An Architecture for Distributed Energies Trading in Byzantine-Based Blockchains

Jianxiong Guo, Xingjian Ding, and Weili Wu, *Senior Member, IEEE*

***Abstract*—With the development of smart cities, not only are all corners of the city connected to each other, but also connected from city to city. They form a large distributed network together, which can facilitate the integration of Distributed Energy Stations (DESs) and corresponding smart aggregators. Nevertheless, because of potential security and privacy protection arising from trustless energies trading, how to make such energies trading go smoothly is a tricky challenge. In this paper, we propose a blockchain-based multiple energies trading (B-MET) system for secure and efficient energies trading by executing a smart contract we design. Because energies trading requires the blockchain in B-MET system to have high throughput and low latency, we design a new byzantine-based consensus mechanism (BCM) based on node's credit to improve efficiency for the consortium blockchain under the B-MET system. Then, we take combined heat and power (CHP) system as a typical example that provides distributed energies. We quantify their utilities and model the interactions between aggregators and DESs in a smart city by a novel multi-leader multi-follower Stackelberg game. It is analyzed and solved by reaching Nash equilibrium between aggregators, which reflects the competition between aggregators to purchase energies from DESs. In the end, we conduct plenty of numerical simulations to evaluate and verify our proposed model and algorithms, which demonstrate their correctness and efficiency completely.**

***Index Terms*—Distributed energies trading, Smart city, consortium blockchain, byzantine consensus, Stackelberg game.**

I. Introduction

THE DEPLOYMENT of Distributed Energy Stations (DESs) based on the Internet built by the development of smart cities has been a hot topic because of its great potential to reduce the consumption of fossil fuels and curb greenhouse gas emission [1]. Considering a smart community equipped with a DES, it is used to supply residents in this community with multiple energies, such as electricity and heat. DES existing in the community can reduce residents' dependence on the centralized supply of energies, such as electricity from power grid and heat from heat station, thus saving resources and reducing the cost of using energies. Moreover, it can sell surplus electricity and heat to the aggregators of power grid and heat station for making revenue. DESs can trade their surplus energies with aggregators that are responsible for collecting energies from their communities in a peer-to-peer (P2P) manner, thereby the multiple energies trading problem discussed in this paper is formulated.

Manuscript received September 14, 2021; revised December 6, 2021 and December 15, 2021; accepted January 10, 2022. Date of publication January 12, 2022; date of current version May 20, 2022. This work was supported in part by the Start-Up Fund from BNU at Zhuhai under Grant 310432104, and in part by the National Science Foundation under Grant 1747818 and Grant 1907472. The editor coordinating the review of this article was C. You. *(Corresponding author: Jianxiong Guo.)*

Jianxiong Guo is with the BNU-UIC Institute of Artificial Intelligence and Future Networks, Beijing Normal University at Zhuhai, Zhuhai 519087, Guangdong, China, and also with the Guangdong Key Laboratory of AI and Multi-Modal Data Processing, BNU-HKBU United International College, Zhuhai 519087, Guangdong, China (e-mail: jianxiongguo@bnu.edu.cn).

Xingjian Ding is with the Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China (e-mail: dxj@bjut.edu.cn).

Weili Wu is with the Department of Computer Science, Erik Jonsson School of Engineering and Computer Science, The University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: weiliwu@utdallas.edu).

Digital Object Identifier 10.1109/TGCN.2022.3142438

Traditional P2P energies trading is performed on the centralized energy management platform, however, such a mechanism has many drawbacks. Traders are often worried about their payment security and privacy protection on the untrusted and opaque third-party centralized platform. This intermediary needs to verify and manage transactions between aggregators and DESs. If suffering from some damages such as single point failure, it will lead to privacy leakage and transaction loss [2]. Thus, it is urgent to establish a secure energies trading system to guarantee the transactions among the distributed Internet of energy can be executed effectively. This encourages the DESs to sell their energies to aggregators without any worries, which promotes the rational utilization of energies.

Blockchain [3] is a distributed database to store verified transactions without a trusted intermediary. A new transaction is required to be validated by a group of authorized participants, and then it can be added into the blockchain. It can be used to construct a secure and reliable energies trading system because of its decentralization, security, and anonymity [4], [5]. Therefore, the blockchain-based energy trading system [6], [7], [8], [9] has been a hot research issue. However, they usually had several obvious drawbacks summarized as follows: 1) they only considered the trading of one kind of energy, especially for electricity trading; 2) The blockchains on which their systems were based usually did not have good scalability and throughput; and 3) Their modelings of energies flow in DESs were too idealized and objective functions were too simplified, which are not realistic. In this paper, we mainly focus on solving these three issues.

First, as we know, most DESs will generate a large amount of heat while generating electricity. Thus, we consider such a scenario of multiple energies trading. In a smart city, it consists of a number of communities, each of which is equipped with a DES. There are two aggregators, electricity aggregator (EA) and heat aggregator (HA), trading with DESs in this city.

The aggregators of different cities are interconnected to form a wide area network. Based on that, we propose a blockchain-based multiple energies trading (B-MET) system to solve the drawback (1), where all aggregators are authorized participants that are required to store the blockchain and complete the consensus process. Thus, this is a consortium blockchain, which is a little different from the public blockchains like Bitcoin and Ethereum. Here, the consortium blockchain is more convenient and flexible to achieve our goal.

Second, we design a smart contract that ensures energies trading to be performed automatically when satisfying pre-defined conditions. However, the traditional blockchains do not have acceptable scalability since proof-based consensus mechanisms have high latency, low throughput, demanding computing power requirement, and so on. Therefore, they are not suitable to our consortium blockchain in B-MET system. To finish the task of energies trading, it needs to have a low latency and high throughput consensus mechanism. Then, we design a new byzantine-based consensus mechanism (BCM) based on node's credit to solve the drawback (2), which reflects the performance of this node in the previous experience of participating in consensus. After each round of consensus, each node's credit should be updated according to its voting result. If its voting is consistent with the result of consensus, its credit will be increased. Otherwise it will be decreased. Their credits affect directly their probabilities of being chosen as the leader and voting weight in next rounds. This not only motivates participants to make the right decision, but also speeds up the consensus process.

Third, there is an interaction between aggregators and DESs in which the aggregator offers a unit price to purchase a kind of energy from DES, and then DES decides the amount of energy they are willing to sell. We take the combined heat and power (CHP) system as an instance of DES and model the realistic energies flow to solve the drawback (3). In a smart city, there are two aggregators, EA and HA. For each DES in this city, its utility consists of two parts: 1) one is to serve the residents living in the community for satisfying their daily consumption and 2) the other is to sell them to the aggregators for gaining revenues. For the aggregators in this city, their gains come from buying energies from DESs at a lower price and selling them at the retail price. Here, we design more practical utility functions for aggregators and DESs by considering the authenticity of model and mathematical solvability. Compared to [7], [8], our model is more consistent with the needs of a real business scenario. To motivate the DESs to sell more energies, the aggregators should offer a higher price to them, but doing so raises costs and may result in lower overall profits. Since the multilevel decision-making processes between aggregators and DESs in a city, we formulate a noval multi-leader multi-follower (MLMF) Stackelberg game to model this bargain between them. Here the aggregators are leaders and DESs are followers. Their goals are to maximize their utilities or profits respectively. This MLMF Stackelberg game is analyzed and solved thoroughly in this paper, and we prove the Nash equilibrium (NE) among aggregators exists and is unique. Because the DESs are always able to respond aggregators with the optimal strategy according to their offered prices, the Stackelberg equilibrium (SE) exists and is unique as well. We propose a distributed algorithm that is guaranteed to reach the unique SE by limited information interactions.

The contributions are summarized as follows: 1) we consider multiple engies trading instead of single energy trading and take the CHP system as an example to demonstrate it; 2) we design an credit-based Byzantine consensus mechanism to improve efficiency and throughput; and 3) we simulate the energies flow in DES as realistically as possible, and establish a MLMF Stackelberg game model, which can be verified theoretically and experimentally.

Organization: Section II discusses the related work. Section III introduces the architecture of B-MET system, describes CHP system, and defines utilities. Section IV presents smart contract and byzantine-based blockchain. Section V introduces the Stackelberg game and discusses the solution. Section VI conducts numerical simulations. Section VII is conclusion.

II. Related Work

Distributed energy systems have been applied widely in many different forms, such as DES [10] and vehicle-to-grid [8], [11], to curb greenhouse gas and save cost. Integrating DESs into a smart grid [12] has attracted more and more researchers to participate recently. This causes the problems of energy management and energy trading. Cecati *et al.* [13] exploited DES to make the cost of power delivery minimized by use of an efficient smart grid management system. Georgilakis and Hatziargyriou [1] summarized the optimally distributed generation placement problem systematically, classified and analyzed current and future research about it. Zhang *et al.* [14] considered microgrid as a local energy supplier for domestic buildings by utilizing DES, and studied optimal scheduling of energy consumption through mixed-integer programming. Nevertheless, the security issue in distributed energy trading is a big challenge. Blockchain [3] has been introduced to address transaction security and privacy protection issues. Mohanta *et al.* [2] reviewed the security issue in Internet of Things (IoT) and gave a detailed analysis about blockchain to solve security issue in IoT. Zhang *et al.* [15] introduced a blockchain-enabled software crowdsourcing platform to integrate task assignment and resource lending by smart contracts.

In the blockchain-based P2P energy trading, Kang *et al.* [6] put forward a localized P2P electricity trading pattern based on consortium blockchain among plug-in hybrid electric vehicles. Li *et al.* [7] proposed a P2P energy trading architecture based on consortium blockchain for the industrial Internet of Things relied on a credit-based payment scheme. Zhou *et al.* [11] considered the scenario of vehicle-to-grid and developed a secure energy trading mechanism based on consortium blockchain. Guo *et al.* [9] studied a blockchain-based energy management system that guarantees secure electricity trading between grid and DESs. However, they only focused on electricity trading between grid and DESs. In this paper, we consider multiple energies trading due to the diversity of energy forms.

Moreover, they lose sight of low throughput and high latency in their proof-based consensus process. In this paper, we try to address it by proposing a new byzantine-based consensus mechanism.

Stackelberg game is an effective tool to model the interactions in energies trading. Maharjan *et al.* [16] studied the demand response management by establishing a Stackelberg game between multiple utility companies and customers to maximize their utilities respectively. Bu and Yu [17] proposed a four-stage Stackelberg game to consider a real-time pricing problem for the electricity retailer in the demand-side management. Chen *et al.* [18] proposed a Stackelberg game-based framework to simulate the multiple resources allocation between cloud server and end users, and found an equilibrium solution by a backward induction process. Yang *et al.* [19] designed a computing resource trading mechanism by a two-level Stackelberg game (leader-level and user-level) for IoT devices. As for Stackelberg game based blockchain mechanisms [20], [21], [22], [23], Xiong *et al.* [20] used Stackelberg game to present an edge computing resource management for mobile proof-of-work blockchains. Yao *et al.* [21] modeled the interactions between cloud server and mines by Stackelberg game, and solved it by multiagent reinforcement learning algorithm. Ding *et al.* [22] attempted to build a secure blockchain network with IoT devices and modeled the interaction by a two-stage Stackelberg game. Guo *et al.* [23] constructed a collaborative mining network among mobile devices, where they adopted Stackelberg game to model interactions between edge and mining networks to get the optimal resource allocation. However, most existing research focused on cases with one leader. Based on our modeling, the interactions between aggregators and DESs is formulated as a MLMF Stackelberg game, which is more complex and realistic.

III. System Architecture

Considering a smart city, it consists of a number of disjoint smart communities, each of which is equipped with a DES responsible for supplying multiple energies, such as electricity and heat, to these residents living in this community. In this city, there are several aggregators, which represent different companies respectively, collecting different kinds of energies from all DESs appertained to this city. The architecture of blockchain-based multiple energies trading (B-MET) system is shown in Fig. 1. In the B-MET system, given a smart city S_i, the entities can be shown as follows.

1) Aggregators: There are two aggregators, electricity aggregator (EA_i) and heat aggregator (HA_i), associated with this smart city S_i. The EA_i (resp. HA_i) is delegated by power grid (resp. heat station) as a monopoly of the energy market. They purchase electric energy (resp. heat energy) generated by DESs in those communities that belong to this smart city.

2) DESs: The city S_i can be partitioned into an uncertain number of disjoint smart communities, denoted by set $\{\mathrm{C}_{i1}, \mathrm{C}_{i2}, \dots, \mathrm{C}_{ij}, \dots\}$. In community C_{ij}, there is a distributed energy station DES_{ij} supplying electricity and heat to the residents living in this community. Besides, DES_{ij} is able to sell surplus electric energy (resp. heat energy) to the corresponding EA_i (resp. HA_i) in order to make revenues.

