{ID}^1 || tx_{ID}^2 || w_n || w_j^v || y_j^v || coin_j || time || Sig_j\}, \quad (2)$$

where tx_{ID}^2 is the hash of transaction tx_2, and $Sig_j = \sigma_j$ is the signature of tx_{ID}^2 using PCP j's private key x_j^v.

4) Reputation-based Consensus Process:

All valid transactions during the consensus time slot ΔT are ordered by timestamps and packaged into a local block by each LAG. In the consensus process, LAGs compete with each other to solve a proof-of-work (PoW) puzzle with a certain difficulty. For each consensus node m, its difficulty of PoW puzzle, ϱ_m, is adjusted dynamically and inversely proportional to its reputation value R_m [21], [22] calculated in Section IV-B, i.e.,

$$\varrho_m = \frac{\varsigma}{\log_2(1 + R_m)}, \quad (3)$$

where $\varsigma > 0$ is the adjustment coefficient. Note that it is easier for a consensus node with higher reputation value to find a valid PoW solution. After the fastest LAG $\widehat{m}$ finds a valid nonce which is audited successfully by other LAGs, the consensus is reached. Then, the newly generated block is added into the append-only blockchain, and LAG $\widehat{m}$ is rewarded with a certain amount of energy coins. In addition, the PCP coalition $\Phi_{\widehat{n}}$ with the most contribution on energy sharing during ΔT is rewarded with small amount of energy coins as an incentive.

B. Reputation Evaluation

To assess the trustworthiness of EV users, PCP owners, and LAG operators, a reputation model is presented based on the ratings recorded in the blockchain. Let $\Lambda_j(t)$ be the set of EVs that have interacted with PCP j during time slot t. Let $Ra_{i,j}^k$ be the weighted rating of EV i in PCP j, i.e.,

$$Ra_{i,j}^k = \log_2\left(1 + \frac{d_{i,\Phi_n}}{v_{\max}} ra_{i,j}^k\right), \quad (4)$$

where d_{i,Φ_n} is the energy demand of EV i in PCP $j \in \Phi_n$, v_{max} is the maximum energy demand, and $ra_{i,j}^k$ is the rating for k^{th} interaction (i.e., charging operation). The credibility value is used to measure the reliability of rating $ra_{i,j}^k$, which is calculated by

$$cre_{i,j}^k(t) = sid_{i,j} \cdot sim_{i,j}^k(t) \cdot e^{-\lambda(t-t_k)}, \tag{5}$$

where $e^{(.)}$ is the time decay function indicating that latest interactions are more important than previous ones, λ is the aging factor, and t_k is kth service time. Here, $sid_{i,j}$ is the social importance degree of EV i in PCP j, i.e.,

$$sid_{i,j} = \frac{\sum_{k \in \mathcal{N}_i} so_{i,k}}{\sum_{i \in \Lambda_j(t)} \sum_{k \in \mathcal{N}_i} so_{i,k}}, \tag{6}$$

where $\mathcal{N}_i$ is the set of neighboring nodes of node i in the social network, and $so_{i,k} \in [0,1]$ is the social relationship between node i and node k. Let $drs_{i,j}^k$ and $mrs_{i,j}^k$ be the dual rating similarity and the mean rating similarity between EV i and PCP j for rating $ra_{j,i}^k$, respectively, i.e.,

$$drs_{i,j}^k = 1 - \left| ra_{i,j}^k - ra_{j,i}^k \right|, \tag{7}$$

$$mrs_{i,j}^k = 1 - \left| ra_{i,j}^k - ra_j(t) \right|, \tag{8}$$

where $ra_j(t) = \frac{\sum_{i=1}^{|\Lambda_j(t)|} \sum_{h=1}^{q_{i,j}(t)} ra_{i,j}^h}{\sum_{i=1}^{|\Lambda_j(t)|} q_{i,j}(t)}$ is the average rating given from EVs in the set $\Lambda_j(t)$ to PCP j, and $q_{i,j}(t)$ is the amount of interactions between EV i in PCP j during time slot t. Then, the similarity value between EV i and PCP j for each rating is $sim_{i,j}^k(t) = drs_{i,j}^k \cdot mrs_{i,j}^k$. To ease computational difficulty, the reputation value of PCP owner j at time slot t can be attained by iteration, i.e.,

