A Secure Charging Scheme for Electric Vehicles With Smart Communities in Energy Blockchain

Zhou Su, Yuntao Wang, Qichao Xu, Minrui Fei, Yu-Chu Tian, and Ning Zhang

***Abstract*—The smart community (SC), as an important part of the Internet of Energy (IoE), can facilitate integration of distributed renewable energy sources and electric vehicles (EVs) in the smart grid. However, due to the potential security and privacy issues caused by untrusted and opaque energy markets, it becomes a great challenge to optimally schedule the charging behaviors of EVs with distinct energy consumption preferences in SC. In this paper, we propose a contract-based energy blockchain for secure EV charging in SC. First, a permissioned energy blockchain system is introduced to implement secure charging services for EVs with the execution of smart contracts. Second, a reputation-based delegated Byzantine fault tolerance consensus algorithm is proposed to efficiently achieve the consensus in the permissioned blockchain. Third, based on the contract theory, the optimal contracts are analyzed and designed to satisfy EVs' individual needs for energy sources while maximizing the operator's utility. Furthermore, a novel energy allocation mechanism is proposed to allocate the limited renewable energy for EVs. Finally, extensive numerical results are carried out to evaluate and demonstrate the effectiveness and efficiency of the proposed scheme through comparison with other conventional schemes.**

***Index Terms*—Contract theory, electric vehicles (EVs), energy blockchain, Internet of Energy (IoE), smart community (SC).**

I. Introduction

RENEWABLE energy sources (RES) and electric vehicles (EVs), hold great potential to ease fossil fuel crisis and reduce gas emissions, which have attracted worldwide attentions [1]–[3]. According to [4]–[6], renewable energy is projected to equal coal and natural gas electricity generation by 2040, and the EV stock will reach 140 million in 2030. However, the rapid RES deployment and the booming EV development can inevitably lead to the profound and everlasting influence on the current smart grid architecture. To integrate and coordinate a large number of distributed RES and EVs, the Internet of Energy (IoE) has emerged as a promising and innovative approach to improve the energy efficiency and sustainability [7]–[9]. Moreover, equipped with RES, a smart community (SC) can be considered as an important component of the IoE, which enables the internal energy generation, storage, and distribution and can exchange energy with external energy entities, e.g., the power grid and EVs [10]–[12]. In the presence of SC, it is desirable to charge a group of EVs using the distributed RES in a cost effective way [13]–[15].

Microgrids are small-scale power systems powered by distributed RES, e.g., solar energy, wind energy, hydropower, etc, which have been demonstrated as a feasible and effective strategy to integrate local available RES into the smart grid [16], [17]. In an SC integrated with microgrids, it allows energy suppliers and consumers to trade energy directly. Such local electricity trading not only reduces the power loss that occurs in electricity transmission but also mitigates the burden of the power grid. As a result, the framework of EV charging in SC involves three energy parties, i.e., the power grid, microgrids, and EVs. Recently, various literatures have been reported to improve the performance of EV charging [18]–[20]. However, most of them only consider two-sided interactions between EVs and microgrids or the power grid and cannot be directly applied to the charging management of EVs in SC. In addition, EV users have different charging preferences on various energy sources in SC, e.g., the clean energy, the traditional energy, or the mixture of them. Therefore, in the presence of SC, it is of necessity to charge a group of EVs considering both the power grid providing traditional energy and microgrids supplying clean energy.

Malicious operators of energy market will heavily threaten EV's security and privacy through various malicious exploitations [21]–[23], e.g., privacy leakage, falsification, node impersonation, advertising fraudulent charging service, etc. To provide secure charging services for EVs, many incentive mechanisms have been proposed and implemented [24], [25], e.g., trust mechanism and monetary approach. However, trust mechanism is neither sustainable nor susceptible for sybil attack and whitewashing attack, while monetary approach relies on trusted centers. Trusted centers may not only leak users' privacy for profit but are vulnerable to be attacked. Blockchain has provided a unique technology for secure energy transaction in a distributed network without trusted agents through the use of an immutable ledger, cryptocurrency, and the execution of smart contracts [26]. The agents execute a consensus protocol for transaction validation, block

Manuscript received June 14, 2018; revised August 21, 2018; accepted August 28, 2018. Date of publication September 10, 2018; date of current version June 19, 2019. This work was supported in part by the Key Project of Science and Technology Commission of Shanghai Municipality under Grant 15220710400, in part by the NSFC under Grant 91746114, Grant 61571286, Grant 61633016, and Grant 61533010, and in part by the Shanghai Key Laboratory of Power Station Automation Technology. *(Corresponding authors: Zhou Su; Minrui Fei; Yu-Chu Tian.)*

Z. Su, Y. Wang, Q. Xu, and M. Fei are with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200072, China (e-mail: zhousu@ieee.org; mrfei@staff.shu.edu.cn).

Y.-C. Tian is with the School of Electrical Engineering and Computer Science, Queensland University of Technology, Brisbane, QLD 4000, Australia (e-mail: y.tian@qut.edu.au).

N. Zhang is with the Department of Computing Science, Texas A&M University at Corpus Christi, Corpus Christi, TX 78412 USA.

Digital Object Identifier 10.1109/JIOT.2018.2869297

generation, and hash chain building over the blocks [27]. However, the widely used proof-of-work consensus protocol wastes a massive expenditure of energy and has slow confirmation of transactions in traditional blockchain applications [28], such as bitcoin. Thus, it is not adaptable in the permissioned energy blockchain. Therefore, it is still an open and vital issue to resolve the security problems for EV charging in SC.

In this paper, to address the aforementioned problems, we exploit a contract theory-based EV charging scheme in SC, secured by permissioned blockchain technology. First, by introducing a novel permissioned energy blockchain system in SC, the preselected EVs can publicly audit and share transaction records without reliance on a trusted intermediary. Afterward, a reputation-based delegated Byzantine fault tolerance (DBFT) consensus algorithm is presented to reach the consensus in an efficient manner in the permissioned energy blockchain. Furthermore, based on the contract theory, the optimal contracts are analyzed and designed by the monopolistic operator to meet EVs' individual energy demand tastes. Finally, a novel energy allocation mechanism is proposed to allocate the limited RES for EVs while maximizing the operator's utility.

In a nutshell, the main contributions of this paper are threefold as follows.

1) First, based on the permissioned blockchain technology, we present a secure EV charging framework in an energy blockchain system in SC, where the preselected EVs can publicly audit and share transaction records without reliance on a trusted intermediary. To reduce the cost of establishing a blockchain in energy-limited EVs, we propose a reputation-based DBFT consensus algorithm within the permissioned energy blockchain context.
2) Second, we leverage the contract game to model the decision process between the aggregator and EVs in the presence of asymmetric information. In the proposed contract game, the aggregator designs the contract menu containing its trading strategies toward all types of EVs. Within the proposed framework, EVs can choose either the traditional energy, clean energy, or the mixture of them to satisfy their individual energy tastes, while maximizing the operator's utility.
3) Third, we propose a dynamic optimal contract assignment and energy allocation algorithm to achieve the optimal contracts and address the problem that the optimal strategies for all EVs may not be always met due to the intermittent and unstable RES supply. We carry out extensive simulation experiments to validate the effectiveness and efficiency of the proposed scheme. It is demonstrated that our proposal can improve both the operator's and EVs' utilities, compared with conventional schemes.

The remainder of this paper is organized as follows. Related work is reviewed in Section II. The system model is introduced in Section III. The energy blockchain is proposed in Section IV. The optimal contract design is proposed in Section V. Performance evaluations are shown in Section VI. The conclusion and the future work are given in Section VII.

II. Related Work

A. Smart Community

Liang *et al.* [29] proposed an efficient service searching scheme for privacy preserving in an SC consisted of networked smart homes. Zhang *et al.* [30] reviewed typical incentive approaches in the smart grid and investigated the cloud-based vehicle-to-vehicle (V2V) energy trading process via a contract theoretical approach. An incentive game-based mechanism for distributed renewable energy management in SC was studied by Tushar *et al.* [31] to improve the operator's profit and minimize the total cost in energy trading.

Bera *et al.* [32] presented a novel cooperative energy consumption framework among communities in the smart grid to mitigate energy consumption cost of users and reduce peak-to-average ratio. Milanes-Montero *et al.* [33] investigated a global control strategy for electric energy micro-storage system in SC to improve the local power quality of demanded current and global power consumption. Common communication security issues and attacks in SCs, especially the GPS spoofing attacks, were researched by He *et al.* [34] and the security mechanisms against GPS spoofing attacks were also studied.

B. Energy Blockchain

Kang *et al.* [35] proposed a novel peer-to-peer (P2P) energy trading model with a consortium blockchain approach to address the privacy preserving and transaction security issues for plug-in hybrid EVs. Based on multisignatures and anonymous encryption methods, Aitzhan and Svetinovic [36] presented a token-based decentralized energy trading system to enable peers to perform transaction anonymously and securely. Li *et al.* [37] exploited the consortium blockchain method to secure distributed energy trading market and formulated a novel energy blockchain system in the industrial IoT.

A novel announcement network named credit-coin was presented by Li *et al.* [38] via blockchain technology to protect vehicles' privacy and motivate users to share traffic information. Mattila *et al.* [39] provided a pragmatic blockchain use case for machine-to-machine energy transactions in a housing society environment. Based on the lightning network and smart contract in the energy blockchain ecosystem, Huang *et al.* [40] presented a decentralized security model to enhance the security of trading between EVs and charging piles in the P2P network.

C. EV Charging Scheduling

Zou *et al.* [19] designed a progressive second price auction game-based mechanism to resolve the large-scale EV charging cooperation problem while ensuring incentive compatibility over a finite horizon. Mohammadi *et al.* [20] proposed a distributed cooperative charging scheme for plug-in EVs (PEVs) to minimize the charging cost for PEV fleets using a receding horizon method. A novel renewable energy pricing scheme in SC was studied by Liu and Hu [10] to minimize the total electricity bill among residential users by using an advanced cross-entropy optimization technique in smart home energy scheduling.