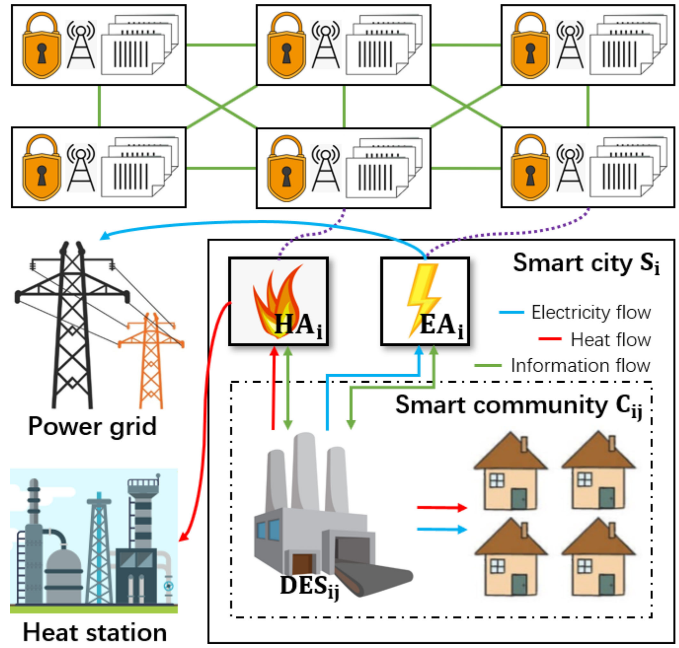


Fig. 1. The architecture of blockchain-based multiple energies trading system.

3) Smart Meters: It is a built-in component installed in each aggregator that monitors the energy flow transferred by each DES in this city in real-time, and decide whether the transaction has been accomplished.

Then, considering a larger ecosystem, such as a country, it is composed of a number of smart cities. This ecosystem $\mathbb{S}$ can be denoted by $\mathbb{S} = \{\mathrm{S}_1, \mathrm{S}_2, \dots, \mathrm{S}_i, \dots\}$. Here, each $\mathrm{S}_i \in \mathbb{S}$ is a smart city in this ecosystem, and $\mathrm{S}_i = \{\{\mathrm{EA}_i, \mathrm{HA}_i\}, \{\mathrm{C}_{i1}, \mathrm{C}_{i2}, \dots, \mathrm{C}_{ij}, \dots\}\}$. For convenience, the notation DES_{ij} can be considered equivalent to C_{ij}. Our B-MET system is established on such an ecosystem, in which all aggregators, including EAs and HAs, are interconnected each other to form a peer-to-peer (P2P) network called "blockchain network", shown in the upper half of Fig. 1. In order to support secure energies trading between aggregators and DESs, we adopt consortium blockchain to construct our B-MET. The blockchain in the B-MET takes all aggregators in the ecosystem as authorized participants, and they are charged with storing the whole blockchain and performing the consensus process. Each aggregator manages and records those transactions between it and DESs in its city. The transactions are packaged into blocks and added into blockchain when the consensus among aggregators is reached.

A. Combined Heat and Power System

Here, the aforementioned DES is implemented by the combined heat and power (CHP) system [24], [25]. The CHP system consumes natural gas to generate electricity and heat that serve its community or sell to the aggregators of its corresponding city, shown in Fig. 2. The gas is fed into the gas turbine (GT) which will generate electricity E_g and emit high-temperature waste heat Q_w. The heat Q_w can be recovered

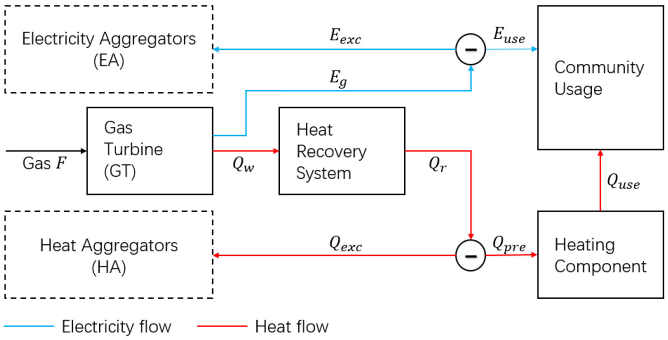


Fig. 2. The structure of combined heat and power (CHP) system.

by heat recovery system that can generate heat Q_r. Here, E_{use} (resp. Q_{use}) is used to supply electricity (resp. heat) to community, and E_{exc} (resp. Q_{exc}) is sold to EA (resp. HA).

Shown as Fig. 2, the total electricity generated by GT is $E_g = E_{use} + E_{exc}$. Measured in days, the units of quantities denoted by E and Q are (J/day). The gas consumption per day F ($\mathrm{m}^3/\mathrm{day}$) can be defined as

$$F = E_g/\big(q \cdot \eta_g\big) = Q_w/\big(q \cdot (1-\eta_g)\big), \tag{1}$$

where q (J/m^3) is the calorific value of natural gas, thereby the total energy generated by F is $q \cdot F$ definitely. The η_g is the electric conversion of GT, percentage energy that transferred to electricity. Given a specific GT, its electric conversion can be considered as a constant. Besides, let η_r be the thermal efficiency of heat recovery system, and $\eta_h = 1$ be the thermal efficiency of heat component. We have $Q_r = Q_w \cdot \eta_r = Q_{pre} + Q_{exc}$ and $Q_{use} = Q_{pre}$ respectively.

For a given CHP system, the electricity (resp. heat) generated by it can be divided into two parts: one is used to serve local residents and another is sold to EA (resp. HA). Thus, we define two dispatching factor $\alpha, \beta \in [0,1]$ for this CHP, where $\alpha = E_{use}/E_g$ is the electric dispatching factor and $\beta = Q_{use}/Q_r$ is the heat dispatching factor. This DES needs to buy natural gas from the gas company. The company is for profit, thus it is valid to assume the gas company always supply enough gas to meet the DES's requirement. Given a smart city S_i and a community $\mathrm{C}_{ij} \in \mathrm{S}_i$, the energy relationships in the CHP system of C_{ij} has been obtained, that is

$$E_{use}^{ij} = \alpha^{ij} \cdot \eta_g \cdot \Big(qF^{ij}\Big), \tag{2}$$

$$E_{exc}^{ij} = \Big(1-\alpha^{ij}\Big) \cdot \eta_g \cdot \Big(qF^{ij}\Big), \tag{3}$$

$$Q_{use}^{ij} = \beta^{ij} \cdot (1-\eta_g) \cdot \eta_r \cdot \Big(qF^{ij}\Big), \tag{4}$$

$$Q_{exc}^{ij} = \Big(1-\beta^{ij}\Big) \cdot (1-\eta_g) \cdot \eta_r \cdot \Big(qF^{ij}\Big). \tag{5}$$

In this model, we assume all the CHPs in the $\mathbb{S}$ has the same efficiency parameters η_g and η_r. Each CHP_{ij} can determine the amount of electricity (resp. heat) that can be sold to EA_i (resp. HA_i) by adjusting its dispatching factor α^{ij} (resp. β^{ij}) autonomously. For example, when α^{ij} is one, it means that CHP_{ij} will not sell any electricity to EA_i.

B. Utility Functions

Considering a smart city S_i, the EA_i (resp. HA_i) offers a unit price p_e^i (resp. p_h^i) to collect surplus electricity (resp. heat) generated by $\mathrm{DES}_{ij} \in \mathrm{S}_i$, where the units of p_e^i and p_h^i are coin/J. For each $\mathrm{DES}_{ij} \in \mathrm{S}_i$, it is a risk-averse agent in the energy market. If DES_{ij} chooses dispatching factor α^{ij}, β^{ij}, and consume natural gas F^{ij}, that is

$$U^{ij}\Big(\alpha^{ij},\beta^{ij},F^{ij}\Big) = W_e^{ij}\Big(E_{use}^{ij}\Big) + W_h^{ij}\Big(Q_{use}^{ij}\Big) + p_e^i \cdot E_{exc}^{ij} + p_h^i \cdot Q_{exc}^{ij} - c_f \cdot F^{ij}, \tag{6}$$

where W_e^{ij} (resp. W_h^{ij}) is the satisfaction function of community C_{ij} that provides electricity (resp. heat) to satisfy the usage of local residents in this community, and E_{use}^{ij}, E_{exc}^{ij}, Q_{use}^{ij}, and Q_{exc}^{ij} are defined from (2) to (5). Here, c_f ($\mathrm{coin/m}^3$) is the unit cost of natural gas.

From our simplified CHP model, we denote the cost of electricity (resp. heat) produced from DES_{ij} by c_e (resp. c_h). Then, the cost (coin/J) of electricity and heat can be quantified, that is $c_e = c_f/q$ and $c_h = c_f/(q \cdot \eta_r)$. Thus, we have $c_f \cdot F^{ij} = \eta_g \cdot c_e \cdot (qF^{ij}) + (1-\eta_g) \cdot c_h \cdot \eta_r \cdot (qF^{ij})$. If the price p_e^i (resp. p_h^i) offered by EA_i (resp. HA_i) is less than the cost c_e (resp. c_h), this DES_{ij} will not sell any electricity (resp. heat) to them. It will reduce the gas intake F^{ij} such that only meet its local requirement. Like this, there is no energies trading between aggregators and DESs, and obviously, it is not what we want to see. Thus, it is reasonable to consider the prices offered by aggregators satisfy $p_e^i \geq c_e$ and $p_h^i \geq c_h$. At this time, for each $\mathrm{DES}_{ij} \in \mathrm{S}_i$, it will produce electricity and heat as much as possible, because of the fact that it is always profitable to sell them to the aggregators. For maximizing its utility, each CHP system will run at full capacity. Here, for each CHP_{ij}, we define its maximum production capacity (maximum gas consumption) per day as F_m^{ij}. Therefore, the utility $U^{ij}(\alpha^{ij},\beta^{ij},F_m^{ij})$ can be denoted by $U^{ij}(\alpha^{ij},\beta^{ij})$, because F_m^{ij} is considered as a constant.

Remark 1: After here, we denote $X^{ij} = \eta_g \cdot (qF_m^{ij})$ and $Y^{ij} = (1-\eta_g) \cdot \eta_r \cdot (qF_m^{ij})$ for convenience.

Based on [8], [16], [26] the natural logarithmic functions were adopted extensively in characterizing the satisfaction of consuming energy. That is

$$W_e^{ij}\Big(E_{use}^{ij}\Big) = k_e^{ij} \cdot \ln\Big(1 + b_e^{ij} \cdot E_{use}^{ij}\Big), \tag{7}$$

$$W_h^{ij}\Big(Q_{use}^{ij}\Big) = k_h^{ij} \cdot \ln\Big(1 + b_h^{ij} \cdot Q_{use}^{ij}\Big), \tag{8}$$

where k_e^{ij} (resp. k_h^{ij}) is a non-negative satisfaction coefficient for electricity (resp. heat) in community C_{ij}, and b_e^{ij} (resp. b_h^{ij}) is a non-negative adaption coefficient for electricity (resp. heat) in this community as well. The adaption coefficients were proposed in [9] first, which aimed to control the variation range of the term $\ln(1+\cdot)$, avoid it growing infinitely. Generally, we let $\ln(1 + b_e^{ij} \cdot E_{use}^{ij}) = 1$ (resp. $\ln(1 + b_h^{ij} \cdot Q_{use}^{ij}) = 1$) when we choose $\alpha^{ij} = 1$ (resp. $\beta^{ij} = 1$) by setting a valid adaption coefficient b_e^{ij} (resp. b_h^{ij}) [9]. Base on that, thereby we can formulate b_e^{ij} and b_h^{ij} as follows:

$$b_e^{ij} = \left(1/X^{ij}\right) \cdot (e-1);\ b_h^{ij} = \left(1/Y^{ij}\right) \cdot (e-1). \quad (9)$$

For aggregators in this city, power grid and heat station are the retailers for electricity and heat, however they do not have pricing power, because the retail prices of electricity and heat subject to government's regulation. Hence, we define a retail price r_e (resp. r_h) of electricity (resp. heat). As a selfish participant, it requires that $p_e^i \in [c_e, r_e]$ and $p_h^i \in [c_h, r_h]$. From (6), if p_e^i (resp. p_h^i) offered by EA_i (resp. HA_i) is too low, each $\mathrm{DES}_{ij} \in \mathrm{S}_i$ will respond with raising its dispatching factor α^{ij} (resp. β^{ij}), and sell less energy to aggregators. If the aggregators offer a high price to purchase energy, their profitable spaces are reduced even if DESs are willing to sell more energies to them. Both of these cases will cause aggregators' profit to be cut down. Therefore, it is important for aggregators to offer an optimal price such that not only encourage DESs to sell more energies, but also ensure sufficient profitability. If EA_i (resp. HA_i)) offers a price p_e^i (resp. p_h^i), its profit function can be defined as

$$V_e^i\left(p_e^i, p_h^i\right) = \left(r_e - p_e^i\right) \cdot \sum_{\mathrm{C}_{ij} \in \mathrm{S}_i} E_{exc}^{ij}, \quad (10)$$

$$V_h^i\left(p_h^i, p_e^i\right) = \left(r_h - p_h^i\right) \cdot \sum_{\mathrm{C}_{ij} \in \mathrm{S}_i} Q_{exc}^{ij}, \quad (11)$$

where V_e^i (resp. V_h^i) is the profit function of the EA_i (resp. HA_i) that collects electricity (resp. heat) from DESs in its city, and E_{exc}^{ij} and Q_{exc}^{ij} are defined in (3) and (5).