$$\begin{aligned} R_j(t) &= \frac{\Xi_R(t)}{\Theta_R(t)} \\ &= \frac{\Xi_R(t-1)e^{-\lambda} + \sum_{i=1}^{|\Lambda_j(t)|} \sum_{k=1}^{q_{i,j}(t)} Ra_{i,j}^k cre_{i,j}^k(t)}{\Theta_R(t-1)e^{-\lambda} + \sum_{i=1}^{|\Lambda_j(t)|} \sum_{k=1}^{q_{i,j}(t)} cre_{i,j}^k(t)} \end{aligned}. \tag{9}$$

We set $\Xi_R(0) = 0.5$ and $\Theta_R(0) = 1$. Obviously, $R_j(t) \in [0,1]$. Similarly, the reputation value $R_i(t)$ of EV user i, and the reputation value $R_m(t)$ of LAG operator m can be computed.

Security Analysis: Since all energy transactions are recorded in the recognized and verifiable blockchain, *malicious EV users* cannot deny the related transactions recorded in the blockchain. Meanwhile, if any *malicious PCP owner* advertises fraudulent charging services, RA can reveal its true identity and penalize it correspondingly. Through reputation evaluation, dishonest or unfair ratings given from malicious users are assigned with low credibility. Therefore, the effect of *bad mouth attack* can be reduced by credibility computing. Since each user can dynamically change pseudonyms (i.e., wallet addresses) for different transactions to send and receive energy coins, the anonymity and unlinkability of users can be achieved for privacy preserving.

By adjusting the difficulty of PoW based on reputation values in consensus phase, the power consumption of honest LAGs is decreased while that of malicious LAGs is increased to motivate LAGs to behave honestly. In addition, each LAG stores a copy of the immutable blockchain which is managed by all LAGs via the consensus process and cannot be tampered with or forged by *malicious LAGs*. Through decentralized permissioned blockchain technology, inherent security risks arisen from *centralized sharing platform* can be removed in blockchain-based PCPSNs.

C. Many-to-one Matching Game

A coalition of PCPs can provide charging services for multiple EVs while each EV can only receive charging service from a specific coalition of PCPs in PCPSNs. Therefore, the charging scheduling problem between EVs and PCPs can be modeled as a many-to-one matching game.

Definition 1 (Many-to-one matching): A many-to-one matching Ψ is defined as a bidirectional mapping between the set of PCP coalitions $\Pi = \{\Pi_1, \cdots, \Pi_m, \cdots, \Pi_M\}$ and the set of EVs $\mathcal{I}$ such that:

- $\forall i \in \mathcal{I}$, each EV i is assigned to at most one PCP coalition in Π, i.e., $\Psi(i) \in \Pi \cup \{\emptyset\}$, and $|\Psi(i)| \in \{0,1\}$.
- $\forall \Phi_n \in \Pi$, each PCP coalition Φ_n is assigned to at most $|\Phi_n|$ EVs, i.e., $\Psi(\Phi_n) \in \mathcal{I} \cup \{\emptyset\}$, and $|\Psi(\Phi_n)| \in \{0, \cdots, |\Phi_n|\}$.

