Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing

Zhenyu Zhou, *Senior Member, IEEE*, Bingchen Wang, Mianxiong Dong, *Member, IEEE*, and Kaoru Ota, *Member, IEEE*

***Abstract*—Smart grid has emerged as a successful application of cyber-physical systems in the energy sector. Among numerous key technologies of the smart grid, vehicle-to-grid (V2G) provides a promising solution to reduce the level of demand–supply mismatch by leveraging the bidirectional energy-trading capabilities of electric vehicles. In this paper, we propose a secure and efficient V2G energy trading framework by exploring blockchain, contract theory, and edge computing. First, we develop a consortium blockchain-based secure energy trading mechanism for V2G. Then, we consider the information asymmetry scenario, and propose an efficient incentive mechanism based on contract theory. The social welfare optimization problem falls into the category of difference of convex programming and is solved by using the iterative convex–concave procedure algorithm. Next, edge computing has been incorporated to improve the successful probability of block creation. The computational resource allocation problem is modeled as a two-stage: 1) Stackelberg leader–follower game and 2) the optimal strategies are obtained by using the backward induction approach. Finally, the performance of the proposed framework is validated via numerical results and theoretical analysis.**

***Index Terms*—Consortium blockchain, contract theory, cyber-physical system (CPS), edge computing, vehicle-to-grid (V2G) energy trading.**

I. Introduction

A. Background and Motivation

CYBER-PHYSICAL systems (CPSs) refer to a great variety of systems where the underlaying physical and computational components are implicitly integrated with each other to improve the adaptability, efficiency, reliability, and usability of physical systems [1], [2]. A typical application of CPSs in the energy sector is the smart grid [3], which employs up-to-date information, communication, and control technologies to optimize the management and operation of power grids. Various researchers have investigated the smart grid from the perspective of cyber-physical integration, such as cyber-physical energy management [4] and cyber-physical attack mitigation [5].

However, the large-scale penetration of intermittent distributed renewable energy sources and uncoordinated electric vehicles (EVs) leads to significant power fluctuation [6]–[9]. In order to maintain the reliable and safe operations of the smart grid, a large number of centralized generators, and energy storage devices have to be deployed, which results in significant capital expenditure and operational expenditure [10]. An alternative choice is to leverage the bidirectional energy-trading capabilities of EVs. Particularly, a large group of EVs can be coordinated to absorb excessive energy during the off-peak time and deliver energy back to the grid during the peak time, which provides a promising solution to flatten out the peak load and reduce the level of demand–supply mismatch without deploying additional generators and storage devices [11], [12]. This new energy trading paradigm is known as vehicle-to-grid (V2G), which is essential to build a safer and more sustainable CPS in the energy sector [13].

The studies on V2G energy trading have received considerable attentions from both industry and academia. A distributed EV cooperation mechanism was proposed in [13], which not only enables the efficient management of charging and discharging operations, but also offers V2G regulation services to support grid operation. Pal and Kumar [14] presented a neighbor connection-based energy scheduling approach, which explores both vehicle-to-home and V2G energy trading to reduce household electricity payments. Despite the above-mentioned advantages, the wide area deployment of V2G still confronts several critical challenges, which are summarized as follows.

First, there lacks a distributed security mechanism for V2G energy trading. Conventional centralized mechanisms rely on a trusted intermediary to manage, audit, and verify every energy transaction [15], which is vulnerable to a series of security threats, such as single point of failure, denial of service attacks, and privacy leakage [16]. For example, a transaction record may be changed, tampered, or deleted by

Manuscript received June 10, 2018; accepted November 17, 2018. Date of publication May 15, 2019; date of current version December 31, 2019. This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61601181, in part by the Fundamental Research Funds for the Central Universities under Grant 2017MS001, in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI under Grant JP16K00117 and Grant JP19K20250, and in part by the KDDI Foundation. This paper was recommended by Associate Editor Y. Yuan. *(Corresponding author: Mianxiong Dong.)*

Z. Zhou and B. Wang are with the State Key Laboratory of Alternate Electrical Power System With Renewable Energy Sources, School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China (e-mail: zhenyu_zhou@ncepu.edu.cn; wbc0203@163.com).

M. Dong and K. Ota are with the Department of Information and Electric Engineering, Muroran Institute of Technology, Muroran 050-8585, Japan (e-mail: mx.dong@csse.muroran-it.ac.jp; ota@csse.muroran-it.ac.jp).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMC.2019.2896323

some malicious middleman attackers. Most of the current works mainly concentrate on EV charging and discharging management [11], [13], [17], [18], while the security and privacy issues have been neglected. Therefore, a distributed security mechanism is indispensable to guarantee the reliable operation of large-scale V2G energy trading in an untrusted and nontransparent energy market.

Second, there lacks an efficient incentive mechanism for V2G energy trading. Due to the increased battery consumption and other costs incurred by discharging, EV owners are reluctant to participate in large-scale V2G energy trading unless they are well compensated. For example, EV owners usually suffer from the problem of range anxiety due to the limited cruising range and the long charging time [19]. Hence, when designing the incentive mechanism, a sufficient amount of energy must be preserved for EV owners in order to reach their destinations. Furthermore, the preference of each EV toward V2G participation belongs to the EV's private information, which is only known by the EV itself. This scenario is called information asymmetry. Most of the previous works, e.g., [11], [13], and [20], have assumed that the EV's information is perfectly known by every entity in the energy market, and cannot be directly applied to V2G energy trading with asymmetric information. Therefore, it is of vital importance to develop an incentive mechanism, which can effectively maximize the economic benefits under the scenario of information asymmetry.

To address the above challenges, we develop a new V2G framework for CPSs, which leverages blockchain, contract theory, and edge computing to enable secure and efficient energy trading [21]. We consider a V2G energy trading scenario which involves three major entities: 1) local energy aggregators (LEAGs); 2) EVs; and 3) edge computing service provider (ESP) [22], [23]. The energy trading between LEAGs and EVs is secured by employing consortium blockchain, in which all the transactions are created, propagated, and verified by authorized LEAGs. Then, we put forward a contract theory-based incentive mechanism to motivate EVs to participate in energy trading. The contract is tailored for the unique characteristic of each EV type to maximize the utility of the LEAG under the constraints of individual rationality (IR), incentive compatibility (IC), and monotonicity. The formulated contract optimization problem falls into the category of difference of convex (DC) programming. We further reduce the total number of IR and IC constraints by exploiting the relationships between adjacent EV types. The simplified problem is solved by using the iterative convex–concave procedure (CCP) algorithm. Several heuristic schemes are also developed as performance benchmarks. Next, edge computing has been incorporated in block creation to reduce transmission as well as processing latency. Specifically, LEAGs can purchase services from the ESP, and offload the computation-intensive proof-of-work puzzles to proximate edge computing nodes. Considering the conflicting objectives of the ESP and LEAGs, the interaction between them is modeled as a two-stage Stackelberg leader–follower game [24], [25], and the optimal service price and service demands are obtained by using the backward induction approach. Finally, we provide a comprehensive theoretical analysis on contract feasibility, performance convergence, game equilibrium, and energy trading security. The relationships among social welfare, EV type, reward, discharged electricity, edge computing service price, and edge computing service demands are elaborated via numerical results.

B. Contributions

The contributions of this paper are summarized as follows.

1) *Consortium Blockchain-Based Secure Energy Trading:* We focus on typical electricity discharging scenario in V2G, and develop a consortium blockchain-based secure energy trading mechanism with moderate cost.
2) *Contract-Based Incentive Mechanism Design:* To optimize the utility of LEAG under information asymmetry, we propose an efficient incentive mechanism for V2G based on contract theoretical modeling.
3) *Edge Computing-Based Task Offloading:* An edge computing-based task offloading mechanism is developed to increase the successful probability of block creation. The optimal pricing strategy of edge computing service is obtained by using Stackelberg game.

The remainder of this paper is organized as follows. Section II shows and compares some related works. Section III introduces the consortium blockchain for secure energy trading. Section IV presents the contract-based incentive mechanism. Section V elaborates the edge computing-based task offloading. Section VI shows the simulation results. Finally, Section VII concludes this paper.

II. Related Work

Blockchain is a specific distributed shared database, which has been illustrated to possess salient advantages, including security, immutability, and decentralization [15]. It allows every transaction to be recorded in a verifiable and permanent way, which is essential to create a distributed, transparent, and secure energy-trading environment. Blockchain has experienced rapid evolutions from version 1.0 to 3.0. While blockchain 1.0 and 2.0 are more related to Bitcoin and cryptcurrencies, as well as transferring contracts or properties, blockchain 3.0 extends its application fields from financial transactions to much broader sectors, including energy, education, government, health, etc. [26]. Recent works have employed blockchain to address the transaction security issues of peer-to-peer energy trading among EVs. Liu *et al.* [27] proposed a decentralized blockchain-enabled EV charging scheme to simultaneously minimize the fluctuation level of the power grid and the EV charging cost. Li *et al.* [28] proposed a blockchain-based peer-to-peer energy trading system for industrial Internet of Things, which relies on a credit-based payment strategy to reduce transaction confirmation latency. Aggarwal *et al.* [29] proposed a blockchain model named *EnergyChain* to enable secure energy trading between smart grid and smart home, which involves miner selection, block creation and validation, and transaction handling. However, due to the high computational cost associated with block creation, blockchain has not been widely deployed in EVs with limited computational capabilities.

To reduce the computational complexity, we propose an edge computing-based consortium blockchain, in which a distributed ledger is created, publicly audited, and shared by multiple authorized nodes with moderate cost. First, unlike conventional blockchain, the distributed shared databases are only maintained by authorized LEAGs [30]. Second, edge computing [31], where computational resources are distributed across network edges, is employed to solve the proof-of-work puzzles of block creation. Compared to centralized cloud computing, edge computing is more suitable to handle large-scale decentralized energy-trading transactions. Since the computational tasks are processed at close proximity to end users, dispensable network hops and transmission latency can be effectively eliminated.

Edge computing has been widely applied in a series of delay-sensitive applications to reduce computational delay. Garg *et al.* [32] proposed a unmanned aerial vehicle (UAV)-enabled edge computing framework where data are transferred from vehicles to edge nodes for real-time processing by leveraging UAVs as intermediate aerial communication devices. A probabilistic data structure-based cyber-threat detection approach was developed to handle the data of vehicles. Zhou *et al.* [33] proposed a new edge computing framework from an air–ground integration perspective, in which the communication and computational resources of both UAVs and vehicles are combined in a complementary manner to provide massive-connectivity low-latency ultrareliable services. In [34], a robust mobile crowd sensing framework was developed by integrating deep learning-based data validation with edge computing-based local processing. Different from the above-mentioned works, we focus on the application scenario of blockchain-based energy trading in V2G, and the application-specific characteristics, such as Hash power, successful probability of block creation, and propagation time of block are taken into account. The computational resource allocation problem is modeled as a two-stage Stackelberg leader–follower game, in which the positions of players are hierarchial, and the leader, i.e., the ESP, can enforce its own strategy upon the followers, i.e., LEAGs.

