IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 27 November 2022, accepted 12 December 2022, date of publication 15 December 2022,
date of current version 21 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3229432

RESEARCH ARTICLE

V2GNet: Robust Blockchain-Based Energy Trading Method and Implementation in Vehicle-to-Grid Network

YUXIAO LIANG, ZHISHANG WANG, (Graduate Student Member, IEEE), AND ABDERAZEK BEN ABDALLAH, (Senior Member, IEEE)

Adaptive Systems Laboratory, Graduate School of Computer Science and Engineering, The University of Aizu, Aizuwakamatsu, Fukushima 965-8580, Japan

Corresponding authors: Yuxiao Liang (d8222116@u-aizu.ac.jp) and Abderazek Ben Abdallah (benab@u-aizu.ac.jp)

This work was supported in part by the University of Aizu Competitive Research Funding, Fukushima, Japan, under Grant UoA-CRF-2022-P7.

ABSTRACT Nowadays, energy trading policies are revolutionizing the efforts and policies geared toward addressing global carbon emissions and protecting the environment. Smart grids and electric vehicles (EVs) are energy-saving tools for efficient power management. Although EVs can act as both energy consumers and suppliers, the effort required to balance the energy supply and demand in typical centralized trading systems inevitably reduces trading reliability. Another challenge is distributing EVs' energy rationally to achieve better demand response and energy utilization. To manage the market securely and efficiently, we propose V2GNet(AEBiS Project: https://web-ext.u-aizu.ac.jp/misc/benablab/aebis.html), a blockchain-based energy trading system using the vehicle-to-grid (V2G) network. The system combines a blockchain of energy exchanges (BoE) and a blockchain of EVs (BoEV), with the distinct transmission of energy requests and offers. Furthermore, to consider energy management from an economic viewpoint, we address the attack issue by proposing a robust energy trading (*RET*) algorithm. The proposed system demonstrates high robustness to malicious attacks. Our experimental results show that the *RET* reduces 30% energy loss when 20% of consumers are attacked. Moreover, malicious exchanges are excluded progressively from the trading market during each trading round. Also, the *RET* algorithm achieves better energy fulfillment and higher profit compared to state-of-the-art approaches.

INDEX TERMS Energy trading, electric vehicles, robustness, vehicle-to-grid.

I. INTRODUCTION

With the advancement in energy storage and bidirectional charging technologies, electric vehicles (EVs) now serve as both energy consumers and suppliers in grids [1], [2], [3]. It is expected that integrating the vehicular network and energy infrastructure will be a viable measure to remedy energy peak load, accelerate the balance of supply and demand, and improve utility efficiency. Unlike conventional vehicles, EVs can provide a reliable optimization for current energy trading. However, many shared EVs and renewables are supported by government subsidies rather than being integrated into the regular electricity market. This is partly because the trading mechanism of the current energy market is neither profitable nor safe for EVs. In current energy trading, market participants keep separate business records of their transactions. A record must be kept for each transaction to verify the trading process. Therefore, individual traders' records are unique and fragmented, prone to a single point of failure. The rapid growth of vehicle-to-grid (V2G) in energy trading is worsening the situation, raising an urgent need for new distributed solutions with higher resilience, confidentiality, and flexibility. In the meantime, a practical trading mechanism is necessary to dispatch energy requests and economically exploit EV capacity.

To address the security issue in EV energy trading, several works have employed blockchain-based distributed architectures [4], [5], [6], [7], [8], [9]. These architectures can be broadly divided into permissionless and permissioned. The permissionless blockchains are public systems that

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

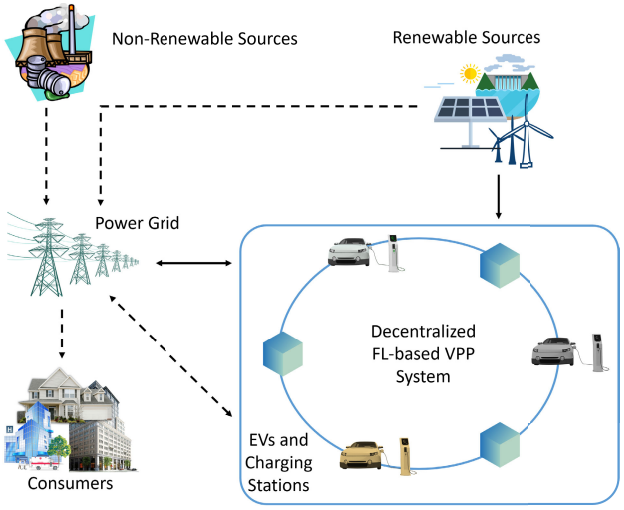

FIGURE 1. Virtual Power Plant (VPP) in Network of EVs (NoEV) [18]. The NoEV integrates a VPP aggregator and EVs in federated learning (FL) and blockchain system.

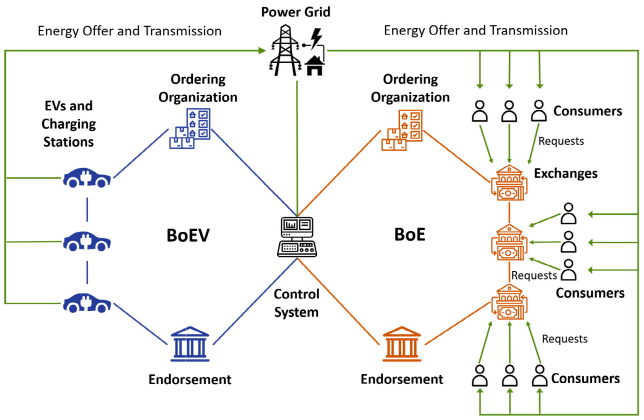

FIGURE 2. Overview of the proposed V2GNet. Each campus' control system (CS) works as a mediator between energy consumers and suppliers (EVs). Each consumer connects and submits the energy request to the energy exchange. The blockchain of exchanges (BoE) integrates exchanges and the CS, where the request lists (exchanges to CS) and notification of supply results (CS to exchanges) are transmitted. Besides, the blockchain of EVs (BoEV) integrates EVs and the CS, where the offer lists (EVs to CS) and notification of discharge tasks (CS to EVs) are transmitted. The CS works as an information mediator, while the power grid works as a mediator for energy transmission between EVs and consumers.

mainly rely on probabilistic consensus algorithms to preserve consistency [10], [11]. However, when multiple ordering nodes receive transactions simultaneously, they can order the transactions differently, resulting in divergent ledgers. The current remedy for this drawback comes at a rather high cost, so arranging transactions in a strict order is crucial. In permission systems, only vetted nodes can generate transactions and participate in the consensus process [12]. A trusted ordering organization consisting of selected nodes can order and bundle transactions for all nodes, thus diminishing the risk of ledger divergence. Nevertheless, because transactions are visible to each node, the nodes of traders still face the risk of internal malicious damage. And a tradeoff must be made between the confidentiality of trade details and the degree of mutual trust.

In addition to the security issue, another concern for V2G energy trading is the optimal dispatch of energy. To achieve efficient energy utilization and high profits, game theoretical pricing mechanisms [13], [14], [15] and auction-based incentive mechanisms [16], [17] are proposed. These works focus on optimal scheduling for either the EV or the consumer side while failing to manage both energy demand and response concurrently.

To our knowledge, state-of-the-art blockchain architectures for V2G networks integrate vehicles and energy customers. However, much communication between the vehicle and customer networks is unnecessary, leading to redundant data transmission and inefficiencies in the system. Besides, for optimal energy distribution, few of those mentioned works consider the scheduling of both EVs and consumers. In addition, the system's resilience to malicious energy consumers and energy exchanges has not been investigated.

To address the challenges mentioned above, based on our previous works on NoEV [18] (as shown in Fig. 1), we propose V2GNet, a blockchain-based campus energy trading system. The architecture of the V2GNet is illustrated in Fig. 2. We establish a blockchain of energy exchanges (BoE) and a blockchain of EVs (BoEV). We also present a detailed energy trading algorithm connecting the consumer/exchange side and EV side. On top of these, we provide a complete analysis of the response time of energy requests. And furthermore, we introduce a security solution called robust energy trading algorithm (*RET*) against malicious attacks while addressing energy fulfillment and profit. The contributions are summarized as follows:

- A comprehensive classification of the state-of-the-art research on energy trading.
- A novel energy trading system based on a cross-cluster architecture containing a blockchain of energy exchanges (BoE) and a blockchain of EVs (BoEV). A control system (CS) is a mediator between the network of exchanges and EVs and participates in both BoE and BoEV.
- An energy trading algorithm introduces the entire workflow of energy request, offer, and allocation between consumers and EVs.
- A complete analysis of the response time of energy requests. We formulate the time analysis by dividing the entire workflow into five stages.
- A robust energy trading algorithm (*RET*) with a penalty mechanism is proposed against malicious attacks from consumers and exchanges.
- An efficient algorithm for energy allocation that ensures the energy fill rate and total profit.

The rest of this paper is organized as follows. In Section II, we discuss the related works on distributed energy supply and trading, secure energy trading systems, aggregated

energy exchange, and EV energy trading systems. In Section III, we present the proposed V2GNet, including the energy trading process, blockchain-enabled data storage and transmission, analysis of response time, and robust energy trading algorithm against malicious consumers and exchanges. Section IV provides the performance evaluation of the proposed V2GNet system. In Section V and VI, the discussion and conclusion are presented.

II. RELATED WORK

This section presents the related works on distributed energy supply and trading, secure energy trading systems, aggregated energy exchange, and EV energy trading systems.