Definition 2 (Preference relation): If EV i prefers PCP coalition Φ_n to $\Phi_{n'}$, for any two disjoint coalitions $\Phi_n, \Phi_{n'} \in \Pi$, the strict preference relation $\succ_i$ is defined over the set of EVs such that:

$$\Phi_n \succ_i \Phi_{n'} \Leftrightarrow U_i(\Phi_n) > U_i(\Phi_{n'}). \tag{10}$$

Similarly, if PCP coalition Φ_n prefers EV i to i', for any two different EVs $i, i' \in \mathcal{I}, i \neq i'$, the strict preference relation $\succ_{\Phi_n}$ is defined over the set of PCP coalitions such that:

$$i \succ_{\Phi_n} i' \Leftrightarrow \Omega_i(\Phi_n) > \Omega_{i'}(\Phi_n), \tag{11}$$

where $\Omega_i(\Phi_n)$ is defined as the utility of PCP coalition Φ_n providing charging service for EV i, i.e., $\Omega_i(\Phi_n) = (p_{\Phi_n} - c_{\Phi_n}) d_{i,\Phi_n} - \delta_1$.

Definition 3 (Stable Matching): A many-to-one matching Ψ is stable, if and only if there does not exist a blocking pair $(\Phi_n \in \Pi, i \in \mathcal{I})$ to block the matching Ψ, i.e.,

$$\nexists (\Phi_n, i), s.t. \, \Phi_n \succ_i \Psi(i) \text{ and } i \succ_{\Phi_n} \Psi(\Phi_n), \tag{12}$$

where $\Psi(i) \neq \Phi_n, i \notin \Psi(\Phi_n)$. Here, $\Psi(i)$ and $\Psi(\Phi_n)$ indicate the current matching results for EV i and PCP coalition Φ_n, respectively.

To obtain the preference list in the proposed matching game, firstly, the utility function of each user need to be established. For EV i requesting energy from PCP coalition Φ_n in LAG m, its utility function can be used to measure the QoE and is defined as:

$$\begin{aligned} U_i(\Phi_n) = \alpha_i \ln(1 + \eta_i R_{\Phi_n} d_{i,\Phi_n}) - \varepsilon_i d_{i,\Phi_n} + \\ \xi(l_{i,grid} - l_{i,\Phi_n}) + (p_{grid} - p_{\Phi_n}) d_{i,\Phi_n} - \delta_1 \end{aligned}, \tag{13}$$

$$s.t. \begin{cases} E_i^{ini} - \xi l_{i,\Phi_n} \geq SoC_i^{min} C_i^{EV}, & (14) \\ E_i^{ini} - \xi l_{i,\Phi_n} + \eta_i d_{i,\Phi_n} \leq C_i^{EV}, & (15) \\ 0 \leq d_{i,\Phi_n} \leq v_{max}, & (16) \\ R_{\Phi_n} \geq \theta_i, & (17) \end{cases}$$

where α_i is a non-negative satisfaction coefficient, $\eta_i \in (0,1)$ is the charging efficiency, $R_{\Phi_n} = \frac{\sum_{j \in \Phi_n} R_j}{|\Phi_n|}$ is the average

reputation value of PCP coalition Φ_n, and d_{i,Φ_n} is the energy demand of EV i in PCP coalition Φ_n. The first term in (13) means the charging satisfaction [23]. ε_i is the unit cost of battery degradation of EV i, ξ is the unit energy consumption rate, l_{i,Φ_n} is the distance between EV i and PCP coalition Φ_n, and $l_{i,grid}$ is the distance between EV i and the public charging station. The fourth term in (13) means the saved expenditure that charging in PCP coalition Φ_n with unit price p_{Φ_n} instead of the public charging station with unit price p_{grid}. δ_1 is the fixed cost for EVs, e.g., operation fee for charging and transaction fee in the blockchain. (14) and (15) are battery energy constraints, where C_i^{EV} is the battery capacity of EV i. (16) is the energy demand constraint. (17) means that only PCP coalitions whose average reputation value is greater than the threshold θ_i can provide charging service for EV i for secure charging.