IV. Byzantine-Based Blockchain

In this section, we will introduce a smart contract used to perform energies trading, and design a novel byzantine-based consensus mechanism based on the B-MET system.

A. Smart Contract

A smart contract is a collection of programmable digital agreement that every participant commit to comply. Under our blockchain-based energies trading ecosystem, a transaction can only happen between aggregators and DESs in the same city. Thereby, considering a city S_i, a smart contract can be decided together by its participants, which consist of an aggregator $k \in \{\mathrm{EA}_i, \mathrm{HA}_i\}$ and a $\mathrm{DES}_{ij} \in \mathrm{S}_i$. We denote such a smart contract by $Contract(k, \mathrm{DES}_{ij}, STime)$. Between anonymous and untrusted entities in a city, the smart contract is able to execute credible transactions without third institutions. Then, the procedure of its smart contract $Contract(k, \mathrm{DES}_{ij}, STime)$ is presented as follows:

1) System Initialization: At the beginning, each $\mathrm{DES}_{ij} \in \mathrm{S_i}$ needs to acquire a unique identification ID_{ij} by registering in the designated institution authorized by government. It will be assigned with its public/private key pair (PK_{ij}, SK_{ij}) and a $Account_{ij}$. That is $\{ID_{ij}, PK_{ij}, SK_{ij}, Account_{ij}\} \leftarrow \mathrm{register}(\mathrm{DES}_{ij})$, where each account is associated with its wallet address and balance, $Account_{ij} \leftarrow \{Address_{ij}, Balance_{ij}\}$. Then, for each aggregator $k \in \{\mathrm{EA}_i, \mathrm{HA}_i\}$ in this city, it has those necessary information $\{ID_k, PK_k, SK_k, Account_k\}$ as well. But there is a credit value $Credit_k$ that represent the reputation of aggregator *k*, thereby we have $Account_k \leftarrow \{Address_k, Balance_k, Credit_k\}$. Here, technologies of asymmetric encryption are usually adopted by current blockchain system for the sake of security, privacy, and data integrity, which can be implemented by some classic encryption algorithms, such as elliptic curve digital signature [27], lattice-based signature [28], and anti-quantum signature [29]. Given a massage *msg* encrypted by DES_{ij}, we have $Hash(msg) = PK_{ij}(SK_{ij}(Hash(msg)))$ and $Hash(msg) = SK_{ij}(PK_{ij}(Hash(msg)))$. Here, the public key works as a pseudonym that is open to all nodes and the private key that is kept by itself. Thus, the unforgeability and integrity is guaranteed.

2) Creation: An aggregator $k \in \{\mathrm{EA}_i, \mathrm{HA}_i\}$ offers a price p_k to buy energy from communities in its city, then DES_{ij} responds it with the amount of energy $x \in \{E_{exc}^{ij}, Q_{exc}^{ij}\}$ that can be sold to *k*. Like this, a new smart contract $Contract(k, \mathrm{DES}_{ij}, STime)$ is generated by signing with their private key respectively. Then, this contract will be broadcasted to all authorized participants (aggregators) in the ecosystem $\mathbb{S}$. After reaching a consensus, this smart contract will be deployed and executed automatically. Each smart contract between aggregator and DES, $Contract(k, \mathrm{DES}_{ij}, STime)$, is associated with several variables, which include account information $(Account_k, Account_{ij})$, offered price p_k, amount of energy *x*, expected transaction time *TransTime*, and timestamp *STime*. To guarantee this contract can be executed successfully, it needs to verify whether aggregator *k* has sufficient balance such that $\mathrm{Balance}_k \geq p_k \cdot x$ and whether DES_{ij} has enough production capacity to supply *x* amount of corresponding energy on time.

3) Execution: The $Contract(k, \mathrm{DES}_{ij}, STime)$ will be executed if current time $t \geq \mathrm{TransTime}$ after reaching a consensus among aggregators in blockchain network. From now on, it begins to trade energy and finish payment. The smart meter in aggregator *k* verifies whether the amount of energy has been transported to the designated location. Then, fed this result from smart meter into the smart contract, if yes, it will execute the payment process automatically, that is $(k, Balance_k - p_k \cdot x)$ and $(\mathrm{DES}_{ij}, Balance_{ij} + p_k \cdot x)$. Here, we design a mechanism that the balance is permitted to be negative. At the moment of payment, the smart contract will complete payment as usual if the *k*'s balance is not enough to pay. In this way, the *k*'s balance will become negative. Then, any contract that aggregator *k* participants in will not be executed until its balance back to be positive.

Generally, the energies trading can be summarized as follows: In a smart city, a DES begins a smart contract with an aggregator by responding it according to its offered price. This contract needs to be verified by the consensus process in blockchain network. Then, it will execute the pre-defined procedure automatically once the trading conditions are met, which achieves the digital currency and energy exchange specified by contract between participants in a secure manner.

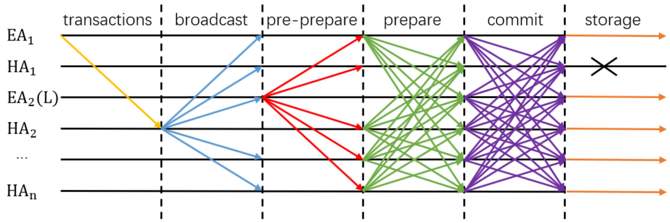


Fig. 3. The consensus process of BCM.

B. Byzantine-Based Consensus Mechanism

As mentioned early, a consensus process is necessary to be performed so as to ensure the consistency of blockchain stored in every authorized node. Castro and Liskov [30] proposed a practical byzantine fault tolerance (PBFT) algorithm, which has been used in consortium blockchain system widely. Based on it and combined with the characteristics of energies trading, we design a new byzantine-based consensus mechanism (BCM). Our consensus process is performed among all aggregators in the ecosystem $\mathbb{S}$, and each of them has a local transaction pool (LTP) to store all transactions it receives. The consensus process is executed round by round, and the time interval of block generation is given by ΔT. There are three main stages shown in Fig. 3, which are pre-prepare, prepare, and commit.

First, let us introduce the credit model, which will be used in leader election to decide whether to reach a consensus. Let $N = \{\mathrm{EA}_1, \mathrm{HA}_1, \mathrm{EA}_2, \mathrm{HA}_2, \ldots\}$ be the collection of consensus nodes. We have known that there is an attribute $\mathit{Credit}_k \in [0, 1]$ for each $k \in N$, where a larger Credit_k implies node *k* is more trustworthy. We denote by $\mathit{Credit}_k(i)$ the credit of node *k* after finishing the *i*-th round consensus. Then, we can define $\mathit{Credit}_k(i+1)$ according to the result of consensus in the $(i+1)$-th round, where this result is whether to add the leader's block into the blockchain. They are (1) When *k* is the leader, we have $\mathit{Credit}_k(i+1) = \min\{1, \mathit{Credit}_k(i) + \Delta_1\}$ if its block is accepted to be added into the blockchain, else $\mathit{Credit}_k(i+1) = \max\{0, \mathit{Credit}_k(i) - \Delta_1\}$ if its block is rejected; and (2) When *k* is not the leader, we have $\mathit{Credit}_k(i+1) = \min\{1, \mathit{Credit}_k(i) + \Delta_2\}$ if its decision is consistent with consensus result; else $\mathit{Credit}_k(i+1) = \max\{0, \mathit{Credit}_k(i) - \Delta_2\}$ if it disagrees with the decision of majority. We usually give $\Delta_1 > \Delta_2 > 0$ and initialize the credit of each consensus node as $\mathit{Credit}_k(0) = 0.5$. When entering the $(i+1)$-th round consensus:

1) Leader Election: The first step in this round is to select a leader from all consensus nodes. This leader election is based on node's credit. Generally speaking, the better the credit value of a node, the more likely it is to be elected as the leader. Thus, the result of leader selection is unpredictable. For a node $k \in N$, the probability that it is elected as the leader of the $(i+1)$-th round consensus is $\Pr[L(i+1) = k]$,

$$\Pr[L(i+1) = k] = \frac{\mathit{Credit}_k(i)}{\sum_{j \in N} \mathit{Credit}_j(i)}, \tag{12}$$

where $L(i+1)$ represents the leader of the $(i+1)$-th round consensus. Obviously, there is no chance to select a node whose credit is zero as the leader.

2) Broadcast: Each aggregator in N broadcasts all transactions which happen in current Δt and co-signed with a DES in its city to the blockchain network. All the consensus nodes will verify whether their received transactions are valid. Those valid transactions will be stored in their LTP but invalid transactions will be discarded.

3) Pre-Prepare: After all non-leader consensus nodes in $N \backslash L(i+1)$ have completed above verification process for received transactions, the leader will package those selected valid transactions in its LTP into a block B_L. Then, the leader signs this block and broadcasts pre-prepare message $(SK_L(B_L), \mathit{pre\text{-}prepare})$ to the blockchain network.

4) Prepare: For each non-leader node $k \in N \backslash L(i+1)$, it will check the identity of leader and verify the pre-prepare message from the leader. The block verification needs to confirm the pointer to the previous block, mercle root is correct and compare the transactions in B_L with the corresponding transactions in its LTP. If node *k* believes B_L is valid, it broadcasts this prepare message $(SK_k(SK_L(B_L)), \mathit{prepare})$ to the blockchain network. All consensus nodes must make decisions in this step, whether to agree or disagree with adding block B_L into the blockchain. Then for each node $k \in N$, it gathers all prepare massages from other consensus node, checks their identities and counts the weighted sum of received prepare messages. Let $A_k(i+1) \subseteq N$ be the set of nodes from which node *k* receives prepare messages, including itself. If satisfying the following inequality, that is

$$\sum_{a \in A_k(i+1)} \Pr[a] \geq \left(2\left\lfloor \frac{|N|-1}{3} \right\rfloor + 1\right)\frac{1}{|N|}, \tag{13}$$

where $\Pr[a] = \mathit{Credit}_a(i)/\sum_{j \in N} \mathit{Credit}_j(i)$, we say node *k* will accept block B_L and broadcast commit message $(SK_k(SK_L(B_L)), \mathit{commit})$ to the blockchain network.

5) Commit: After sending their commit messages, they should waiting commit messages from other consensus node. For each node $k \in N$, its consensus process is completed until it receive sufficient commit messages such that $\sum_{a \in B_k(i+1)} \Pr[a] \geq (2\lfloor(|N|-1)/3\rfloor + 1)/|N|$, where $B_k(i+1) \subseteq N$ is the set of nodes from which node *k* receives commit message, including itself.

6) Add a Block and Update Credits: If a consensus node accepts the new block B_L, it will be appended into the blockchain in a linear and chronological order. Any failure occurs in these three stages will terminate the current consensus (do not add the new block). Besides, before finishing this round, we need to update the credits of all the consensus nodes according to the credit model. In next round, the consensus process will perform based on their new credits.

There are two kinds of failures that can terminate the current round: (1) The leader sends invalid block or do not send its packaged block before the deadline; and (2) Too many malicious nodes do not breadcast prepare messages even though this block is valid. Shown as node HA_1 in Fig. 3, it is a faulty node. The credit of those nodes that make mistakes in this consensus process will be reduced. Let f be the number of malicious nodes. According to [30], supposing $f \leq \lfloor(|N|-1)/3\rfloor$, the faults can be tolerated by the consensus

TABLE I
THE FREQUENTLY USED NOTATIONS SUMMARIZATION

Notation	Description
$\mathrm{S}, C_j \in \mathrm{S}$	A smart city and communities in it
EA, HA	Electricity and heat aggregator in S
α_j, β_j	Electricity and heat dispastching of C_j
X^j, Y^j	Two constant defined in Remark 1
U^j	Utility of DES_j in C_j
k_e^j, k_h^j	Satisfaction coefficient for electricity, heat
b_e^j, b_h^j	Adaption coefficient for electricity, heat
M_{min}^j	Constraint of minimun used energy in C_j
p_e, p_h	Prices offered by EA and HA
c_e, r_e, c_h, r_h	$p_e \in [c_e, r_e]$ and $p_h \in [c_h, r_h]$
V_e, V_h	Utilities (profits) of EA and HA
$\lambda_1, \lambda_2, \lambda_3$	Three Lagrange's multipliers

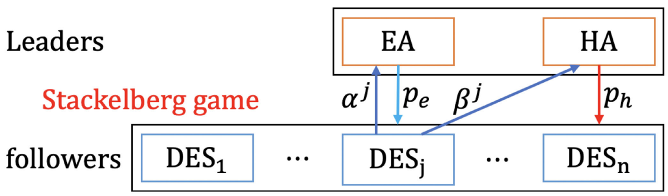


Fig. 4. The interactions of MLMF Stackelberg game between aggregators and DESs in city S.

system with $|N|$ nodes. In our BCM, each consensus node's credit is initialized as a constant, thereby $2\lfloor(|N|-1)/3\rfloor+1$ normal nodes can make sure that (13) is satisfied. As the consensus process performs more and more times, the normal nodes' credits increase but malicious nodes' credits decrease gradually. Therefore, the credits in this system will be more accumulative in those normal nodes. According to (13), the number of prepare message and commit message required to reach a consensus declines, which helps reduce latency and improve throughput. In summary, secure and traceable energies trading and digital currency exchange can be guaranteed by our proposed B-MET system.