A. DISTRIBUTED ENERGY SUPPLY & TRADING

In the conventional energy market, energy flows unilaterally from generation companies to consumers [19]. Such grids are mature in containing fossil-fired power plants yet cannot absorb changing renewables and minor suppliers. Though some research tries to establish bidirectional energy systems upon the conventional centralized ones [20], the conflict between energy trading security and transparency remains a dilemma. As a result, distributed energy supply and trading systems are growing globally to optimize outdated market systems and relieve energy shortages. Fig. 3 gives a brief classification of the energy trading types. Luo et al. proposed a distributed electricity trading system to facilitate trusted and secured peer-to-peer electricity sharing among consumers [21]. Yahaya et al. [22] proposed a secured Peer-to-Peer energy trading model with an authentication layer to defend against impersonation attacks and an energy trading layer to minimize the number of malicious validators.

B. SECURE ENERGY TRADING SYSTEMS

Some related works [23], [24], [25], [26], and [27] focus on optimizing the system performance by maximizing overall trading welfare, minimizing trading overhead, and enhancing resilience in unpredicted outages. Nevertheless, their neglect of trading security can be fatal, for data leaks, malicious tampering, and intentional attacks may lead to considerable losses during energy trading. For this reason, abundant references highlight trading security in their energy systems. Khorasan et al. [28] proposed a decentralized peer-to-peer energy trading scheme for secure forward market trading using the primal-dual gradient method. Ma et al. [29] introduced a novel secure communication scheme to prevent potential false data injection attacks and other cyber risks. Although these works strengthen energy trading security through different solutions, recently, blockchain has been employed by many researchers as an ideal way to reinforce systematic security in distributed energy trading. Yang et al. [30] proved the blockchain effective in securing the distributed control systems against false data injection attacks in a hierarchical prosumer microgrid. Gai et al. [12] presented a consortium blockchain-oriented approach to solving the privacy leakage without restricting trading functions. Aitzhan and Svetinovic [31] addressed the transaction security in decentralized smart grid energy trading by implementing proof-of-concept, multi-signatures, and anonymous encrypted messaging streams. And Li et al. [32] introduced a blockchain-combined superconducting energy storage unit to avoid transaction failure in EV Peer-to-Peer energy trading.

C. AGGREGATED ENERGY EXCHANGE

Among blockchain-based energy trading solutions, several systems relating to charging stations, renewable trading, or intelligent households employ peer-to-peer energy trading. Doan et al. [33] improved consumer profits through peer-to-peer energy trading and a double auction-based game theoretic approach. Kang et al. [3] also proposed a localized peer-to-peer electricity trading model for plug-in hybrid electric vehicles in smart grids. Hassan et al. [34] developed a blockchain-based approach for secure and private microgrid energy auctions. Gao et al. [35] developed and validated an intelligent microgrid management system to secure Singapore's energy market by leveraging the inherent synergy between Peer-to-Peer blockchain and fog computing. Alskaif et al. [36] proposed households' strategies for bilateral trading preferences in a local Peer-to-Peer energy market using permissioned blockchain.

These blockchain-based peer-to-peer energy systems mostly trade with limited counterparts and have a relatively high consensus cost, which lowers the overall trading welfare and throughput. By contrast, distributed trading systems with aggregators can organize market orders among authorized traders to cut the matching overhead in a free market. Plenty of papers have been devoted to the very research orientation. Tesfamicael et al. [37] put forward a blockchain application for secure macro grid energy trading of mega power generation. Huang et al. [38] proposed a multi-objective optimization model and a genetic sorting algorithm to ensure the security and privacy of energy trading within a multi-blockchain. Aggarwal et al. [11] proposed an energy trading blockchain scheme across EVs, charging stations, and utility centers. Aggregated blockchain systems are also applied to Industrial IoT [39], [40] and smart building [41], [42] to address the security and fairness challenges in energy trading.

D. EV ENERGY TRADING SYSTEMS

The rapid rise of EV fleets in V2G energy network hampers the implementation of aggregated trading systems. This is because the energy trading mechanism needs to maintain scalability for more EVs and consumers while keeping the efficiency and security of the blockchain system. To solve these bottlenecks, some trading mechanisms in V2G energy systems take game-theoretic solutions, such as Yu et al. [13] optimized the Bayesian game in PEV microgrids to share energy with maximized profit, and Yassine et al. [14] adopted cloudlet residing aggregators and a dynamic double auction model to trade electricity. Others apply an incentive-driven

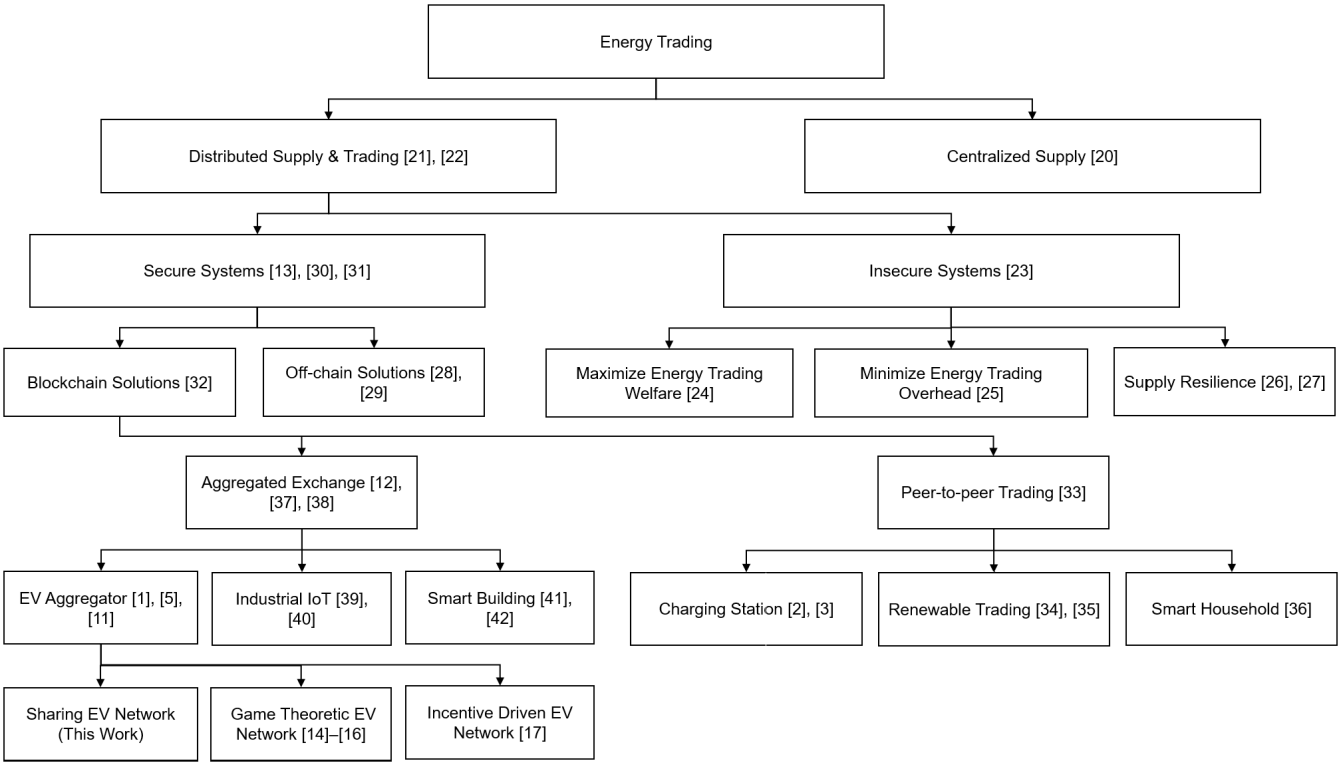

FIGURE 3. Overview of energy trading classification. According to the system structure, energy trading systems can be roughly divided into centralized ones and distributed ones. Distributed energy supply and trading systems can be further divided by their functions and security features.

strategy, like Kim et al. [16], who formulated a trading incentive mechanism for EVs and mobile charging stations. In V2G energy networks, the trading parties are virtually known entities with a certain degree of trust and acting for a common purpose. However, most game-theoretic V2G networks only regard their traders as competitors and take non-cooperative games, which is an excessive drag on the network scalability. On the other hand, the incentive-driven V2G networks usually require a native cryptocurrency to fuel the trading execution, which increases the time and computational costs and adds some significant risk. In such a context, an active energy distribution strategy for V2G trading under more cooperative and sharing situations needs to be considered.

III. V2GNET

This section presents the proposed V2GNet. The overall architecture is depicted in Fig. 2. The section is divided into four parts: 1) Energy trading process in V2GNet; 2) Blockchain-enabled data storage and transmission; 3) Analysis of response time; 4) Robust energy trading algorithm against malicious consumers and exchanges.

A. ENERGY TRADING PROCESS IN V2GNET

The proposed energy trading process for V2GNet is illustrated in Fig. 4. The energy exchanges receive energy requests from connected consumers and forward them to the control system (CS). The CS then informs the EVs about the energy requested. Each EV checks its availability based on remaining energy and future tasks. The available EV responds to the CS about its EV ID and the amount of energy requested. The CS obtains both the consumers' energy requests and the EVs' energy offers, then selects the successful bidder using the *RET* algorithm (see Section III-D4). The result comprises two lists, namely the charge, and the discharge list. The charge list contains information about winning consumers and the amount of energy supplied. The discharge list holds information about the selected EVs that supply energy. The charge list is sent to the exchanges, and each consumer receives a notification afterward. The discharge list is not transmitted to the vehicular network, but each EV receives instructions on whether to discharge or not. Finally, the payment clearing is performed on the CS side.