For PCP j in coalition Φ_n in LAG m, its utility function can be used to measure the QoE and is defined as

$$V_j(\Phi_n) = s_j \cdot \left(\sum_{i\in\Gamma_n} p_{\Phi_n} d_{i,\Phi_n} - \sum_{i\in\Gamma_n} c_{\Phi_n} d_{i,\Phi_n} - |\Phi_n|\,\delta_2\right), \tag{18}$$

$$s.t. \begin{cases} p_{\Phi_n} \le p_{grid}, & (19)\\ |\Gamma_n| \le |\Phi_n|, & (20)\\ \sum_{i\in\Gamma_n} d_{i,\Phi_n} \le \sum_{j\in\Phi_n} E_j^{PV}, & (21)\\ R_i \ge \theta_{\Phi_n}, \forall i \in \Gamma_n, & (22) \end{cases}$$

where s_j is the contribution of PCP j in PCP coalition Φ_n, which is associated with its reputation value R_j and available clean energy resources E_j^{PV}, i.e., $s_j = \frac{R_j E_j^{PV}}{\sum_{j\in\Phi_n} R_j E_j^{PV}}$. Γ_n is the set of EVs that is accepted to receive charging service in coalition Φ_n, p_{Φ_n} is the charging price of coalition Φ_n, c_{Φ_n} is the charging cost of coalition Φ_n, and δ_2 is the fixed cost for the coalition. (19) is the charging price constraint. (20) means the number of EVs charging in coalition Φ_n should be no more than the total available charging outlets. (21) means the total charging demand of EVs in Γ_n should be no more than the available solar energy resource in coalition Φ_n. (22) means that only trustworthy EVs whose reputation value is larger than the threshold θ_{Φ_n} can be accessed to coalition Φ_n to enhance the sharing security.

Secondly, we analyze the optimal strategies of EV users on the energy demand in different PCP coalitions. Here, the first derivative of EV i's utility function with respect to d_{i,Φ_n} is

$$\frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} = \frac{\alpha_i \eta_i R_{\Phi_n}}{1+\eta_i R_{\Phi_n} d_{i,\Phi_n}} - \varepsilon_i + p_{grid} - p_{\Phi_n}. \tag{23}$$

The second derivative of $U_i(\Phi_n)$ with respect to d_{i,Φ_n} satisfies

$$\frac{\partial^2 U_i(\Phi_n)}{\partial {d_{i,\Phi_n}}^2} = -\frac{\alpha_i \eta_i^2 {R_{\Phi_n}}^2}{\left(1+\eta_i R_{\Phi_n} d_{i,\Phi_n}\right)^2} < 0, \tag{24}$$

which implies that $U_i(\Phi_n)$ is strictly concave with respect to d_{i,Φ_n}. Furthermore, we have

$$\lim_{d_{i,\Phi_n}\to 0} \frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} = p_{\theta_1} - p_{\Phi_n}, \tag{25}$$

$$\lim_{d_{i,\Phi_n}\to v_{max}} \frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} = p_{\theta_2} - p_{\Phi_n}. \tag{26}$$

Here, we define $p_{\theta_1} = \alpha_i \eta_i R_{\Phi_n} - \varepsilon_i + p_{grid}$ and $p_{\theta_2} = \frac{\alpha_i \eta_i R_{\Phi_n}}{1+\eta_i R_{\Phi_n} v_{max}} - \varepsilon_i + p_{grid}$ as the critical prices and consider the following three cases:

Case 1: If $p_{grid} \ge p_{\Phi_n} \ge p_{\theta_1}$, since $p_{\theta_1} > p_{\theta_2}$, we have $\lim_{d_{i,\Phi_n}\to 0} \frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} \le 0$ and $\lim_{d_{i,\Phi_n}\to v_{max}} \frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} < 0$. Therefore, the optimal charging demand is $d^*_{i,\Phi_n} = 0$. In this case, there does not exist any energy trading between EV i and PCP coalition Φ_n.

Case 2: If $0 < p_{\Phi_n} \le p_{\theta_2}$, we can derive that $\lim_{d_{i,\Phi_n}\to 0} \frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} > 0$ and $\lim_{d_{i,\Phi_n}\to v_{max}} \frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} \ge 0$. Therefore, the optimal charging demand is $d^*_{i,\Phi_n} = v_{max}$.