V. MULTIPLE ENERGIES TRADING: A STACKELBERG APPROACH

A non-cooperative Stackelberg game generally refers to the multilevel decision-making processes of a number of independent decision-makers in response to the decision taken by the leading player of the game [31]. In this section, we put forward a multi-leader multi-follower (MLMF) Stackelberg game to model the interactions in above smart contract between aggregators and DESs. The frequently used notations in this paper are shown in Table I. Considering a specific city $\mathrm{S} \in \mathbb{S}$, we omit the subscript *i* for simplicity in subsequent analysis. Then, the MLMF Stackelberg game $\mathbb{G}$ in $\mathrm{S} \in \mathbb{S}$ can be defined as

$$\mathbb{G} = \left\{\mathrm{S}, \mathbb{P}, \mathbb{D}, \{V_e, V_h\}, \left\{U^j\right\}_{\mathrm{C}_j \in \mathrm{S}}\right\}. \tag{14}$$

The interactions of MLMF Stackelberg game $\mathbb{G}$ between aggregators and DESs in $\mathrm{S} \in \mathbb{S}$ is shown in Fig. 4, and its components are shown as follows.

1) Players Set S: The aggregators HA and EA act as leaders, and offer a price respectively to the DESs. Then, $\mathrm{DES}_j \in \mathrm{S}$ act as followers, and decide on the amount of electricity and heat they want to sell respectively according to the offered prices.

2) Strategy Spaces $\mathbb{P}$ and $\mathbb{D}$: Let $\mathbb{P} = [c_e, r_e] \times [c_h, r_h]$ be the strategy space of two aggregators, where we say $\{p_e, p_h\} \in \mathbb{P}$ is a feasible strategy of HA and EA. Then, let $\mathbb{D} = \times_{\mathrm{C}_j \in \mathrm{S}}\{[0,1]\times[0,1]\}$ be the strategy space of all DESs in this city, and we have $\{\alpha^j, \beta^j\}_{\mathrm{C}_j \in \mathrm{S}} \in \mathbb{D}$ is a feasible strategy of DESs.

3) Utility Functions $\{V_e, V_h\}$ and $\{U^j\}_{\mathrm{C}_j \in S}$: Each player in this game aims to maximize its utility or profit, which reflects the quality of strategy that this player chooses. $\{V_e, V_h\}$ is the profits of aggregators, defined in (10) and (11); and $\{U^j\}_{\mathrm{C}_j \in \mathrm{S}}$ are the utilities of DESs in S, defined in (6).

A. DESs (Followers) Side Analysis

Given a price strategy $\{p_e, p_h\} \in \mathbb{P}$ offered by two aggregators in city S, each $\mathrm{DES}_j \in \mathrm{S}$ decides the amount of electricity E_{use}^j (resp. heat Q_{use}^j) that sold to the EA (resp. HA) by adjusting its dispatching factor α^j (resp. β^j). Thus, each $\mathrm{DES}_j \in \mathrm{S}$ aims to choose its optimal dispatching factors $\{\alpha^j, \beta^j\}$ according to $\{p_e, p_h\}$ by solving the following optimization problem ($\mathrm{OP_{DES}}$). Defined by M_{min}^j the minimum amount of energy that is required to maintain the basic life for those residents living in this community, we have

$$\max_{\{\alpha^j, \beta^j\}} \quad U^j\left(\alpha^j, \beta^j\right), \tag{15}$$

$$\text{s.t.} \quad E_{use}^j + Q_{use}^j \geq M_{min}^j; \left\{\alpha^j, \beta^j\right\} \in [0,1] \times [0,1]. \tag{16}$$

To ensure reasonableness, the E_{min}^j should be in a valid range, thus we have $M_{min}^j \in (\max\{X^j, Y^j\}, X^j + Y^j)$. It means that this minimum requirement is larger than the production capacity of electricity or heat separately, which implies that α^j and β^j are impossible to approach zero definitely. Hence, the restrictions on (16) can be converted equivalently to constraint (17), that is

$$X^j \cdot \alpha^j + Y^j \cdot \beta^j \geq M_{min}^j; \ \alpha^j \leq 1, \beta^j \leq 1. \tag{17}$$

Thus, the $\mathrm{OP_{DES}}$ problem consists of (15) and (17) from now on, which is a convex optimization problem.

Lemma 1: The $\mathrm{OP_{DES}}$ is a convex optimization problem.

Proof: The domain enclosed by (17) is closed and bounded, then the compactness is found immediately. The convexity of this domian is trivial because it can be enclosed by three linear restrictions. The domain of $\mathrm{OP_{DES}}$ is an convex set.

Next, it is sufficient to show that the objective function defined in (15) is continously differentiable and concave. First, its first-order derivatives is

$$\frac{\partial U^j}{\partial \alpha^j} = X^j \cdot \left(\frac{k_e^j b_e^j}{1 + b_e^j X^j \alpha^j} - p_e\right), \tag{18}$$

$$\frac{\partial U^j}{\partial \beta^j} = Y^j \cdot \left(\frac{k_h^j b_h^j}{1 + b_h^j Y^j \beta^j} - p_h \right). \tag{19}$$

Denote by H^j the Hessian matrix of U^j, we have

$$H^j = \begin{bmatrix} U_{\alpha\alpha}^j & U_{\alpha\beta}^j \\ U_{\beta\alpha}^j & U_{\beta\beta}^j \end{bmatrix}, \tag{20}$$

where $U_{\alpha\alpha}^j = \partial^2 U^j / \partial {\alpha^j}^2$, $U_{\alpha\beta}^j = \partial^2 U^j / \partial \alpha^j \partial \beta^j$, $U_{\beta\alpha}^j = \partial^2 U^j / \partial \beta^j \partial \alpha^j$, and $U_{\beta\beta}^j = \partial^2 U^j / \partial {\beta^j}^2$. Then, these second-order derivatives are

$$\frac{\partial^2 U^j}{\partial {\alpha^j}^2} = -\frac{{X^j}^2 k_e^j {b_e^j}^2}{\left(1 + b_e^j X^j \alpha^j\right)^2}, \ \frac{\partial^2 U^j}{\partial \alpha^j \partial \beta^j} = 0, \tag{21}$$

$$\frac{\partial^2 U^j}{\partial {\beta^j}^2} = -\frac{{Y^j}^2 k_h^j {b_h^j}^2}{\left(1 + b_h^j Y^j \beta^j\right)^2}, \ \frac{\partial^2 U^j}{\partial \beta^j \partial \alpha^j} = 0. \tag{22}$$

Thus, we have $U_{\alpha\alpha}^j < 0$ and $U_{\beta\beta}^j < 0$, which indicates that $\partial^2(-U^j)/\partial {\alpha^j}^2 > 0$ and $U_{\beta\beta}^j = \partial^2(-U^j)/\partial {\beta^j}^2 > 0$. From here, the Hassian matrix of $-U^j$ is positive definite, thereby $-U^j$ is a convex function and our objective U^j is a concave function. The $\mathrm{OP_{DES}}$ is a convex problem. ■

Therefore, to maximize a concave function, the stationary solution is unique and optimal. Let $\partial U^j / \partial \alpha^j = 0$ and $\partial U^j / \partial \beta^j = 0$, we have

$$\alpha_\circ^j = \frac{1}{X^j} \left(\frac{k_e^j}{p_e} - \frac{1}{b_e^j} \right); \ \beta_\circ^j = \frac{1}{Y^j} \left(\frac{k_h^j}{p_h} - \frac{1}{b_h^j} \right). \tag{23}$$

Here, we need to note that the setting of parameter k_e^j (resp. k_h^j) must be in a valid range such that $\alpha_\circ^j \in (0, 1)$ (resp. $\beta_\circ^j \in (0, 1)$) for any offered price $p_e \in [c_e, r_e]$ (resp. $p_h \in [c_h, r_h]$). Or else, this utility function is monotone, and it is meaningless to adjust its dispatching factors. Base on that, thereby we can restrict k_e^j and k_h^j as follows:

$$k_e^j \in \left(\frac{r_e X^j}{e - 1}, \frac{c_e X^j}{1 - 1/e} \right); \ k_h^j \in \left(\frac{r_h Y^j}{e - 1}, \frac{c_h Y^j}{1 - 1/e} \right), \tag{24}$$

where it assume $r_e < e \cdot c_e$ (resp. $r_h < e \cdot c_h$), or else no such k_e^j (resp. k_h^j) can keep $\alpha_\circ^j \in (0, 1)$ (resp. $\beta_\circ^j \in (0, 1)$) satisfied for any offered prices.

Sequentially, we use Lagrange's multipliers λ_1, λ_2 and λ_3 for constraint (17), thereby the $\mathrm{OP_{DES}}$, defined in (15) and (17), can be converted to the following form $L^j(\alpha^j, \beta^j, \lambda_1, \lambda_2, \lambda_3)$, that is

$$\begin{aligned} L^j = {} & U^j\left(\alpha^j, \beta^j\right) + \lambda_1 \left(X^j \cdot \alpha^j + Y^j \cdot \beta^j - M_{min}^j \right) \\ & + \lambda_2 \left(1 - \alpha^j\right) + \lambda_3 \left(1 - \beta^j\right), \end{aligned} \tag{25}$$

where we denote by $Z^j = X^j + Y^j - M_{max}^j$. Then, based on (25), the complementary slackness conditions (KKT conditions) of $\mathrm{OP_{DES}}$ are demonstrated as follows:

$$\frac{\partial L^j}{\partial \alpha^j} = \frac{\partial U^j}{\partial \alpha^j} + \lambda_1 X^j - \lambda_2 = 0, \tag{26}$$

$$\frac{\partial L^j}{\partial \beta^j} = \frac{\partial U^j}{\partial \beta^j} + \lambda_1 Y^j - \lambda_3 = 0, \tag{27}$$

$$\lambda_1 \cdot \left(X^j \cdot \alpha^j + Y^j \cdot \beta^j - M_{min}^j \right) = 0, \tag{28}$$

$$\lambda_2 \cdot (1 - \alpha^j) = 0, \tag{29}$$

$$\lambda_3 \cdot (1 - \beta^j) = 0, \tag{30}$$

$$\lambda_1 \geq 0, \ \lambda_2 \geq 0, \ \lambda_3 \geq 0, \ \text{and constraints (17)}. \tag{31}$$

The optimal solutions of $\mathrm{OP_{DES}}$, shown as (15) and (17), can take one of the following four cases, that is

1) Case 1: For $\alpha^j < 1$ and $\beta^j < 1$, we have $\lambda_2 = \lambda_3 = 0$. Look at (28), if $\lambda_1 = 0$, substitute it into (26) and (27), we can get a solution $\{\alpha_\circ^j, \beta_\circ^j\}$ according to (23). Then, we need to check whether the constraint (17) can be satisfied. If yes, the optimal solution is $\{\alpha_\circ^j, \beta_\circ^j\}$. If no, it means $\lambda_1 > 0$ and $X^j \cdot \alpha^j + Y^j \cdot \beta^j - M_{min}^j = 0$. At this time, by solving (26) and (27), we have

$$\alpha_\diamond^j = \frac{1}{X^j} \left(\frac{k_e^j}{p_e - \lambda_1} - \frac{1}{b_e^j} \right), \tag{32}$$

$$\beta_\diamond^j = \frac{1}{Y^j} \left(\frac{k_h^j}{p_h - \lambda_1} - \frac{1}{b_h^j} \right). \tag{33}$$

Substitute (32) and (33) into (28),

$$A^j {\lambda_1}^2 + B^j \lambda_1 + C^j = 0, \tag{34}$$

where $A^j = M_{min}^j + 1/b_e^j + 1/b_h^j$, $B^j = k_e^j + k_h^j - A^j(p_e + p_h)$, and $C^j = A^j p_e p_h - k_e^j p_h - k_h^j p_e$. By solving (34), we have two solutions, they are

$$\lambda_1 = \frac{-B^j \pm \sqrt{{B^j}^2 - 4 A^j C^j}}{2 A^j}. \tag{35}$$

Here, it is easy to verify $B^j < 0$ and $C^j > 0$ based on (9), (24), and $M_{min}^j \in (\max\{X^j, Y^j\}, X^j + Y^j)$, thus it is possible that $\Delta^j = {B^j}^2 - 4 A^j C^j < 0$. If $\Delta^j < 0$, there is no real solution; else we need to check whether the λ_1 defined on (35) satisfies $\lambda_1 > 0$. If $\lambda_1 > 0$, substitute (35) into (32) and (33), we obtain a solution $\{\alpha_\diamond^j, \beta_\diamond^j\}$. If it is feasible, namely $\alpha_\diamond^j, \beta_\diamond^j < 1$, the optimal solution can be determined by $\{\alpha_\diamond^j, \beta_\diamond^j\}$.