The following describes the process on the EV side and the CS side. The EV's process begins with "Start A." At first, If an EV is not yet connected to the grid and/or is currently performing a charge/discharge process, it cannot participate in preceding processes. Otherwise, the vehicle checks its remaining power (*EP*) and predicts the energy consumption (*ECP*) shortly. If the remaining energy is not enough, the vehicle must be recharged. The energy consumption prediction method is presented in [43]. Therefore, only EVs with sufficient energy and connected to the power grid are considered "available" for energy supply. When an available EV receives energy requesting information from the CS, the EV sends a response that includes the amount of energy to

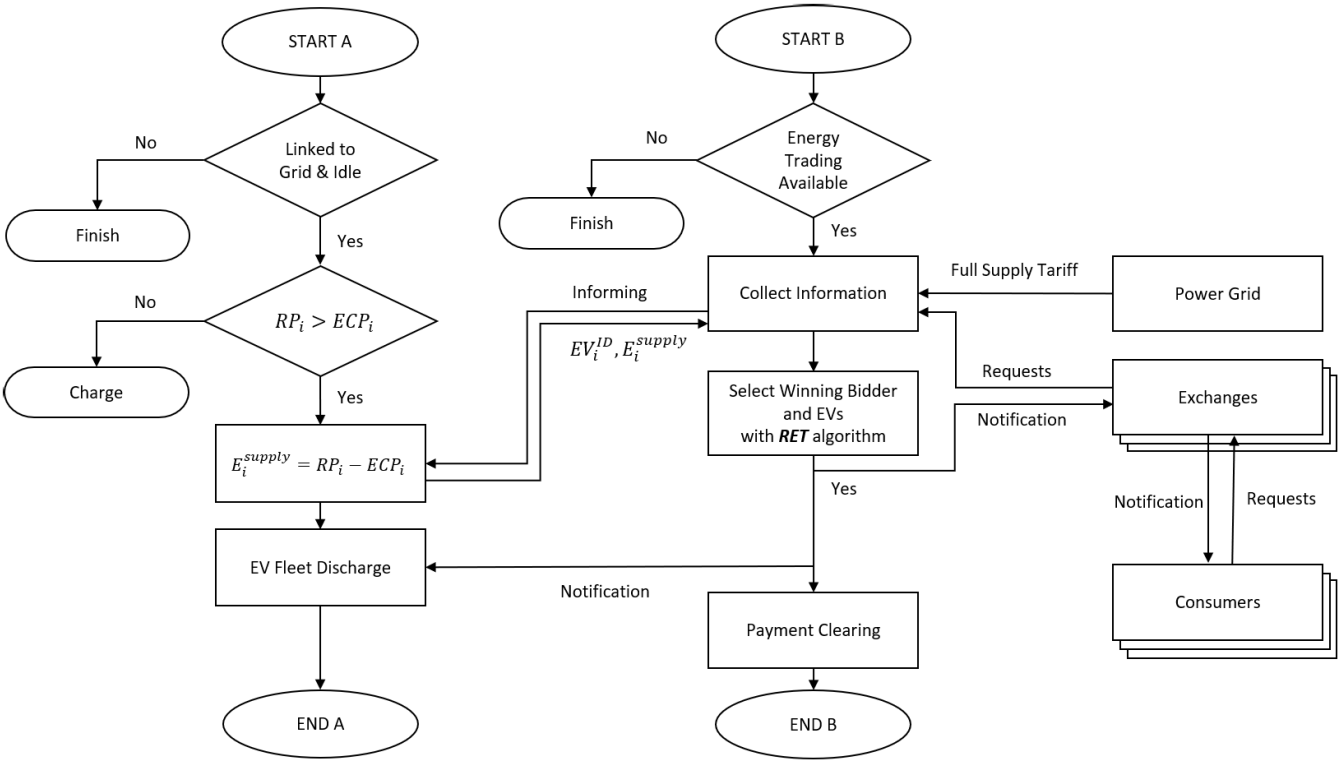

FIGURE 4. Energy trading algorithm in V2GNet for both EV side and CS side. The EV side begins from "Start A" and the CS side begins from "Start B." The power grid provides CS with a full supply tariff. The exchanges collect energy requests from consumers and communicate with the CS.

be supplied and its identification. Afterward, the EV begins discharging when it receives the discharge notification from the CS.

The process on the CS side begins with "Start B." Initialization of the CS indicates that energy trading is now available. The CS collects energy requests from consumers and informs the EVs about the start of energy trading, then receive information about energy offers from EVs. To decide which consumer receives energy from which EV, the *RET* algorithm is performed. However, the information of all selected consumers is not required for the selected EVs. Similarly, the information about all selected EVs is needless for selected consumers. Therefore, these details are not transmitted for efficiency and confidential reasons.

B. BLOCKCHAIN-ENABLED DATA STORAGE AND TRANSMISSION

The proposed V2GNet includes a blockchain of electric vehicles (BoEV) and a blockchain of exchanges (BoE), as shown in Fig. 5. According to the workflow of the proposed (energy trading) algorithm, we divide data storage and transmission into four parts: 1) First-time operation in BoE; 2) First-time operation in BoEV; 3) Second-time operation in BoEV; 4) Second-time operation in BoE.

The first-time operation in BoE starts when an exchange receives all requests from affiliated consumers. The exchange accumulates all requests into a request list and stores the list in a transaction. Then, the exchange broadcasts the transaction and waits for a response from other exchanges. Each exchange is associated with a transaction pool where whenever the transaction pool is full, i.e., all the transactions have been collected, the exchange will send the transactions to be endorsed by a group of endorsing exchanges. Once the endorsement is completed, the transactions are transmitted to the ordering organization, where transactions are ordered in a fixed sequence and packed into a new block. The block is broadcast to all exchanges for verification and after the block is verified, the CS downloads the block and obtains the request lists. Each request list is associated with the exchange and is consolidated into a larger, single request list.

Operation in the BoEV begins when EVs receive the energy requesting information from the CS. An available EV packs its ID number and the amount of offered energy into a new transaction and then broadcast it to other EV nodes. When the transaction pool is full, the EV will send the transactions to be endorsed by a group of endorsing EVs. Once the endorsement is completed, the transactions are transmitted to the ordering EVs, where transactions are ordered in a fixed sequence and packed into a new block. The block is broadcast to all EVs for verification. After the block is verified, the CS downloads the block and obtains the offers from EVs, and then converted them into an offer list.

The preceding operation in the BoEV begins when the CS finishes bidder selection. Then, the CS generates a result list of selected consumers (energy consumers) and selected EVs (energy suppliers) simultaneously. For an EV that is selected

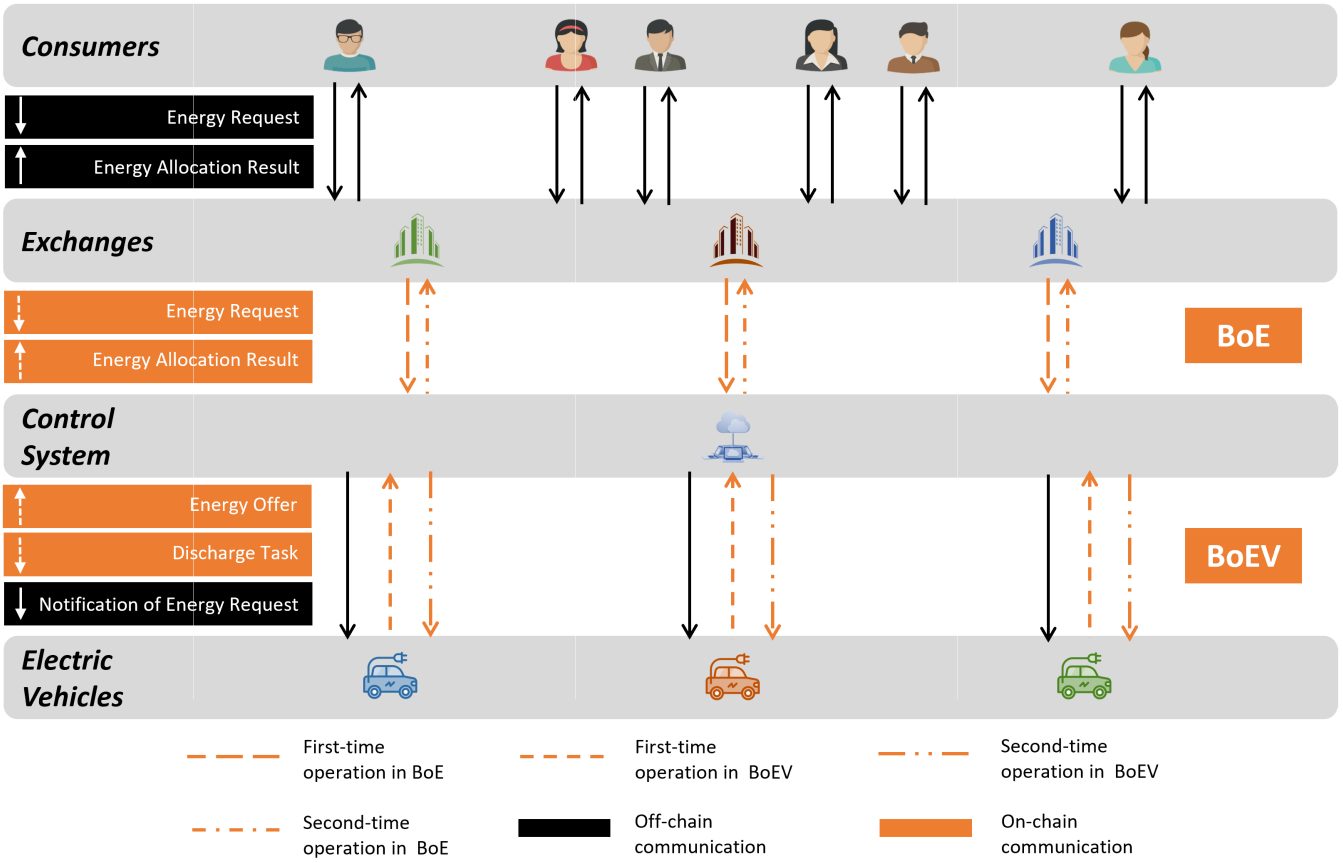

FIGURE 5. Overview of the proposed blockchain of exchanges (BoE) and blockchain of EVs (BoEV). Each trading round performs the two-time operation in BoE and BoEV, respectively. Communication between consumers and exchanges does not take place on the blockchain. Moreover, the control system informs EVs about energy demand without the blockchain. The off-chain communication is colored black, and the on-chain communication is colored orange.

to supply energy, its ID and amount of energy to be supplied are recorded on the list, and If an EV is not selected, the information "*unselected*" is written on the list instead. The EVs' result list is stored in a transaction from the CS side, which is endorsed by the endorsing EVs. The transaction is packed in a block, verified, and recorded by the EV nodes. Afterward, each EV downloads the block and acquires the result list of selected EVs.