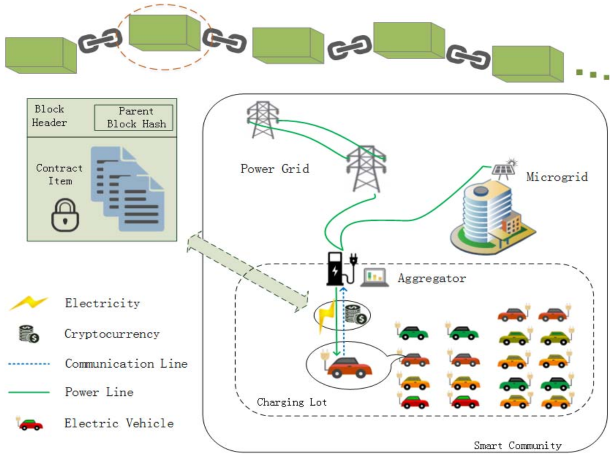


Fig. 1. System model.

A contract game-based direct energy trading framework was proposed by Zhang *et al.* [41] to model the decision making process of electricity operators and consumers in vehicular edge computing network. Yang *et al.* [42] presented the coordinate EV charging mechanism in a microgrid powered by wind power generators via a Markov decision process approach. By using stochastic dynamic programming methods, Wu *et al.* [43] investigated the energy management in a smart home integrated with PEVs to address the problem of intermittent RES supply while minimizing the electricity cost.

III. System Model

A. Network Model

Blockchain is an open, distributed data storage mechanism which is designed to efficiently record transactions among participants without a trusted intermediary. Blockchain can be either public, where transactions are verified by groups of independent nodes, or permissioned, where only authorized individuals can process new transactions [44]. Blockchain is a continuously growing sequence of blocks, each hash-chained with the previous block. As shown in Fig. 1, the permissioned energy blockchain system in a SC is mainly composed of the following entities.

1) Aggregator: The aggregator in SC acts as a monopolistic operator of the energy market, which operates multiple charging piles and coordinates the charging behaviors of a group of EVs in the charging lots. The aggregator can obtain energy from both the power grid and the local microgrid, i.e., photovoltaics (PV) systems. On one hand, the aggregator manages all rooftop solar panels installed in multiple buildings in SC and sells the harvested solar energy to EVs. On the other hand, the aggregator purchases energy from the power grid with unit price p_g and sells the traditional energy to EVs.

2) EVs: The set of EVs in the charging lots in SC is denoted as $\mathcal{I} = \{1, \ldots, i, \ldots, I\}$. EVs, as the energy consumers, can choose to purchase energy either from the power grid, or PV systems, or the mixture of them in SC. EVs with different energy consumption preferences are classified into different types. We define θ_i as the desired perception of clean energy in the total energy consumption of EV i. The set of EV types is defined as $\Theta = \{\theta_1, \theta_2, \ldots, \theta_I\}$. To some extent, θ_i indicates the preference or the type of EV i and is only known by itself. Moreover, the aggregator has no exact knowledge about EV's preference θ_i, but it knows the distribution of EV's type θ_i. Without loss of generality, we assume $\underline{\theta} = \theta_1 < \theta_2 < \cdots < \theta_I = \overline{\theta}$, and $0 \le \underline{\theta} < \overline{\theta} \le 1$.

3) Smart Meters: A built-in smart meter in each EV records the amount of energy consumption to verify whether the transaction has been accomplished to authorize the payment.

4) Microgrid: The PV system, as the local microgrid in SC, is operated by the aggregator and is made up of multiple solar panels installed on the rooftop of community buildings. Suppose the number of solar panels in SC is K and the solar irradiance at time slot t is $I_{\text{light}}(t)$. Let η_{pv} and S be the energy conversion efficiency and the area of each solar panel, respectively. Thus, the energy output of solar panels at time slot t can be achieved through the following formula [45]:

$$E_{\text{pv}}(t) = \eta_{\text{pv}} \cdot S \cdot K \cdot I_{\text{light}}(t). \tag{1}$$

Due to the intermittent and unstable characteristics of solar energy generation, the energy storage system (ESS) is often used to balance the solar energy supply and demand. When the solar energy is surplus, ESS will be in charging state, otherwise it is in discharging state when facing shortages of solar energy. Let $E_{\text{ess}}(t)$ and C_{ess} represent the battery energy of ESS and the capacity of ESS, respectively. To prolong the battery life, we have $0.2C_{\text{ess}} \le E_{\text{ess}}(t) \le C_{\text{ess}}$ [46]. Let $E_{\text{res}}(t)$ be the total available clean energy supply for EV charging. Thus, we have

$$E_{\text{res}}(t) = E_{\text{pv}}(t) + \eta_{\text{ess}}(E_{\text{ess}}(t) - 0.2C_{\text{ess}}) \tag{2}$$

where η_{ess} denotes the discharging efficiency of ESS.

B. Utility Function

The monopolistic operator provides a set of the energy quantities $\{x(\theta_i) \in \Omega\}$ and the corresponding prices $\{\pi(\theta_i) \in \Pi\}$ for its customers. Here, the set of contract items consisting of the energy-price combinations is defined as $\Psi = \{(x(\theta_i), \pi(\theta_i)) | \, \forall \theta_i \in \Theta\}$. Where $x(\theta_i)$ is the energy demand of type-θ_i EV, and $\pi(\theta_i)$ represents the price that type-θ_i EV pays to the aggregator for energy consumption. Obviously, the energy demand of EV can neither be negative nor infinity, i.e., $\Omega = \{x(\theta_i) | 0 \le x(\theta_i) \le (C_i/\eta_i)\}$, where η_i is the charging efficiency of EV i, and C_i is the capacity of EV i, respectively. Besides, EVs can decide whether to receive charging services from the aggregator or not. Where $x(\theta_i) = 0$ indicates that EV i will not purchase any electricity from the aggregator and correspondingly will not pay any price to the aggregator.

Each EV user is a risk-averse agent in the energy market, where the utility function should be a concave, nondecreasing function of its demand for energy. If EV i chooses the contract item $(x(\theta_i), \pi(\theta_i))$, its utility function can be defined as

$$U(\theta_i, x(\theta_i)) = V(\theta_i, x(\theta_i)) - \pi(\theta_i) \tag{3}$$

where $V(\theta_i, x(\theta_i))$ is the satisfaction function that EV i achieves from energy consumption. Based on [31],

[47], and [48], the natural logarithmic function has been extensively accepted in modeling the utilities of energy buyers. Thus, we use the logarithmic function to model the relationship between EV's satisfaction and demand including the clean energy demand and traditional energy demand, which is shown as [49]

$$V(\theta_i, x(\theta_i)) = \alpha \ln[1 + \omega\theta_i x(\theta_i) + \omega_0(1-\theta_i)x(\theta_i)] \tag{4}$$

where α is the non-negative satisfaction coefficient, ω is the environmental friendliness coefficient representing the cleanliness of RES generation, and ω_0 indicates the cleanliness of traditional fossil energy. In general, we assume $\omega > \omega_0 > 0$. It is easy to see that $([\partial V(\theta_i, x(\theta_i))]/\partial\theta_i) \geq 0$, $([\partial V(\theta_i, x(\theta_i))]/\partial x(\theta_i)) > 0$, and $([\partial^2 V(\theta_i, x(\theta_i))]/\partial x(\theta_i)^2) < 0$. EV i will choose the contract item $(x(\theta_i) = 0, \pi(\theta_i) = 0)$ if its utility is negative. It is obvious that $V(\theta_i, 0) = 0$ and $U(\theta_i, 0) = 0$.

Here, we define $R(x(\theta_i))$ as the utility of the aggregator that obtains from a contract item $(x(\theta_i), \pi(\theta_i))$ of EV i. Then we have

$$R(x(\theta_i)) = \pi(\theta_i) - C(\theta_i, x(\theta_i)). \tag{5}$$

Obviously, a rational aggregator would not accept negative utility from a specific charging service. Thus we can conclude that $\Pi = \{\pi(\theta_i)|\pi(\theta_i) \geq C(\theta_i, x(\theta_i))\}$. The cost function is composed of the cost of solar energy generation, the payment for purchasing electricity from the power grid, and the subsidy offered by the government, which can be expressed as

$$C(\theta_i, x(\theta_i)) = \left(c_{\text{pv}} - r_{\text{pv}}\right)\theta_i x(\theta_i) + p_g(1-\theta_i)x(\theta_i) + c_0 \tag{6}$$

where c_{pv} and r_{pv} are the unit cost and the unit subsidy for energy generation of solar panels, respectively. $c_0 > 0$ is the fixed cost mainly including transaction cost, storage cost, etc. For generality, we assume that $0 \leq c_{\text{pv}} - r_{\text{pv}} \leq p_g$, which means that the ultimate unit cost of RES generation is no more than the electricity market price of the power grid. Then we can obtain $([\partial C(\theta_i, x(\theta_i))]/\partial\theta_i) \leq 0$, $([\partial C(\theta_i, x(\theta_i))]/\partial x(\theta_i)) \geq 0$, and $([\partial^2 C(\theta_i, x(\theta_i))]/\partial x(\theta_i)^2) = 0$. Thus, for the aggregator, the overall utility function can be written as

$$R = \sum_{i=1}^{I} \tau_{\theta_i}(\pi(\theta_i) - C(\theta_i, x(\theta_i))) \tag{7}$$

where τ_{θ_i} describes the ratio of type-θ_i EVs in all EVs. We have $\tau_{\theta_i} = [N_{\theta_i}/(\sum_{i\in\mathcal{I}} N_{\theta_i})]$, where N_{θ_i} is the number of type-θ_i EVs. We further define the social surplus in the energy trading between the aggregator and the specific EV as the sum of both utilities, i.e.,

$$\begin{aligned} S(\theta_i, x(\theta_i)) &= R(x(\theta_i)) + U(\theta_i, x(\theta_i)) \\ &= V(\theta_i, x(\theta_i)) - C(\theta_i, x(\theta_i)). \end{aligned} \tag{8}$$

According to (4) and (6), we can conclude $([\partial^2 S(\theta_i, x(\theta_i))]/\partial x(\theta_i)^2) < 0$. Similarly, the overall social surplus in the energy market can be written as

$$S = \sum_{i=1}^{I} \tau_{\theta_i}[V(\theta_i, x(\theta_i)) - C(\theta_i, x(\theta_i))]. \tag{9}$$

Algorithm 1 Smart Contract Implementation Algorithm

Init():
Input: i, ID_i, $pNum_i$
$\{Cer_i, PK_i, SK_i, address_i\} \leftarrow$ register(ID_i, $pNum_i$)
Create():
Input: $deposit_s$, $deposit_i$, x_i, π_i, $pPrice$, $tTime$, $tStamp$
verify($deposit_s$), verify($deposit_i \geq \pi_i$)
Invoke():
Input: m_s, m_i
verify($t \geq tTime$)
$Penalty_s \leftarrow$ penalty(x_i, m_s, m_i, $pPrice$)
send(i, $deposit_i - \pi_i + Penalty_s$)
send(s, $deposit_s + \pi_i - Penalty_s$)

For simplicity, in what follows, we rewrite τ_{θ_i}, N_{θ_i}, $x(\theta_i)$, and $\pi(\theta_i)$ as τ_i, N_i, x_i, and π_i, respectively.