Case 3: If $p_{\theta_2} < p_{\Phi_n} < p_{\theta_1}$, we have $\lim_{d_{i,\Phi_n}\to 0} \frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} > 0$ and $\lim_{d_{i,\Phi_n}\to v_{max}} \frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} < 0$. Therefore, the optimal charging demand can be resolved by $\frac{\partial U_i(\Phi_n)}{\partial d_{i,\Phi_n}} = 0$, i.e.,

$$d^*_{i,\Phi_n} = \frac{\alpha_i}{\varepsilon_i + p_{\Phi_n} - p_{grid}} - \frac{1}{\eta_i R_{\Phi_n}}. \tag{27}$$

Above all, the optimal strategy of EV i on energy demand from PCP coalition Φ_n is denoted as:

$$d^*_{i,\Phi_n} = \begin{cases} 0, & p_{\theta_1} \le p_{\Phi_n} \le p_{grid} \\ \frac{\alpha_i}{\varepsilon_i + p_{\Phi_n} - p_{grid}} - \frac{1}{\eta_i R_{\Phi_n}}, & p_{\theta_2} < p_{\Phi_n} < p_{\theta_1} \\ v_{\max}, & 0 < p_{\Phi_n} \le p_{\theta_2}. \end{cases} \tag{28}$$

To find the stable matching pairs between EVs and PCP coalitions, a matching algorithm is presented in Algorithm 1. Here, a linear pricing function is adopted to determine the charging price of each PCP coalition by considering the remaining energy resources, i.e.,

$$p_{\Phi_n} = \frac{\kappa_{\Phi_n} R_{\Phi_n}}{E_{\Phi_n} - D_{\Phi_n} + 1} + \chi_{\Phi_n}, \tag{29}$$

where $E_{\Phi_n} - D_{\Phi_n}$ denotes the residual solar energy of coalition Φ_n, κ_{Φ_n} is the price parameter, and χ_{Φ_n} is the cost parameter.

Theorem 1*:* The matching results $\Psi^* = \{\Psi_m^*\}_{m=1}^M$ derived from the Algorithm 1 is stable.

Proof. Obviously, Algorithm 1 can converge since users' preference lists, i.e., EPL and CPL, are finite. Assume that there exists a case where EV $i, i' \in \mathcal{I}$ are assigned to PCP coalitions $\Phi_n, \Phi_{n'} \in \Pi_m$, respectively, in the stable matching results. If there exists a blocking pair (Φ_n, i') such that EV i' prefers PCP coalition Φ_n to $\Phi_{n'}$ and PCP coalition Φ_n prefers EV i' to i. Then, according to steps 3–14 in Algorithm 1, EV i' should be assigned to PCP coalition Φ_n, which contradicts with the condition that EV i' is assigned to PCP coalition $\Phi_{n'}$. Thus, the blocking pair does not exist and the matching results obtained from Algorithm 1 is guaranteed to be stable. Theorem 1 is proved.

V. PERFORMANCE EVALUATIONS

A. Simulation Setup

We consider three communities in PCPSN and each community contains 10 PCPs. The available hourly solar energy of each PCP is uniformly distributed in $[8, 15]$ kWh. The social relation values among users follow a uniform distribution