The preceding operation in the BoE begins when the result list of selected consumers is generated. The result list has the ID of each selected consumer. Also, the period of energy supply and the trading price is recorded in the list. The consumers' result list is stored in a transaction in the CS, endorsed by the endorsing exchanges. The transaction is packed in a block, verified, and recorded by the exchange nodes. After that, each exchange downloads the block and acquires selected consumers' results. The result list contains the supply information of all exchanges, so each exchange reserves the information regarding its consumers and then creates a notification for each of them.

C. ANALYSIS OF RESPONSE TIME

For an active consumer, we define the response time as the time from when the consumer submits the energy request until it receives the notification about the energy supply. "*Active*" means the consumer participates in the trading at this round. For the whole system, we define the response time as the time from when the first consumer submits the energy request until the last consumer receives the notification about the energy supply. Since there is a minor difference between these two definitions, we will explain them in Fig. 6.

We consider a group of exchanges $\{E_i\}, i \in N$, N is the number of exchanges. An exchange E_i contains a group of active consumers $\{C_{ij}\}, j \in M_i$, M_i is the number of consumers. Also, a group of EVs is denoted by $\{EV_i\}, i \in K$, K is the number of EVs. We divide the entire response process into five phases: 1) Request List Preparation, 2) Consensus of Request Lists; 3) Consensus of Offer List; 4) Energy Allocation, and 5) Notification.

1) REQUEST LIST PREPARATION

The time a consumer C_{ij} sends a request to the exchange E_i is denoted by t_{ij}^r. The time E_i receives all requests depends on the latest consumer. The corresponding time t_i^r is formulated as:

$$t_i^r = max(t_{i1}^r, t_{i2}^r, \cdots, t_{im_i}^r) \quad (1)$$

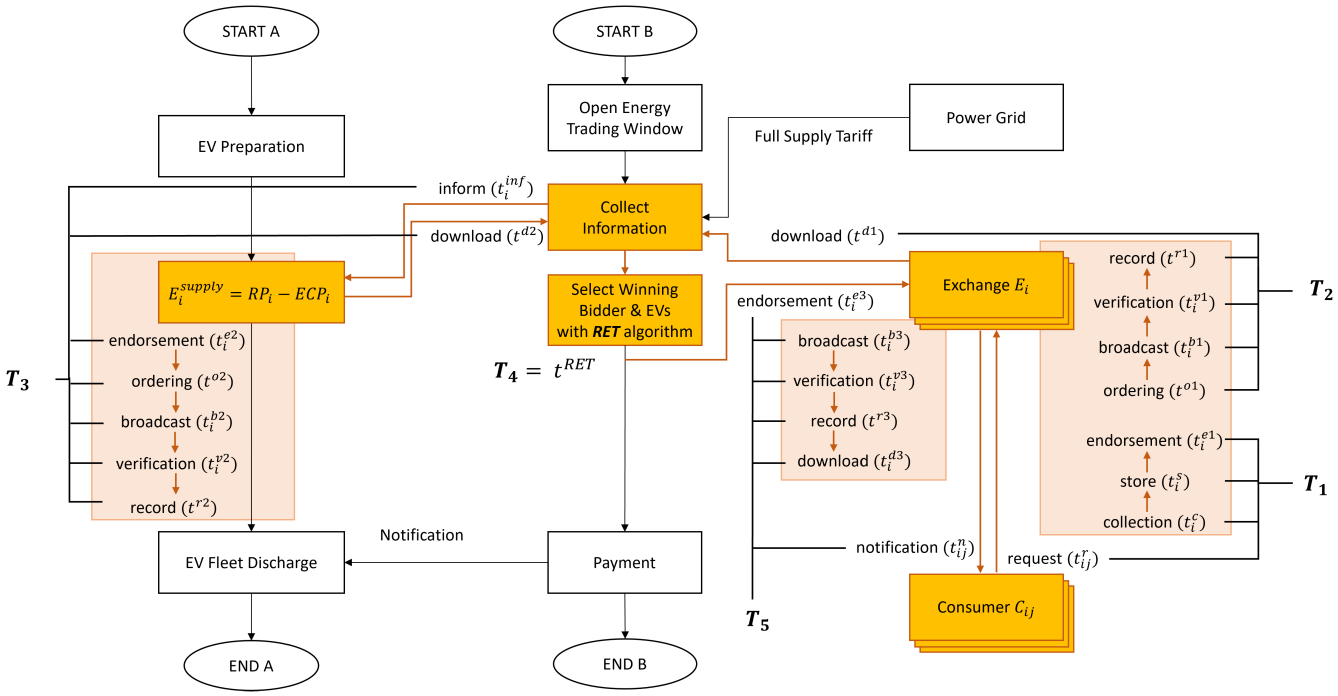

FIGURE 6. Analysis of Response Time in V2GNet. The whole workflow can be divided into five stages. T_1: From the request submission until the endorsement of transactions (containing request lists) is finished. T_2: From the ordering of transactions until the CS collects the request lists. T_3: From the CS informs EVs until it receives offers from EVs. T_4: Select winning consumers and offers with *RET* algorithm. T_5: From the endorsement of the result about winning consumers until the consumers receive the notification.

Subsequently, the collection of requests is organized into a request list and stored in a transaction TX_i, which costs time t_i^c. Each exchange broadcasts its transaction and receives transactions from other exchanges. For an exchange E_i, the time until all transactions stored in the transaction pool is denoted by t_i^s. Once a transaction pool is prepared, the corresponding exchange sends these transactions to be endorsed by a group of endorsing exchanges. The endorsement time associated with E_i is denoted by ${t_i}^{e1}$. And the time consumption depends on the first exchange that finishes this phase. The time cost for exchange E_i in *Phase I* is denoted by:

$$t_i = t_i^r + t_i^c + t_i^s + {t_i}^{e1} \tag{2}$$

Therefore, the total time for request list preparation is:

$$T_1 = min(t_1, t_2, \cdots, t_i, \cdots, t_N) \tag{3}$$

2) CONSENSUS OF REQUEST LISTS

When the exchange receives acknowledgments from endorsing nodes, the transactions are transmitted to the ordering organization. They are arranged in a fixed order based on a consensus protocol and then packed into a new block. The ordering time is denoted by t^{o1}. The block is broadcast to all nodes for verification and the time of broadcasting to each node is denoted by $t_i^{b1}, i \in N$. The time of verification of each node is denoted by $t_i^{v1}, i \in N$. After block verification, each node records the block on its ledger, and the recording time is denoted by t^{r1}. The CS downloads the block(s) and obtains the request lists, and the corresponding time is denoted by t^{d1}. The total time for consensus of request lists is

$$T_2 = t^{o1} + max(t_1^{b1} + t_1^{v1}, \cdots, t_N^{b1} + t_N^{v1}) + t^{r1} + t^{d1} \tag{4}$$

3) CONSENSUS OF OFFER LIST

The CS notifies the EV fleet of the new trading round, and the notification time to EV_i is denoted by t_i^{inf}. If EV_i is available to discharge, it generates a transaction containing its ID and the available energy. Available EVs send their transactions to be endorsed by a group of endorsing EVs, and the endorsement time associated with EV_i is denoted by ${t_i}^{e2}$. When the EV receives the acknowledgment from endorsing nodes, the transactions are transmitted to the ordering organization, arranged in a fixed order, and packed into a new block. The ordering time is denoted by t^{o2}. The block is broadcast to all nodes for verification. The time of the broadcasting and the verification of each node is denoted by $t_i^{b2}, i \in K$ and $t_i^{v2}, i \in K$, respectively. After block verification, each node records the block on its ledger, and the recording time is denoted by t^{r2}. More so, the CS downloads the block and obtains a collection of offers which is then stored in an offer list, and the corresponding time is denoted by t^{d2}. The total time for consensus of the offer list is

$$\begin{aligned} T_3 = {} & min(t_1^{inf} + t_1^{e2}, \cdots, t_K^{inf} + t_K^{e2}) + t^{o2} \\ & + max(t_1^{b2} + t_1^{v2}, \cdots, t_K^{b2} + t_K^{v2}) + t^{r2} + t^{d2} \end{aligned} \tag{5}$$

4) ENERGY ALLOCATION SCHEDULING

After the request and the offer list are prepared on the CS side, the CS begins scheduling energy allocation using the proposed RET algorithm. The time consumption of the RET depends on the following factors: 1) The total number of energy requests; 2) The total number of energy offers; 3) The results of energy trading (energy demand fill rate, number of fulfilled requests, and total profit) from the last trading round. We denote the time consumption of this phase by t^{RET}, $T_4 = t^{RET}$.