C. Attack Model

In SC, malicious participants in energy market may threaten EV's security and privacy. Here, we define the following three kinds of attackers or adversaries.

1) *Malicious Energy Provider:* A malicious aggregator who advertises fraudulent charging services without enough solar energy.
2) *Malicious Energy Consumer:* A malicious EV pretends that it has not received any charging service from the aggregator and refuses to pay the money.
3) *Malicious Trusted Third Party:* The malicious trust center may not only disclose EV's privacy but tamper EV's reputation value for profit. While the reputation value of each EV is stored in the trust center in trust mechanism [50].

IV. ENERGY BLOCKCHAIN

A. Smart Contract

Within the blockchain context, a smart contract is a set of digital commitments resided on the blockchain that contract participants are agreed with [51]. Smart contracts permit credible transactions to be executed automatically in a prescribed manner among disparate, anonymous parties without third parties. Here, a detailed overview of the smart contract implementation is presented in Algorithm 1.

1) The *Init* function performs system initialization. After registration at a trusted authority, e.g., a government department, EV i gets its certificate Cer_i which is used to uniquely identify itself through binding its identity ID_i and license plate number $pNum_i$. EV i joins the blockchain network with its certificate Cer_i and gets its public/private key pair (PK_i, SK_i) and wallet address $address_i$. Here, the aggregator's account contains its wallet address $address_s$, available RES E_{res}, account balance $Balance_s$, and public/private key pair (PK_s, SK_s). Each EV's account includes its wallet address $address_i$, account balance $Balance_i$, current credit value cr_i, reputation value Re_i, certificate Cer_i, and public/private key pair $(\text{PK}_i, \text{SK}_i)$. To ensure the authenticity and integrity of information transmission, asymmetric encryption technology is employed in the

blockchain. If

$$D_{PK_i}\big(\mathrm{Sig}_{SK_i}(H(m))\big) = H(m) \tag{10}$$

then the data integrity and unforgeability can be guaranteed. Where $\mathrm{Sig}_{SK_i}(\cdot)$ is the digital signature of sender i with its private key, $D_{PK_i}(\cdot)$ is the decryption function with sender i's public key, and $H(m)$ is the hash digest of message m.

2) The *Create* function deploys a new smart contract to the blockchain after the aggregator and EV i make an agreement on the contract items and sign with their private keys, respectively. After reaching consensus in the blockchain network, which is detailedly presented in Section IV-B, a smart contract is successfully deployed and can be accessed by all network agents. Each smart contract maintains a set of state variables including the seller's and buyer's account addresses $(account_s, account_i)$, the energy demand x_i, the corresponding payment π_i, the transaction time *tTime*, the timestamp *tStamp*, and the penalty price *pPrice*. To ensure the implementation of the smart contract, the aggregator and EV i should move enough deposit from their wallet addresses to the contract address, respectively, to prevent a malicious seller/buyer from advertising/submitting a fraudulent charging service.

3) The *Invoke* function can be called after reaching consensus. Then, the smart contract executes automatically if $t \geq$ *tTime* and performs the energy transaction and financial settlement. The smart contract reads inputs from both seller's and buyer's smart meters (m_s, m_i) to verify whether the amount of electricity has been produced and consumed, respectively. Any necessary penalties will be assigned by calling the *Penalty* function. Afterward, the system periodically updates the state ledger of blockchain, such as the balances in the buyers' accounts, the residual energy in sellers' accounts, and the state variables in smart contracts.

Here, the charging process can be simplified as follows. EV first makes a new smart contract with the aggregator through energy blockchain network. Then it will navigate to the charging lot in SC and wait for charging service. Once the trading conditions are satisfied, the smart contract will execute automatically and perform the corresponding energy and cryptocurrency exchange between the buyer and the seller in a prescribed manner.

B. Consensus Process

To ensure that each node has a copy of the recognized version of the whole ledger, the public audit stage, i.e., the consensus process should be carried out. Based on [52], a reputation-based DBFT consensus algorithm is proposed in Algorithm 2 to reach consensus efficiently in the energy blockchain. The consensus process needs to go through the following steps.

1) Leader Election: EVs have two types of roles in the V2V network: ordinary nodes and consensus nodes. Ordinary nodes only relay, transfer, exchange, and accept ledger data, while consensus nodes are authorized to perform the consensus process. Any EV node can vote for a delegator, i.e., a consensus node, in the V2V network. The voting weight of each node is determined by its stake, i.e., reputation value. The top M delegators by voting are selected, denoted as the set $\mathcal{M} = [1, \ldots, m, \ldots, M]$. Based on [52], we assume that $M \geq 3f + 1$, where f is the maximum number of malicious nodes in the V2V network. Here, the time interval of block generation and delegator election are denoted as ΔT_1 and ΔT_2, respectively. The reputation value Re_i of EV node $i \in \mathcal{I}$ is defined as

$$Re_i = \frac{\sum_{j=0}^{\xi} cr_{i,j} \cdot \varphi_j}{\xi + 1} \tag{11}$$

Algorithm 2 Reputation-Based DBFT Consensus Algorithm

1: $v = 0$, $k = 1$. All nodes get the same block height h by synchronizing the blocks.
2: The leader p is determined by using (13).
3: **Input:** transaction set $\mathcal{Q}$
4: **for** $m \in \mathcal{M}$ **do**
5:   **for** $tx \in \mathcal{Q}$ **do**
6:     **if** verifyTx(tx) = true **then**
7:       $S_{tx} \leftarrow$simulate(tx)
8:       $\mathcal{S}_m \leftarrow S_{tx}$
9:     **else**
10:       $\mathcal{Q}_m \leftarrow \mathcal{Q} \backslash \{tx\}$
11:     **end if**
12:   **end for**
13:   $\mathcal{B}_m \leftarrow$ buildBlock($\mathcal{Q}_m, \mathcal{S}_m$)
14: **end for**
15: **if** $m = p$ **then**
16:   broadcast $\big\langle$Proposal, $h, \upsilon, p, \mathcal{B}, Sig_{SK_m}(H(\mathcal{B}))\big\rangle$;
17: **end if**
18: **Input:** candidate block $\mathcal{B}$, local state set $\mathcal{S}_i$
19: **for** $m \in \mathcal{M}$ and $m \neq p$ **do**
20:   **if** verifyBlock($\mathcal{B}$) = false **then**
21:     go to step 33;
22:   **end if**
23:   $S_p \leftarrow$ getState($\mathcal{B}$)
24:   **if** $\mathcal{S}_p = \mathcal{S}_m$ **then**
25:     broadcast $\Big\langle$Confirm, $h, \upsilon, m, Sig_{SK_p}(H(\mathcal{B}))\Big\rangle$;
26:   **else**
27:     go to step 33;
28:   **end if**
29:   **if** $t \leq \Delta T_1$ and count(*confirmMsg*) $\geq M - f$ **then**
30:     $cr_m := cr_m + \Delta_1, \forall m \in \mathcal{M} \backslash \{p\}$, $cr_p := cr_p + \Delta_2$.
31:     publish a new block $\mathcal{B}$ and begin the next round;
32:   **else**
33:     $v_k = v + k$;
34:     broadcast $\langle$ChangeView, $h, \upsilon, m, v_k\rangle$;
35:     **if** count(v_k) $\geq M - f$ **then**
36:       $v = v_k$, $cr_m := cr_m + \Delta_1$, $cr_p := cr_p - \Delta_2$.
37:       go to step 2;
38:     **else**
39:       $k := k + 1$, go to step 33;
40:     **end if**
41:   **end if**
42: **end for**

where φ_j is the time decay function which captures the nature that previous credit value may be out of date quickly. ξ is the current times of election and can be obtained by $\xi = \lfloor t/\Delta T_2 \rfloor$, where t is the current time slot and $\lfloor\cdot\rfloor$ is the floor function. $cr_{i,j}$ is the credit value of node i within jth election interval. Here, the exponential decay function is adopted for modeling the time decay, which is given as

$$\varphi_j = e^{-\lambda\cdot(\xi - j)} \tag{12}$$

where $\lambda > 0$ is the rate of decay. Here, the credit value is initialized by $cr_{i,0} = 1, \forall i \in \mathcal{I}$. If $Re_i \leq Re_{\min}$, EV i will be added into the blacklist and will never have the chance to perform the consensus process, where $Re_{\min}$ is a predefined threshold. To stimulate EVs to join in the consensus process, we assume that EVs with higher reputation value can enjoy more community welfare, e.g., higher charging priority, shorter charging queuing time, etc.

Here, the leader p in the consensus nodes is determined by

$$p = (h - v) \bmod M + 1 \tag{13}$$

where h is the current block height, v is the index of view, initialized by $v = 0$.

2) Building Block Concurrently: The detailed process is shown in steps 3–17, where $\mathcal{Q}_m$ is the transaction set, $\mathcal{S}_m$ is the state set, tx is a transaction record, S_{tx} is the changed state after executing the smart contract that transaction tx specifies, $\mathcal{B}_m$ is the local block created by node m, $verifyTx(tx)$ is to verify the validity of a transaction tx, $simulate(tx)$ is to simulatively execute the smart contract that transaction tx specifies, $bulidBlock(\mathcal{Q}_m, \mathcal{S}_m)$ is to build local block with the transaction set $\mathcal{Q}_m$ and the state set $\mathcal{S}_m$.

When a smart contract is made between EV i and the aggregator, EV i broadcasts it to the network. All consensus nodes collect all transactions during a certain time and validate each transaction independently before relaying it. Invalid transactions are discarded. Then consensus nodes simulatively execute the smart contracts and record the changed states into their local state ledgers, respectively. All valid transactions are collected by each consensus node during a certain period, ordered by the timestamp and packaged into a block concurrently. Each block contains a cryptographic hash to the prior block in the blockchain. After all nonleader consensus nodes have already completed this process, the delegated leader will broadcast the *proposalMsg* message in step 16 and send its candidate block to other consensus nodes.