Another challenge in V2G energy trading is the incentive design. There exists some work which have addressed the incentive design problem in V2G by exploiting robust optimization theory [11], Stackelberg game [35], genetic algorithm [36], etc. A generalized Stackelberg game-based pricing scheme was proposed to optimize the operations of V2G from the perspective of energy and reserve [35]. Ghofrani *et al.* [36] developed a genetic algorithm-based EV charging and discharging mechanism to minimize the penalty cost of wind power imbalance as well as the EV discharging expenses. Nevertheless, all these works rely on a common assumption that the EV-side information is perfectly known by the LEAG, while information asymmetry has been neglected. In this paper, we consider the more realistic scenario where the precise EV-side information is unknown, and develop a contract-based incentive mechanism to maximize the expected utility of LEAG based on contract theory. Contract theory provides a powerful tool to address the incentive problem with asymmetric information [37], and has already been widely applied in various applications, including device-to-device communications [38], cognitive radio [37], and small-cell caching systems [39].

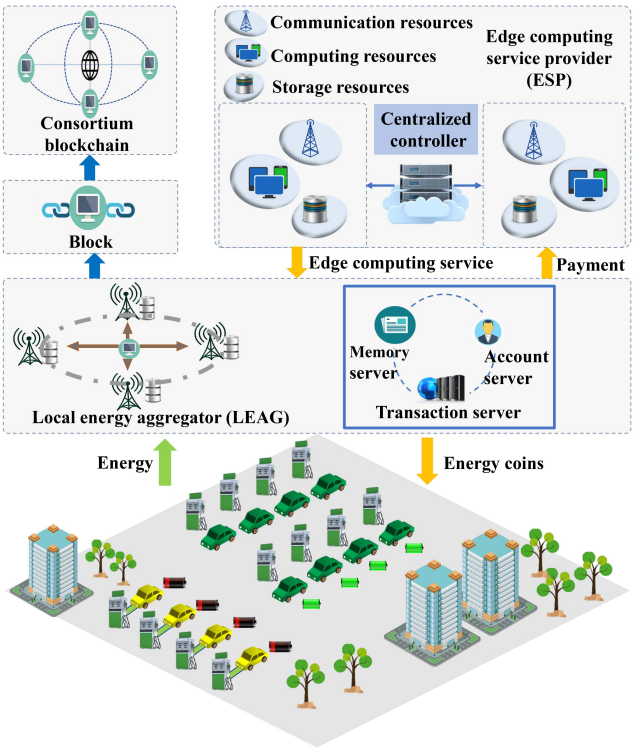


Fig. 1. Consortium blockchain-based secure energy trading for V2G.

In summary, we investigate the feasibility of integrating consortium blockchain, contract theory, and edge computing to realize secure and efficient V2G energy trading in CPSs. The proposed framework can effectively improve transaction security and privacy protection, motivate EVs to participate in energy trading, and increase the successful probability of block creation.

III. Consortium Blockchain-Based Secure Energy Trading Framework

The consortium blockchain-based secure energy trading for V2G is shown in Fig. 1, which consists of three major entities: 1) EV; 2) LEAG; and 3) ESP. The specific capability and functionality of each entity are elaborated as follows.

A. EV

EVs with bi directional energy trading capabilities are able to play different roles. On the one hand, an EV can act as an energy producer by discharging its battery to provide electricity during the peak time. On the other hand, it can also act as an energy consumer by charging its battery with cheaper electricity while helping to absorb the excess energy during the off-peak time. With a properly designed incentive mechanism, each EV can actively adjust its charging and discharging behaviors to maximize its individual payoff. The details for how to design the incentive mechanism will be illustrated in Section IV-B.

B. LEAG

The LEAG provides an array of energy trading services, including information collection, status monitoring, and charging/discharging coordination. For example, during the peak time, the LEAG can employ a group of discharging EVs to produce energy in response to local peak load demands. Meanwhile, the EVs which participate in the energy trading will obtain dedicated payments for their contributions to local supply demand balance. Here, energy coin which is one kind of digital cryptocurrency is utilized as the payment for the energy trading.

There are three major components in the LEAG: 1) a memory server; 2) an account server; and 3) a transaction server. All of the transaction records in the consortium blockchain are stored in the memory server. The digital assets of each EV in terms of energy coins are stored in a digital wallet. To preserve privacy, the true address of the wallet is replaced by a set of public keys, e.g., random pseudonyms. Each EV also has a transaction account which stores all of its transaction records. The mapping relationships between random wallet addresses and corresponding transaction account are maintained in the account server. The transaction server is responsible to implement incentive mechanisms and coordinate charging and discharging activities.

C. ESP

The ESP with unified control of the integrated computation, communication, and storage resources provides edge computing services for LEAGs. The ESP issues a price for its service, and each LEAG determines the service demand to be purchased based on the price. Then, the computation-intensive proof-of-work puzzles can be offloaded from an LEAG to its proximate edge computing nodes instead of being processed locally or by remote cloud nodes. The details for how to model the interactions between the ESP and LEAGs, and how to design the optimal service price and service demands will be illustrated in Section V.

The operation details of the consortium blockchain-based secure energy trading are explained as follows. Existing cryptographic algorithms, including elliptic curve digital signature algorithm (ECDSA), Boneh–Boyen short signature, and SHA-256, have been employed. In the beginning, each EV has to register with a legitimate authority to obtain its public key, privacy key, and certificate. The public/privacy keys can be generated and distributed by the authority. The certificate represents a unique identity for the EV via binding its registration information. Each EV has a set of wallet addresses issued by the authority. During initialization, an EV finds the wallet address that is used by its nearest LEAG and verifies the wallet integrity. Afterward, it downloads the corresponding data from the memory server.

The secrecy of the private key is maintained by the EV for signing transactions, while the public key is shared with other authorized entities to verify its signatures [40]. The public/privacy keys can be generated by using some specific algorithms, such as ECDSA [41], a new signature scheme based on lattice [42], a novel anti-quantum transaction authentication scheme in the blockchain [43], etc.

After energy trading, a discharging EV will receive the specified reward if the corresponding contract item has been successfully fulfilled. The energy coins are transferred from the LEAG to the wallet address of the EV. The transaction is digitally signed by the LEAG to ensure its integrity and authenticity, and then is broadcasted to the network. The other LEAGs not only check the transaction via analyzing the digital signature, but also check whether the LEAG which issues this transaction is authorized to spend the energy coin or not. A fake transaction will be discarded, and only valid transactions are included in a new block.

Next, to add the new block to the blockchain, all the authorized LEAGs start the mining process, in which they compete to find a valid proof of work similar to Bitcoin [44]. This process requires to find a random value α, combined with the hash of the previous block header Φ and the hash of transactions, which satisfies $\text{Hash}(\alpha + \Phi) < \beta$. Here, β represents the level of difficulty [45]. If an LEAG finds a valid proof of work, it will broadcast the result to other authorized LEAGs. Upon receiving the result, the other LEAGs verify it and determine whether to accept it or not. If a majority of LEAGs agree on the result, i.e., a consensus has been reached, then the new block will be added to the blockchain, and the LEAG which created this block will be rewarded by a certain amount of energy coins. Finally, the amount of energy coins that is transferred from the LEAG to the EV will be received in the EV's wallet.

It requires extremely high computational power to create a false block, find a valid proof of work before other LEAGs, and control the majority of the LEAGs [26]. Furthermore, malicious attacks which try to modify the transaction records can be prevented since each validated block is linked to the previous block via secure cryptography methods. Any change of a transaction will affect both the block containing it and subsequent blocks.

If the computational capability of an LEAG is limited, it can purchase edge computing services from the ESP. Then, the computation-intensive proof-of-work process is handled by nearby edge computing nodes with powerful computation capabilities, and the successful probability of block creation will be significantly improved. We assume that transaction verification is handled locally by LEAGs in order to reduce the cost of purchasing computing service. The reason is the computational complexity of transaction verification is much lower that of block creation, i.e., mining. Taking Bitcoin for example, the level of difficulty is dynamically adjusted after every 2016 blocks to guarantee that the block generation time is exactly 600 s [46]. As the total computational power of the overall network increases continuously, the difficulty is also increased accordingly to maintain the fixed block generation time. Nevertheless, the proposed framework can be easily extended to the scenario where both block creation and transaction verification are offloaded to edge computing nodes.

The data shared among EVs, LEAGs, and ESP also suffer from the chosen-plaintext attack (CPA) and chosen-ciphertext attack (CCA). CPA represents an attack strategy for cryptanalysis in which the ciphertexts for arbitrary plaintexts are

available to the attacker [47]. CCA represents another attack model in which the cryptanalyst collect information from decryptions of chosen ciphertexts and try to recover the secret key based on the collected information. Since how to mitigate CPA and CCA has already been intensively investigated, it is ignored here due to space limitation and is left to the future work. Interested readers can refer to related works [47]–[50].

The decentralized consensus can be guaranteed due to the following two reasons. First, the ESP mainly makes a revenue by selling computing services, and is not rewarded for block creation. Thus, it does not have a strong incentive to cheat in verification. Second, a new block is verified by every LEAG independently according to the same rules. If some dishonest LEAGs accept some fake transactions in a new block, the other honest LEAGs will update their own copy of the blockchain without using the invalid block. As a result, the fake block branch is much shorter than the valid branch, which will be discarded since LEAGs only maintain a copy of the longest chain [51].

IV. Contract-Based Incentive Mechanism for V2G Energy Trading

A. EV Type Modeling

We use EV type to quantify the preference of an EV toward discharging, which is only known by the EV itself. A higher-type EV is more willing to participate in the V2G energy trading and discharge a larger amount of electricity to gain a higher reward. It is intuitive that EVs with higher types are more preferred by the LEAG. For the sake of simplicity, we assume that the set of EV types belongs to a discrete and finite space. The EV type is defined as follows.

Definition 1: Considering a parking lot with K discharging EVs, these EVs can be sorted in an ascending order based on their preferences and classified into K types. If the set of EV types is denoted as $\Theta = \{\theta_1, \ldots, \theta_k, \ldots, \theta_K\}$, then we have

$$\theta_1 < \cdots < \theta_k < \cdots < \theta_K, k = 1, \ldots, K. \tag{1}$$

In the following, we derive the specific expression of the EV type. Considering type θ_k EV, the stage of charge (SoC) is calculated as [52]

$$\mathrm{SoC}_k^c = \frac{E_k^c}{E_{k,\max}} \tag{2}$$

where E_k^c represents the amount of currently available energy, and $E_{k,\max}$ is the battery capacity. After discharging, the remaining SoC should satisfy the minimum energy requirement of traveling, which is given by

$$\frac{E_k^c - L_k}{E_{k,\max}} \geq \chi(d_k) \tag{3}$$

where L_k is the required amount of electricity and d_k is the distance that has to be traveled before the next charging. $\chi(d_k)$ denotes the minimum electricity required to travel the distance d_k, which is a monotonically increasing function of d_k. By combining (2) and (3), we can derive the discharging capability, which is given by

$$L_k \leq \left[\mathrm{SoC}_k^c - \chi(d_k)\right] E_{k,\max}. \tag{4}$$

Hence, type θ_k can be defined as

$$\theta_k := \left[\mathrm{SoC}_k^c - \chi(d_k)\right] E_{k,\max}. \tag{5}$$

Remark 1: From (5), it is observed that θ_k is positively proportional to SoC_k^c and $E_{k,\max}$, and inversely proportional to $\chi(d_k)$. For example, a larger EV type represents that either the EV has more energy available, or it will not travel a long distance in the near future.