5) NOTIFICATION

When energy allocation is scheduled, the CS broadcasts a notification to endorsing exchanges, including 1) Winning consumer ID, 2) Amount of energy supply, and 3) Period of energy supply. After the endorsement, whose time is denoted by t^{e3}, the CS packs the winning requests into a block. Then the ordering organization broadcasts the block to all exchanges for verification. The time of the broadcasting and the verification of each node is denoted by $t_i^{b3}, i \in N$ and $t_i^{v3}, i \in N$, respectively. Next, the verified block is recorded in the ledger of each exchange, and the recording time is denoted by t^{r3}. Each exchange downloads the block and obtains the notification. For the exchange E_i, the corresponding time is denoted by t_i^{d3}. Finally, E_i notifies its consumers whether their requests are selected in the energy auction. The notification time for a consumer C_{ij} is denoted by t_{ij}^n; however, the time when all notifications are received depends on the last consumer. The notification time for an exchange E_i is formulated as:

$$t_i^n = max(t_{i1}^n, t_{i2}^n, \cdots, t_{im_i}^n) \tag{6}$$

Until all the consumers receive notifications, the total time consumption of this phase is:

$$\begin{aligned} T_5 = t^{e_3} + max(t_1^{b3} + t_1^{v3}, \cdots, t_N^{b3} + t_N^{v3}) \\ + t^{r3} + max(t_1^{d3} + t_1^n, \cdots, t_n^{d3} + t_N^n) \end{aligned} \tag{7}$$

In summary, the response time for one complete trading round is:

$$T^{response} = T_1 + T_2 + T_3 + T_4 + T_5 \tag{8}$$

For a consumer C_{ij}, the response time is:

$$\begin{aligned} &T^{response} \\ &= T_1 + T_2 + T_3 + T_4 + t^{e_3} \\ &\quad + max(t_1^{b3} + t_1^{v3}, \cdots, t_N^{b3} + t_N^{v3}) + t^{r3} + t_i^{d3} + t_{ij}^n \end{aligned} \tag{9}$$

D. ROBUST ENERGY TRADING ALGORITHM AGAINST MALICIOUS CONSUMERS AND EXCHANGES

1) CONSUMER ATTACK

Fig. 7 describes an attack scenario caused by a consumer. Consumer C_i falsifies multiple fake requests (Request i_1 to i_m). These fake requests contain the same or different data about the time of electric usage, input electric power, bid price, etc. When a large portion of fake requests is selected, a group of EVs are thus assigned discharge tasks but cannot properly discharge. Moreover, the requests from other consumers are therefore not met. To counter consumer attacks, in our proposed strategy, we consider two issues, one is multiple requests, and the other one is fake requests. First, we deal with multiple requests coming from a single consumer. We reserve the request with the latest submission time and discard all others. After that, we deal with fake requests. The fake requests are difficult to detect. Thus we get around this problem by focusing on the malicious consumer directly. A penalty list P_i is initialized and is empty. We set a risk parameter denoted by γ_1. The theoretical and practical energy supply with respect to C_i is denoted by s^t and s^p respectively. When $s^t = s^p$ at any trading round, C_i is considered trustful and not malicious. If $s^t > s^p$, we denote the percentage of fulfilled energy supply by pct_i:

$$pct_i = s^p / s^t \tag{10}$$

When $pct_i < 1 - \gamma_1$, C_i is considered "*malicious*" now. A penalty value $pct_i + \gamma_1$ is added into P_i. When $pct_i \geq 1 - \gamma_1$, if P_i is not empty, $p_{ij} \in P_i$, $n(P_i)$ is the element number of P_i, then the last element of P_i is removed. If a consumer is "*malicious*", his/her request cannot be fully met. Given an initial demand d_i, the actual demand that can be met is denoted by d_i^{met}:

$$\begin{cases} d_i^{met} = d_i & \text{if } P_i = \emptyset \\ d_i^{met} = d_i \prod_{j=1}^{n(P_i)} p_{ij} & \text{if } P_i \neq \emptyset \end{cases} \tag{11}$$

2) EXCHANGE ATTACK

In V2GNet, all energy exchanges are protected by permissioned blockchain, where participants must have proven identities to transact on the network. This shields exchanges

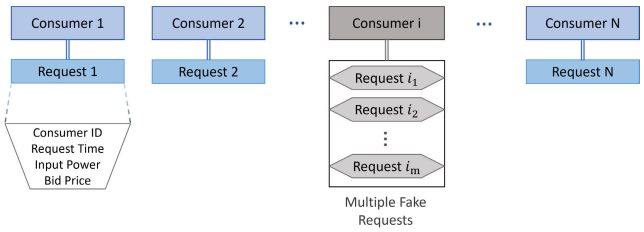

FIGURE 7. Example of consumer attack. A malicious consumer C_i submits multiple fake requests (i_1 to i_m).

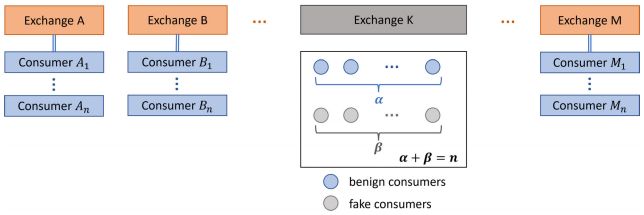

FIGURE 8. Example of an exchange attack. A malicious exchange E_K is associated with n consumers, including α benign consumers and β fake consumers.

Algorithm 1 Robust Energy Trading Algorithm

Require:
A set of request lists from each exchange $\{R_i^0\}, i \in N$, total request list $\{r_{ij}\}, i \in N, j \in N_i$, exchange ID $\{ID_i^E\}$, consumer ID $\{ID_{im}^C\}, m \in M_i$, bid tariff $\{B_{ij}\}$, submission time of request $\{t_{ij}^r\}$, and quantity of energy demand $\{d_{ij}\}$
Offer list $\{O_k\}, k \in K$, EV ID $\{ID_k^{EV}\}$, amount of energy offer $\{o_k\}$
Capacity of charging pile W
A set of penalty lists for consumers $\{P_{im}\}$
A set of penalty lists for exchanges $\{Q_i\}$
Ensure: A list of selected requests and a list of selected offers
Initialize an empty list R^W for winning requests
Initialize an empty list O^W for winning offers
Initialize an empty list A for storing the maximum number of requests to be fulfilled regarding each exchange
Initialize an empty list Π for storing expected profit of each request
Initialize a list U for recording whether an offer has been selected. All elements are set to zero.
for $\forall i \in N$ and $\forall m \in M_i$:
  for $\forall p, q \in N_i$:
    if $t_{ip}^r > t_{iq}^r$:
      remove r_{iq} from $\{r_{ij}\}$ and R_i
      remove q from N_i
for $\forall i \in N$ and $\forall j \in N_i$:
  if $P_{im} \neq \emptyset$:
    $d_{ij} = d_{ij} \prod_{l=1}^{n(P_{im})} p_{iml}$
  Calculate expected profit π_{ij} regarding each request,
  $\pi_{ij} \leftarrow B_{ij} \times d_{ij}$, add π_{ij} into Π
Rearrange $\{r_{ij}\}$ according to Π in descending order.
for $\forall i \in N$:
  if $Q_i = \emptyset$:
    $a_i = n(R_i^0)$
  else:
    $a_i = \left\lfloor n(R_i^0) \prod_{l=1}^{n(Q_i)} q_{il} \right\rfloor$
  add a_i into A
for $\forall k \in K$:
  $o_k = min(o_k, W)$
Rearrange $\{O_k\}$ according to $\{o_k\}$ in descending order
while $\{r_{ij}\} \neq \emptyset$ or $\exists u_k \in U, u_k = 0$:
  for $\forall r_{ij} \in \{r_{ij}\}$:
    if $a_i > 0$:
      for $k = 1, k$ in K, k++
        if $d_{ij} \leq o_k$ and $k = K$ and $u_k = 0$:
          $u_k \leftarrow 1$
          $r^w \leftarrow$ exchange ID, consumer ID, d_{ij}
          add r^w into R^W
          $o^w \leftarrow$ EV ID, d_{ij}
          add o^w into O^W
          remove r_{ij} from $\{r_{ij}\}$
          $a_i \leftarrow a_i - 1$
          break
        else if $d_{ij} \leq o_k$ and $d_{ij} > o_{k+1}$ and $u_k = 0$:
          $u_k \leftarrow 1$
          $r^w \leftarrow$ exchange ID, consumer ID, d_{ij}
          add r^w into R^W
          $o^w \leftarrow$ EV ID, d_{ij}
          add o^w into O^W
          remove r_{ij} from $\{r_{ij}\}$
          $a_i \leftarrow a_i - 1$
          break
        else if $d_{ij} > o_k$ and $u_k = 0$:
          $u_k \leftarrow 1$
          $r^w \leftarrow$ exchange ID, consumer ID, o_k
          add r^w into R^W
          $o^w \leftarrow$ EV ID, o_k
          add o^w into O^W
          $r_{ij} \leftarrow r_{ij} - o_k$
return R^W and O^W

against direct intrusion such as data scrubbing or tempering. Nevertheless, latent malicious exchanges could sneak in from round one, and manipulated exchanges could be depraved over any trading process. For every trading round, each exchange is supposed to upload a request list of its consumers' energy demands. Those malicious exchanges generate fake request lists by meddling with the real ones or fabricating fake requests for their consumers. Fig. 8 depicts a malicious exchange E_K that fabricates a group of fake consumers. To minimize the damage of malicious exchanges, we designed a strategy that gradually lessens their winning chance in bidding. For example, for a single exchange E_K. A penalty list Q_K is initialized and is empty. We set a risk parameter γ_2. After the CS performs the *RET* algorithm, the set of selected requests is denoted by R_K. The set of fulfilled requests in R_K is denoted by R'_K. Finally, the percentage of fulfilled requests is denoted by pct_K:

$$pct_K = \frac{n(R'_K)}{n(R_K)} \tag{12}$$

When $pct_K < 1 - \gamma_2$, E_K is considered "*malicious*" now. A penalty value $pct_K + \gamma_2$ is added into Q_K. When $pct_K \geq 1 - \gamma_2$, if Q_K is not empty, $q_{Kj} \in Q_K$, $n(Q_K)$ is the element number of Q_K, then the last element of Q_K is removed.