In the sequential model [53], the leader first builds the candidate block, then the rest of consensus nodes build their local blocks. By comparison, in the proposed concurrent model, the consensus nodes build local blocks in parallel, which can significantly shorten the time of verifying a candidate block.

3) Verifying Candidate Block: The detailed process is shown in steps 18–42, where $\mathcal{S}_p$ is the state set in the received block, $verifyBlock(\mathcal{B})$ is to verify the validity of the received block, $getState(\mathcal{B})$ is to get the states from the received block.

Each nonleader consensus node compares the local state set with the state set in the received block. If the verification passes, each nonleader consensus node broadcasts the *confirmMsg* message with its signature in the network in step 25. Otherwise, the view change will be triggered and the nonleader consensus node will broadcast the *changeviewMsg* message in step 34. Once any consensus node receives at least $M-f$ same v_k from distinct consensus nodes, the view change is finished and the next round of consensus process will start. If consensus node m doubts the proposal received from leader p and triggers the view change successfully, then the credit value of consensus node m, current leader p will be changed by Δ_1 and $-\Delta_2$ in step 36, respectively, where $\Delta_2 > \Delta_1 > 0$.

4) Publishing New Block: Any consensus node, upon receiving no less than $M - f$ amount of *confirmMsg* message from other distinct consensus nodes within ΔT_1, reaches consensus and publishes a new block. Then the credit value of each consensus node m and leader p' who eventually produces the block will be increased by Δ_1 and Δ_2 as a reward in step 30, respectively. After reaching consensus, the new block is added into the blockchain in a linear and chronological order, which contains a cryptographic hash to the prior block. Any node synchronizes its local copy of the blockchain with the new block and prepares for the next round of consensus process.

Based on [52], our proposal provides $f = \lfloor (M-1)/3 \rfloor$ fault tolerance to a consensus system which comprises M consensus nodes, and the blockchain system cannot be forked within the tolerance range.

Through the execution of smart contracts, the trading process, i.e., the energy and cryptocurrency exchange, can be executed automatically and safely in the untrusted energy market. If a malicious aggregator advertises fraudulent charging services without enough RES, the corresponding punishment will be carried out according to the smart contract. Additionally, each transaction is recorded in the recognized ledger in the blockchain, and EVs cannot deny it.

In the energy blockchain system, all reputation values are recorded in the blockchain instead of the centralized trust center. On one hand, due to overwhelming cost, it is hard to compromise all consensus nodes in the blockchain network to tamper the current credit value. On the other hand, since each block is hash-chained with the previous one, the historical reputation values and transactions in each block are unforgeable.

V. Optimal Contract Design

In this section, based on the contract theory, we analyze the optimal contracts that are made between the aggregator and each EV in Section IV-A to maximize the utilities of both sides. First, we present the feasibility of the contract. Then the optimal contracts are analyzed. Finally, an energy allocation mechanism is designed in limited energy trading market.

A. Contract Formulation

According to the revelation principle [54], a feasible contract means that each self-interested EV truthfully selects the contract item for its type to maximize its utility. Based on the contract theory [55], a contract is feasible if the following two constraints are satisfied simultaneously for all types of EVs.

Definition 1: Individual rationality (IR) constraint, whereby type-θ_i EV receives a non-negative utility by choosing the contract item (x_i, π_i), i.e.,

$$\alpha \ln[1 + (\omega\theta_i + \omega_0(1 - \theta_i))x_i] - \pi_i \geq 0 \quad \forall\theta_i \in \Theta. \quad (14)$$

Definition 2: Incentive compatible (IC) constraint, whereby type-θ_i EV would prefer to choose the contract item for type θ_i rather than that for type θ_j, i.e.,

$$\begin{aligned} &\alpha \ln[1 + (\omega\theta_i + \omega_0(1 - \theta_i))x_i] - \pi_i \\ &\quad \geq \alpha \ln\big[1 + (\omega\theta_i + \omega_0(1 - \theta_i))x_j\big] - \pi_j \quad \forall\theta_j \neq \theta_i. \end{aligned} \quad (15)$$

Thus the aggregator, as the contract designer, will establish the optimal contracts for all types of EVs, denoted by the set $\Psi^* = \{(x_i^*, \pi_i^*), \forall\theta_i \in \Theta\}$, to maximize its utility as follows:

$$\begin{aligned} \mathcal{P}1 : \quad &\max_{\{(x_i \in \Omega, \pi_i \in \Pi)\}} \sum_{i=1}^{I} \tau_i(\pi_i - C(\theta_i, x_i)) \\ &\text{s.t.} \quad \begin{cases} \text{IR constraint in (14)} \\ \text{IC constraint in (15).} \end{cases} \end{aligned} \quad (16)$$

B. Feasibility of Contract

Note that the above maximization problem has I amount of IR constraints and $I(I-1)$ amount of IC constraints, the computational complexity of solving $\mathcal{P}1$ grows rapidly as the number of EVs, i.e., I, increases. To attain the solution of $\mathcal{P}1$, IR and IC constraints should be simplified. We first consider reducing IR constraints through Lemma 1.

Lemma 1: Suppose IC constraint in (15) holds for all types of EVs, then IR constraint in (14) can be replaced by

$$\alpha \ln[1 + (\omega\theta_1 + \omega_0(1 - \theta_1)x_1)] - \pi_1 \geq 0. \quad (17)$$

Proof: Since IC constraint holds for all EV types which satisfy $\theta_1 < \theta_2 < \cdots < \theta_I$, then we have

$$\begin{aligned} &\alpha \ln[1 + (\omega\theta_i + \omega_0(1 - \theta_i))x_i] - \pi_i \\ &\quad \geq \alpha \ln[1 + ((\omega - \omega_0)\theta_i + \omega_0)x_1] - \pi_1 \\ &\quad \geq \alpha \ln[1 + ((\omega - \omega_0)\theta_1 + \omega_0)x_1] - \pi_1. \end{aligned} \quad (18)$$

To satisfy IR constraint for all types of EVs, we only need to guarantee that $\alpha \ln[1 + ((\omega - \omega_0)\theta_1 + \omega_0)x_1] - \pi_1 \geq 0$. This completes our proof. ■

Next, we present the necessary conditions for IC constraints through Lemmas 2 and 3.

Lemma 2: If EV's utility function satisfies the Spence-Mirrless condition (SMC), then for any $\theta_i > \theta_j$ and $x_i \geq x_j$, $\forall i, j \in \mathcal{I}$, the following inequality holds:

$$V(\theta_i, x_i) - V\big(\theta_i, x_j\big) \geq V\big(\theta_j, x_i\big) - V\big(\theta_j, x_j\big). \quad (19)$$

Proof: Obviously, it holds when $x_j = 0$ due to $V(\theta_i, 0) = V(\theta_j, 0) = 0$ and $([\partial V(\theta, x)]/\partial\theta) \geq 0$. In the case that $x_i \geq x_j > 0$, note that the SMC holds, i.e., $(\partial/\partial\theta)[-([\partial U/\partial x]/[\partial U/\partial\pi])] > 0$, then we can obtain $([\partial^2 V(\theta, x)]/[\partial x \partial\theta]) > 0$. By the fundamental theorem of calculus, we have

$$\begin{aligned} &V(\theta_i, x_i) - V\big(\theta_i, x_j\big) - V\big(\theta_j, x_i\big) + V\big(\theta_j, x_j\big) \\ &\quad = \int_{x_j}^{x_i} \frac{\partial V(\theta_i, x)}{\partial x} dx - \int_{x_j}^{x_i} \frac{\partial V\big(\theta_j, x\big)}{\partial x} dx \\ &\quad = \int_{x_j}^{x_i} \left(\int_{\theta_j}^{\theta_i} \frac{\partial^2 V(\theta, x)}{\partial x \partial\theta} d\theta \right) dx \\ &\quad \geq 0. \end{aligned} \quad (20)$$

This completes our proof. ■

Lemma 3: For any contract satisfies IC constraint, the monotonicity constraint holds, i.e., $x_i \geq x_j$, if and only if $\theta_i \geq \theta_j$.

Proof: Since IC constraints are satisfied for both EV type θ_i and θ_j, then we have $V(\theta_i, x_i) - \pi_i \geq V(\theta_i, x_j) - \pi_j$ for type-θ_i EV, and $V(\theta_j, x_j) - \pi_j \geq V(\theta_j, x_i) - \pi_i$ for type-θ_j EV. Combining the above two equations, we can obtain

$$V(\theta_i, x_i) + V\big(\theta_j, x_j\big) \geq V\big(\theta_i, x_j\big) + V\big(\theta_j, x_i\big). \quad (21)$$

Substituting (4) into (21), we can simplify (21) as $\alpha(\omega - \omega_0)(\theta_i - \theta_j)(x_i - x_j) \geq 0$. Thus, if $\theta_i \geq \theta_j$, we have $x_i \geq x_j$ due to $\omega > \omega_0$. This completes our proof. ■

Then, we present the corresponding sufficient conditions for IC constraints through Lemmas 4 and 5.

Lemma 4 [Local Downward Incentive Constraints (LDICs)]: For all types θ_i, $i \in \mathcal{I}$, if the LDICs are satisfied, i.e.,

$$V(\theta_i, x_i) - \pi_i \geq V(\theta_i, x_{i-1}) - \pi_{i-1} \quad (22)$$

and $x_1 \leq x_2 \leq \cdots \leq x_I$, then for $\forall j \leq i, j \in \mathcal{I}$, IC constraints will hold, i.e., $V(\theta_i, x_i) - \pi_i \geq V(\theta_i, x_j) - \pi_j$.

Proof: Consider the LDICs for three types $\theta_{i-1} < \theta_i < \theta_{i+1}$, we have

$$V(\theta_{i+1}, x_{i+1}) - \pi_{i+1} \geq V(\theta_{i+1}, x_i) - \pi_i \quad (23)$$

and (22). According to Lemma 2, since the SMC is satisfied, for $\theta_{i+1} > \theta_j$ and $x_i \geq x_{i-1}$, we have

$$V(\theta_{i+1}, x_i) - V(\theta_{i+1}, x_{i-1}) \geq V(\theta_i, x_i) - V(\theta_i, x_{i-1}). \quad (24)$$

According to (22)–(24), we have

$$V(\theta_{i+1}, x_{i+1}) - \pi_{i+1} \geq V(\theta_{i+1}, x_{i-1}) - \pi_{i-1}. \quad (25)$$

By iterating, we can conclude that the LDICs hold for all types $\theta_j, \forall j \leq i$, indicating that IC constraints are satisfied. This completes our proof. ■

Lemma 5 [Local Upward Incentive Constraints (LUICs)]: For all types θ_i, $i \in \mathcal{I}$, if the LUICs are satisfied, i.e.,

$$V(\theta_i, x_i) - \pi_i \geq V(\theta_i, x_{i+1}) - \pi_{i+1} \quad (26)$$

and $x_1 \leq x_2 \leq \cdots \leq x_I$, then for $\forall j \geq i, j \in \mathcal{I}$, IC constraints will hold, i.e., $V(\theta_i, x_i) - \pi_i \geq V(\theta_i, x_j) - \pi_j$.