2) Case 2: For $\alpha^j = 1$ and $\beta^j < 1$, we have $\lambda_3 = 0$. Look at (28), if $\lambda_1 = 0$, substitute it into (27), we can get a solution $\{1, \beta_\circ^j\}$ according to (23). Then, we need to check whether the constraint (17) can be satisfied and $\lambda_2 = \partial U^j / \partial \alpha^j \geq 0$. If yes, the optimal solution $\{1, \beta_\circ^j\}$. If no, it means $\lambda_1 > 0$ and $Y^j \cdot \beta^j + X^j - M_{min}^j = 0$. According to (27), we have $\beta_\square^j$ which is shown as (33). Substitute (33) into (28),

$$\left(\frac{k_h^j}{p_h - \lambda_1} - \frac{1}{b_h^j} \right) + X^j - M_{min}^j = 0. \tag{36}$$

By solving (36), we have

$$\lambda_1 = p_h - \frac{k_h^j b_h^j}{b_h^j \left(M_{min}^j - X^j \right) + 1}. \tag{37}$$

If $\lambda_1 > 0$ and $\lambda_2 = \partial U^j / \partial \alpha^j + \lambda_1 X^j \geq 0$, substitute (37) into (33), we obtain a solution $\{1, \beta^j_\square\}$. If we have $\beta^j_\square < 1$, the optimal solution can be determined by $\{1, \beta^j_\square\}$.

3) Case 3: For $\alpha^j < 1$ and $\beta^j = 1$, we have $\lambda_2 = 0$. Look at (28), if $\lambda_1 = 0$, substitute it into (26), we can get a solution $\{\alpha^j_\circ, 1\}$ according to (18). Then, we need to check whether the constraint (17) can be satisfied and $\lambda_3 = \partial U^j / \partial \beta^j \geq 0$. If yes, the optimal solution is $\{\alpha^j_\circ, 1\}$. If no, it means $\lambda_1 > 0$ and $X^j \cdot \alpha^j + Y^j - M^j_{min} = 0$. According to (26), we have $\alpha^j_\square$ which is shown as (32). Substitute (32) into (28),

$$\left(\frac{k^j_e}{p_e - \lambda_1} - \frac{1}{b^j_e}\right) + Y^j - M^j_{min} = 0. \tag{38}$$

By solving (38), we have

$$\lambda_1 = p_e - \frac{k^j_e b^j_e}{b^j_e\left(M^j_{min} - Y^j\right) + 1}. \tag{39}$$

If $\lambda_1 > 0$ and $\lambda_3 = \partial U^j / \partial \beta^j + \lambda_1 Y^j \geq 0$, substitute (39) into (32), we obtain a solution $\{\alpha^j_\square, 1\}$. If we have $\alpha^j_\square < 1$, the optimal solution can be determined by $\{\alpha^j_\square, 1\}$.

4) Case 4: For $\alpha^j = 1$ and $\beta^j = 1$, we have $\lambda_1 = 0$ because we have assumed $M^j_{min} \leq X^j + Y^j$ before. Substitute it into (26) and (27), we have

$$\left(\alpha^j_\diamond = 1\right) = \frac{1}{X^j}\left(\frac{k^j_e X^j}{\lambda_2 + p_e X^j} - \frac{1}{b^j_e}\right), \tag{40}$$

$$\left(\beta^j_\diamond = 1\right) = \frac{1}{Y^j}\left(\frac{k^j_h Y^j}{\lambda_3 + p_h Y^j} - \frac{1}{b^j_h}\right). \tag{41}$$

By solving (40) and (41), we have

$$\lambda_2 = \frac{k^j_e X^j}{X^j + 1/b^j_e} - p_e X^j;\ \lambda_3 = \frac{k^j_h Y^j}{Y^j + 1/b^j_h} - p_h Y^j \tag{42}$$

According to (9), (24), the maximum value of λ_2 can be obtained when giving $k^j_e = c_e X^j / (1 - 1/e)$. Substitute it into (42), we have $\lambda_2 < c_e - p_e \leq 0$ because of $p_e \in [c_e, r_e]$. By using the same way, we have $\lambda_3 < c_h - p_h \leq 0$ because of $p_h \in [c_h, r_h]$ as well. It does not satisfy (31), thus this solution {1, 1} is not feasible and cannot occur. The final result will be in one of these four cases.

To sum up, offered a price strategy $\{p_e, p_h\} \in \mathbb{P}$ by aggregators, the optimal response of each $\mathrm{C}_j \in \mathrm{S}$ will be obtained by above procedure. It is one of the three cases, except case 4, that depends on the offered prices, minimum requirement M^j_{min}, and choice of satisfaction coefficient k^j_e and k^j_h. Since the expressions of the solution is very complicated, we cannot give a unified formal expression to summarize the results that contains all cases.

B. Aggregators (Leaders) Side Analysis

After receiving the responses E^j_{exc} (resp. Q^j_{exc}) of all C_j in city S, the profit gained by aggregators EA (resp. HA) can be determined according to (10) and (11). They assume each $\mathrm{DES}_j \in \mathrm{S}$ will respond to them with the optimal strategy according to their offered price. Thus, EA and HA aim to choose its optimal prices $\{p^*_e, p^*_h\}$ by solving the following optimization problem ($\mathrm{OP_{AGS}}$), that is

$$\max_{\{p_e\}} V_e(p_e, p_h)\ \text{ s.t. }\ p_e \in [c_e, r_e], \tag{43}$$

$$\max_{\{p_h\}} V_h(p_h, p_e)\ \text{ s.t. }\ p_h \in [c_h, r_h]. \tag{44}$$

where EA (resp. HA) attempts to select an optimal price p^*_e (resp. p^*_h) to maximize its profit given p_h (resp. p_e). The objective function, shown in (10) (resp. (11)), is strictly concave and continuous differentiable with respect to p_e (resp. p_h), which will be proved in Lemma 2.

First, we consider electricity aggregator EA alone. Feeding a price p_e into $V_e(\cdot, p_h)$, the response $\alpha^j(p_e, p_h)$ of each $\mathrm{DES}_j \in \mathrm{S}$ must be in one of the following four events: 1) $\alpha^j = \alpha^j_\circ$; 2) $\alpha^j = 1$; 3) $\alpha^j = \alpha^j_\diamond$; and 4) $\alpha^j = \alpha^j_\square$. Then, its first-order derivatives are

$$\begin{aligned}
\partial \alpha^j / \partial p_e &= -k^j_e / \left(X^j {p_e}^2\right) && (45)\\
&= 0 && (46)\\
&= -k^j_e / \left(X^j (p_e - \lambda_1)^2\right),\ \lambda_1 = (35) && (47)\\
&= -k^j_e / \left(X^j (p_e - \lambda_1)^2\right),\ \lambda_1 = (39). && (48)
\end{aligned}$$

where it is one-to-one correspondences between (45)−(48) and event (1)-(4). Then, the first-order derivative of EA's objective function is

$$\frac{\partial V_e}{\partial p_e} = -\sum_{\mathrm{C}_j \in \mathrm{S}} X^j \left(\left(1 - \alpha^j\right) + (r_e - p_e)\frac{\partial \alpha^j}{\partial p_e}\right). \tag{49}$$

Combined with (45)–(48), let $\partial V_e / \partial p_e = 0$, we can get a solution $\hat{p}_e$ that maximizes $V_e(\cdot, p_h)$ given p_h. However, this $\hat{p}_e$ is constrained on the range of $[c_e, r_e]$, thus the optimal price strategy $\bar{p}_e$ of EA is shown as follows:

$$\bar{p}_e = \begin{cases} r_e, & \text{if } \hat{p}_e \geq r_e \\ c_e, & \text{if } \hat{p}_e \leq c_e \\ \hat{p}_e, & \text{if } c_e < \hat{p}_e < r_e. \end{cases} \tag{50}$$

Due to the fact that the profit function $V_e(\cdot, p_h)$ given p_h is strictly concave with respect to p_e, it increases first and then decreases with the increase of p_e. Thus, the maximum profit is obtained at the price of r_e when $\hat{p}_e \geq r_e$; Similarly, the maximum profit is obtained at the price of c_e when $\hat{p}_e \leq c_e$; else obtained at stationary point.

Then, we consider heat aggregator HA alone. Feeding a price p_h into $V_h(\cdot, p_e)$, the respone $\beta^j(p_e, p_h)$ of each $\mathrm{DES}_j \in \mathrm{S}$ must be in one of the following four events: 5) $\beta^j = \beta^j_\circ$; 6) $\beta^j = 1$; 7) $\beta^j = \beta^j_\diamond$; and 8) $\beta^j = \beta^j_\square$. Then, its first-order derivatives are

$$\begin{aligned}
\partial \beta^j / \partial p_h &= -k^j_h / \left(Y^j {p_h}^2\right) && (51)\\
&= 0 && (52)\\
&= -k^j_h / \left(Y^j (p_h - \lambda_1)^2\right),\ \lambda_1 = (35) && (53)\\
&= -k^j_h / \left(Y^j (p_h - \lambda_1)^2\right),\ \lambda_1 = (37). && (54)
\end{aligned}$$

where it is one-to-one correspondences between (51)–(54) and event (5)–(8). Then, the first-order derivative of HA's objective function is

$$\frac{\partial V_h}{\partial p_h} = -\sum_{\mathrm{C}_j \in \mathrm{S}} Y^j \left(\left(1 - \beta^j\right) + (r_h - p_h) \frac{\partial \beta^j}{\partial p_h} \right). \quad (55)$$

Let $\partial V_h / \partial p_h = 0$, we can get a solution $\hat{p}_h$ that maximizes $V_h(\cdot, p_e)$ given p_e. Similar to (50), constrained on the range of $[c_h, r_h]$, the optimal price $\bar{p}_h$ of HA can be formulated similar to the analysis of (50) from its concavity.

C. Stackelberg Equilibrium

The aggregators, EA and HA in a smart city S, play a non-cooperative game with each other to offer the unit prices for electricity and heat. They all want to maximize their profit according to their profit function defined on (10) and (11). We denote this game between aggregators by $\mathbb{A} = \{\{\mathrm{HA}, \mathrm{EA}\}, \mathbb{P}, \{V_e, V_h\}\}$ and introduce the concept of the Nash equilibrium (NE) shown as follows:

Definition 1: (NE): Given a game $\mathbb{A}$, a feasible price strategy $\{\tilde{p}_e, \tilde{p}_h\} \in \mathbb{P}$ is the NE if no player can improve its profit by changing its strategy unilaterally, that is

$$V_e(\tilde{p}_e, \tilde{p}_h) \geq V_e(p_e, \tilde{p}_h);\ V_h(\tilde{p}_h, \tilde{p}_e) \geq V_h(p_h, \tilde{p}_e). \quad (56)$$

At the NE, no aggregator attempts to offer a new price again because they all achieve their mutually satisfactions respectively (No one can improve its profit further). Then, we need to study the existence and uniqueness of the NE of game $\mathbb{A}$ between two aggregators in a city.

Lemma 2: The NE of game $\mathbb{A}$ between aggregators always exist and is unique.

Proof: The strategy space in game $\mathbb{A}$ has been denoted by $\mathbb{P} = [c_e, r_e] \times [c_h, r_h]$, which is a convex, closed, and non-empty subset of the space $\mathbb{R}^2$. Take aggregator EA as an example, α^j is the responsive dispatching factor given the offered price $\{p_e, p_h\} \in \mathbb{P}$ from community $\mathrm{C}_j \in \mathrm{S}$. From (45)–(48), its second-order derivatives are

$$\partial^2 \alpha^j / \partial {p_e}^2 = 2k_e^j / \left(X^j {p_e}^3 \right) \quad (57)$$
$$= 0 \quad (58)$$
$$= 2k_e^j / \left(X^j (p_e - \lambda_1)^3 \right),\ \lambda_1 = (35) \quad (59)$$
$$= 2k_e^j / \left(X^j (p_e - \lambda_1)^3 \right),\ \lambda_1 = (39), \quad (60)$$

where they correspond to event (1)–(4). Here, $\partial^2 \alpha^j / \partial {p_e}^2 > 0$ in (57) trivially. $\partial^2 \alpha^j / \partial {p_e}^2 > 0$ in (59) and (60) since $p_e - \lambda_1 > 0$ based on (32). Then, the second-order derivative of EA's objective function is

$$\frac{\partial^2 V_e}{\partial {p_e}^2} = \sum_{\mathrm{C}_j \in \mathrm{S}} X^j \left(2 \cdot \frac{\partial \alpha^j}{\partial p_e} - (r_e - p_e) \frac{\partial^2 \alpha^j}{\partial {p_e}^2} \right). \quad (61)$$

Here, observe that $\partial \alpha^j / \partial p_e \leq 0$ from (45)–(48), and $\partial^2 \alpha^j / \partial {p_e}^2 \geq 0$ from (57)–(60), we have $\partial^2 V_e / \partial {p_e}^2 \leq 0$. Thus, $V_e(\cdot, p_h)$ is concave with respect to p_e.