Given an initial request list R_K^0 from E_K, the maximum amount of requests that can be met is denoted by a_K^{met}:

$$\begin{cases} a_K^{met} = n(R_K^0) & \text{if } Q_K = \emptyset \\ a_K^{met} = \left\lfloor n(R_K^0) \prod_{j=1}^{n(Q_K)} q_{Kj} \right\rfloor & \text{if } Q_K \neq \emptyset \end{cases} \tag{13}$$

3) MATCHING STRATEGY BETWEEN REQUESTS AND EVs

For maximum profitability and the best possible energy utilization, the CS must reorder both the requests and the offer lists first. Each request is associated with an expected profit for the request list, which is the product of input power and unit bid tariff. The request list is reordered based on the expected profit in descending order. The offer list is reordered based on the amount of energy supplied. Furthermore, the CS begins allocating energy between requests and offers, starting from the request with the highest profit. Given a request, the CS traverses the offer list, and if an offer cannot meet the demand of the request, the CS allocates the offer to this request and moves on to the next offer until the entire demand for the request is met. To minimize the waste of EV energy, if more than one offer meets the demand of the request, the offer with the least energy supply is selected. The procedure ends when all requests are fulfilled or all offers are selected.

4) ROBUST ENERGY TRADING ALGORITHM

Based on our approach against malicious consumers and exchanges and the matching strategy between requests and EVs, A summary of the proposed robust energy trading algorithm is as shown in Algorithm 1. We denote the set of request lists from each exchange by $\{R_i^0\}, i \in N$, N is the number of exchanges. The total request list is denoted by $\{r_{ij}\}, i \in N, j \in N_i$, N_i is the number of requests of exchange E_i. We have

$$\{r_{ij}\} = \bigcup R_i^0 \tag{14}$$

Each r_{ij} contains an exchange ID (ID_i^E) and a consumer ID (ID_{im}^C, $m \in M_i$. M_i is number of consumers of exchange E_i), (B_{ij}) a bid tariff, submission time of request denoted by (t_{ij}^r), and quantity of energy demand denoted by (d_{ij}). We denote the offer list by $\{O_i\}, i \in K$, where K is the number of available EVs and offers. Each O_i contains the EV ID (ID_i^{EV}) and the amount of energy to be offered denoted by (o_i). W denotes the capacity of the charging pile. We also denote two risk parameters by γ_1 and γ_2, the penalty list for consumer C_{ij} by P_{ij} and for exchange E_i by Q_i. We initialize an empty list R^W for winning requests and an empty list O^W for winning offers. In addition, we initialize an empty list Π for storing the expected profit of each request and a list U for recording whether an offer has been selected. All element in U is set to zero by default and when an offer O_k has been selected, $u_k \in U$ is set to one.

We only reserve one request with the latest submission time for each consumer while discarding the rest. We then adjust the amount of energy request according to the penalty list of the consumer given by Equation 11. The request list $\{r_{ij}\}$ is rearranged according to the expected profit regarding each request in descending order. Also, the maximum number of energy requests could be fulfilled for each exchange is adjusted according to Equation 13. For each offer O_k, the amount of offered energy o_k is adjusted according to the capacity of charging pile W:

$$o_k = min(o_k, W) \tag{15}$$

The offer list $\{O_k\}$ is rearranged according to the amount of offered energy in descending order. Begin with the first request, we select a group of offers that gives the best possible match. If the demanded energy can be met by at least one offer, we select the offer having the least energy amount. Otherwise, we select the offer with the largest energy supply and move on to the next offer until the energy demand can be met. It is worth noting that once an offer is selected, it is added to the winning offer list and will be considered unavailable in the round. Also, if a request is fulfilled, we add it to the winning request list and move on to the subsequent request. The matching procedure ends when all the requests have been fulfilled or all the offers have been selected.

At last, we analyze the time complexity of the RET algorithm. There are 5 loops in the RET algorithm. As shown in Algorithm 1, the first loop starts from line 11 and ends at line 15. In the loop, we keep the request with the latest timestamp of each consumer and then discard the other redundant requests from the same consumer. The time complexity of loop 1 is $O(NM_i)$. The second loop starts from line 16 and ends at line 20. Here we deal with malicious consumers by applying the consumer penalty list P_{im} to their energy requests. And the time complexity of loop 2 is $O(NN_i)$. Since we already cut the number of requests in loop 1, $O(NN_i) = O(NM_i)$. The third loop starts from line 22 and ends at line 27. Here we deal with malicious exchanges by applying the exchange penalty list Q_i, and the time complexity of loop 3 is $O(N)$. The fourth part starts at line 28 and ends at line 29. Here we define the amount of each energy offer, and the time complexity of loop 4 is $O(K)$. The fifth loop starts from line 31 and ends at line 59. Here we distribute available EVs for energy consumers. And the time complexity of loop 5 is $O(NM_iK)$. Besides, in line 21 and line 30 we rearrange the energy demand list and offer list, respectively. And their time complexities are both taken as $O(n^2)$. Therefore, the overall time complexity of Algorithm 1 is:

$$\begin{aligned} T(n) &= O(NM_i + NM_i + N + K + NM_iK) \\ &\quad + 2O(n^2) = O(n^3 + 4n^2 + 2n) = O(n^3) \end{aligned} \tag{16}$$

IV. EVALUATION

This subsection verifies our proposed energy trading system's security properties and economic efficiency.

A. EVALUATION METHODOLOGY

To show that the proposed system achieves better energy demand satisfaction and higher profit, we compare the system with an action-based incentive scheme as offered by [16] and a double auction mechanism as proposed by [14]. We experiment 100 times using different request and EV number combinations for the following examples; request numbers to 100, 150, 200, and 400, and EV numbers to 50, 100, 150, and 200, respectively. In addition, to show the robustness

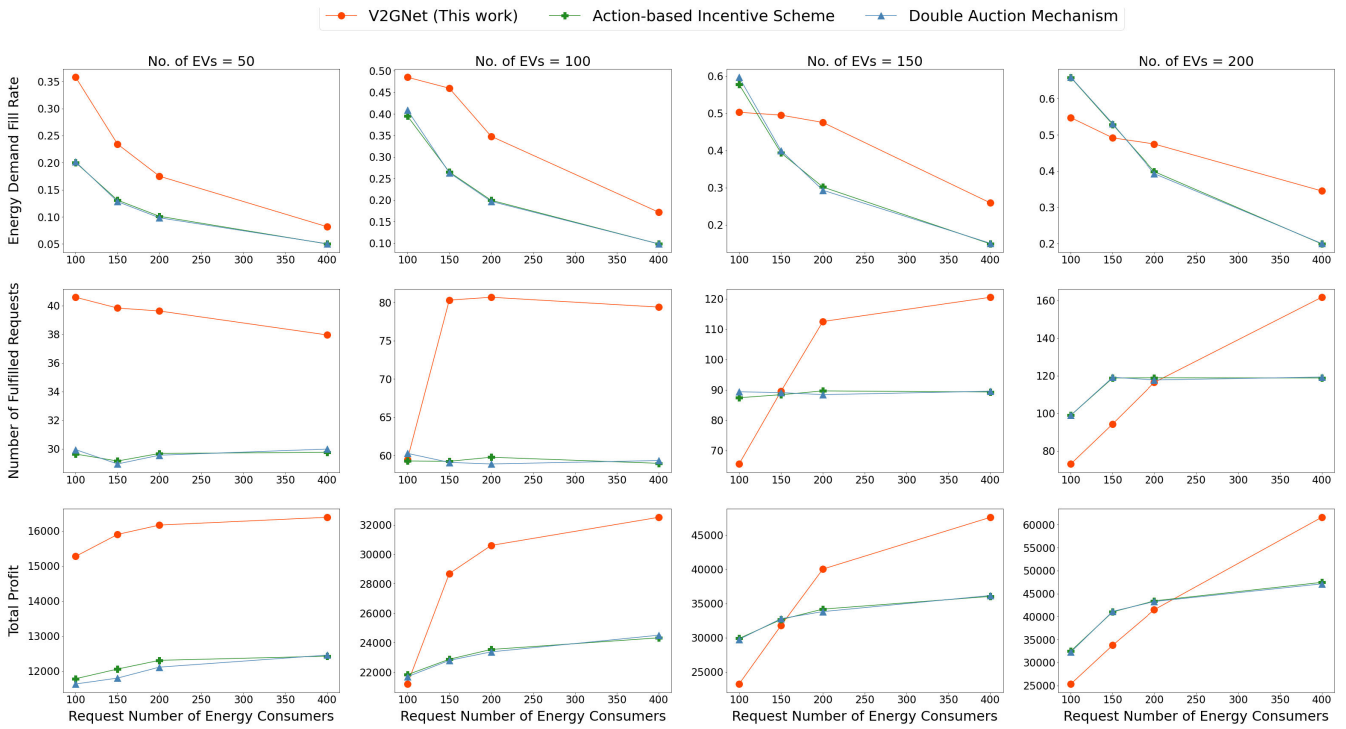

FIGURE 9. Comparison between V2GNet (this work), the action-based incentive scheme [16] and the double auction mechanism [14]. We used a different combination of EV and request amount, as shown in Table 1. We considered three evaluation indicators: 1) Energy Demand Fill Rate; 2) Number of Fulfilled Requests; 3) Total Profit.