Algorithm 1 Many-to-one Matching Algorithm

Input: The charging price of each PCP coalition p_{Φ_n}, the total solar energy of each coalition $E_{\Phi_n} = \sum_{j \in \Phi_n} E_j^{PV}$, and the optimal energy demand of each EV d^*_{i,Φ_n}.
Output: The stable matching pairs $\Psi^*_m = \{AccList_n\}_{n=1}^{|\Pi_m|}, \forall m \in \mathcal{M}$.
Repeat
Each EV i ranks the order of coalitions and stores them in its preference list EPL_i based on its utility defined in (13) and constraints (14)–(17).
EV i chooses the first item in EPL_i to request energy.
Each PCP coalition Φ_n filters EVs that send charging request to itself and satisfy constraint (22). Then, it stores the ranking of EVs in its preference list CPL_n in descending order based on its utility $\Omega(\Phi_n) = \sum_{j \in \Phi_n} V_j(\Phi_n)$, where $V_j(\Phi_n)$ is defined in (18).
if $|CPL_n| \leq |\Phi_n|$ and $\sum_{i \in CPL_n} d_{i,\Phi_n} \leq E_{\Phi_n}$ **then**
  Each PCP coalition Φ_n accepts all charging requests in CPL_n, and stores into its acceptance list $AccList_n$.
else
  Each PCP coalition Φ_n selects the set $\Gamma_n \subseteq CPL_n$ to provide charging services by solving the problem:

$$\arg\max_{\Gamma_n} \{\Omega(\Phi_n)\} = \arg\max_{\Gamma_n} \left\{\sum_{i \in \Gamma_n} d_{i,\Phi_n}\right\} \quad s.t.(20)(21). \tag{30}$$

  Each PCP coalition updates its acceptance list by $AccList_n = \Gamma_n$, and rejects other EVs in $CPL_n \backslash \Gamma_n$.
  Each PCP coalition updates the number of available charging outlets $|\Phi_n|$, and the used clean energy resources D_{Φ_n}.
end if
Until $AccList_n$ of all PCP coalitions remains unchanged.

TABLE I
SIMULATION PARAMETERS

Parameters	Values	Parameters	Values
v_{max}	15 kWh	C_i^{EV}	$[20, 30]$ kWh
α_i	$[1.5, 2]$	$so_{i,j}$	$[0, 1]$
η_i, ε_i	$0.85, 2.5$	$\theta_i, \theta_{\Phi_n}$	$0.7, 0.7$
ξ_i	0.1	δ_1, δ_2	$0.2, 0.2$
p_j	$[4, 5]$cent/kWh	c_j	$[0.2, 0.4]$cent/kWh
p_{grid}	6.5 cent/kWh	$l_{i,m}$	$\{0.5, 1.2, 2.0\}$mile

within $[0, 1]$. The rating of each EV/PCP on a malicious or normal PCP/EV is random in $[0, 0.5]$ or $(0.5, 1]$, respectively. The ratios of malicious PCP and malicious EV are equal to 0.6. Other parameters are listed in Table I.

The following metrics are used to evaluate the performance of the proposed scheme. *Secure sharing efficiency (SSE):* the proportion of clean energy demanded by normal EVs to the total clean energy supply of PCPs. *Average utility of EVs:* the average of EVs' utilities during energy trading in PCPSN.

B. Simulation Results

We compare the proposed scheme with the matching scheme without reputation evaluation (MWR) [24] and the random scheme. In the MWR scheme, the charging service is scheduled by the matching game while the reputation evaluation and the PCP coalitions are absent. In the random scheme, each EV selects the PCP and obtains the energy demand from PCPs at random.

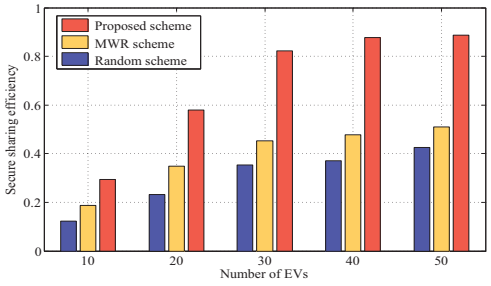

Fig. 2. SSE versus number of EVs in different schemes.

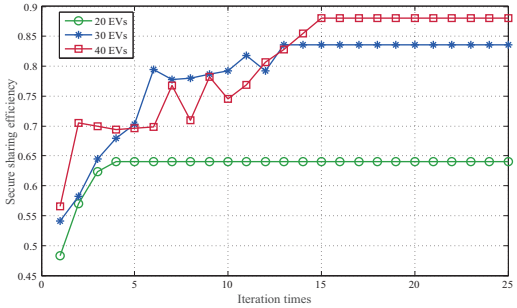

Fig. 3. SSE versus number of matching iterations.