From (51)−(54), its second-order derivatives are

$$\partial^2 \beta^j / \partial {p_h}^2 = 2k_h^j / \left(Y^j {p_h}^3 \right) \quad (62)$$
$$= 0 \quad (63)$$
$$= 2k_h^j / \left(Y^j (p_h - \lambda_1)^3 \right),\ \lambda_1 = (35) \quad (64)$$
$$= 2k_h^j / \left(Y^j (p_h - \lambda_1)^3 \right),\ \lambda_1 = (37), \quad (65)$$

where they correspond to event (5)–(8). Then, the second-order derivative of HA's objective function is

$$\frac{\partial^2 V_h}{\partial {p_h}^2} = \sum_{\mathrm{C}_j \in \mathrm{S}} Y^j \left(2 \cdot \frac{\partial \beta^j}{\partial p_h} - (r_h - p_h) \frac{\partial^2 \beta^j}{\partial {p_h}^2} \right). \quad (66)$$

By similar analysis, we have $\partial^2 V_h / \partial {p_h}^2 \leq 0$ and $V_h(\cdot, p_e)$ is concave with respect to p_h. Thus, game $\mathbb{A}$ is a concave 2-person game. Because of their concavity, the Nash equilibrium exists and is unique according to [32]. ■

In a smart city S, the aggregators offer the price strategy $\{p_e, p_h\} \in \mathbb{P}$ in the first stage, then each $\mathrm{DES}_j \in \mathrm{S}$ decides its optimal dispatching strategy $\{\alpha^j, \beta^j\}$ according to the offered prices in the second stage. It formulates a MLMF Stackelberg game $\mathbb{G}$ between aggregators and DESs, shown as (14). The optimal strategy set $\{\{\tilde{p}_e, \tilde{p}_h\}, \{\bar{\gamma}^l\}_{\mathrm{C}_l \in \mathrm{S}}\}$, where $\bar{\gamma}^l$ is the optimal response of community $\mathrm{C}_l \in \mathrm{S}$ based on its previous leaders' prices, can be obtained at the Stackelberg equilibrium (SE), defined as follows.

Definition 2: (SE): Given a game $\mathbb{G}$ defined as (14), a feasible strategy $\{\{\tilde{p}_e, \tilde{p}_h\}, \{\bar{\gamma}^l\}_{\mathrm{C}_l \in \mathrm{S}}\}$ is the SE if no player, including leaders and followers, can improve its utility or profit by changing its strategy unilaterally, that is

$$U^j\left(\tilde{p}, \left\{ \bar{\gamma}^l \right\}_{\mathrm{C}_l \in \mathrm{S}} \right) \geq U^j\left(\tilde{p}, \gamma^j \cup \left\{ \bar{\gamma}^l \right\}_{\mathrm{C}_l \in \mathrm{S} \setminus \mathrm{C}_j} \right), \quad (67)$$
$$V_e\left(\tilde{p}, \left\{ \bar{\gamma}^l \right\}_{\mathrm{C}_l \in \mathrm{S}} \right) \geq V_e\left(\{p_e, \tilde{p}_h\}, \left\{ \bar{\gamma}^l \right\}_{\mathrm{C}_l \in \mathrm{S}} \right), \quad (68)$$
$$V_h\left(\tilde{p}, \left\{ \bar{\gamma}^l \right\}_{\mathrm{C}_l \in \mathrm{S}} \right) \geq V_h\left(\{\tilde{p}_e, p_h\}, \left\{ \bar{\gamma}^l \right\}_{\mathrm{C}_l \in \mathrm{S}} \right). \quad (69)$$

where we denote prices $\tilde{p}^i = \{\tilde{p}_e^i, \tilde{p}_h^i\}$ and $\gamma^j = \{\alpha^j, \beta^j\}$ is any feasible strategy that the DES_j can give.

After reaching the SE, none of them tends to change its strategy again because they cannot improve their utilities or profits further by changing unilaterally. Then, we need to study the existence and uniqueness of the SE of game $\mathbb{G}$ between aggregators and DESs in a city.

Theorem 1: The SE of game $\mathbb{G}$ between aggregators and DESs always exist and is unique.

Proof: In this game $\mathbb{G}$, the aggregators will offer prices to purchase energies in their city first. From Lemma 2, a NE always exists and is unique between aggregators. According to the analysis on DESs, they respond to aggregators with their optimal dispatching strategies based on the offered prices. Thus, the SE always exists and is unique. ■

D. Distributed Algorithm

In order to find the NE between aggregators based on the optimal responses from DESs, we adopt the sub-gradient technique [33], [34], [35] for determining price strategies. It is shown in Algorithm 1. In Algorithm 1, each aggregator is assigned with its lowest price. At this time, the dispatching factors of each DES in this city is closest to one, which should

Algorithm 1 Find NE

Input: Game $\mathbb{G}$ in a city S and a small step Δ
Output: Price strategy $\{\tilde{p}_e, \tilde{p}_h\}$

Initialize: $\{\tilde{p}_e, \tilde{p}_h\} \leftarrow \{c_e, c_h\}$
while True **do**
  $\{x, y\} \leftarrow \{\tilde{p}_e, \tilde{p}_h\}$
  // Consider aggregator EA
  if $V_e(\tilde{p}_e+\Delta, \tilde{p}_h) \geq V_e(\tilde{p}_e, \tilde{p}_h)$ and $V_e(\tilde{p}_e+\Delta, \tilde{p}_h) \geq V_e(\tilde{p}_e-\Delta, \tilde{p}_h)$ **then**
    $\tilde{p}_e \leftarrow \min\{r_e, \tilde{p}_e + \Delta\}$
  else if $V_e(\tilde{p}_e - \Delta, \tilde{p}_h) \geq V_e(\tilde{p}_e, \tilde{p}_h)$ and $V_e(\tilde{p}_e - \Delta, \tilde{p}_h) \geq V_e(\tilde{p}_e + \Delta, \tilde{p}_h)$ **then**
    $\tilde{p}_e \leftarrow \max\{c_e, \tilde{p}_e - \Delta\}$
  end if
  // Consider aggregator HA
  if $V_h(\tilde{p}_h+\Delta, \tilde{p}_e) \geq V_h(\tilde{p}_h, \tilde{p}_e)$ and $V_h(\tilde{p}_h+\Delta, \tilde{p}_e) \geq V_h(\tilde{p}_h-\Delta, \tilde{p}_e)$ **then**
    $\tilde{p}_h \leftarrow \min\{r_h, \tilde{p}_h + \Delta\}$
  else if $V_h(\tilde{p}_h - \Delta, \tilde{p}_e) \geq V_h(\tilde{p}_h, \tilde{p}_e)$ and $V_h(\tilde{p}_h - \Delta, \tilde{p}_e) \geq V_h(\tilde{p}_h + \Delta, \tilde{p}_e)$ **then**
    $\tilde{p}_h \leftarrow \max\{c_h, \tilde{p}_h - \Delta\}$
  end if
  if $\{x, y\} = \{\tilde{p}_e, \tilde{p}_h\}$ **then**
    Break
  end if
  // Reduce Δ once for each iteration
  $\Delta \leftarrow \delta \cdot \Delta$
end while
return $\{\tilde{p}_e, \tilde{p}_h\}$

be in feasible space defined on (17). Then, considering aggregator EA, in each iteration, it updates its price in manner of increasing by Δ or decreasing by Δ, where Δ is a given small step. According to current prices $\{\tilde{p}_e, \tilde{p}_h\}$, we compare the profits of EA by offering a price $\tilde{p}_e$, $\tilde{p}_e + \Delta$, and $\tilde{p}_e - \Delta$, then choose the best one and update the price $\tilde{p}_e$. Considering aggregator HA similarly, we compare the profits of HA by offering a price $\tilde{p}_h$, $\tilde{p}_h + \Delta$, and $\tilde{p}_h - \Delta$, then choose the best one and update the price $\tilde{p}_h$. At last, we update Δ with $\delta \cdot \Delta$ where $\delta \in (0, 1)$ is a attenuation factor.

Theorem 2: Given an initial price strategy and step Δ, the Nash equilibrium of game $\mathbb{A}$ can be obtained by the sub-gradient algorithm, shown in Algorithm 1.

Proof: Based on the conclusion of [33], [34], the sub-gradient algorithm can converge to an optimal solution in convex optimization. The objective functions of aggregators are concave, thus they cannot improve its profit by changing strategies unilaterally when reaching the optimal solution. ∎

According to Lemma 2 and Theorem 2, the NE returned by Algorithm 1 is the unique NE between EA and HA. Then, the followers (DESs) always respond to leaders (EA and HA) with their optimal strategies (dispatching factors). Based on Theorem 1, this NE is the point of SE definitely.

VI. Numerical Simulations

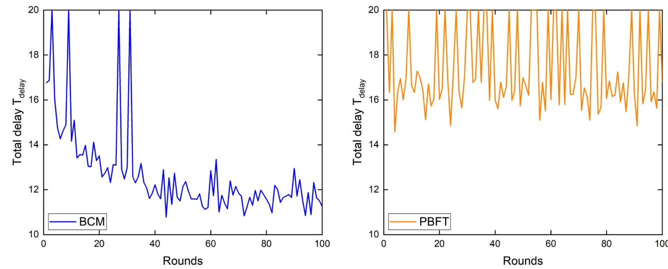
In this section, we conduct several experiments to test our byzantine-based consensus mechanism (BCM) and model the energies trading in a smart city.

A. Simulation Setup

To test our BCM, we give a blockchian network with 100 aggregators (consensus nodes) in which 30% of aggregators are malicious nodes. Initially, we set $Credit_k(0) = 0.5$ for each $k \in M$, $\Delta_1 = 0.05$ and $\Delta_2 = 0.01$. Here, we only focus on the consensus decision process, namely the prepare stage and commit stage. The delay of each stage in each round is sampled from interval (0, 10) according to the Gaussian distribution *N*(5, 2). Therefore, the total delay T_{delay} in each round can be denoted by

$$T_{delay} = T_{prepare} + T_{commit} \in (0, 20]. \tag{70}$$

From here, we can know the maximum time to complete one round consensus is 20. If the censensus cannot be reached after this deadline, we think that this consensus has failed. For example, the leader in this round is a malicious node and it broadcast a invalid block. It cannot receive enough prepare message and commit message, thereby this consensus fails and total delay is 20.



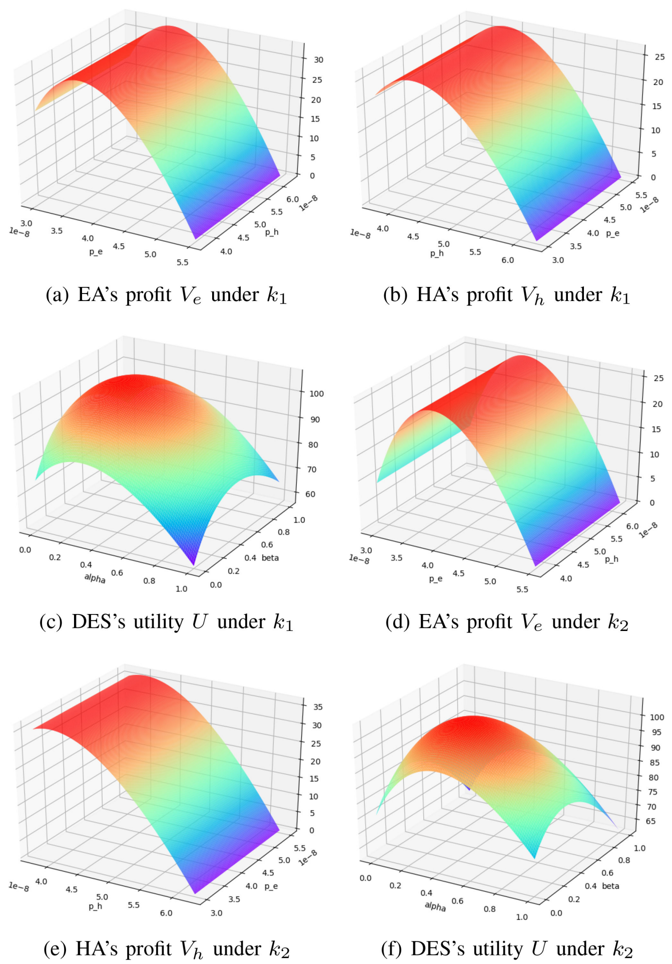
(a) BCM (b) PBFT

Fig. 5. The total delays of consensus under the BCM and PBFT.

To model the energies trading, we consider a city S $= \{\{\mathrm{EA}, \mathrm{HA}\}, \{\mathrm{C}_1, \ldots, \mathrm{C}_j, \ldots, \mathrm{C}_n\}\}$ where we denote the number of communities in this city by *n*. At the standard atmosphere, the calorific value of natural gas is $q = 3.6 \times 10^7$ J/m^3 on average. The retail price of electricity in U.S. is 0.2 dollar/kw.h. According to the conversion relationship of 1 kw·h $= 3.6 \times 10^6$ J, it is 5.5×10^{-8} dollar/J. Equivalently, we regard it as $r_e = 5.5 \times 10^{-8}$ coin/J in our B-MET system. The electric conversion of GT is $\eta_g = 0.5$. We define the maximum gas consumption $F_m^j = 200\ \mathrm{m}^3/\mathrm{day}$ and its unit price $c_f = 1.08\ \mathrm{coin/m}^3$. Thus, we have $c_e = 3.00 \times 10^{-8}$ coin/J and $p_e \in [3.00 \times 10^{-8}, 5.50 \times 10^{-8}]$ for the EA definitely. The efficiency of heat recovery system is given by $\eta_r = 0.8$, thereby we have $c_h = 3.75 \times 10^{-8}$ coin/J. The retail price of heat is $r_h = 6.25 \times 10^{-8}$ coin/J. Thus, we have $p_h \in [3.75 \times 10^{-8}, 6.25 \times 10^{-8}]$ for the HA definitely. According to (9), we have $b_e^j = 4.773 \times 10^{-10}$ and $b_h^j = 5.966 \times 10^{-10}$. Then according to (24), we have $k_e^j \in [115.24, 170.85]$ and $k_h^j \in [104.76, 170.85]$.