of our proposed algorithm, we simulate experiments on consumer attacks and exchange attacks, respectively. The configuration is as shown in Table 1. For consumer attacks, we simulate a single-consumer scenario with one malicious node and several multi-consumer scenarios with 5, 10, and 20 malicious nodes. Each malicious node submits up to 10 fake requests. We compare trading performance differences first under no attack and then under consumer attack. Also, we evaluate how the *RET* algorithm serves as an advantage to the trading system while considering these three indicators: 1) Energy demand fill rate; 2) Number of fulfilled requests; 3) Total profit. For the exchange attack, we create one malicious exchange and two benign exchanges. Therefore, each exchange is associated with 100 consumers while the malicious exchange is associated with 50 benign and 50 malicious consumers. Three indicators are considered: 1) Energy Fulfillment; 2) Number of fulfilled requests, and 3) Total profit. The meaning of each indicator is as follows:

- ***Energy demand fill rate***: the percentage of energy demand met.
- ***Energy Fulfillment***: total amount of energy demand met.
- ***Number of fulfilled requests***: the number of energy requests fulfilled.
- ***Total profit***: total profit of energy trading.

B. EVALUATION RESULTS

As shown in Fig. 9, the V2GNet demonstrates a higher energy demand fill rate, number of fulfilled requests, and total profit compared to the action-based incentive scheme and double auction mechanism. Increasing the number of EVs from 50 to 200, the proposed algorithm extends its lead in fill rate from 0.04 to 0.18 and can fulfill 10 to 40 more requests compared to the other methods. The performance on total profit is improved as well.

We then compare the system performance of energy trading under three scenarios: 1) No attack; 2) Apply *RET* algorithm under consumer attack; 3) Do not apply *RET* algorithm under consumer attack. The trading efficiency is presented by the energy demand fill rate, the number of fulfilled requests, and total profit. Fig. 10 demonstrates that the efficiency drops dramatically when there is an increase in the number of malicious consumers. For instance, if there

TABLE 1. Configuration for the simulation.

Input Feature	Value	Unit
Discharge Capacity	0 to 10	kWh, Int
Charge Capacity	1 to 20	kWh, Int
Request Time Slot	21 to 22	-, Float
No. of Consumers	100, 150, 200, 400	-, Int
No. of EVs	50, 100, 150, 200	-, Int
No. of Exchange	3	-, Int
No. of Malicious Exchanges	1	-, Int
No. of Malicious Consumers	1, 5, 10, 20, 50	-, Int
Maximum No. of Requests from One Malicious Consumer	10	-, Int
Bid Price	22.39 to 42.84	JPY, Float

[1] The currency code for the Japanese Yen is JPY.

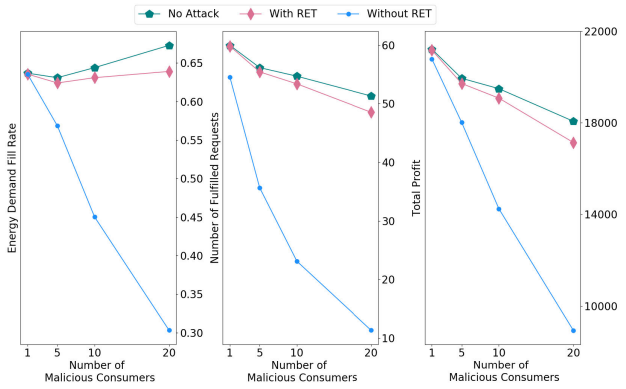

FIGURE 10. Comparison between three instances of consumer attack: 1) No attack; 2) Apply *RET* algorithm under consumer attack; 3) Do not apply *RET* algorithm under consumer attack. Three evaluation indicators are considered: 1) Energy Demand Fill Rate; 2) Number of Fulfilled Requests; 3) Total Profit.

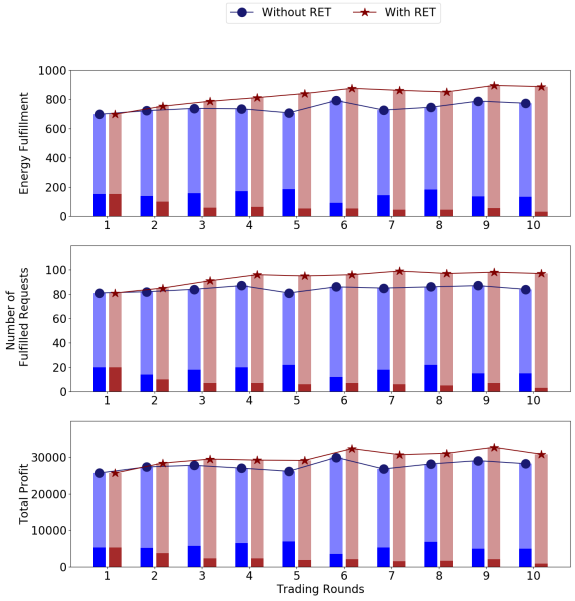

FIGURE 11. Comparison between two scenarios of consumer attack: 1) Apply *RET* algorithm under exchange attack; 2) Do not apply *RET* algorithm under exchange attack. Three evaluation indicators are considered: 1) Energy Fulfillment; 2) Number of Fulfilled Requests; 3) Total Profit. The darker parts show the proportion of indicators occupied by energy requests from malicious exchanges.

are 20 malicious consumers in the exchange, the energy demand fill rate drops from 68% to 30% under the consumer attack, while with *RET* protection, the energy demand fill rate can maintain 64%. The *RET* also blocks most of the damage caused by consumer attacks on the total trading profit and fulfilled request number, thus improving the system's robustness against malicious consumers.

To validate the effectiveness of *RET* against malicious exchange attacks, we present the energy fulfillment, number of fulfilled requests, and total profit during consecutive energy bidding. As observed from Fig. 11, there is no difference between the index of the system with and without *RET* algorithm at the first trading round. As the round of auction iteration increases from 1 to 10, in the system without *RET* the proportion of traded energy, fulfilled requests, and profit occupied by malicious exchange all keep changing around their initial levels, while the matched index in the system with *RET* all drop progressively. The amount of traded energy, number of fulfilled requests, and total profit in the system with *RET* also transcend the system without *RET* round by round, respectively. This shows that the *RET* gradually eliminates the adverse effect of malicious exchange attacks.

V. DISCUSSION

A two-blockchain architecture is proposed to transmit and store energy requests and offer data separately. Although the communication overhead is heavily reduced, there is still room for improvement. A significant increase in vehicle numbers can lead to unavoidable delays due to the asynchronous communication in EVs. In BoE networks, the challenge of exchange asynchronous also exists; however, time sliding is one possible solution to this problem. Also, the proposed system treats each energy trading round in an ideal way, i.e., the information sent from consumers or EVs is not updated until the next round. This could be another problem when a consumer cancels or modifies his request or there is any sudden failure on EVs or charging stations. To overcome this issue, a group of EVs is set aside for such occurrences in the future. The proposed *RET* algorithm against malicious attacks focuses on the result of energy allocation after each trading round. However, detecting the authentication of a request directly is still challenging. One idea is to deploy a prediction model targeting an exchange or a consumer to recognize abnormal submissions.

VI. CONCLUSION

In this work, we proposed V2GNet, a blockchain-based network for sharing EVs to achieve robust vehicle-to-grid energy trading. First, an appealing classification is presented for the latest energy trading research subjects. The setup of a novel energy trading system based on a blockchain of energy exchanges and a blockchain of EVs provides a feasible cross-cluster architecture for the secure trading workflow of energy request, offer, and allocation. The V2GNet deploys a control system as an intermediary between EVs and energy exchanges, for the control system is integrated into both the blockchain of exchanges and the blockchain of EVs. Meanwhile, the response time regarding energy requests is defined, and a complete analysis of the response time is provided by five divided stages. For the auctioning model, this work proposed a robust energy trading (RET) algorithm with a penalty mechanism to address malicious attacks from consumers and exchanges. The RET algorithm can also ensure the energy fill rate and total trading profit by allocating energy efficiently. Through extensive simulation experiments and evaluation, the paper demonstrates that the proposed RET algorithm in V2GNet achieves better energy fulfillment and higher profit compared to the state-of-the-art

approaches, including an action-based incentive scheme and double auction mechanism. In addition, the RET algorithm can reduce 30% energy loss when 20% of consumers are under malicious attacks, and gradually exclude malicious exchanges from the auction market as the trading rounds grow. In our future work, we plan to work on a multi-campus scenario and integrate multiple control systems into an extensive trading network to make the V2GNet more scalable and decentralized. We also plan to explore smart trading anticipation and private EV scenarios.

REFERENCES

[1] H. N. Abishu, A. M. Seid, Y. H. Yacob, T. Ayall, G. Sun, and G. Liu, "Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 946–960, Jan. 2022.

[2] M. Baza, A. Sherif, M. M. E. A. Mahmoud, S. Bakiras, W. Alasmary, M. Abdallah, and X. Lin, "Privacy-preserving blockchain-based energy trading schemes for electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9369–9384, Sep. 2021.

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

[4] A. Sadiq, M. U. Javed, R. Khalid, A. Almogren, M. Shafiq, and N. Javaid, "Blockchain based data and energy trading in internet of electric vehicles," *IEEE Access*, vol. 9, pp. 7000–7020, 2021.