Proof: This proof is similar to Lemma 4. ■

Here, we summarize the necessary and sufficient conditions for feasible contracts through the following lemma.

Lemma 6: For any contract $\Psi = \{(x_i, \pi_i)\}, i = 1, 2, \ldots, I$, its feasibility is equivalent to the following constraints:

$$\begin{cases} x_1 \leq x_2 \leq \cdots \leq x_I & (27) \\ 0 \leq \pi_1 \leq V(\theta_1, x_1) & (28) \\ \pi_{k-1} + \phi \leq \pi_k \leq \pi_{k-1} + \varphi, k = 2, 3, \ldots, I & (29) \end{cases}$$

where $\phi = V(\theta_{k-1}, x_k) - V(\theta_{k-1}, x_{k-1})$ and $\varphi = V(\theta_k, x_k) - V(\theta_k, x_{k-1})$.

Proof: see Appendix A. ■

In addition, we prove that the best price is unique for any fixed feasible energy demands through Lemma 7.

Lemma 7: If the aggregator's utility is maximized with fixed demand $x_1 \le x_2 \le \cdots \le x_I$, then the unique optimal price $\{\pi_i^*\}$ satisfies

$$\begin{cases} V(\theta_1, x_1) - \pi_1^* = 0 \\ V(\theta_i, x_i) - \pi_i^* = V(\theta_i, x_{i-1}) - \pi_{i-1}^*, \ i = 2, 3, \ldots, I. \end{cases} \tag{30}$$

Proof: see Appendix B. ■

C. Optimality of Contract

Based on the above analysis in Lemmas 1 − 7, IR and IC constraints can be replaced by (32)–(34), and the optimization problem $\mathcal{P}1$ in (16) can be simplified as

$$\mathcal{P}2: \max_{\{(x_i\in\Omega, \pi_i\in\Pi)\}} \sum_{i=1}^{I} \tau_i(\pi_i - C(\theta_i, x_i)) \tag{31}$$

$$\text{s.t.} \begin{cases} x_1 \le x_2 \le \cdots \le x_I & (32) \\ V(\theta_1, x_1) - \pi_1 = 0 & (33) \\ V(\theta_i, x_i) - \pi_i = V(\theta_i, x_{i-1}) - \pi_{i-1}, i \ge 2. & (34) \end{cases}$$

To derive the optimal contracts in the problem $\mathcal{P}2$, we first solve the relaxed problem without the monotonicity constraint (32), then we check whether the acquired solution meets this constraint. By iterating on (33) and (34), we can acquire the price assignment as follows:

$$\pi_i = V(\theta_1, x_1) + \sum_{k=1}^{i} \varphi_k \tag{35}$$

where

$$\varphi_k = \begin{cases} V(\theta_k, x_k) - V(\theta_k, x_{k-1}), & k = 2, \ldots, I \\ 0, & k = 1. \end{cases} \tag{36}$$

Substituting (35) into (31), the relaxed problem of (31) without monotonicity constraint (32) can be further replaced by

$$\max_{\{(x_i\in\Omega, \pi_i\in\Pi)\}} \sum_{i=1}^{I} \tau_i\left(V(\theta_1, x_1) + \sum_{k=1}^{i} \varphi_k - C(\theta_i, x_i)\right). \tag{37}$$

Let

$$\psi_i = \begin{cases} V(\theta_i, x_i) - V(\theta_{i+1}, x_i), & i = 1, \ldots, I-1 \\ 0, & i = I. \end{cases} \tag{38}$$

Note that $\sum_{i=1}^{I} \tau_i \sum_{k=1}^{i} \varphi_k = \sum_{i=1}^{I} \tau_i V(\theta_i, x_i) + \sum_{i=2}^{I} \tau_i \sum_{k=1}^{i-1} \psi_k$ and $\sum_{i=2}^{I} \tau_i \sum_{k=1}^{i-1} \psi_k = \sum_{i=1}^{I} \psi_i \sum_{k=i+1}^{I} \tau_k$, then we can rewrite (37) as

$$\max_{\{(x_i\in\Omega, \pi_i\in\Pi)\}} \sum_{i=1}^{I} \left(\tau_i V(\theta_i, x_i) + \psi_i \sum_{k=i+1}^{I} \tau_k - \tau_i C(\theta_i, x_i)\right). \tag{39}$$

Let $\Lambda_i = \tau_i V(\theta_i, x_i) + \psi_i \sum_{k=i+1}^{I} \tau_k - \tau_i C(\theta_i, x_i)$, then the optimal demand can be achieved by maximizing Λ_i, i.e.,

$$\bar{x}_i^* = \operatorname*{argmax}_{x_i\in\Omega} \Lambda_i. \tag{40}$$

Obviously, $\bar{x}_i^*$ can be attained at the point which satisfies $(\partial\Lambda_i/\partial x_i)|_{x_i=x_i^*} = 0$ and $(\partial^2\Lambda_i/\partial x_i^2)|_{x_i=x_i^*} < 0$ simultaneously, or at the boundary points, i.e., 0 and (C_i/η_i). If $\Delta > 0$ is satisfied, then the optimal energy demand $\bar{x}_i^*$ can be attained, i.e.,

$$\bar{x}_i^* = \begin{cases} \frac{\alpha AB - AC - BC + \sqrt{\Delta}}{2ABC}, & i = 1, 2, \ldots, I-1 \\ \frac{\alpha}{C} - \frac{1}{A}, & i = I \end{cases} \tag{41}$$

where A, B, C, h, and Δ are abbreviations for

$$\begin{cases} A = \omega\theta_i + \omega_0(1-\theta_i) & (42) \\ B = \omega\theta_{i+1} + \omega_0(1-\theta_{i+1}) & (43) \\ C = \left(c_{\text{pv}} - r_{\text{pv}}\right)\theta_i + p_g(1-\theta_i) & (44) \\ h = \sum_{k=i+1}^{I} \tau_k/\tau_i & (45) \\ \Delta = (\alpha AB - AC - BC)^2 \\ \quad - 4ABC \cdot (C - \alpha A - \alpha(A-B)h). & (46) \end{cases}$$

If $\{\bar{x}_i^*\}$ is a feasible demand assignment, i.e., $\{\bar{x}_i^*\}$ is a nondecreasing sequence, then we have $\{x_i{}^*\} = \{\bar{x}_i^*\}$. However, for general distribution of EV types, $\{\bar{x}_i^*\}$ may be infeasible and should be adjusted by bunching and ironing mechanism [54]. The following lemma is introduced to design such a mechanism.

Lemma 8: Suppose that $X_i(x), i = 1, \ldots, K$ are concave functions on x, and $\bar{x}_i = \operatorname{argmax}_{x_i} X_i(x_i)$. If $\bar{x}_1 \ge \bar{x}_2 \ge \cdots \ge \bar{x}_K$, then we can obtain $x_1^* = x_2^* = \cdots = x_K^*$, where

$$x_k^* = \operatorname*{argmax}_{x_i} \sum_{k=1}^{K} X_i(x_i) \quad \forall k = 1, \ldots, K \tag{47}$$

and $x_1 \le x_2 \le \cdots \le x_K$.

We refer to [56] for the detailed proving process. Accordingly, if $\{\bar{x}_i^*\}$ is infeasible, an infeasible subsequence can be defined as $\{\bar{x}_m^*, \bar{x}_{m+1}^*, \ldots, \bar{x}_n^*\} \subseteq \{\bar{x}_i^*\}$. By means of Lemma 8, we can adjust the infeasible subsequence to be feasible by solving the single variable problem in (47) using a binary searching approach. The detailed process is presented in Algorithm 3, where the maximum iteration number in steps 5–8 is $I - 1$. Therefore, the optimal demand assignment $\{x_i^*\}$ can be derived. Substituting x_i^* into (35), then the optimal price assignment $\{\pi_i^*\}$ can be acquired as

$$\pi_i^* = V\left(\theta_1, x_1^*\right) + \sum_{k=1}^{i} \varphi_k^* \tag{48}$$

where φ_k^* can be obtained by substituting x_k^* and x_{k-1}^* into (36).

D. Energy Allocation

In the above analysis, we assume the total available RES is sufficient for EV charging in optimal contracts, i.e., $E_{\text{res}} \ge \sum_{i=1}^{I} N_i\theta_i x_i^*$, where E_{res} is the total available solar energy for EV charging. However, in practical implements, the solar energy generation in SC is always limited, i.e., $E_{\text{res}} < \sum_{i=1}^{I} N_i\theta_i x_i^*$, especially for the system with a large number of EVs. Thus, a proper energy allocation scheme should be designed to efficiently allocate the limited RES to EVs.