B. Simulation Results

The total delays of consensus under the BCM and PBFT are shown in Fig. 5. Shown as (a) in Fig. 5, we have two observations. Under our BCM, the trend of total delay decreases gradually as the round increases. After about the 40-th round, the total delay stabilizes and fluctuates in a small range. Besides, there will no longer be a total delay of 20 because credits are accumulated to normal nodes, which leads to those malicious nodes not being selected as a leader. Compared to

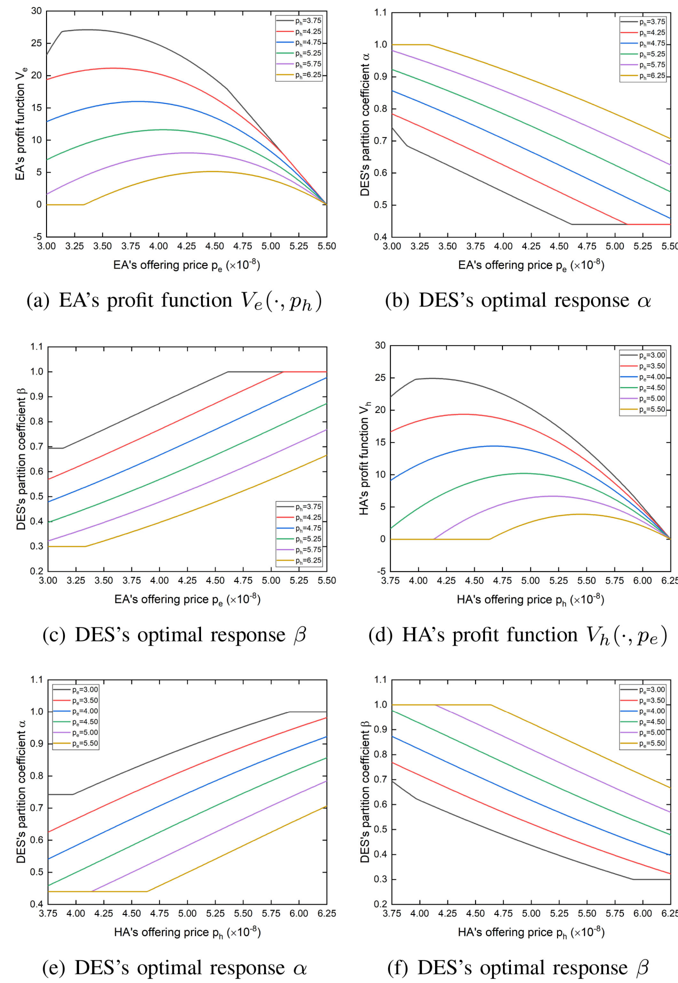


(a) EA's profit V_e under k_1 (b) HA's profit V_h under k_1

(c) DES's utility U under k_1 (d) EA's profit V_e under k_2

(e) HA's profit V_h under k_2 (f) DES's utility U under k_2

Fig. 6. The objective function of entities, including EA, HA, and DES, in city S under the setting k_1 and k_2.



(a) EA's profit function $V_e(\cdot, p_h)$ (b) DES's optimal response α

(c) DES's optimal response β (d) HA's profit function $V_h(\cdot, p_e)$

(e) DES's optimal response α (f) DES's optimal response β

Fig. 7. The objective functions of aggregators and DES's optimal responses in city S under the setting M_1.

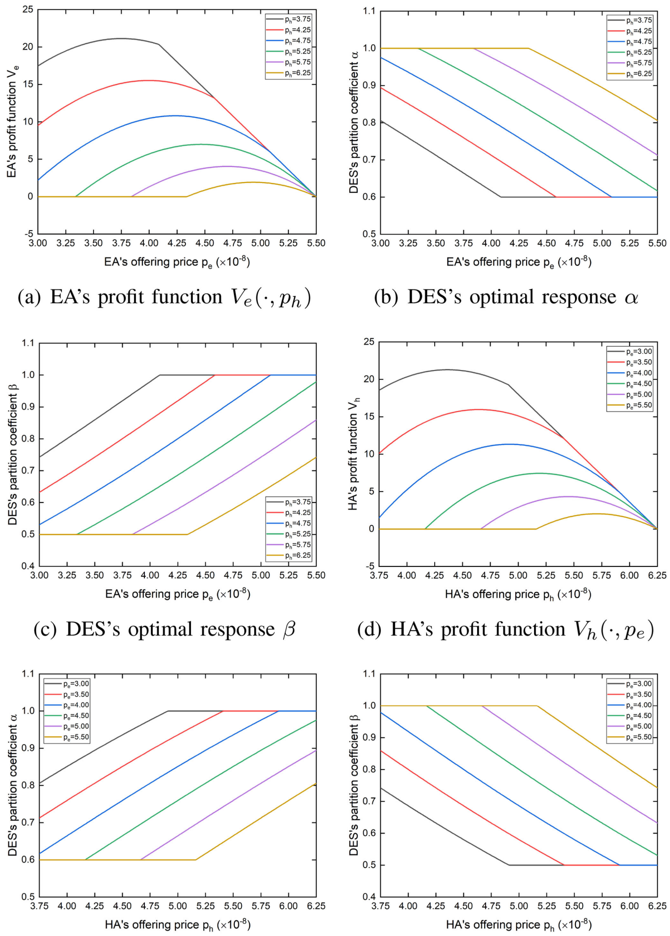
(b) in Fig. 5, we conclude that the delay of consensus process is improved significantly by our BCM, thereby increasing the throughput of B-MET system.

Then, we demonstrate the interactions of energies trading in a smart city, which can be summarized as five parts.

1) Concavity of Functions: Considering a city S that has only one community, we define this DES's satisfaction coefficient under two settings $k_1 = (k_e, k_h) = (143.05, 137.81)$ and $k_2 = (k_e, k_h) = (159.73, 117.98)$. Fig. 6 draws the objective function of entities in city S under the two settings, where we define the minimum energy restriction at OP_{DES} as $M_{min} = 0$. It means that there is no restriction on DES to choose their partition coefficients in order to demonstrate complete functional properties. Shown as Fig. 6, the profit functions of aggregators and utility function of this DES are obviously concave, which validates the conclusions in Lemma 1 and Lemma 2.

2) Effect of Satisfaction Coefficients: Let us look at (d), (e), (f) in Fig. 6. We increase k_e but decrease k_b under the setting k_2. Shown as (d), as k_e increases, the maximum point that obtains the maximum profit for EA moves toward the positive direction. It implies that the EA has to offer a higher price to buy electricity from DES in order to gain the maximum profit, because electricity used to serve community can contribute more utility than before. Similarly, shown as (e), as k_h decreases, the maximum point that obtains the maximum profit for HA moves toward the negative direction. From (f), as k_e increases and k_h decreases, the maximum point that obtains the maximum utility for DES according to $p_e = p_h = 4.5 \times 10^{-8}$ moves from $(\alpha_\circ, \beta_\circ) = (0.301, 0.481)$ in (c) to $(0.404, 0.328)$ in (f). Thus, we have $\alpha_\circ$ (resp. $\beta_\circ$) increases with the growth of k_e (resp. k_h).

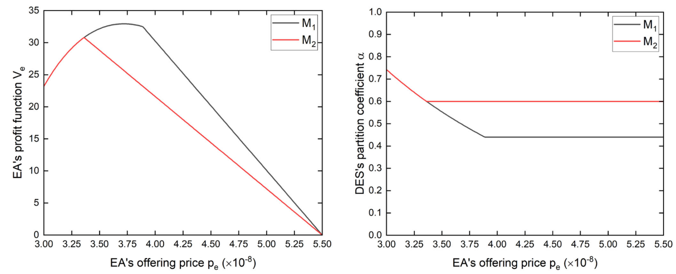
3) Competition Between EA and HA: From the definition of OP_{DES}, we have a restriction that requires a feasible solution must satisfy $X \cdot \alpha + Y \cdot \beta \geq M_{min}$ and $M_{min} \in (\max\{X, Y\}, X + Y)$. Here, we all adopt satisfaction coefficient $k_1 = (k_e, k_h) = (143.05, 137.81)$. In this part, we consider two different settings, that is $M_1 = 0.7 \times \max\{X, Y\} + 0.3 \times (X + Y)$ and $M_2 = 0.5 \times \max\{X, Y\} + 0.5 \times (X + Y)$ where $M_1 < M_2$. In order to demonstrate the effect of restrictions clearly, we use 2D figures instead of 3D figures. Fig. 7 and Fig. 8 draw the objective functions of aggregators and optimal responses of DES according to aggregators' offered prices in city S under the two settings. Let us discuss the typical black curve, shown as (a) with $p_h = 3.75 \times 10^{-8}$ in Fig. 7. At the beginning, EA's profit increases from $p_e = 3 \times 10^{-8}$ to 3.13×10^{-8} where DES's α decreases but β keeps constant. This response implies that DES's optimal strategy can be



(a) EA's profit function $V_e(\cdot, p_h)$ (b) DES's optimal response α (c) DES's optimal response β (d) HA's profit function $V_h(\cdot, p_e)$ (e) DES's optimal response α (f) DES's optimal response β

Fig. 8. The objective functions of aggregators and DES's optimal responses in city S under the setting M_2.

obtained at $(\alpha_\circ, \beta_\circ)$ where the first-order derivative is equal to zero. Then, the middle section is a smooth curve, where DES's response is at the tight border $X \cdot \alpha + Y \cdot \beta = M_1$. In this section, we can see DES's response α decreases linearly and β increases linearly. Finally starting from $p_e = 4.5 \times 10^{-8}$, EA's profit decreases linearly because of $\beta = 1$. Let us look at the yellow curve, shown as (a) with $p_h = 6.25 \times 10^{-8}$ in Fig. 7. At the beginning, EA's profit is equal to zero since DES responds with $(\alpha = 1, \beta = 0.3)$. Due to the high price offered by EA and low price offered by EA, all electricity should be partitioned to meet the minimum energy restriction and only sell heat for making revenue. For Fig. 8, compared with Fig. 7, we find that these functions show some structural changes as M_{min} increases. The restriction M_2 in Fig. 8 is larger than M_1 in Fig. 7, which indicates the DES has to use more energy to serve its community. Shown as (a), (d) in Fig. 8, we can know that the DES's optimal strategy cannot be obtained at stationary points $(\alpha_\circ, \beta_\circ)$. All DES's responses are at the tight border $X \cdot \alpha + Y \cdot \beta = M_2$. Besides, the sections of $\alpha = 1$ or $\beta = 1$ are much larger than that under the restriction M_1. However, no matter what M_{min} is, the EA (HA) always needs to offer an increasing price in order to get its maximum profit as the price offered by HA (EA) increases. This reflects the competition between aggregators, which is different from



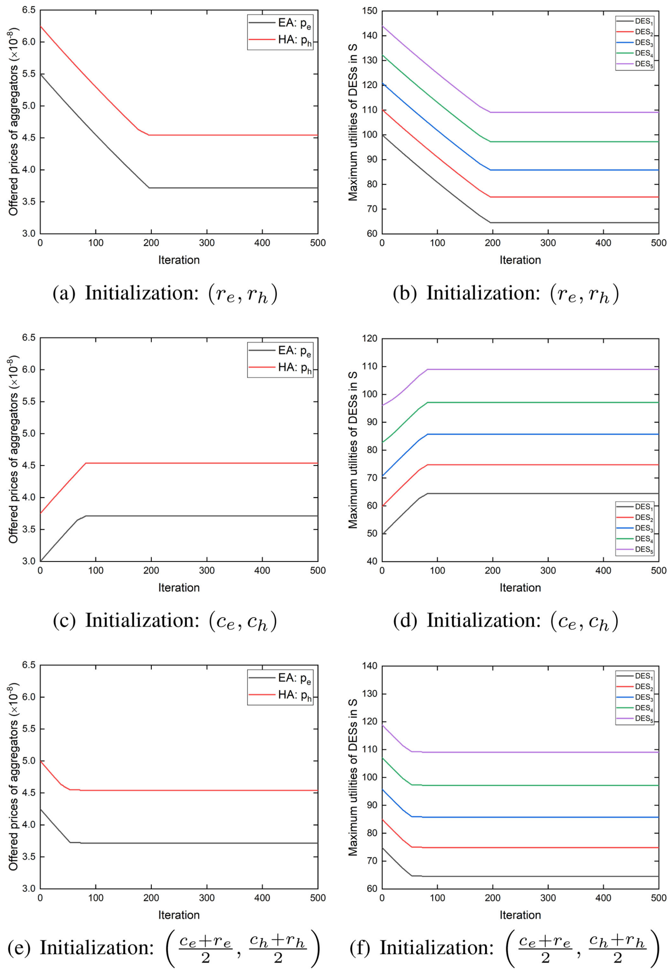
(a) EA's profit function $V_e(\cdot)$ (b) DES's optimal response α

Fig. 9. The objective function of EA and DES's optimal response in city S without trading with HA.

that there is no restriction in Fig. 6. Therefore, the restriction settings in $\mathrm{OP_{DES}}$ have significant effects on the objective functions of aggregators and optimal responses of DES.