In the information asymmetry scenario, the LEAG does not know the specific type of each EV, but only has the knowledge of the probability distribution of each type. We assume that the LEAG knows that there are a total of K types of discharging EVs and an EV belongs to type θ_k with a probability P_k, i.e., $\sum_{k=1}^{K} P_k = 1$.

B. Contract Formulation

Instead of providing the same contract for EVs with different types, a contract which consists of K contract items is designed for K types of discharging EVs, i.e., one for each type. For example, the contract item designed for type θ_k EV is denoted as (L_k, R_k), where L_k denotes the required electricity and R_k is the dedicated reward in terms of energy coins. The contract is defined as $\mathcal{C} = \{(L_k, R_k)\ \forall k \in \mathcal{K}\}$, where $\mathcal{K} = \{1, \ldots, k, \ldots, K\}$.

Considering the K types of EVs, the expected utility of the LEAG is calculated as

$$U_L(\{L_k\}, \{R_k\}) = K \sum_{k=1}^{K} P_k(\gamma_L L_k - R_k) \tag{6}$$

where γ_L is the unit value of electricity for the LEAG.

Remark 2: A contract item $(L_k = 0, R_k = 0)$ means that type θ_k EV does not intend to participate in discharging. On the other hand, the LEAG will benefit from the EV discharging only if $\gamma_L L_k - R_k \geq 0$. Otherwise, the LEAG has no incentive to employ type θ_k EV for discharging.

The utility function of type θ_k EV which accepts the contract item (L_k, R_k) is given by

$$U_k^{EV}(L_k, R_k) = \theta_k m(R_k) - \gamma L_k \tag{7}$$

where γ is the unit cost of discharging the battery. $\theta_k m(R_k)$ represents the value of R_k for type θ_k EV. The function $m(R_k)$ is a monotonically increasing concave function of R_k, where $m(0) = 0$, $m'(R_k) > 0$, and $m''(R_k) < 0$. Without loss of generality, $m(R_k)$ can be defined as a quadratic function, i.e.,

$$m(R_k) = -\frac{a}{2} R_k^2 + bR_k \tag{8}$$

where a and b are assumed as constants, which should satisfy $m'(R_k) > 0$ and $m''(R_k) < 0$. Nevertheless, the proposed scheme can be extended to other forms.

The expected social welfare is the total sum utility of the LEAG and the K EVs, which is given by

$$SW(\{L_k\}, \{R_k\}) = U_L(\{L_k\}, \{R_k\}) + K \sum_{k=1}^{K} P_k U_k^{EV}(L_k, R_k). \tag{9}$$

The utility of LEAG maximization problem under asymmetric information is formulated as

$$\begin{aligned}\text{P1:}\ \max_{\{L_k\},\{R_k\}}\ & U_L(\{L_k\},\{R_k\})\\ \text{s.t.}\ & C_1: \theta_k m(R_k) - \gamma L_k \geq 0, \text{(IR)}\\ & C_2: \theta_k m(R_k) - \gamma L_k \geq \theta_k m(R_{k'}) - \gamma L_{k'}, \text{(IC)}\\ & C_3: 0 \leq R_1 < \cdots < R_k < \cdots < R_K\\ & C_4: L_k \leq \theta_k\\ & \forall k, k' \in \mathcal{K} \end{aligned} \tag{10}$$

where C_1, C_2, and C_3 represent the IR, IC, and monotonicity constraints, respectively. C_4 represents the upper bound of L_k.

Definition 2: The IR, IC, and monotonicity constraints are defined as follows.

1) *IR Constraint:* Type θ_k EV, $\forall k \in \mathcal{K}$, will get a non-negative payoff if it selects the contract item (L_k, R_k).
2) *IC Constraint:* The IC constraint ensures the *self-revealing* property of the contract. For instance, type θ_k EV $\forall k \in \mathcal{K}$, will get the maximum payoff if and only if it selects the contract item (L_k, R_k) designed for its own type.
3) *Monotonicity Constraint:* The reward of type θ_k EV $\forall k \in \mathcal{K}$, should be higher than that of type θ_{k-1} EV, and lower than that of type θ_{k+1} EV.

Based on the IR, IC, and monotonicity constraints, the following properties can be derived.

Lemma 1: For any $k, k' \in \mathcal{K}$, if $\theta_k > \theta_{k'}$, then $R_k > R_{k'}$. $R_k = R_{k'}$ if and only if $\theta_k = \theta_{k'}$.

Lemma 2: For any $L_k, R_k \in \mathcal{C}$, the following inequalities hold:

$$\begin{aligned} &0 \leq R_1 \leq \cdots \leq R_k \leq \cdots \leq R_K\\ &0 \leq L_1 \leq \cdots \leq L_k \leq \cdots \leq L_K\\ &0 \leq U_1^{EV} \leq \cdots \leq U_k^{EV} \leq \cdots \leq U_K^{EV}. \end{aligned} \tag{11}$$

Proof: The detailed proof of Lemmas 1 and 2 are omitted here due to space limitation. A similar proof can be found in [38]. ■

C. Optimal Contract Design Under Information Asymmetry

1) Contract Feasibility: First, we define the sufficient and necessary conditions for contract feasibility.

Theorem 1 (Contract Feasibility): The contract $\mathcal{C} = \{(L_k, R_k)\ \forall k \in \mathcal{K}\}$ is feasible if and only if all the following conditions are satisfied.

1) $0 \leq R_1 \leq \cdots \leq R_k \leq \cdots \leq R_K$ and $0 \leq L_1 \leq \cdots \leq L_k \leq \cdots \leq L_K$.
2) $\theta_1 m(R_1) - \gamma L_1 \geq 0$.
3) For any $k \in \{2, \ldots, K\}$, $\gamma L_{k-1} + \theta_{k-1}[m(R_k) - m(R_{k-1})] \leq \gamma L_k \leq \gamma L_{k-1} + \theta_k[m(R_k) - m(R_{k-1})]$.

Proof: The detailed proof of Theorem 1 is omitted here due to space limitation. A similar proof can be found in [37, Appendix D]. ■

2) Problem Transformation: The utility of LEAG maximization problem P1 involves K IR constraints and $K(K-1)$ IC constraints. To provide a tractable solution, the following procedures are carried out to simplify the problem.

Step 1 (IR Constraints Elimination): For type θ_k EV, $k \in \mathcal{K}, k \neq 1$, we can derive

$$\theta_k m(R_k) - \gamma L_k \geq \theta_k m(R_1) - \gamma L_1 > \theta_1 m(R_1) - \gamma L_1 \geq 0 \tag{12}$$

where the first inequality is due to the IC constraint, the second inequality is due to $\theta_k > \theta_1$, and the third inequality is due to the IR constraint. Hence, if the IR constraint of type θ_1 EV is guaranteed, then the IR constraints of EVs with higher types are automatically satisfied.

Step 2 (IC Constraints Elimination): We define the IC constraints between type θ_k and type $\theta_{k'}$, $k' \in \{1, \ldots, k-1\}$, as downward incentive constraints (DICs). Similarly, the IC constraints between type θ_k and type $\theta_{k'}$, $k' \in \{k+1, \ldots, K\}$, are defined as upward incentive constraints (UICs). In the following, we will show that both the DICs and UICs can be reduced.

We consider three adjacent EV types, i.e., $\theta_{k-1} < \theta_k < \theta_{k+1}$, which satisfy

$$\theta_{k+1} m(R_{k+1}) - \gamma L_{k+1} \geq \theta_{k+1} m(R_k) - \gamma L_k \tag{13}$$

$$\theta_k m(R_k) - \gamma L_k \geq \theta_k m(R_{k-1}) - \gamma L_{k-1} \tag{14}$$

where (13) denotes the DIC between type θ_{k+1} and type θ_k, and (14) denotes the DIC between type θ_k and θ_{k-1}.

By combining $R_{k+1} \geq R_k \geq R_{k-1}$, we have

$$\theta_{k+1} m(R_{k+1}) - \gamma L_{k+1} \geq \theta_{k+1} m(R_{k-1}) - \gamma L_{k-1}. \tag{15}$$

Therefore, if the DIC between type θ_{k+1} and θ_k holds, then the DIC between θ_{k+1} and θ_{k-1} also holds. The DIC constraints can be extended downward from type θ_{k-1} to type θ_1, which are given by

$$\begin{aligned} \theta_{k+1} m(R_{k+1}) - \gamma L_{k+1} &\geq \theta_{k+1} m(R_{k-1}) - \gamma L_{k-1}\\ &\geq \cdots\\ &\geq \theta_{k+1} m(R_1) - \gamma L_1. \end{aligned} \tag{16}$$

Thus, we demonstrate that if the DICs between adjacent types hold, then all the DICs hold automatically. Similarly, we can demonstrate that if the UICs between adjacent types hold, then all the UICs hold automatically.

Based on the above analysis, the K IR constraints and $K(K-1)$ IC constraints can be reduced to 1 and $K-1$, respectively. P1 is rewritten as

$$\begin{aligned}\text{P2:}\ \max_{\{L_k\},\{R_k\}}\ & U_L(\{L_k\},\{R_k\})\\ \text{s.t.}\ & C_1: \theta_1 m(R_1) - \gamma L_1 \geq 0, \text{(IR)}\\ & C_2: \theta_k m(R_{k-1}) - \gamma L_{k-1} \leq \theta_k m(R_k) - \gamma L_k, \text{(IC)}\\ & C_3, C_4, k = 2, \ldots, K. \end{aligned} \tag{17}$$

3) Optimal Contract With Reduced Constraints: We can prove that the objective of P2 is a concave function by checking the Hessian matrix. However, convex programming cannot be directly applied here because the constraint C_2 involves the difference of two concave functions, i.e., $\theta_k m(R_{k-1}) - \gamma L_{k-1}$ and $\theta_k m(R_k) - \gamma L_k$. Therefore, the CCP algorithm proposed in [53] is adopted to solve P2, which is summarized in Algorithm 1.