Here, each type-θ_i EV will select the optimal contract (x_i^*, π_i^*) designed by the aggregator. According to (5), the utility of the aggregator by selling energy x_i^* to a type-θ_i EV is

$$R(x_i^*) = \pi_i^* - C(\theta_i, x_i^*). \tag{49}$$

We define $\hat{x}_i$ as the social optimal energy demand for type-θ_i EV, i.e., $\hat{x}_i = \arg\max_{x_i} S(\theta_i, x_i)$, where $S(\theta_i, x_i)$ is the social surplus defined in (8). $\hat{x}_i$ can be attained by the first-order optimality condition for $S(\theta_i, x_i)$ with respect to x_i, i.e., $([\partial S(\theta_i, x_i)]/\partial x_i) = ([\partial V(\theta_i, x_i)]/\partial x_i) - ([\partial C(\theta_i, x_i)]/\partial x_i) = 0$. Here, the aggregator and EVs are assumed to be selfish and rational, so the social optimal demands may not be adopted by both sides in the energy market. However, the maximum social surplus provides an upper bound of the sum of utilities for both sides. Then, the difference between the utilities that the aggregator obtains from a type-θ_{i+1} EV and a type-θ_i EV can be acquired as

$$\begin{aligned} R(x_{i+1}^*) - R(x_i^*) &= \pi_{i+1}^* - \pi_i^* - C(\theta_{i+1}, x_{i+1}^*) \\ &\quad + C(\theta_i, x_i^*) \\ &= V(\theta_{i+1}, x_{i+1}^*) - V(\theta_{i+1}, x_i^*) \\ &\quad - C(\theta_{i+1}, x_{i+1}^*) + C(\theta_i, x_i^*) \\ &= S(\theta_{i+1}, x_{i+1}^*) - S(\theta_{i+1}, x_i^*) + C(\theta_i, x_i^*) \\ &\quad - C(\theta_{i+1}, x_i^*). \end{aligned}$$

To analyze the above utility difference, first we rewrite Λ_i in (40) as $\Lambda_i = \tau_i S(\theta_i, x_i) + \psi_i \sum_{k=i+1}^{I} \tau_k$. Note that $([\partial S(\theta_i, x_i)]/\partial x_i)|_{x_i=\hat{x}_i} = 0$ and $(\partial \Lambda_i/\partial x_i)|_{x_i=x_i^*} = 0$. Since

$$\frac{\partial \psi_i}{\partial x_i} = \frac{\alpha(\omega-\omega_0)(\theta_i-\theta_{i+1})}{[1+(\omega\theta_i+\omega_0(1-\theta_i))x_i]\big[1+(\omega\theta_{i+1}+\omega_0(1-\theta_{i+1}))x_i\big]} < 0$$

and $\tau_i > 0$, then we have $([\partial S(\theta_i, x_i)]/\partial x_i)|_{x_i=x_i^*} > 0$. Since $([\partial^2 S(\theta_{i+1}, x_i)]/\partial {x_i}^2) < 0$, we can conclude that $([\partial S(\theta_i, x_i)]/\partial x_i)$ is monotonically decreasing with x. Thus, due to $([\partial S(\theta_i, x_i)]/\partial x_i)|_{x_i=x_i^*} > ([\partial S(\theta_i, x_i)]/\partial x_i)|_{x_i=\hat{x}_i} = 0$, we have $x_i^* \leq \hat{x}_i$. Considering that $\{x_i^*\}$ is the nondecreasing sequence, we can further obtain

$$x_i^* \leq x_{i+1}^* \leq \hat{x}_{i+1}. \tag{50}$$

Since $([\partial^2 S(\theta_{i+1}, x_i)]/\partial {x_i}^2) < 0$ and $([\partial S(\theta_{i+1}, x_i)]/\partial x_i)|_{x_i=\hat{x}_{i+1}} = 0$, it is obvious that $S(\theta_{i+1}, x)$ is monotonically increasing with x when $x \leq \hat{x}_{i+1}$. Thus, we can obtain $S(\theta_{i+1}, x_{i+1}^*) \geq S(\theta_{i+1}, x_i^*)$. Since $[\partial C(\theta_i, x_i)/\partial \theta_i] = (c_{\text{pv}} - r_{\text{pv}} - p_g)x_i \leq 0$, we have $C(\theta_i, x_i^*) \geq C(\theta_{i+1}, x_i^*)$.

From the above analysis, we can conclude $R(x_{i+1}^*) \geq R(x_i^*)$. It means that the aggregator can achieve higher utility from a higher type EV other than a lower one in optimal contracts. Thus, the aggregator can maximize its utility by selectively selling the RES to EVs with higher type in the limited energy trading market. We define $\theta_c \in \Theta$ as the critical type which satisfies $\sum_{i=c}^{I} N_i \theta_i x_i^* \geq E_{\text{res}}$ and $\sum_{i=c+1}^{I} N_i \theta_i x_i^* < E_{\text{res}}$. The aggregator will sell the limited RES to EVs upon the critical type. Therefore, in limited energy trading, the optimal contract $\tilde{\Psi} = \{(\tilde{x}_i, \tilde{\pi}_i) \mid \forall \theta_i \in \Theta\}$ is given by

$$(\tilde{x}_i, \tilde{\pi}_i) = \begin{cases} (0, 0), & \text{if } \theta_i < \theta_c \\ (x_i^*, \pi_i^*), & \text{if } \theta_i \geq \theta_c. \end{cases} \tag{51}$$

Algorithm 3 Dynamic Optimal Contract Assignment and Energy Allocation Algorithm

1: **Input:** Λ_i, N_i, θ_i, Θ, Ω
2: **for** $\theta_i \in \Theta$ **do**
3: initiate $x_i^* = \bar{x}_i^* = \underset{x_i \in \Omega}{argmax}\, \Lambda_i$ by (40);
4: **end for**
5: **while** $\{x_i^*\}$ is not feasible **do**
6: find an infeasible subsequence $\{\bar{x}_m^*, \bar{x}_{m+1}^*, \cdots, \bar{x}_n^*\}$;
7: assign the optimal demand by

$$x_k^* = \underset{x}{\operatorname{argmax}} \sum_{i=m}^{n} \Lambda_i(x), \forall k = m, m+1, \cdots, n \tag{53}$$

8: **end while**
9: **for** $\theta_i \in \Theta$ **do**
10: assign the optimal price π_i^* by (48);
11: **end for**
12: **if** $E_{res} < \sum_{i=1}^{I} N_i \theta_i x_i^*$ **then**
13: adjust the optimal contracts by (51);
14: **end if**
15: **Output:** The optimal contract $\tilde{\Psi} = \{(\tilde{x}_i, \tilde{\pi}_i) \mid \forall \theta_i \in \Theta\}$, and the maximum utility of the aggregator $\tilde{R}$ by (52).

Obviously, the set of EV type engaged in limited energy trading is $\tilde{\Theta} = \{\theta_c, \theta_{c+1}, \ldots, \theta_I\}$. Note that there must be a part of EVs that cannot acquire energy from the aggregator. Therefore, the overall utility of the aggregator is no longer given by (7) and is denoted as

$$\tilde{R} = \sum_{\theta_i \in \tilde{\Theta}} \tau_i \left(\pi_i^* - C(\theta_i, x_i^*)\right). \tag{52}$$

Here, a dynamic optimal contract assignment and energy allocation algorithm is proposed to obtain the optimal contract in the limited energy trading market, which is presented in steps 12–14 in Algorithm 3.

VI. Performance Evaluations

A. Simulation Setup

In the simulation, we consider the scenario that one aggregator provides feasible contracts for 100 EVs in a SC. The upper and lower bound of EV type are set as 1 and 0, respectively. The daily PV output data is acquired from a typical day in [57]. Other parameters are listed in Table I.

B. Simulation Results

Figs. 2 and 3 show the optimal demand and price with respect to various environmental friendliness coefficient ω, respectively. We observe that both the demand and price in optimal contract increase with ω, as well as the critical type value θ_c. The reason behind is that higher ω indicates higher satisfaction of energy consumption, leading to higher energy demand and correspondingly higher price that each EV should pay to the aggregator. However, due to the total available RES is limited, the aggregator will not provide energy for EVs whose types are lower than the critical type value

TABLE I
SIMULATION PARAMETERS

Parameters	Values
I: the number of EV i.	100
ω_0: the cleanliness of traditional energy.	1
ω: the cleanliness of solar energy.	10
θ_i: the type of EV i.	uniform in [0,1]
C_i: the capacity of EV i.	25 kW
C_{ess}: the capacity of ESS.	100 kW
η_i: the charging efficiency of EV i.	90%
η_{ess}: the discharging efficiency of ESS.	90%
α: the satisfaction coefficient of EV.	4.0
c_{pv}: the unit cost of solar energy generation.	3.0 cents/kWh
r_{pv}: the unit subsidy for solar energy generation.	1.0 cents/kWh
p_g: the market energy price of the power grid.	6.0 cents/kWh
c_0: the fixed cost of the aggregator.	10.0 cents

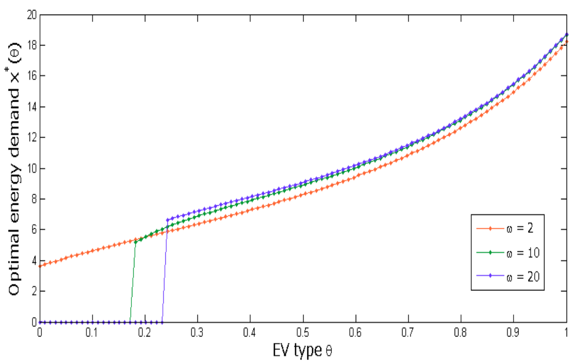


Fig. 2. Optimal energy demand $x^*(\theta)$ with different EV types and ω.

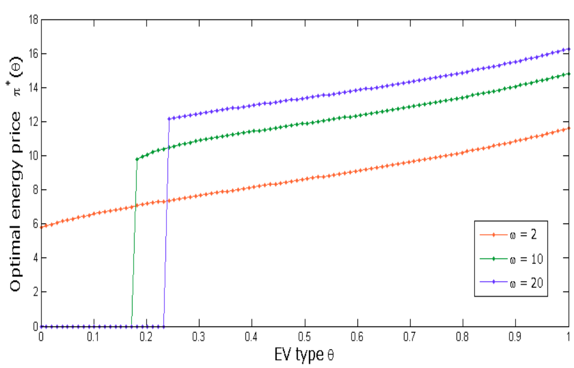


Fig. 3. Optimal energy price $\pi^*(\theta)$ with different EV types and ω.

according to the analysis in Section V-D. Meanwhile, due to higher energy demand of each EV, the critical type value also increases.

Figs. 4 and 5 present the optimal energy demand and price under different distributions of EV type, respectively. In case (a), EV's type θ is independent and follows the uniform distribution. In case (b), EV's type θ is independent and follows the binomial distribution with the parameter $p = 0.5$. The red stellate curves in Figs. 4 and 5 denote the social optimal demand which maximizes the social surplus and the related social optimal price, respectively. It can be seen that the demand in optimal contract is less than the social optimal demand. From economic aspect, comparing with social surplus maximization, the aggregator tends to reduce the demands for EVs with lower type and accordingly raises the prices for EVs with higher

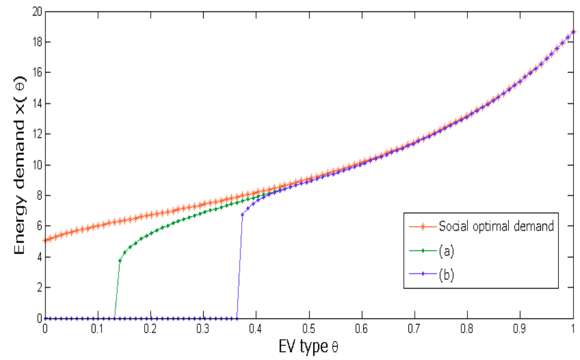


Fig. 4. Energy demand assignments $x(\theta)$ in the optimal contracts with different distributions of EV type θ.