[5] J. Kim, J. Lee, S. Park, and J. K. Choi, "Battery-wear-model-based energy trading in electric vehicles: A naive auction model and a market analysis," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4140–4151, Jul. 2019.

[6] A. A. Al-Obaidi and H. E. Z. Farag, "Decentralized quality of service based system for energy trading among electric vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6586–6595, Jul. 2022.

[7] J. Kim, J. Lee, and J. K. Choi, "Joint demand response and energy trading for electric vehicles in off-grid system," *IEEE Access*, vol. 8, pp. 130576–130587, 2020.

[8] C.-C. Lin, D.-J. Deng, C.-C. Kuo, and Y.-L. Liang, "Optimal charging control of energy storage and electric vehicle of an individual in the internet of energy with energy trading," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2570–2578, Jun. 2018.

[9] G. Sun, F. Zhang, D. Liao, H. Yu, X. Du, and M. Guizani, "Optimal energy trading for plug-in hybrid electric vehicles based on fog computing," *IEEE Internet Things J.*, vol. 6, no. 20, pp. 2309–2324, Apr. 2019.

[10] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5799–5812, Jun. 2020.

[11] S. Aggarwal, N. Kumar, and P. Gope, "An efficient blockchain-based authentication scheme for energy-trading in V2G networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6971–6980, Oct. 2021.

[12] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.

[13] Y. Yu, G. Li, and Z. Li, "A game theoretical pricing mechanism for multi-microgrid energy trading considering electric vehicles uncertainty," *IEEE Access*, vol. 8, pp. 156519–156529, 2020.

[14] A. Yassine, M. S. Hossain, G. Muhammad, and M. Guizani, "Double auction mechanisms for dynamic autonomous electric vehicles energy trading," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7466–7476, Aug. 2019.

[15] Y. Yu, S. Chen, and Z. Luo, "Residential microgrids energy trading with plug-in electric vehicle battery via stochastic games," *IEEE Access*, vol. 7, pp. 174507–174516, 2019.

[16] O. T. Thi Kim, T. H. T. Le, M. J. Shin, V. Nguyen, Z. Han, and C. S. Hong, "Distributed auction-based incentive mechanism for energy trading between electric vehicles and mobile charging stations," *IEEE Access*, vol. 10, pp. 56331–56347, 2022.

[17] W. Zhong, K. Xie, Y. Liu, C. Yang, and S. Xie, "Topology-aware vehicle-to-grid energy trading for active distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2137–2147, Jan. 2018.

[18] Z. Wang and A. B. Abdallah, "A robust multi-stage power consumption prediction method in a semi-decentralized network of electric vehicles," *IEEE Access*, vol. 10, pp. 37082–37096, 2022.

[19] H. Khaloie, J.-F. Toubeau, F. Vallee, C. S. Lai, and L. L. Lai, "An innovative coalitional trading model for a biomass power plant paired with green energy resources," *IEEE Trans. Sustain. Energy*, vol. 13, no. 2, pp. 892–904, Apr. 2022.

[20] M. R. Hamouda, M. E. Nassar, and M. M. A. Salama, "Centralized blockchain-based energy trading platform for interconnected microgrids," *IEEE Access*, vol. 9, pp. 95539–95550, 2021.

[21] F. Luo, Z. Y. Dong, J. Murata, Z. Xu, and G. Liang, "A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4097–4108, Sep. 2018.

[22] A. S. Yahaya, N. Javaid, A. Almogren, A. Ahmed, S. M. Gulfam, and A. Radwan, "A two-stage privacy preservation and secure peer-to-peer energy trading model using blockchain and cloud-based aggregator," *IEEE Access*, vol. 9, pp. 143121–143137, 2021.

[23] T. Zhou and B. Francois, "Energy management and power control of a hybrid active wind generator for distributed power generation and grid integration," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 95–104, Jan. 2011.

[24] S. Z. Tajalli, T. Niknam, and A. Kavousi-Fard, "Stochastic electricity social welfare enhancement based on consensus neighbor virtualization," *IEEE Trans. Ind. Electron.*, vol. 66, no. 12, pp. 9571–9580, Dec. 2019.

[25] D. Gregoratti and J. Matamoros, "Distributed energy trading: The multiple-microgrid case," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2551–2559, Apr. 2015.

[26] T. R. B. Kushal and M. S. Illindala, "Decision support framework for resilience-oriented cost-effective distributed generation expansion in power systems," *IEEE Trans. Ind. Appl.*, vol. 57, no. 2, pp. 1246–1254, Mar. 2021.

[27] L.-J. Yang, Y. Zhao, C. Wang, P. Gao, and J.-H. Hao, "Resilience-oriented hierarchical service restoration in distribution system considering microgrids," *IEEE Access*, vol. 7, pp. 152729–152743, 2019.

[28] M. Khorasany, Y. Mishra, and G. Ledwich, "A decentralized bilateral energy trading system for peer-to-peer electricity markets," *IEEE Trans. Ind. Electron.*, vol. 67, no. 6, pp. 4646–4657, Jun. 2020.

[29] Y. Ma, J. Qiu, X. Sun, and Y. Tao, "A multi-stage information protection scheme for CDA-based energy trading market in smart grids," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2305–2317, May 2022.

[30] J. Yang, J. Dai, H. B. Gooi, H. D. Nguyen, and P. Wang, "Hierarchical blockchain design for distributed control and energy trading within microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3133–3144, Jul. 2022.

[31] 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. 2018.

[32] Z. Li, S. Chen, and B. Zhou, "Electric vehicle peer-to-peer energy trading model based on SMES and blockchain," *IEEE Trans. Appl. Supercond.*, vol. 31, no. 8, pp. 1–4, Nov. 2021.

[33] H. T. Doan, J. Cho, and D. Kim, "Peer-to-peer energy trading in smart grid through blockchain: A double auction-based game theoretic approach," *IEEE Access*, vol. 9, pp. 49206–49218, 2021.

[34] M. Ul Hassan, M. H. Rehmani, and J. Chen, "DEAL: Differentially private auction for blockchain-based microgrids energy trading," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 263–275, Apr. 2020.

[35] G. Gao, C. Song, T. G. T. A. Bandara, M. Shen, F. Yang, W. Posdorfer, D. Tao, and Y. Wen, "FogChain: A blockchain-based peer-to-peer solar power trading system powered by fog AI," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5200–5215, Apr. 2022.

[36] T. AlSkaif, J. L. Crespo-Vazquez, M. Sekuloski, G. van Leeuwen, and J. P. S. Catalao, "Blockchain-based fully peer-to-peer energy trading strategies for residential energy systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 231–241, Jan. 2022.

[37] A. D. Tesfamicael, V. Liu, M. Mckague, W. Caelli, and E. Foo, "A design for a secure energy market trading system in a national wholesale electricity market," *IEEE Access*, vol. 8, pp. 132424–132445, 2020.

[38] X. Huang, Y. Zhang, D. Li, and L. Han, "A solution for bi-layer energy trading management in microgrids using multi-blockchain," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13886–13900, Aug. 2022.

[39] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6564–6574, Oct. 2020.
[40] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[41] A. T. Eseye, M. Lehtonen, T. Tukia, S. Uimonen, and R. J. Millar, "Optimal energy trading for renewable energy integrated building microgrids containing electric vehicles and energy storage batteries," *IEEE Access*, vol. 7, pp. 106092–106101, 2019.
[42] F. Wang, "Smart households' aggregated capacity forecasting for load aggregators under incentive-based demand response programs," *IEEE Trans. Ind. Appl.*, vol. 56, no. 2, pp. 1086–1097, Jan. 2020.
[43] Z. Wang, M. Ogbodo, H. Huang, C. Qiu, M. Hisada, and A. B. Abdallah, "AEBIS: AI-enabled blockchain-based electric vehicle integration system for power management in smart grid platform," *IEEE Access*, vol. 8, pp. 226409–226421, 2020.

YUXIAO LIANG received the B.S. degree in civil engineering from Tianjin University, China, in 2016, and the M.S. degree in geotechnical engineering from the China University of Mining and Technology, China, in 2020. He is currently pursuing the Ph.D. degree with the Adaptive Systems Laboratory (ASL), The University of Aizu. He is also a member of the ASL, The University of Aizu. His current research interests includeV2G energy trading and power management in smart grid. He is also interested in a robust cognitive neuromorphic system with online learning.

ZHISHANG WANG (Graduate Student Member, IEEE) received the B.S. degree in computer science from Wuhan University, China, in 2014, and the M.S. degree in computer science from the University of Freiburg, Germany, in 2019. He is currently pursuing the Ph.D. degree with the Adaptive Systems Laboratory (ASL), The University of Aizu. He is also a member of the ASL, The University of Aizu. His current research interests include machine learning systems, collaborative learning, blockchain, and trustworthy AI. He is also interested in event-driven neuromorphic systems targeted for a new generation of brain-inspired computing technologies and adaptive edge computing systems.

ABDERAZEK BEN ABDALLAH (Senior Member, IEEE) received the Ph.D. degree in computer engineering from The University of Electro-Communications, Tokyo, in 2002. From April 2014 to March 2022, he was the Head of the Computer Engineering Division, The University of Aizu, Japan, where he has been the Dean of the School of Computer Science and Engineering, since April 2022, He is currently a Full Professor with The University of Aizu. He is the author of four books, four registered and eight provisional Japanese patents, and more than 150 publications in peer-reviewed journal articles and conference papers. His research interests include adaptive/self-organizing systems, brain-inspired computing, interconnection networks, and AI-powered cyber-physical systems. He is a Senior Member of ACM.