Algorithm 1 CCP-Based Contract Optimization

1: **Input:** $R_{k,0}[\tau]$, Θ, γ_L, γ.
2: **Output:** $\{\hat{L}_k\}$, $\{\hat{R}_k\}$
$\tau := 0$
3: **Repeat**
4: Transform the concave function $f_k(R_k)$ $\forall k \in \mathcal{K}$, into an affine function by using (18).
5: Transform **P2** into a convex programming problem.
6: Obtain $\{\hat{L}_k[\tau]\}$ and $\{\hat{R}_k[\tau]\}$ by using KKT conditions.
7: Update. $\tau := \tau + 1$, $R_{k,0}[\tau+1] = \hat{R}_k[\tau] \forall k \in \mathcal{K}$.
Until satisfying the stopping criterion (20).

Denote $f_k(R_k) = \theta_k m(R_k)$. Since $f_k(R_k)$ is differentiable with regards to R_k, $f_k(R_k)$ can be approximated by using its first-order Taylor series expansion as

$$f_k(R_k) \approx f_k\big(R_{k,0}[\tau]\big) + \nabla f_k\big(R_{k,0}[\tau]\big)\big(R_k - R_{k,0}[\tau]\big) \quad (18)$$

where $R_{k,0}[\tau]$ represents the initial point at iteration τ.

Hence, the constraint C_2 with the difference of two concave functions is transformed to the difference of a concave function and an affine function, which is written as

$$\tilde{C}_2 : \theta_k m(R_{k-1}) - \gamma L_{k-1} \le f_k\big(R_{k,0}[\tau]\big) + \nabla f_k\big(R_{k,0}[\tau]\big) \times \big(R_k - R_{k,0}[\tau]\big). \quad (19)$$

By replacing C_2 with $\tilde{C}_2$, P2 is transformed into a convex programming problem, and can be easily solved by using Karush–Kuhn–Tucker (KKT) conditions. At each iteration τ, the local optimal solutions $\hat{L}_k[\tau]$ and $\hat{R}_k[\tau]$ are obtained by solving the transformed convex problem. Then, the initial point for Taylor series expansion at iteration $\tau + 1$ is defined as $R_{k,0}[\tau+1] = \hat{R}_k[\tau]$. Next, the above iteration is repeated to derive a new local optimal solution.

The iterative process terminates until a predefined stopping criterion is satisfied. For example, the improvement in the social welfare is less than or equal to some positive threshold ϵ, i.e.,

$$U_L\Big(\big\{\hat{L}_k[\tau+1]\big\}, \big\{\hat{R}_k[\tau+1]\big\}\Big) - U_L\Big(\big\{\hat{L}_k[\tau]\big\}, \big\{\hat{R}_k[\tau]\big\}\Big) \le \epsilon. \quad (20)$$

Theorem 2 (Convergence): At any iteration τ, the obtained $\{\hat{L}_k[\tau]\}$ and $\{\hat{R}_k[\tau]\}$ are feasible. Furthermore, $\{SW\}_{\tau=0}^{\infty}$ is non-decreasing, and will converge to the maximum social welfare, i.e.,

$$U_L\Big(\big\{\hat{L}_k[\tau]\big\}, \big\{\hat{R}_k[\tau]\big\}\Big) \le U_L\Big(\big\{\hat{L}_k[\tau+1]\big\}, \big\{\hat{R}_k[\tau+1]\big\}\Big). \quad (21)$$

Proof: The detailed proof of Theorem 2 is omitted here. A similar proof can be found in [53]. ■

D. Optimal Contract Design Without Information Asymmetry

If there exists a selfish LEAG which is precisely aware of each EV's type, it can further increase its profit as long as each EV only accepts the contract item designed for its own type. In this scenario, the LEAG has to ensure that the payoff of each EV is non-negative. Otherwise, the EVs have no incentive to accept the contract item. To this end, the contract item has to meet the IR constraint. Furthermore, the contract item has to satisfy the following property.

Lemma 3: In the contract design without information asymmetry, any contract item $(L_k, R_k) \in \mathcal{C}$ should satisfy $\theta_k m(R_k) = \gamma L_K$. That is, the payoff for any EV is zero.

Proof: Lemma 3 can be proved by contradiction. Given an optimal contract item (R_k, L_k), if $\theta_k m(R_k) - \gamma L_k > 0$, then the LEAG can increase its utility by increasing L_k until $\theta_k m(R_k) - \gamma L_k = 0$. This contradicts with the assumption that (L_k, R_k) is optimal. ■

Thus, by enforcing the utility of each EV to be zero, the social welfare is equivalent to the utility of the LEAG. The corresponding optimization problem is formulated as

$$\begin{aligned} \text{P3:} \max_{\{L_k\},\{R_k\}} \quad & U_L(\{L_k\}, \{R_k\}) \\ \text{s.t.} \quad & C_1 : \theta_k m(R_k) - \gamma L_k = 0 \\ & C_2 : 0 \le R_1 < \cdots < R_k < \cdots < R_K \\ & C_3, C_4 \ \forall k \in \mathcal{K}. \end{aligned} \quad (22)$$

To solve (22), we have to work out the solutions of K quadratic equations, i.e., $\theta_k m(R_k) - \gamma L_k = 0$ $\forall k \in \mathcal{K}$. Assuming that R_{k1} and R_{k2} are the two solutions of the kth quadratic equation, the optimal solution is given by

$$(\{L_k\}, \{R_k\}) = \arg\max_{\{R_k\} \in (\{R_{k1}\}, \{R_{k2}\})} (U_L(\{L_{k1}\}, \{R_{k1}\}), U_L(\{L_{k2}\}, \{R_{k2}\})). \quad (23)$$

Lemma 4: In the contract design without information asymmetry, for any EV type θ_k, $k \in \mathcal{K}$, R_k is fixed regardless of θ_k.

Proof: Substituting $\theta_k m(R_k) - \gamma L_k = 0$ into (9), it can be verified that the social welfare SW increases monotonically with $\sum_{k=1}^{K} L_k$. Hence, the LEAG can increase L_k until $L_k = \theta_k$. Next, substituting $L_k = \theta_k$ into $\theta_k m(R_k) - \gamma L_k = 0$, we have $m(R_k) = \gamma_L$, which means that R_k is fixed regardless of θ_k. ■

V. Edge Computing-Based Computational Task Offloading

A. Hierarchical Game Formulation

In order to win the block mining competition, an LEAG can purchase edge computing services from the ESP to enlarge its computational capability. We assume that there are N LEAGs, and the set of LEAGs is denoted as $\mathcal{N}$. The service demand of the nth LEAG is denoted as s_n. For the nth LEAG, the successful probability of block creation, i.e., P_n, depends on two factors: 1) its relative hash power $P_{n,h}$ [54] and 2) its block orphaning probability $P_{n,o}$ [44], which are explained as follows.

The relative hash power of the nth LEAG is defined as the ratio of its computational power with respect to the total computational power, i.e.,

$$P_{n,h}(s_n) = \frac{s_n}{s_n + \sum_{n' \in \mathcal{N}, n' \ne n} s_{n'}}, n \in \mathcal{N} \quad (24)$$

where $P_{n,h} > 0$ and $\sum_{j \in \mathcal{N}} P_{j,h} = 1$.

Upon finding a valid proof-of-work, the nth LEAG has to broadcast the created block to the other LEAGs in order to reach a consensus. If the nth LEAG happens to choose a large block which propagates slowly due to the data size, then the block is more likely to be discarded due to the high transmission latency. Accordingly, the chance of the nth LEAG to win the competition of block mining will be diminished. This phenomenon is called orphaning [44]. By assuming that the block propagation time follows a Poisson distribution, the orphaning probability is given by

$$P_{n,o} = 1 - e^{-\frac{\Delta t(D_n)}{T}} \tag{25}$$

where T denotes the expected block interval time, which is 10 min in Bitcoin. $\Delta t(D_n)$ denotes the relative propagation time of a block with size D_n, which is defined as

$$\Delta t(D_n) = t(D_n) - t(0). \tag{26}$$

Here, $t(D_n)$ is the propagation time to deliver a block with size D_n and $t(0)$ presents the lag of the communication channel, i.e., the time required for delivering the block header. $t(0)$ is bounded by the constraint $t(0) \geq d_c/c$, where d_c denotes the transmission distance, and c denotes the speed of light.

Based on the approach proposed in [44], $t(D_n)$ can be approximated by using its first-order Taylor series expansion around $D_n = 0$ as

$$t(D_n) \approx t(0) + \nabla t|_{D_n=0}\, D_n \tag{27}$$

where the second term of (27) is partially related to the carrying capacity of the communication channel. Based on the Shannon–Hartley theorem, it can be written as $\nabla t|_{D_n=0} = 1/(G_1 G_2)$, where G_1 and G_2 present the channel capacity and coding gain, respectively. Hence, by taking $\nabla t|_{D_n=0} = 1/(G_1 G_2)$ and (27) into (26), $\Delta t(D_n)$ is written as

$$\Delta t(D_n) = t(D_n) - t(0) \approx \frac{D_n}{G_1 G_2}. \tag{28}$$

The successful probability of block creation, i.e., P_n, is given by

$$\begin{aligned} P_n(s_n) &= P_{n,h}(s_n)\big(1 - P_{n,o}\big) \\ &= \frac{s_n}{s_n + \sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}} e^{-\frac{D_n}{G_1 G_2 T}}. \end{aligned} \tag{29}$$

Once the consensus process is successful, the nth LEAG will gain a revenue which consists of two parts: 1) the reward for its contribution to block creation Q_n and 2) the transaction fee M_n. The net revenue of the nth LEAG can be calculated as the expected profit minus the service cost, i.e.,

$$U_{n,b}(s_n) = (Q_n + M_n) P_n(s_n) - p_c s_n \tag{30}$$

where p_c is the unit service price of edge computing.

The utility of the ESP is defined as the total revenue obtained from service provisioning minus the operation cost, i.e.,

$$U_E(p_c) = \sum_{n \in \mathcal{N}} p_c s_n - \gamma_c \sum_{n \in \mathcal{N}} s_n \tag{31}$$

where γ_c is the unit cost of service provisioning.

Owing to the dominant market position of the ESP compared to LEAGs, the competitive interaction between the ESP and LEAGs can be modeled as a two-stage Stackelberg leader–follower game. In the first stage, the ESP is the leader that determines the unit service price p_c, and obtains the revenue from LEAGs for solving the offloaded proof-of-work puzzles. In the second stage, the LEAGs act as the followers, and determine the service demand to be purchased. The two-stage Stackelberg leader–follower game is formulated as follows.

Stage 1: The service price optimization problem is solved in the first stage, which is formulated as

$$\begin{aligned} \text{P4:} \max_{p_c} \;& U_E(p_c) \\ \text{s.t.} \;& C_5 : p_{c,\min} \leq p_c \leq p_{c,\max} \end{aligned} \tag{32}$$

where $p_{c,\min}$ and $p_{c,\max}$ denote the minimum and maximum bounds of the unit service price.