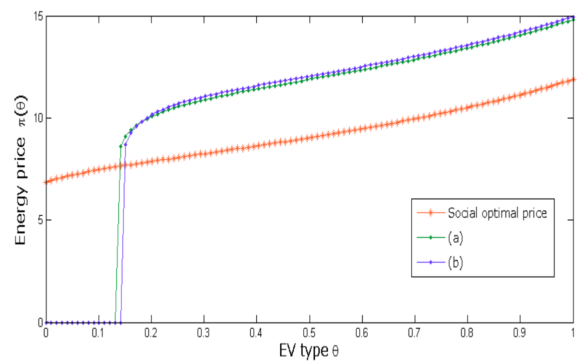


Fig. 5. Energy price assignments $\pi(\theta)$ in the optimal contracts with different distributions of EV type θ.

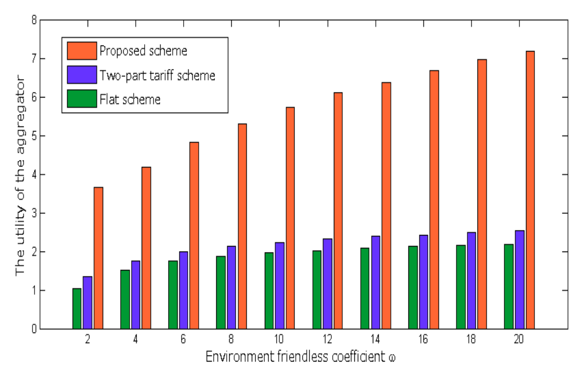


Fig. 6. Operator's utility R in three schemes with different ω.

type for maximizing its utility. Figs. 2 and 4 also prove that the optimal energy demand in the optimal contract satisfies the monotonicity condition, i.e., constraint (32) with various values of ω and different distributions of θ, respectively.

In Figs. 6 and 7, we compare the proposed scheme with two conventional schemes: the two-part tariff scheme and the flat scheme. In the two-part tariff scheme, the relation between energy demand and its corresponding price can be acquired as $\pi(\theta) = P \cdot x(\theta) + Z$, where the operator only specifies a unit energy price P and a constant charging fee Z for each type of EV. In the flat scheme, the unit price P and the charging fee Z are the same for all types of EVs.

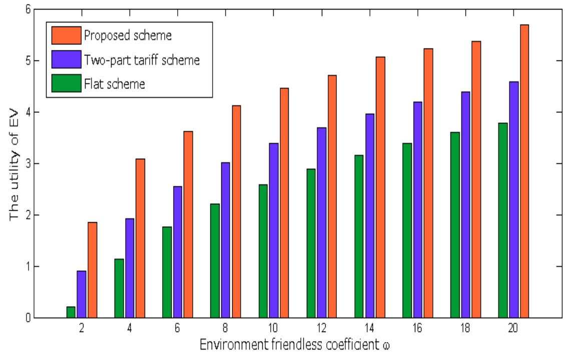


Fig. 7. EV's utility U in three schemes with different ω.

Figs. 6 and 7 illustrate the utility of the operator and 70-th EV under various ω, respectively. The higher ω means cleaner generation of RES, and higher EV's satisfaction of energy consumption. From Fig. 6, our proposal attains higher utility of the aggregator than other two schemes. The utility increases with ω in the proposed scheme and the two-part tariff scheme, while basically stays unchangeable in the flat scheme. In the flat scheme, the unit price is fixed and identical for all types of EVs, thus the operator cannot adjust the unit price for higher utility. In the two-part tariff scheme, the energy price is linear with the energy demand, leading the operator's utility to grow slowly. In the proposal, the relationship between energy price and energy demand is nonlinear, thus the operator's utility is relatively high and can be maximized by designing optimal contracts.

From Fig. 7, our proposal attains higher utility of 70-th EV than other two schemes. The utility increases with ω in three schemes. The reason is that higher ω means higher EV's satisfaction of energy consumption, leading to higher EV's utility. In the two-part tariff scheme, EV can relatively improve its utility than that in the flat scheme since the unit price and the charging fee are adjustable. In the proposal, EV's utility can be maximized by selecting the optimal contracts.

According to the above-mentioned results, the optimal contract in limited energy trading market can be acquired in our proposal. In addition, the aggregator and EV can separately attain an improved utility in the proposed scheme.

VII. Conclusion

In this paper, we have proposed a contract-based secure charging scheme for EVs in energy blockchain system. First, we have formulated an energy blockchain system in SC integrated with EVs and RES. Second, a reputation-based DBFT algorithm has presented to reach the consensus efficiently in the permissioned blockchain. Third, the optimal contracts have been analyzed based on the contract theory to satisfy EVs' individual energy consumption preferences and maximize the operator's utility. Finally, simulation results have shown that the optimal contracts can be acquired and our proposal outperforms the conventional schemes for achieving higher utilities of the operator and EVs. For the future work, we will further extend this paper into the multioperator market with competition influence.

Appendix A
Proof of Lemma 6

1) *Necessity:* First, we prove that if all contracts are feasible, i.e., IR and IC constraints are satisfied, then the above three constraints hold. The necessity of condition (27) can be proved by Lemma 3. The necessity of the conditions (28) and (29) can be proved through IR and IC contractions. According to IR constraint for type θ_1, we have $V(\theta_1, x_1) - \pi_1 \leq 0$. According to IC constraints for type θ_{k-1} and θ_k, we have $V(\theta_{k-1}, x_{k-1}) - \pi_{k-1} \geq V(\theta_{k-1}, x_k) - \pi_k$ and $V(\theta_k, x_k) - \pi_k \geq V(\theta_k, x_{k-1}) - \pi_{k-1}$, respectively. Thus, constraints (27)–(29) hold if all contracts are feasible.

2) *Sufficiency:* Next, we need to prove that if the three conditions are satisfied, then all contracts are feasible. Obviously, if there is only one EV type, then only IR constraint should be considered, i.e., $V(\theta_1, x_1) - \pi_1 \geq 0$. According to constraint (28), we can conclude that in this case the contract is feasible. Since constraint (28) holds, according to Lemma 1, we can conclude all IR constraints hold. Since constraints (27) and (29) are supposed to be met, according to Lemmas 4 and 5, we can conclude all IC constraints hold. Thus, all contracts are feasible if constraints (27)–(29) hold. This completes our proof.

Appendix B
Proof of Lemma 7

1) *Optimality:* It is obvious that the conditions in Lemma 6 are satisfied, then the contract $\Psi = \{(x_i, \pi_i)\}$ is feasible. Here, due to the demand $\{x_i\}$ is fixed, the sum of cost, i.e., $\sum_{i=1}^{I} \tau_i C(\theta_i, x_i)$, is constant. Then the maximum utility can be obtained by maximizing the sum of prices, i.e., $\sum_{i=1}^{I} \tau_i \pi_i$. We assume there exists a feasible price $\{\tilde{\pi}_i\}$ which satisfies $\sum_{i=1}^{I} \tau_i \tilde{\pi}_i > \sum_{i=1}^{I} \tau_i \pi_i^*$. Obviously, there is at least one price $\tilde{\pi}_i > \pi_i^*$. To satisfy the feasibility of the contract, according to Lemma 4, $\{\tilde{\pi}_i\}$ should satisfies $\tilde{\pi}_{i-1} \geq \tilde{\pi}_i - V(\theta_i, x_i) + V(\theta_i, x_{i-1})$. Since $\tilde{\pi}_i > \pi_i^*$, combining with (30), we can obtain

$$\tilde{\pi}_{i-1} > \pi_i^* - V(\theta_i, x_i) + V(\theta_i, x_{i-1}) = \pi_{i-1}^*. \tag{54}$$

Continuing the above process until $i = 2$, we have $\tilde{\pi}_1 > \pi_1^* = V(\theta_1, x_1)$, which contradicts the IR constraint for type θ_1. Thus, $\{\tilde{\pi}_i\}$ does not exist and $\{\pi_i^*\}$ is the optimal price.

2) *Uniqueness:* We assume there is a feasible price assignment $\{\tilde{\pi}_i\} \neq \{\pi_i^*\}$ which satisfies $\sum_{i=1}^{I} \tau_i \tilde{\pi}_i = \sum_{i=1}^{I} \tau_i \pi_i^*$. Clearly, there exists at least one price $\tilde{\pi}_i \neq \pi_i^*$. Without loss of generality, we assume $\tilde{\pi}_i > \pi_i^*$. Here, the same logic leads to the same conclusion that $\tilde{\pi}_1 > \pi_1^* = V(\theta_1, x_1)$. Thus, $\{\tilde{\pi}_i\}$ does not exist and the optimal price in (30) is unique. This completes our proof.

References

[1] H. Peng, L. Liang, X. Shen, and G. Y. Li, "Vehicular communications: A network layer perspective," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2018.2833427.

[2] Q. Xu, Z. Su, Q. Zheng, M. Luo, and B. Dong, "Secure content delivery with edge nodes to save caching resources for mobile users in green cities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2550–2559, Jun. 2018.

[3] T. Fu, P. Liu, Y. Ding, and Y. Zhang, "Secure and efficient large content broadcasting in mobile social networks," *IEEE Access*, vol. 6, pp. 42108–42118, 2018.

[4] Renewables 2016: Global Status Report. *Renewable Energy Policy Network*. Accessed: Jun. 1, 2018. [Online]. Available: http://www.ren21.net/wp-content/uploads/2016/06/GSR2016FullReport.pdf

[5] *Global EV Outlook Understanding the Electric Vehicle Landscape to 2020*. Accessed: Jun. 1, 2018. [Online]. Available: https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2016.pdf

[6] Z. Su *et al.*, "An edge caching scheme to distribute content in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5346–5356, Jun. 2018.

[7] Y. Wu, L. P. Qian, J. Zheng, H. Zhou, and X. S. Shen, "Green-oriented traffic offloading through dual connectivity in future heterogeneous small cell networks," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 140–147, May 2018.

[8] X. Liu, Y. Liu, A. Liu, and L. T. Yang, "Defending ON-OFF attacks using light probing messages in smart sensors for industrial communication systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3801–3811, Sep. 2018, doi: 10.1109/TII.2018.2836150.