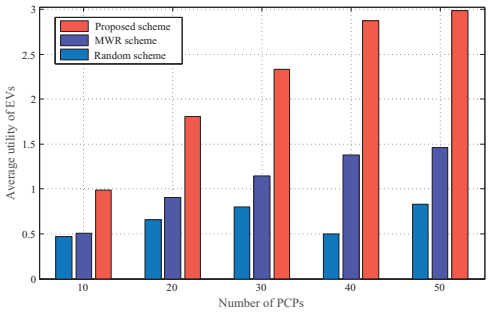

Fig. 4. Average utility of EVs versus number of PCPs in different schemes.

Fig. 2 shows the SSE in three schemes when the number of EVs changes. It can be seen that the proposed scheme outperforms other schemes by achieving a higher SSE. In the MWR scheme, due to the absence of reputation evaluation, the customers of PCPs' charging services can be malicious EVs. In the random scheme, the solar energy resources are randomly allocated to EVs where a part of resources may not be used. In the proposed scheme, EVs and PCP coalitions can form the optimal matching pairs to improve energy efficiency through Algorithm 1. In addition, trustworthy PCPs and EVs can be selected through the proposed reputation model to provide and receive secure charging services in PCPSNs, respectively.

Fig. 3 presents the convergence of the proposed many-to-one matching algorithm when the number of EVs varies. From Fig. 3, it can be seen that the SSE with 20, 30, 40 EVs is converged to be stable by 4, 13, 15 iterations, respectively. The fewer number of EVs in the simulation, the faster convergence to the stable SSE. Moreover, since more clean energy resources are allocated by more EVs, the simulation with a larger number of EVs can obtain a higher SSE.

Fig. 4 demonstrates the average utility of EVs in three schemes when the number of PCPs changes. Here, the number of EVs is set as $I = 40$. It can be observed that our proposal attains a higher average utility for EVs than other two schemes, and the average utility of EVs increases with the increase of the number of PCPs. The reason is that, in the MWR scheme, each PCP has limited clean energy resource and the cooperation among PCPs is absent. Thus, EVs with higher energy demand may not attain satisfied energy resources in the MWR scheme, resulting in a relative lower average utility. In the random scheme, EVs randomly obtain clean energy resources from PCPs without cooperation and competition, causing the average utility of EVs is low. In the proposed scheme, on one hand, PCPs can cooperatively form coalitions to reallocate energy resources within each coalition. On the other hand, EVs and PCP coalitions can compete with each other to attain the optimal matching results via the proposed matching algorithm. Thus, EVs can achieve optimal utilities in the proposal.

VI. Conclusion

In this paper, we have proposed a blockchain-based secure PCP sharing scheme with EVs in PCPSNs. Based on BLS multi-signature, a secure PCP sharing protocol is developed to efficiently implement the blockchain into PCPSNs. A reputation model is designed to identify malicious users while considering users' social features. To optimally schedule the charging process, we further present a matching game to optimally schedule the energy strategies of EVs and PCPs. In addition, simulation results show that our proposal outperforms other conventional schemes with improved RE efficiency, better user utility, and enhanced charging security. In the future work, we will extend this work by considering the existence of discharging EVs in PCPSNs.

Acknowledge

This work is supported in part by NSFC (no. 61571286, U1808207, 91746114), and Shanghai Key Laboratory of Power Station Automation Technology.

References

[1] Z. Moghaddam, I. Ahmad, D. Habibi and Q. V. Phung, "Smart Charging Strategy for Electric Vehicle Charging Stations," *IEEE Transactions on Transportation Electrification*, vol. 4, no. 1, pp. 76–88, Mar. 2018.