Stage 2: The service demand optimization problem is solved in the second stage, which is formulated as

$$\begin{aligned} \text{P5:} \max_{s_n} \;& U_{n,b}(s_n) \\ \text{s.t.} \;& C_6 : s_{n,\min} \leq s_n \leq s_{n,\max} \end{aligned} \tag{33}$$

where $s_{n,\min}$ is the minimum computational resources (hash power) required by the nth LEAG, and $s_{n,\max}$ represents the maximum computational resources that can be provided by the ESP.

B. Equilibrium Analysis

The optimal price and the optimal service demands can be derived by using the backward induction approach [24].

1) Solution of the Second-Stage Optimization Problem: First, given a service price p_c, the second-stage service demand optimization problem P5 is solved for each LEAG. During the service demand optimization, every LEAG competes with each other to maximize its own relative hash power, and thus, to maximize its successful probability of block creation. From (24), we can observe that the relative hash power of the nth LEAG not only depends on its strategy s_n, but also depends on the strategies of the other LEGAs, e.g., $s_{n'}$, $n' \in \mathcal{N}$, $n' \neq n$. Therefore, the competition among N LEAGs can be modeled as an N-player noncooperative game. Denote the optimal strategy of the nth LEAG as s_n^*, and let $\mathbf{s}_{-n}^* = \{s_{n'}, n' \in \mathcal{N}, n' \neq n\}$ represent the set of optimal strategies of the other LEAGs in the set N excluding the nth LEAG. We have the following properties.

Theorem 3 (Nash Equilibrium): The set of optimal service demand strategies, i.e., $\{s_n^*, \mathbf{s}_{-n}^*\}$ $\forall n \in \mathcal{N}$, constitutes a Nash equilibrium of the second-stage N-player noncooperative game.

Proof: For any feasible s_n, $n \in \mathcal{N}$, we have

$$U_{n,b}\big(s_n^*, \mathbf{s}_{-n}^*, p_c\big) \geq U_{n,b}\big(s_n, \mathbf{s}_{-n}^*, p_c\big). \tag{34}$$

Hence, $\{s_n^*, \mathbf{s}_{-n}^*\}$ constitutes a Nash equilibrium. ■

Theorem 4 (Nash Equilibrium Existence): A Nash equilibrium exists in the second-stage N-player noncooperative game.

Proof: Based on [55], a Nash equilibrium exists if the following two conditions are satisfied.

1) $\{s_n, n \in \mathcal{N}\}$ is a nonempty compact convex subset of a Euclidean space.
2) $U_{n,b}(s_n)$ is continuous and quasi concave with regards to s_n.

First, for any $n \in \mathcal{N}$, the strategy space $[s_{n,\min}, s_{n,\max}]$ is a convex, continuous, compact, and nonempty subset of the Euclidean space, which satisfies the first condition.

Second, the second-order derivative of (30) with regards to s_n is given by

$$\frac{\partial^2 U_{n,b}}{\partial s_n^2} = (Q_n + M_n)\frac{\partial^2 P_{n,b}}{\partial s_n^2} e^{-\frac{D_n}{CGT}} < 0 \tag{35}$$

where

$$\frac{\partial^2 P_{n,h}}{\partial s_n^2} = -2\frac{\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}}{\left(s_n + \sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}\right)^3} < 0. \tag{36}$$

This proves that $U_{n,b}(s_n)$ is concave with regards to s_n. Therefore, a Nash equilibrium exists in the second-stage N-player noncooperative game. ∎

Theorem 5 (Best Response): Given $\mathbf{s}^*_{-n}$, the best response function of the nth LEAG, i.e., $B_n(\mathbf{s}^*_{-n})$, is given by (38).

Proof: Since $U_{n,b}(s_n)$ is concave with regards to s_n and C_6 is affine, P5 is a standard convex programming problem. By setting the first-order derivative of (30) to zero, i.e., $(\partial U_{n,b}/\partial s_n) = 0$, we have

$$\hat{s}_n = \sqrt{\frac{(Q_n + M_n)\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}}{p_c e^{\frac{D_n}{G_1 G_2 T}}}} - \sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}. \tag{37}$$

The optimal solution s_n^* can be obtained as

$$s_n^* = B_n\left(\mathbf{s}^*_{-n}\right) = \begin{cases} s_{n,\min}, & \hat{s}_n < s_{n,\min} \\ \hat{s}_n, & s_{n,\min} \leq \hat{s}_n \leq s_{n,\max} \\ s_{n,\max}, & \hat{s}_n > s_{n,\max}. \end{cases} \tag{38}$$

∎

Theorem 6 (Nash Equilibrium Uniqueness): If the condition

$$\frac{2(N-1)e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n} < \sum_{n \in \mathcal{N}} \frac{e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n} \tag{39}$$

is satisfied, then the Nash equilibrium of the second-stage N-player noncooperative game is unique.

Proof: The Nash equilibrium is unique if the best response function of any LEAG, e.g., $B_n(\mathbf{s}^*_{-n})$ $\forall n \in \mathcal{N}$, is a standard function. Based on [55], $B_n(\mathbf{s}^*_{-n})$ is a standard function if the following conditions are satisfied.

1) *Positivity:* $B_n(\mathbf{s}^*_{-n}) > 0$.
2) *Monotonicity:* If $\mathbf{s}^*_{-n} \geq \tilde{\mathbf{s}}^*_{-n}$, then $B_n(\mathbf{s}^*_{-n}) \geq B_n(\tilde{\mathbf{s}}^*_{-n})$.
3) *Scalability:* For all $\psi > 1$, $\psi B_n(\mathbf{s}^*_{-n}) > B_n(\psi \mathbf{s}^*_{-n})$.

First, to prove positivity, we have to prove that

$$B_n\left(\mathbf{s}^*_{-n}\right) = \mathbf{s}^*_{-n} > 0. \tag{40}$$

By setting $(\partial U_{n,b}/\partial s_n) = (Q_n + M_n)(\partial P_{n,h}/\partial s_n) e^{-(D_n/G_1 G_2 T)} - p_c = 0$, we can obtain

$$\frac{\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}}{\left(\sum_{n \in \mathcal{N}} s_n\right)^2} = \frac{p_c e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n}. \tag{41}$$

Take the summation of all miners, i.e., $\sum_{n \in \mathcal{N}}$, for both sides of (41), we have

$$\frac{(N-1)\sum_{n \in \mathcal{N}} s_n}{\left(\sum_{n \in \mathcal{N}} s_n\right)^2} = \sum_{n \in \mathcal{N}} \frac{p_c e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n} \tag{42}$$

which can be written as

$$\sum_{n \in \mathcal{N}} s_n = \frac{N-1}{\sum_{n \in \mathcal{N}} \frac{p_c e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n}}. \tag{43}$$

Besides, from (41), we can derive the expression of $\sum_{n \in \mathcal{N}} s_n$ as

$$\sum_{n \in \mathcal{N}} s_n = \sqrt{\frac{(Q_n + M_n)\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}}{p_c e^{\frac{D_n}{G_1 G_2 T}}}}. \tag{44}$$

By substituting (43) into (44) and utilizing the condition (39), we have

$$\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'} = \left(\frac{N-1}{\sum_{n \in \mathcal{N}} \frac{p_c e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n}}\right)^2 \frac{p_c e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n}. \tag{45}$$

By taking the square of both sides of (39), and multiplying both sides with p_c, we get the expression

$$\left(\frac{N-1}{\sum_{n \in \mathcal{N}} \frac{p_c e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n}}\right)^2 \frac{p_c e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n} < \frac{Q_n + M_n}{4 p_c e^{\frac{D_n}{G_1 G_2 T}}}. \tag{46}$$

Substituting (46) into (45), we have

$$\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'} < \frac{Q_n + M_n}{4 p_c e^{\frac{D_n}{G_1 G_2 T}}} < \frac{Q_n + M_n}{p_c e^{\frac{D_n}{G_1 G_2 T}}}. \tag{47}$$

Multiplying both sides of (47) with $\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}$ and taking the square root, we can derive that

$$\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'} < \sqrt{\frac{(Q_n + M_n)\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}}{p_c e^{\frac{D_n}{G_1 G_2 T}}}}. \tag{48}$$

Thus, the positivity condition can be proved as

$$s_n^* = \sqrt{\frac{(Q_n + M_n)\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}}{p_c e^{\frac{D_n}{G_1 G_2 T}}}} - \sum_{n' \in \mathcal{N}, n' \neq n} s_{n'} > 0. \tag{49}$$

Next, we prove that the response function B_n is monotone. If $\tilde{\mathbf{s}}_{-n} < \mathbf{s}_{-n}$, then the expression of $B_n(\mathbf{s}_{-n} - B_n(\tilde{\mathbf{s}}_{-n}))$ is provided in (50), as shown at the top of the next page. If (50) is positive, then both the two functions of the right side, i.e., g_1 and g_2, should also be positive. Since $\tilde{\mathbf{s}}_{-n} < \mathbf{s}_{-n}$, it can

$$B_n(\mathbf{s}_{-n}) - B_n(\tilde{\mathbf{s}}_{-n}) = \sqrt{\frac{Q_n + M_n}{p_c e^{\frac{D_n}{G_1 G_2 T}}}}\left(\sqrt{\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}} - \sqrt{\sum_{n' \in \mathcal{N}, n' \neq n} \tilde{s}_{n'}}\right) - \left(\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'} - \sum_{n' \in \mathcal{N}, n' \neq n} \tilde{s}_{n'}\right)$$
$$= \underbrace{\left(\sqrt{\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}} - \sqrt{\sum_{n' \in \mathcal{N}, n' \neq n} \tilde{s}_{n'}}\right)}_{g_1} \underbrace{\left(\sqrt{\frac{Q_n + M_n}{p_c e^{\frac{D_n}{G_1 G_2 T}}}} - \sqrt{\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}} - \sqrt{\sum_{n' \in \mathcal{N}, n' \neq n} \tilde{s}_{n'}}\right)}_{g_2} \tag{50}$$

be easily proved that $g_1 > 0$. By using $g_1 > 0$, g_2 can be written as

$$g_2 > \sqrt{\frac{Q_n + M_n}{p_c e^{\frac{D_n}{G_1 G_2 T}}}} - 2\sqrt{\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}}. \tag{51}$$

By taking the square root of both sides of (47), we have

$$g_2 > \sqrt{\frac{Q_n + M_n}{p_c e^{\frac{D_n}{G_1 G_2 T}}}} - 2\sqrt{\sum_{n' \in \mathcal{N}, n' \neq n} s_{n'}} > 0. \tag{52}$$

Thus, we have $B_n(\mathbf{s}_{-n}) - B_n(\tilde{\mathbf{s}}_{-n}) = g_1 g_2 > 0$. This completes the proof of monotonicity.