[9] Y. Wu, J. Chen, L. P. Qian, J. Huang, and X. S. Shen, "Energy-aware cooperative traffic offloading via device-to-device cooperations: An analytical approach," *IEEE Trans. Mobile Comput.*, vol. 16, no. 1, pp. 97–114, Jan. 2017.

[10] Y. Liu and S. Hu, "Renewable energy pricing driven scheduling in distributed smart community systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 5, pp. 1445–1456, May 2017.

[11] Y. Wang, Z. Su, and Q. Xu, "A game theoretical charging scheme for electric vehicles in smart community," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, 2018, pp. 1–5.

[12] H. Peng *et al.*, "Resource allocation for cellular-based inter-vehicle communications in autonomous multiplatoons," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11249–11263, Dec. 2017.

[13] X. Cheng, R. Zhang, and L. Yang, "Consumer-centered energy system for electric vehicles and the smart grid," *IEEE Intell. Syst.*, vol. 31, no. 3, pp. 97–101, May/Jun. 2016.

[14] S. Bahrami and M. Parniani, "Game theoretic based charging strategy for plug-in hybrid electric vehicles," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2368–2375, Sep. 2014.

[15] N. Rahbari-Asr and M.-Y. Chow, "Cooperative distributed demand management for community charging of PHEV/PEVs based on KKT conditions and consensus networks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 1907–1916, Aug. 2014.

[16] L. K. Wiginton, H. T. Nguyen, and J. M. Pearce, "Quantifying rooftop solar photovoltaic potential for regional renewable energy policy," *Comput. Environ. Urban Syst.*, vol. 34, no. 4, pp. 345–357, 2010.

[17] M. Huang, A. Liu, N. Xiong, T. Wang, and A. V. Vasilakos, "A low-latency communication scheme for mobile wireless sensor control systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2018.2833204.

[18] J. Spínola, P. Faria, and Z. Vale, "Model for the integration of distributed energy resources in energy markets by an aggregator," in *Proc. IEEE Manchester PowerTech*, 2017, pp. 1–6.

[19] S. Zou, Z. Ma, X. Liu, and I. Hiskens, "An efficient game for coordinating electric vehicle charging," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2374–2389, May 2017.

[20] J. Mohammadi, G. Hug, and S. Kar, "A fully distributed cooperative charging approach for plug-in electric vehicles," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3507–3518, Jul. 2018.

[21] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 88–98, Aug. 2017.

[22] S. Paul and Z. Ni, "Vulnerability analysis for simultaneous attack in smart grid security," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, 2017, pp. 1–5.

[23] Z. Su *et al.*, "A secure content caching scheme for disaster backup in fog computing enabled mobile social networks," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2018.2849984.

[24] J. Wang, J. Tang, D. Yang, E. Wang, and G. Xue, "Quality-aware and fine-grained incentive mechanisms for mobile crowdsensing," in *Proc. IEEE 36th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2016, pp. 354–363.

[25] Y. Wu *et al.*, "Optimal power allocation and scheduling for non-orthogonal multiple access relay-assisted networks," *IEEE Trans. Mobile Comput.*, to be published, doi: 10.1109/TMC.2018.2812722.

[26] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[27] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[28] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[29] X. Liang, K. Zhang, R. Lu, X. Lin, and X. Shen, "EPS: An efficient and privacy-preserving service searching scheme for smart community," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3702–3710, Oct. 2013.

[30] K. Zhang *et al.*, "Incentive-driven energy trading in the smart grid," *IEEE Access*, vol. 4, pp. 1243–1257, 2016.

[31] W. Tushar *et al.*, "Three-party energy management with distributed energy resources in smart grid," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2487–2498, Apr. 2015.

[32] S. Bera, S. Misra, and D. Chatterjee, "C2C: Community-based cooperative energy consumption in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4262–4269, Sep. 2018.

[33] M. I. Milanes-Montero *et al.*, "Smart community electric energy micro-storage systems with active functions," *IEEE Trans. Ind. Appl.*, vol. 54, no. 3, pp. 1975–1982, May/Jun. 2018.

[34] D. He, S. Chan, Y. Qiao, and N. Guizani, "Imminent communication security for smart communities," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 99–103, Jan. 2018.

[35] J. Kang *et al.*, "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.

[36] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2016.

[37] Z. Li *et al.*, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[38] L. Li *et al.*, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[39] J. Mattila *et al.*, "Industrial blockchain platforms: An exercise in use case development in the energy industry," Res. Inst. Finnish Econ., Helsinki, Finland, ETLA Working Papers, Oct. 2016.

[40] 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.

[41] B. Zhang, C. Jiang, J. Yu, and Z. Han, "A contract game for direct energy trading in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2873–2884, Jul. 2018.

[42] Y. Yang *et al.*, "Distributed coordination of EV charging with renewable energy in a microgrid of buildings," *IEEE Trans. Smart Grid*, to be published.

[43] X. Wu, X. Hu, X. Yin, and S. Moura, "Stochastic optimal energy management of smart home with PEV energy storage," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 2065–2075, May 2018.

[44] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Honolulu, HI, USA, 2017, pp. 557–564.

[45] W. Tushar, J. A. Zhang, C. Yuen, D. B. Smith, and N. Ul Hassan, "Management of renewable energy for a shared facility controller in smart grid," *IEEE Access*, vol. 4, pp. 4269–4281, 2016.

[46] T. Ma and O. A. Mohammed, "Optimal charging of plug-in electric vehicles for a car-park infrastructure," *IEEE Trans. Ind. Appl.*, vol. 50, no. 4, pp. 2323–2330, Jul./Aug. 2014.

[47] Z. Fan, "A distributed demand response algorithm and its application to PHEV charging in smart grids," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1280–1290, Sep. 2012.

[48] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A Stackelberg game approach," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 120–132, Mar. 2013.

[49] X. Lu, Y. Li, X. Gan, Y. Xu, and J. Yao, "Contract-based content delivery in 5G converged networks," *China Commun.*, vol. 14, no. 12, pp. 120–133, Dec. 2017.

[50] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 121–132, Apr. 2015.

[51] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[52] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement.*, New Orleans, LA, USA, Feb. 1999, pp. 173–186.

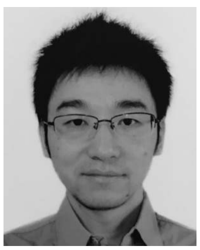
[53] L. Yu *et al.*, "Smart-contract execution with concurrent block building," in *Proc. IEEE Symp. Service Orient. Syst. Eng. (SOSE)*, San Francisco, CA, USA, 2017, pp. 160–167.

[54] P. Bolton and M. Dewatripont, *Contract Theory*. Cambridge, MA, USA: MIT Press, 2005.

[55] Y. Liu, X. Zhong, Y. Yan, J. Wang, and W. Saad, "Incentives in cooperative networks: A contract-theoretic perspective," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, pp. 1–13, Dec. 2014.

[56] L. Gao, X. Wang, Y. Xu, and Q. Zhang, "Spectrum trading in cognitive radio networks: A contract-theoretic modeling approach," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 843–855, Apr. 2011.

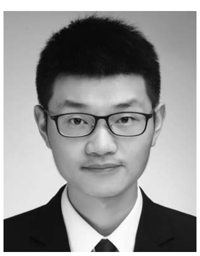
[57] University of Queensland. (2018). *UQ Solar Photovoltaic Data*. [Online]. Available: http://solar.uq.edu.au/user/reportPower.php



Zhou Su received the Ph.D. degree from Waseda University, Tokyo, Japan, in 2003.

His current research interests include multimedia communication, wireless communication, and network traffic.

Dr. Su was a recipient of the Best Paper Award of IEEE CyberSciTech 2017, WiCon 2016, and the Funai Information Technology Award for Young Researchers in 2009. He is an Associate Editor of *IET Communications* and the *IEICE Transactions on Communications*. He is the Chair of the Multimedia Services and Applications Over Emerging Networks Interest Group of the IEEE Comsoc Society, the Multimedia Communications Technical Committee. He also served as the Co-Chair of several international conferences, including IEEE VTC Spring 2016 and IEEE CCNC 2011. He is a TPC member of some flagship conferences, including IEEE INFOCOM, IEEE ICC, and IEEE Globecom.



Yuntao Wang received the master's degree from the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China.

His current research interests include smart grid and vehicular networks.

Qichao Xu received the Ph.D. degree from the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China.

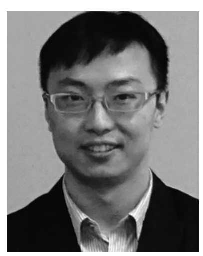
His current research interests include wireless network architecture and vehicular networks.

Minrui Fei received the B.Sc., M.Sc., and the Ph.D. degrees from Shanghai University, Shanghai, China, in 1984, 1992, and 1997, respectively.

He is a Professor with Shanghai University, the Vice Chairman of the Chinese Association for System Simulation, and the Standing Director of the China Instrument and Control Society. His current research interests include networked advanced control and system implementation, distributed and field bus control systems, key technology and applications in multifield bus conversion and performance evaluation, as well as the application of virtual reality and digital simulation in industry.

Yu-Chu Tian received the Ph.D. degree in computer and software engineering from the University of Sydney, Sydney, NSW, Australia, in 2009, and the Ph.D. degree in industrial automation from Zhejiang University, Hangzhou, China, in 1993.

He is with the School of Electrical Engineering and Computer Science, Queensland University of Technology, Brisbane, QLD, Australia, where he is currently a Professor. His current research interests include big data computing, distributed computing, cloud computing, real-time computing, computer networks, and control systems.



Ning Zhang received the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2015.

He was a Post-Doctoral Research Fellow with the BBCR Group, University of Waterloo, and with the University of Toronto, Toronto, ON. He is currently an Assistant Professor with the Department of Computing Science, Texas A&M University at Corpus Christi, Corpus Christi, TX, USA. His current research interests include next generation wireless networks, software defined networking, vehicular networks, and physical layer security.

Dr. Zhang was a recipient of the Best Paper Award of IEEE Globecom 2014 and IEEE WCSP 2015. He is an Associate Editor of IEEE ACCESS and *IET Communications* and was a Lead Guest Editor of *Wireless Communications and Mobile Computing* and the *International Journal of Distributed Sensor Networks*, and a Guest Editor of *Mobile Information System*.