[2] Global EV Outlook Understanding the Electric Vehicle Landscape to 2020. [Online]. Available: https://www.iea.org/publications/freepublications/publication/Global_EV_Outlook_2016.pdf, 2016.

[3] H. Zhang, Z. Hu, Z. Xu and Y. Song, "An Integrated Planning Framework for Different Types of PEV Charging Facilities in Urban Area," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2273–2284, Sep. 2016.

[4] Y. Hou, Y. Chen, Y. Jiao, J. Zhao, H. Ouyang, P. Zhu, D. Wang and Y. Liu, "A resolution of sharing private charging piles based on smart contract," *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Guilin*, pp. 3004–3008, 2017.

[5] E. Thompson, R. Ordonez-Hurtado, W. Griggs, J. Y. Yu, B. Mulkeen and R. Shorten, "On charge point anxiety and the sharing economy," *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), Yokohama*, pp. 1–6, 2017.

[6] Y. Cao, T. Wang, O. Kaiwartya, G. Min, N. Ahmad and A. H. Abdullah, "An EV Charging Management System Concerning Drivers' Trip Duration and Mobility Uncertainty," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 4, pp. 596–607, Apr. 2018.

[7] C. Luo, Y. Huang and V. Gupta, "Stochastic Dynamic Pricing for EV Charging Stations With Renewable Integration and Energy Storage," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1494–1505, Mar. 2018.

[8] J. Li, C. Li, Y. Xu, Z. Y. Dong, K. P. Wong and T. Huang, "Noncooperative Game-Based Distributed Charging Control for Plug-In Electric Vehicles in Distribution Networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 1, pp. 301–310, Jan. 2018.

[9] S. Huckle, R. Bhattacharya, M. White and N. Beloff, "Internet of Things, Blockchain and Shared Economy Applications," *Procedia Computer Science*, vol. 98, pp. 461–466, 2016.

[10] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[11] D. Boneh, M. Drijvers and G. Neven, "Compact Multi-signatures for Smaller Blockchains," *Advances in Cryptology – ASIACRYPT 2018, Springer*, vol. 11273, pp. 435–464, 2018.

[12] R. Zhang, X. Cheng and L. Yang, "Energy Management Framework for Electric Vehicles in the Smart Grid: A Three-Party Game," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 93–101, 2016.

[13] Y. Song, Y. Zheng and D. J. Hill, "Optimal Scheduling for EV Charging Stations in Distribution Networks: A Convexified Model," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1574–1575, Mar. 2017.

[14] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino and G. Zizzo, "A Technical Approach to the Energy Blockchain in Microgrids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4792–4803, Nov. 2018.

[15] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 1 Sep-Oct. 2018.

[16] 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 Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[17] X. Huang, C. Xu, P. Wang and H. Liu, "LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[18] T. Ma and O. A. Mohammed, "Optimal Charging of Plug-in Electric Vehicles for a Car-Park Infrastructure," *IEEE Transactions on Industry Applications*, vol. 50, no. 4, pp. 2323–2330, 2014.

[19] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[20] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian and N. Zhang, "A Secure Charging Scheme for Electric Vehicles with Smart Communities in Energy Blockchain," *IEEE Internet of Things Journal*. doi: 10.1109/JIOT.2018.2869297, 2018.

[21] M. Conti, E. Sandeep Kumar, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[22] Y. Wang, Z. Su and N. Zhang, "BSIS: Blockchain based Secure Incentive Scheme for Energy Delivery in Vehicular Energy Network," *IEEE Transactions on Industrial Informatics*. doi: 10.1109/TII.2019.2908497.

[23] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing and T. Basar, "Dependable Demand Response Management in the Smart Grid: A Stackelberg Game Approach," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, Mar. 2013.

[24] M. Zeng, S. Leng, Y. Zhang and J. He, "QoE-Aware Power Management in Vehicle-to-Grid Networks: A Matching-Theoretic Approach," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2468-2477, Jul. 2018.