Finally, we will prove the scalability of (38) as follows:

$$\psi B_n(\mathbf{s}^*_{-n}) - B_n(\psi \mathbf{s}^*_{-n}) = \left(\psi - \sqrt{\psi}\right)\sqrt{\frac{(Q_n + M_n)\sum\limits_{n' \in \mathcal{N}, n' \neq n} s_{n'}}{p_c e^{\frac{D_n}{G_1 G_2 T}}}} > 0. \tag{53}$$

Hence, the best response function of any LEAG is a standard function and the Nash equilibrium is unique. ■

2) Solution of the First-Stage Optimization Problem: Based on the optimal service demand strategies of all the LEAGs obtained in the second stage, the first-stage service price optimization problem can be solved. By substituting the Nash equilibrium of the second-stage N-player noncooperative game into (31), the utility of the ESP U_E can be written as

$$U_E(p_c) = (p_c - \gamma_c)\frac{N-1}{p_c \sum_{n' \in \mathcal{N}} \frac{e^{\frac{D_{n'}}{G_1 G_2 T}}}{Q_{n'} + M_{n'}}}. \tag{54}$$

Then, we have the following properties.

Theorem 7 (Concavity): P4 is a standard convex optimization problem.

Proof: We can prove that the second-order derivative of (54) is negative, which is given by

$$\frac{\partial U_E}{\partial p_c} = -2\frac{\gamma_c(N-1)}{p_c^3 \sum_{n \in \mathcal{N}} \frac{e^{\frac{D_n}{G_1 G_2 T}}}{Q_n + M_n}} < 0. \tag{55}$$

This complete the proof. ■

Since P4 is a convex optimization problem, the optimal solution p_c^* can be easily solved by using KKT conditions. We have the following property.

Theorem 8 (Stackelberg Equilibrium): The Nash equilibrium of the second-stage N-player noncooperative game $\{s_n^*, \mathbf{s}_{-n}^*\}$ and the optimal solution of the first-stage service price optimization problem p_c^* constitute the Stackelberg equilibrium.

Proof: For any feasible s_n, $n \in \mathcal{N}$, we have

$$U_{n,b}(s_n^*, \mathbf{s}_{-n}^*, p_c^*) \geq U_{n,b}(s_n, \mathbf{s}_{-n}^*, p_c^*). \tag{56}$$

Furthermore, for any feasible p_c, we have

$$U_E(s_n^*, \mathbf{s}_{-n}^*, p_c^*) \geq U_E(s_n^*, \mathbf{s}_{-n}^*, p_c). \tag{57}$$

This completes the proof. ■

VI. Simulation Results and Analysis

In this section, we validate the proposed scheme via simulations.

A. Contract Feasibility and Social Welfare

We consider a parking lot with one LEAG and $K = 20$ EVs. We assume that the EV type follows a Gaussian distribution. For any EV, the battery capacity is 24 kWh, and the unit discharging cost is 10 cents/kWh, i.e., $\gamma = 10$. The unit revenue of electricity for the LEAG is 13 cents/kWh, i.e., $\gamma_L = 13$. The contract without information asymmetry and the linear-pricing scheme studied in [38] are utilized for the purpose of comparison. In the linear-pricing scheme, the LEAG does not distinguish EVs by their types, and offers a unified price ρ to all the EVs. There exists a linear relationship between the reward and discharged electricity, e.g., $R_k = \rho L_k$, $k = 1, \ldots, K$.

Fig. 2(a) and (b) shows the discharged electricity and the reward, respectively. It is observed that both the reward and the discharged electricity increase monotonically with the EV type, which follows Lemma 2. Furthermore, numerical results show that the contract without information asymmetry demands much higher amounts of electricity from EVs, but offers EVs with the same reward, which is consistent with Lemma 4. In the linear-pricing scheme, the amount of discharged electricity is lower than the other schemes, which represents that the unified pricing scheme cannot effectively motivate EVs to participate in the energy trading.

Fig. 2(c) shows the relationship between utilities of type 4, type 8, and type 12 EV and contract items. It is validated that the proposed contract is incentive compatible. An EV can achieve its maximum utility if and only if it selects the contract item dedicated for its type. Furthermore, we can observe that the utility of EV increases with the EV type, which is explained in Lemma 2.

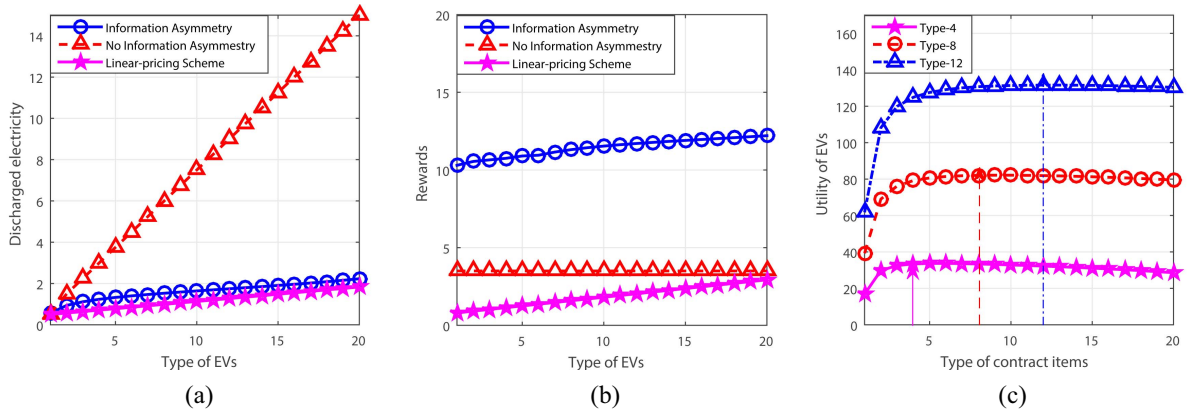


Fig. 2. Contract feasibility: (a) discharged electricity; (b) reward; and (c) EV's utility.

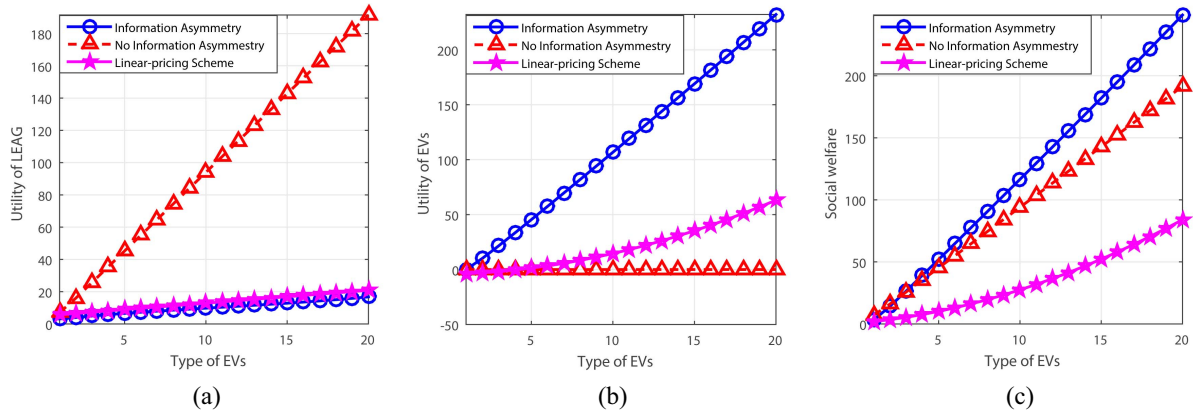


Fig. 3. System performance: (a) LEAG's utility; (b) EV's utility; and (c) social welfare.

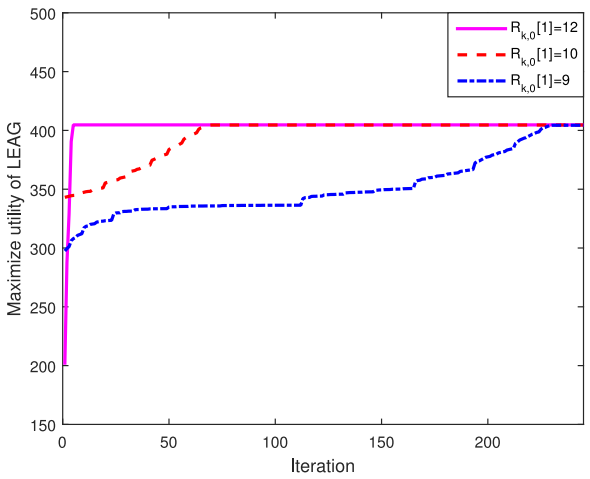


Fig. 4. Convergence performance of the proposed CCP-based solution.

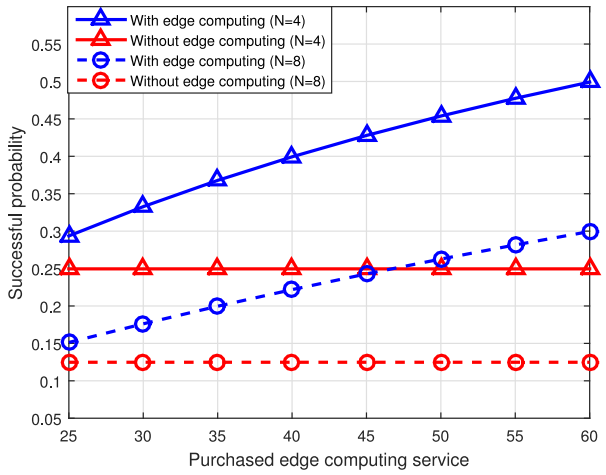


Fig. 5. Successful probability versus purchased amount of services.

Fig. 3(a) and (b) shows the utility of the LEAG and the utilities of EVs, respectively. Without information asymmetry, the LEAG can achieve a much higher utility, while the utility of any EV remains zero, which is consistent of Lemma 3. Thus, the presence of information asymmetry actually protects EVs from over-exploitation since the precise knowledge of EV type is unknown to the LEAG. The linear-pricing scheme achieves the worst performance since the type of EV has not been fully exploited.

Fig. 3(c) shows the relationship between social welfare and EV type. The contract without information asymmetry performs worse than the contract with information asymmetry. The reason is that under complete information, the utility of any EV is exactly zero, which significantly decreases the social welfare. The linear-pricing scheme achieves the lowest

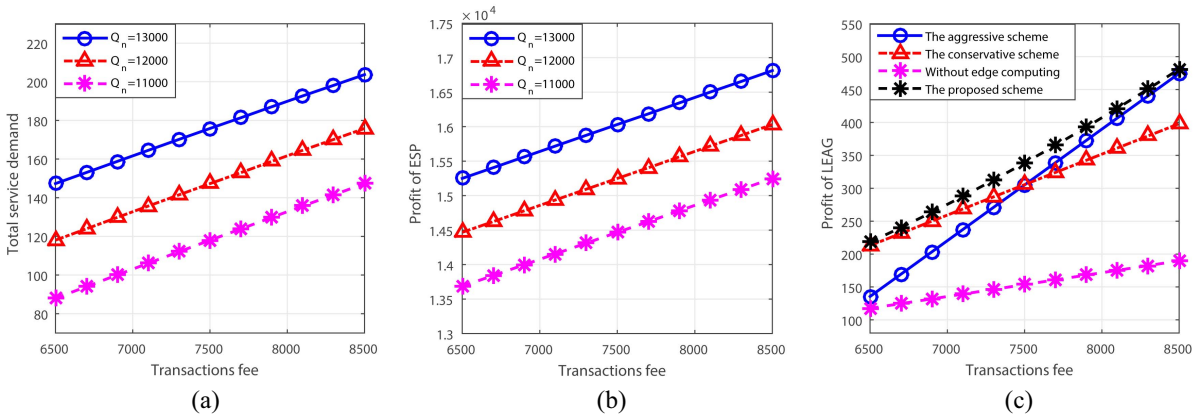


Fig. 6. Efficiency of task offloading: (a) total service demand; (b) profit of ESP; and (c) profit of LEAG.

social welfare because the information of EV type has been neglected.