4) No Competition: In this case, we assume the heat will not be traded with HA, thus we constantly have $\beta = 1$. Thus, the constraint (17) can be transformed to $(M_{min} - Y)/X \leq \alpha \leq 1$. Now, the offered price p_h is nothing to do with us, and the utility function of this DES is univariate. Given the price p_e offered by EA, the DES responds with $\alpha_\circ$ by letting $dU/d\alpha = 0$ if $(M_{min} - Y)/X \leq \alpha_\circ \leq 1$; otherwise responds with the one that makes its utility larger from $(M_{min} - Y)/X$ and 1. Fig. 9 draws the objective function of EA and optimal response of DES according to EA's offered price in city S without trading with HA. Shown as (a) in Fig. 7, (a) in Fig. 8, and (a) in Fig. 9, the profit obtained by EA when not trading with HA becomes larger because there is no competition between EA and HA. Shown as (b) in Fig. 9, we can see that the electric dispatching factor decreases first and then keeps constant as the EA's offering price increases. Besides, the inflection point appears later under the setting M_2 since $M_1 < M_2$, which meets our expectation.

5) Stackelberg Equilibrium: Considering a city S that has five communities, we define these DES_j's satisfaction coefficients as $k^j = (k_e^j, k_h^j)$ where $j \in \{1, \ldots, 5\}$. We assume $k^1 = (115.24, 137.81)$, $k^2 = (129.14, 137.81)$, $k^3 = (143.04, 137.81)$, $k^4 = (156.94, 137.81)$, and $k^5 = (170.85, 137.81)$ in this part. Fig. 10 draws the process of converging to the SE with different initializations under the restriction M_1. Here, the parameters defined in Algorithm 1 is given by $\Delta = 1 \times 10^{-10}$ and $\delta = 0.999$. The initialization (r_e, r_h) implies to give $\{\tilde{p}_e, \tilde{p}_h\} \leftarrow \{r_e, r_h\}$ in line 3 of Algorithm 1. Take (a) and (b) in Fig. 10 as an example, at the beginning, the aggregators offer the highest prices, thus they hardly gain any profit. By interacting with the five DES, the aggregators decrease their offering prices gradually in each iteration in order to improve profits. At approximately 100-th iteration, they cannot improve their revenues by changing their strategies unilaterally, thus reaching the NE. The DESs in S always respond aggregators with their optimal strategies, thus the SE can be reached. From (a), (c), and (e) in Fig. 10, we can see that they can reach the same equilibrium point regardless of what initialization is. However, the initialization affects the rate of convergence, and a good initialization can converge to the equilibrium point quickly. Fig. 11 draws the



(a) Initialization: (r_e, r_h) (b) Initialization: (r_e, r_h)

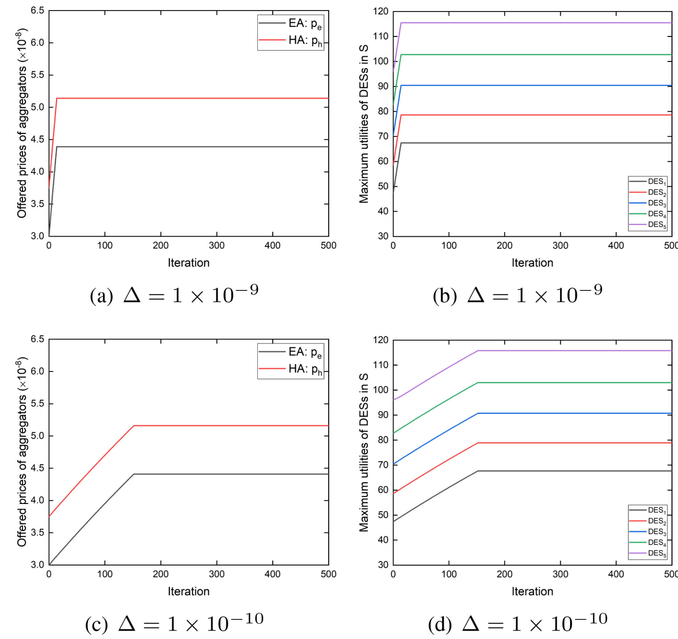
(c) Initialization: (c_e, c_h) (d) Initialization: (c_e, c_h)

(e) Initialization: $\left(\frac{c_e+r_e}{2}, \frac{c_h+r_h}{2}\right)$ (f) Initialization: $\left(\frac{c_e+r_e}{2}, \frac{c_h+r_h}{2}\right)$

Fig. 10. The process of converging to SE with different initializations under the restriction M_1.

process of converging to the SE with different Δ under the restriction M_2. Here, we adopt the initialization (c_e, c_h) and $\delta = 0.999$ as well. From (a), (c) in Fig. 11, they can quickly approach to equilibrium point when we adopt the larger Δ. Nevertheless, it has to wait for Δ to drop to a relatively low level in order to improve this solution further. Therefore, how to choose the value of Δ depends on your demand. If we do not require high accuracy but high speed, it is recommended to choose a large Δ; otherwise we should choose a small one. According to Fig. 6, Fig. 7, and Fig. 8, it indicates that our model meets the requirements to form MLMF SE. According to Fig. 10 and Fig. 11, the SE can be reached definitely by limited iterations. At this time, each players achieves its best state.

6) Centralized v.s. Distributed: For the aggregators, it is hard to know the complete information about all DESs in its city. Even if knowing partial coefficients, such as coefficient satisfactions, the settings of minimum energy restriction are very flexible, which will change with the fluctuations of the community population, season, and other factors. The optimal responses from DES are unpredictable. Thereby the aggregators can only obtain feedback information of DESs in a distributed manner, that is to update their offering price iteratively by interacting with DESs in their city.



(a) $\Delta = 1 \times 10^{-9}$ (b) $\Delta = 1 \times 10^{-9}$

(c) $\Delta = 1 \times 10^{-10}$ (d) $\Delta = 1 \times 10^{-10}$

Fig. 11. The process of converging to with different Δ under the restriction M_2.

VII. Conclusion

In this paper, we studied multiple energies trading problem systematically. First, we proposed an architecture of B-MET system to address the security and privacy protection issues in distributed energy trading. In order to reduce latency and improve throughput, we introduce a credit model and design a new byzantine-based consensus mechanism based on it. Then, we model the interactions between aggregators and DESs in a smart city by MLMF Stackelberg game, which is more complex and realistic than the models that have appeared before. We solve it step by step, show the existence and uniqueness of SE, and design a sub-gradient algorithm to find NE between aggregators. Finally, the results of numerical simulations indicate that our model is valid, and verify the correctness and efficiency of our algorithm.

An important contribution is to improve the Byzantine-based consensus mechanism by introducing a credit model, in which the consensus can be achieved by the sum of the credits of voting nodes rather than the number of voting nodes. This is intuitively correct. However, we have not given strict proof of its correctness, which is also our main work in the next stage. In the future, we hope to verify whether this credit-based Byzantine consensus mechanism is Byzantine fault-tolerant and promote its applications. Besides, we will focus on investigating how Byzantine fault-tolerance is related to credit models and how we can quantify the relationship between the credit model and performance improvement of this mechanism. This is critical for developing more efficient consensus algorithms.

References

[1] P. S. Georgilakis and N. D. Hatziargyriou, "Optimal distributed generation placement in power distribution networks: Models, methods, and future research," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3420–3428, Aug. 2013.

[2] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of IoT using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 881–888, Jan. 2021.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, 2008, p. 21260.

[4] M. U. 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, Mar./Apr. 2020.

[5] X. Liu, S. X. Sun, and G. Huang, "Decentralized services computing paradigm for blockchain-based data governance: Programmability, interoperability, and intelligence," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 343–355, Mar./Apr. 2020.

[6] 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.

[7] 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.

[8] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.

[9] J. Guo, X. Ding, and W. Wu, "A blockchain-enabled ecosystem for distributed electricity trading in smart city," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 2040–2050, Feb. 2021.

[10] D. W. Wu and R. Z. Wang, "Combined cooling, heating and power: A review," *Progr. Energy Combustion Sci.*, vol. 32, nos. 5–6, pp. 459–495, 2006.

[11] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.

[12] J. C. Vasquez, J. M. Guerrero, J. Miret, M. Castilla, and L. G. De Vicuña, "Hierarchical control of intelligent microgrids," *IEEE Ind. Electron. Mag.*, vol. 4, no. 4, pp. 23–29, Dec. 2010.

[13] C. Cecati, C. Citro, A. Piccolo, and P. Siano, "Smart operation of wind turbines and diesel generators according to economic criteria," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4514–4525, Oct. 2011.

[14] D. Zhang, N. Shah, and L. G. Papageorgiou, "Efficient energy consumption and operation management in a smart building with microgrid," *Energy Convers. Manag.*, vol. 74, pp. 209–222, Oct. 2013.

[15] W. Zhang, Z. Hong, and W. Chen, "Hierarchical pricing mechanism with financial stability for decentralized crowdsourcing: A smart contract approach," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 750–765, Jan. 2021.

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

[17] S. Bu and F. R. Yu, "A game-theoretical scheme in the smart grid with demand-side management: Towards a smart cyber-physical power infrastructure," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 22–32, Jun. 2013.

[18] Y. Chen, Z. Li, B. Yang, K. Nai, and K. Li, "A Stackelberg game approach to multiple resources allocation and pricing in mobile edge computing," *Future Gener. Comput. Syst.*, vol. 108, pp. 273–287, Jul. 2020.

[19] Z. Yang, K. Liu, Y. Chen, W. Chen, and M. Tang, "Two-level Stackelberg game for IoT computational resource trading mechanism: A smart contract approach," *IEEE Trans. Services Comput.*, early access, Sep. 18, 2020, doi: 10.1109/TSC.2020.3024729.

[20] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[21] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3602–3609, Jun. 2019.

[22] X. Ding, J. Guo, D. Li, and W. Wu, "An incentive mechanism for building a secure blockchain-based Internet of Things," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 477–487, Jan.–Mar. 2021.

[23] S. Guo, Y. Dai, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5549–5561, May 2020.

[24] P. J. Mago and L. M. Chamra, "Analysis and optimization of CCHP systems based on energy, economical, and environmental considerations," *Energy Build.*, vol. 41, no. 10, pp. 1099–1106, 2009.

[25] D. Gvozdenac, B. G. Urošević, C. Menke, D. Urošević, and A. Bangviwat, "High efficiency cogeneration: CHP and non-CHP energy," *Energy*, vol. 135, pp. 269–278, Sep. 2017.

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

[27] 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, 2001.

[28] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.

[29] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[30] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[31] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. Philadelphia, PA, USA: Soc. Ind. Appl. Math., 1998.

[32] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave N-Person games," *Econometrica J. Econometric Soc.*, vol. 33, no. 3, pp. 520–534, 1965.

[33] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[34] Y. Xiao, G. Bi, and D. Niyato, "A simple distributed power control algorithm for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3594–3600, Nov. 2011.

[35] H. Zhang, Y. Xiao, L. X. Cai, D. Niyato, L. Song, and Z. Han, "A multi-leader multi-follower Stackelberg game for resource management in LTE unlicensed," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 348–361, Jan. 2017.

Jianxiong Guo received the B.E. degree from the School of Chemistry and Chemical Engineering, South China University of Technology, Guangzhou, Guangdong, China, in 2015, and the Ph.D. degree from the Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA, in 2021. He is currently an Assistant Professor with the BNU-UIC Institute of Artificial Intelligence and Future Networks, Beijing Normal University at Zhuhai, and also with the Guangdong Key Laboratory of AI and Multi-Modal Data Processing, BNU-HKBU United International College, Zhuhai, Guangdong, China. His research interests include social networks, algorithm design, data mining, IoT application, blockchain, and combinatorial optimization.

Xingjian Ding received the B.E. degree in electronic information engineering from Sichuan University in 2012, the M.S. degree in software engineering from Beijing Forestry University in 2017, and the Ph.D. degree from the School of Information, Renmin University of China in 2021. He is currently an Assistant Professor with the School of Software Engineering, Beijing University of Technology. His research interests include wireless rechargeable sensor networks, approximation algorithms design and analysis, and blockchain.

Weili Wu (Senior Member, IEEE) received the M.S. and Ph.D. degrees from the Department of Computer Science, University of Minnesota, Minneapolis, MN, USA, in 1998 and 2002, respectively. She is currently a Full Professor with the Department of Computer Science, The University of Texas at Dallas, Richardson, TX, USA. Her research mainly deals in the general research area of data communication and data management. Her research focuses on the design and analysis of algorithms for optimization problems that occur in wireless networking environments and various database systems.