Fig. 4 shows the convergence performance of the proposed CCP-based solution. Three initial points, i.e., $\{R_{k,0}[1]\} = 12, 10,$ and 9 are chosen to characterize the impact of initial point on the convergence speed. As the iteration number increases, all the three cases converge to the optimal social welfare. Particularly, the case with $\{R_{k,0}[1]\} = 12$ only requires ten iterations to reach convergence. The reason is that 12 is closest to the average value of the optimal rewards shown in Fig. 2(b) (which is 12.66). In comparison, the case with $\{R_{k,0}[1]\} = 9$ requires more than 200 iterations.

B. Edge Computing-Based Computational Task Offloading

To verify the benefits brought by edge computing, we consider two cases with four and eight LEAGs, i.e., $N = 4$ and $N = 8$, respectively. In the case of $N = 4$, we assume that edge computing service is not available to the first three LEAGs, and we fix their computational power as 10, 20, and 30, respectively. Meanwhile, we assume that the fourth LEAG can purchase service from the ESP and vary its purchased service demand to demonstrate the impact on the successful probability of block creation. In the case of $N = 8$, the computational power of the first seven LEAGs is fixed in the range $[10, 40]$. The conventional scheme without the assistance of edge computing is used for comparison [30]. We assume that D_n follows a normal distribution, i.e., $\mathcal{N}(\mu_{D_n}, \sigma^2_{D_n})$, where $\mu_{D_n} = 200$ and $\sigma^2_{D_n} = 10$.

Fig. 5 shows the successful probability versus the purchased service demand. When the service demand purchased from the ESP is 55, simulation results demonstrate that the successful probability of the proposed edge computing-based scheme outperforms that of the conventional scheme by 92.4% and 124.6% in the cases of $N = 4$ and $N = 8$, respectively. The reason is that the relative computational power of the LEAG which has access to edge computing services can be increased by orders of magnitudes compared to those LEAGs which only rely on their local computational power.

Fig. 6 shows the total service demand, the profit of the ESP, and the average profit of the LEAG versus the transaction fee M_n. The simulation parameters are $s_{n,\min} = 90$, $s_{n,\max} = 210$, $p_{c,\min} = 0$, $p_{c,\max} = 15$, $Q_n = 12000$, $\gamma_c = 3$, $G_1 = 50$, $G_2 = 4$, and $N = 50$. Fig. 6(a) and (b) demonstrates that both the total service demand and the profit of the ESP increase monotonically with the transaction fee. The reason behind is that the increased transaction fee provides a larger incentive for LEAGs to purchase more services from the ESP. This not only improves the successful probability of LEAGs but also increases the profit of the ESP. Furthermore, it is observed that both the total service demand and the profit of the ESP increase monotonically with the block creation reward Q_n, which is also due to the fact that a higher reward provides a greater motivation for LEAGs to buy more services.

Fig. 6(c) shows the average profit of the nth LEAG achieved by four different schemes: 1) the proposed scheme; 2) the conventional scheme without edge computing; 3) the aggressive scheme in which the nth LEAG always purchases the maximum amount of services $s_{n,\max}$; and 4) the conservative scheme in which the nth LEAG always purchases the minimum amount of services $s_{n,\min}$. It is clear that the proposed scheme outperforms the other three heuristic schemes because the LEAG's strategy is optimized with regards to the transaction fee. When the transaction fee is low, the conservative scheme performs better than the aggressive scheme. It is not worth to buy more services because the expected profit cannot compensate the cost of purchasing services. In comparison, when the transaction fee is high enough, the LEAG should purchase a larger amount of services to increase the chance of winning because the expected profit is much higher than the service cost. Under all scenarios, the conventional scheme without edge computing performs the worst due to the reason explained in Fig. 5.

C. Privacy and Security Analysis

In this section, we provide the privacy and the security analysis.

1) Anonymity: Instead of using its true identity, each EV uses a unique public key to communicate with others, which

prevents malicious attackers from tracking an EV's identity. Furthermore, an EV can change its public key after each transaction to avoid the linking attack, i.e., the different pieces of data belonging to the same EV are linked together to deanonymize the EV.

2) Authentication: In the process of proof-of-work, every transaction has to be publicly audited and authenticated by authorized LEAGs. It is impossible to compromise all of the authorized LEAGs in the network.

3) Integrity: Once a block has been appended into the blockchain, it contains the hash of the previous block, and its own hash will be contained in the subsequent block. Therefore, it is infeasible to modify the block unless the majority of the computational power are controlled by a malicious attacker. Moreover, the transaction data contained in a block are encrypted with asymmetric encryption techniques. It takes a tremendous cost to decrypt the encrypted data without knowing the private key.

4) Transparency: Since the blockchain technology is open source, any user, software developer, and service provider can have access to the blockchain and monitor the corresponding transaction data. That is, the transaction data are not saved in one single node and are transparent to all entities. As a result, any malicious data modification can be noticeable and traceable.

VII. Conclusion

In this paper, we proposed a secure and efficient V2G energy trading framework for CPSs by combining blockchain, edge computing, and contract theory. Specifically, a contract-based incentive mechanism was developed to motivate EVs to participate in energy trading, and the energy trading between EVs and LEAGs is secured by exploiting consortium blockchain. Furthermore, an edge computing-based task offloading mechanism was proposed to relieve the computation burden of LEAGs and increase the successful probability of block creation. The numerical results and theoretical analysis show that the proposed framework achieves good performance in terms of contract feasibility, task offloading, and security. Some important conclusions are summarized as follows.

First, the proposed framework enables efficient energy trading under information asymmetry. The asymmetric information of EV type can be effectively elicited by the incentive-compatible contract, i.e., an EV's type is automatically revealed by observing its selection of contract items. Second, the CCP-based contract optimization algorithm can effectively maximize the expected utility of the LEAG. However, the determination of initial point has a significant impact on the convergence performance of CCP. Thus, how to select initial point to increase the convergence speed requires further investigation. Third, the successful probability of block creation can be effectively improved by utilizing edge computing. Simulation results demonstrate that the successful probability can be increased by 124.6% with the presence of eight LEAGs.

In future works, we will investigate the more complicated scenario where even the statistical knowledge of the EV type is unknown, and study how to leverage machine learning-based approaches to infer the corresponding knowledge.

References

[1] S. A. Seshia, S. Hu, W. Li, and Q. Zhu, "Design automation of cyber-physical systems: Challenges, advances, and opportunities," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 36, no. 9, pp. 1421–1434, Sep. 2017.

[2] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "FCSS: Fog computing based content-aware filtering for security services in information centric social networks," *IEEE Trans. Emerg. Topics Comput.*, to be published.

[3] C.-K. Tham and T. Luo, "Sensing-driven energy purchasing in smart grid cyber-physical system," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 43, no. 4, pp. 773–784, Jul. 2013.

[4] M. Ban, M. Shahidehpour, J. Yu, and Z. Li, "A cyber-physical energy management system for optimal sizing and operation of networked nanogrids with battery swapping stations," *IEEE Trans. Sustain. Energy*, vol. 10, no. 1, pp. 491–502, Dec. 2019.

[5] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[6] Z. Zhou, J. Gong, Y. He, and Y. Zhang, "Software defined machine-to-machine communication for smart energy management," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 52–60, Oct. 2017.

[7] E. Zio and G. Sansavini, "Vulnerability of smart grids with variable generation and consumption: A system of systems perspective," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 43, no. 3, pp. 477–487, May 2013.

[8] A. Jindal, J. S. Aujla, N. Kumar, and S. Misra, "Sustainable smart energy cyber-physical system: Can electric vehicles suffice its needs?" in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[9] Z. Zhou *et al.*, "Dependable content distribution in D2D-based cooperative vehicular networks: A big data-integrated coalition game approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 3, pp. 953–964, Mar. 2018.

[10] A. H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 3, pp. 320–331, Dec. 2010.

[11] Z. Zhou *et al.*, "Robust energy scheduling in vehicle-to-grid networks," *IEEE Netw.*, vol. 31, no. 2, pp. 30–37, Mar./Apr. 2017.

[12] H. Li, K. Ota, and M. Dong, "Energy cooperation in battery-free wireless communications with radio frequency energy harvesting," *ACM Trans. Embed. Comput. Syst.*, vol. 17, no. 2, pp. 1–44, Apr. 2018.

[13] E. L. Karfopoulos, K. A. Panourgias, and N. D. Hatziargyriou, "Distributed coordination of electric vehicles providing V2G regulation services," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 2834–2846, Jul. 2016.

[14] S. Pal and R. Kumar, "Electric vehicle scheduling strategy in residential demand response programs with neighbor connection," *IEEE Trans. Ind. Informat.*, vol. 14, no. 3, pp. 980–988, Mar. 2018.

[15] 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.

[16] W. L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in IoT-based smart grid communications," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, Oct. 2017.

[17] Y. Cao *et al.*, "An EV charging management system concerning drivers' trip duration and mobility uncertainty," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 48, no. 4, pp. 596–607, Apr. 2018.

[18] Z. Zhou *et al.*, "Social big-data-based content dissemination in Internet of Vehicles," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 768–777, Feb. 2018.

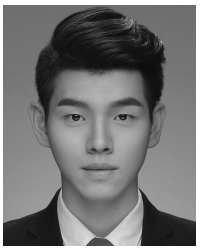
[19] V. R. Tannahill, D. Sutanto, K. M. Muttaqi, and M. A. Masrur, "Future vision for reduction of range anxiety by using an improved state of charge estimation algorithm for electric vehicle batteries implemented with low-cost microcontrollers," *IET Elect. Syst. Transport.*, vol. 5, no. 1, pp. 24–32, Feb. 2015.

[20] Y. Wu *et al.*, "Optimal pricing and energy scheduling for hybrid energy trading market in future smart grid," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1585–1596, Dec. 2015.
[21] H. Li, K. Ota, and M. Dong, "Learning IoT in edge: Deep learning for the Internet of Things with edge computing," *IEEE Netw.*, vol. 32, no. 1, pp. 96–101, Jan./Feb. 2018.
[22] J. Xu, K. Ota, and M. Dong, "Saving energy on the edge: In-memory caching for multi-tier heterogeneous networks," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 102–107, May 2018.
[23] L. Li, K. Ota, and M. Dong, "DeepNFV: A lightweight framework for intelligent edge network functions virtualization," *IEEE Netw.*, vol. 33, no. 1, pp. 136–141, Jan./Feb. 2019.
[24] Z. Zhou *et al.*, "Game-theoretical energy management for energy Internet with big data-based renewable power forecasting," *IEEE Access*, vol. 5, pp. 5731–5746, 2017.
[25] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, to be published.
[26] V. Gatteschi, F. Lamberti, C. D. C. Pranteda, and V. Santamaría, "To blockchain or not to blockchain: That is the question," *IT Prof.*, vol. 20, no. 2, pp. 62–74, Apr. 2018.
[27] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.
[28] 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.
[29] S. Aggarwal *et al.*, "EnergyChain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem," in *Proc. ACM MobiHoc Workshop Netw. Cybersecurity Smart City*, Los Angeles, CA, USA, Jun. 2018, p. 1.
[30] 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.
[31] D. Sahinel, C. Akpolat, M. A. Khan, F. Sivrikaya, and S. Albayrak, "Beyond 5G vision for IOLITE community," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 41–47, Jan. 2017.
[32] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "UAV-empowered edge computing environment for cyber-threat detection in smart vehicles," *IEEE Netw.*, vol. 32, no. 3, pp. 42–51, May/Jun. 2018.
[33] Z. Zhou, J. Feng, L. Tan, Y. He, and J. Gong, "An air-ground integration approach for mobile edge computing in IoT," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 40–47, Aug. 2018.
[34] Z. Zhou *et al.*, "Robust mobile crowd sensing: When deep learning meets edge computing," *IEEE Netw.*, vol. 32, no. 4, pp. 54–60, Jul./Aug. 2018.
[35] Y. Li *et al.*, "An interactive decision making model based on energy and reserve for electric vehicles and power grid using generalized Stackelberg game," *IEEE Trans. Ind. Appl.*, to be published.
[36] M. Ghofrani, A. Arabali, M. Etezadi-Amoli, and M. S. Fadali, "Smart scheduling and cost-benefit analysis of grid-enabled electric vehicles for wind power integration," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2306–2311, Sep. 2014.
[37] L. Duan, L. Gao, and J. Huang, "Cooperative spectrum sharing: A contract-based approach," *IEEE Trans. Mobile Comput.*, vol. 13, no. 1, pp. 174–187, Jan. 2014.
[38] Y. Zhang, L. Song, W. Saad, Z. Dawy, and Z. Han, "Contract-based incentive mechanisms for device-to-device communications in cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2144–2155, Oct. 2015.
[39] T. Liu *et al.*, "Design of contract-based trading mechanism for a small-cell caching system," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6602–6617, Oct. 2017.
[40] Q. Wang, X. Li, and Y. Yu, "Anonymity for bitcoin from secure escrow address," *IEEE Access*, vol. 6, pp. 12336–12341, 2017.
[41] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Security*, vol. 1, no. 1, pp. 36–63, Aug. 2001.
[42] Y.-L. Gao *et al.*, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.
[43] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5394–5401, 2018.
[44] P. R. Rizun, "A transaction fee market exists without a block size limit," Working Paper, Aug. 2015. [Online]. Available: https://www.bitcoinunlimited.info/resources/feemarket.pdf
[45] D. He, N. Kumar, S. Zeadally, and H. Wang, "Certificateless provable data possession scheme for cloud-based smart grid data management systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 3, pp. 1232–1241, Mar. 2018.
[46] D. Khovratovich, C. Rechberger, and A. Savelieva, "Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family," in *Proc. Int. Conf. FAST Softw. Encryption*, Washington, DC, USA, Mar. 2012, pp. 244–263.
[47] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ, USA: Wiley, 2001.
[48] Y. Wang and J. Gao, "A regulation scheme based on the ciphertext-policy hierarchical attribute-based encryption in bitcoin system," *IEEE Access*, vol. 6, pp. 16267–16278, 2018.
[49] Y. Zheng and J. Seberry, "Immunizing public key cryptosystems against chosen ciphertext attacks," *IEEE J. Sel. Areas Commun.*, vol. 11, no. 5, pp. 715–724, Jun. 1993.
[50] M. Abdalla, F. Benhamouda, and D. Pointcheval, "Public-key encryption indistinguishable under plaintext-checkable attacks," *IET Inf. Security*, vol. 10, no. 6, pp. 288–303, Nov. 2016.
[51] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/en/
[52] G.-C. Hsieh, L.-R. Chen, and K.-S. Huang, "Fuzzy-controlled Li-ion battery charge system with active state-of-charge controller," *IEEE Trans. Ind. Electron.*, vol. 48, no. 3, pp. 585–593, Jun. 2001.
[53] T. Lipp and S. Boyd, "Variations and extension of the convex–concave procedure," *Optim. Eng.*, vol. 17, no. 2, pp. 263–287, Jun. 2016.
[54] N. Houy, "The bitcoin mining game," *The Ledger*, 2016, pp. 53–68. [Online]. Available: http://www.ledgerjournal.org/ojs/index.php/ledger/article/view/13
[55] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA, USA: MIT Press, 1994.

Zhenyu Zhou (M'11–SM'17) received the M.E. and Ph.D. degrees in global information and telecommunication studies from Waseda University, Tokyo, Japan, in 2008 and 2011, respectively.

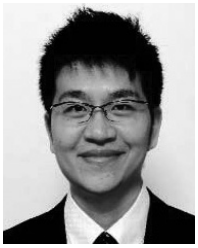
From 2012 to 2013, he was the Chief Researcher with the Department of Technology, KDDI, Tokyo. Since 2013, he has been an Associate Professor with the School of Electrical and Electronic Engineering, North China Electric Power University, Beijing, China. His current research interests include green communications, vehicular communications, and smart grid communications.

Dr. Zhou was a recipient of the IEEE Vehicular Technology Society "Young Researcher Encouragement Award" in 2009, the "Beijing Outstanding Young Talent Award in 2016, the IET Premium Award in 2017, and the IEEE ComSoc Green Communications and Computing Technical Committee 2017 Best Paper Award. He served as an Associate Editor for IEEE ACCESS and *EURASIP Journal on Wireless Communications and Networking* and a Guest Editor for *IEEE Communications Magazine* and *Transactions on Emerging Telecommunications Technologies*. He also served as the Workshop Co-Chair for IEEE Globecom 2018 and IEEE ISADS 2015, and a TPC Member for IEEE Globecom, IEEE CCNC, IEEE ICC, IEEE APCC, IEEE VTC, and IEEE Africon. He is a Voting Member of IEEE Standard Association P1932.1 Working Group.



Bingchen Wang is currently pursuing the B.S. degree in smart grid information engineering with North China Electric Power University, Beijing, China.

His current research interests include green communications and smart grid.



Mianxiong Dong (M'13) received the B.S., M.S., and Ph.D. degrees in computer science and engineering from the University of Aizu, Aizuwakamatsu, Japan.

He is currently an Associate Professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Muroran, Japan. He was a JSPS Research Fellow with the School of Computer Science and Engineering, University of Aizu. He was a Visiting Scholar with the BBCR Group, University of Waterloo, Waterloo, ON, Canada, supported by JSPS Excellent Young Researcher Overseas Visit Program from 2010 to 2011. His current research interests include wireless networks, cloud computing, and cyber-physical systems.

Dr. Dong was a recipient of the IEEE TCSC Early Career Award 2016, the IEEE SCSTC Outstanding Young Researcher Award 2017, the 12th IEEE ComSoc Asia–Pacific Young Researcher Award 2017, the Funai Research Award 2018, the NISTEP Researcher 2018 (one of only 11 people in Japan) in recognition of significant contributions in science and technology, the Best Paper Awards from IEEE HPCC 2008, IEEE ICESS 2008, ICA3PP 2014, GPC 2015, IEEE DASC 2015, IEEE VTC 2016-Fall, and FCST 2017, the 2017 IET Communications Premium Award, and the IEEE ComSoc CSIM Best Conference Paper Award 2018. He was selected as a Foreigner Research Fellow (a total of three recipients all over Japan) by NEC C&C Foundation in 2011. He serves as an Editor for the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE NETWORK, IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE CLOUD COMPUTING, and IEEE ACCESS, as well as a Leading Guest Editor for *ACM Transactions on Multimedia Computing, Communications and Applications*, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, and IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS. He has been serving as the Vice Chair of IEEE Communications Society Asia/Pacific Region Information Services Committee and Meetings and Conference Committee, the Leading Symposium Chair of IEEE ICC 2019, the Student Travel Grants Chair of IEEE GLOBECOM 2019, and the Symposium Chair of IEEE GLOBECOM 2016 and 2017. He is currently a member of Board of Governors and Chair of Student Fellowship Committee of IEEE Vehicular Technology Society, and Treasurer of IEEE ComSoc Japan Joint Sections Chapter.

Kaoru Ota (M'12) was born in Aizu-Wakamatsu, Japan. She received the B.S. degree in computer science and engineering from the University of Aizu, Aizuwakamatsu, Japan, in 2006, the M.S. degree in computer science from Oklahoma State University, Stillwater, OK, USA, in 2008, and the Ph.D. degree in computer science and engineering from the University of Aizu in 2012.

She is currently an Assistant Professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Muroran, Japan. From 2010 to 2011, she was a Visiting Scholar with the University of Waterloo, Waterloo, ON, Canada. She was also a Japan Society of the Promotion of Science Research Fellow with Kato-Nishiyama Laboratory, Graduate School of Information Sciences, Tohoku University, Sendai, Japan, from 2012 to 2013. Her current research interests include wireless networks, cloud computing, and cyber-physical systems.

Dr. Ota was a recipient of the Best Paper Awards from ICA3PP 2014, GPC 2015, IEEE DASC 2015, IEEE VTC 2016-Fall, and FCST 2017, the 2017 IET Communications Premium Award, the IEEE ComSoc CSIM Best Conference Paper Award 2018, the IEEE TCSC Early Career Award 2017, and the 13th IEEE ComSoc Asia–Pacific Young Researcher Award 2018. She is an Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE COMMUNICATIONS LETTERS, *Peer-to-Peer Networking and Applications* (Springer), *Ad Hoc & Sensor Wireless Networks*, *International Journal of Embedded Systems* (Inderscience), and *Smart Technologies for Emergency Response & Disaster Management* (IGI Global), as well as a Guest Editor of *ACM Transactions on Multimedia Computing, Communications and Applications* (leading), IEEE INTERNET OF THINGS JOURNAL, *IEEE Communications Magazine*, IEEE NETWORK, IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, *IEICE Transactions on Information and Systems*, and *Ad Hoc & Sensor Wireless Networks* (Old City Publishing).