A Blockchain-Enabled Ecosystem for Distributed Electricity Trading in Smart City

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

***Abstract*—Along with the development in the Internet of Things technology and smart city, a distributed network has been formed among cities. This makes it easy to integrate distributed electric energy into the power grid, thus become an efficient way to use energy. However, how to guarantee the security and privacy protection of distributed electricity trading has not been solved effectively. In this article, we propose a blockchain-based electricity trading (B-ET) ecosystem and design a smart contract to ensure transactions are conducted in a safe and reliable manner. To overcome the shortcomings of high latency in traditional Proof-of-Work (PoW) consensus, we proposed a credit-based PoW consensus mechanism by integrating the concept of "stake" to improve the consortium blockchain under the B-ET ecosystem. Then, we take combined cooling, heating, and power (CCHP) system as an example that supplies distributed energy, and model its interactions with the agent of power grid by a novel Stackelberg game. We show that the optimal utilities of entities in a city can be obtained at the Stackelberg equilibrium by a distributed algorithm, which is guaranteed to exist and be unique. In the end, we conduct a number of numerical simulations to evaluate our proposed model and verify our algorithms, which demonstrate their correctness and efficiency completely.**

***Index Terms*—Blockchain, credit-based Proof of Work (PoW), distributed electricity trading, smart city, Stackelberg game.**

I. Introduction

To REDUCE the cost of energy and emission of greenhouse gas, distributed energy stations (DESs) combined with multiple energy sources have been developed effectively in the last decades [1]. Consider a smart community equipped with a DES, it can be used to supply necessary energies, such as cool, heat, and electricity, for residents living in this community. In addition to this, it reduces the dependence on centralized energy supply for instance the power grid, thereby increasing efficiency and reducing the cost of energy usage. Because in the traditional power grid, the electricity generated from the centralized node, such as power plant, has to be transmitted by a complex mesh, which results in high losses during transmission and thus low efficiency [2], [3]. The deployment of the Internet of Things (IoT) and smart cities has connected cities to each other, which makes the use of distributed energy more flexible and diversified. Based on that, the surplus electricity left by a DES can be integrated into the power grid, in other words, the DES can sell its electricity to the agent of power grid (APG) for making revenue. Thus, the distributed electricity trading problem between the APG and DESs is formulated and discussed in this article.

Traditional peer-to-peer (P2P) electricity trading relies on a centralized trading platform, but such a mechanism has many drawbacks. The payment security and privacy protection are vulnerable when trading in this untrusted third centralized platform, which needs to manage and store the transactions between the AGP and DESs. If attacked by some damages such as a single point of failure, it will result in data loss and privacy leakage [4]. Therefore, it is imperative to design a secure and reliable electricity trading system that ensure trading among the distributed Internet of Energy can be performed. It stimulates the DESs to sell their electricity to APG at ease, which promotes the rational use of energy.

With this in mind, blockchain is an effective technique to address the aforementioned problem. Blockchain is a public and distributed ledger that permits nodes to trade with each other without a trusted intermediary [5]. Here, a new transaction is validated by a group of authorized nodes first and then added into the blockchain in a permanent and tamper-resistant manner. Based on its decentralization, a secure and reliable electricity trading system can be constructed [6], [7]. Consider a smart city, it consists of a number of communities, each of which is equipped with a DES. There is an agent, namely, APG, trading with DESs in this city. The agents of all cities are interconnected to form a wide area network and then formulate a trading ecosystem. Based on that, we propose a blockchain-based electricity energies trading (B-ET) ecosystem, which is a consortium blockchain where all agents are authorized participants required to store the blockchain and complete the consensus process.

The B-ET ecosystem can be divided into two subsystems, called the Internet-of-Energy (IoE) subsystem and blockchain subsystem. Each IoE subsystem is a single city made up of interconnections between the APG and DESs in this city. Here, we design a smart contract that guarantees electricity trading to be performed automatically when the trading conditions are satisfied. The blockchain subsystem is constructed on the P2P network that connects all APGs of cities in the ecosystem, which stores complete data about the blockchain distributedly. The transactions produced by some APG are required

Manuscript received June 2, 2020; revised July 11, 2020; accepted August 9, 2020. Date of publication August 12, 2020; date of current version January 22, 2021. This work was supported in part by the National Science Foundation under Grant 1747818 and Grant 1907472. *(Corresponding author: Jianxiong Guo.)*

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

Xingjian Ding is with the School of Information, Renmin University of China, Beijing 100872, China.

Digital Object Identifier 10.1109/JIOT.2020.3015980

to be verified and reached consensus across all APGs in the ecosystem. The proof-based mechanisms, such as Proof of Work (PoW) and Proof of Stack (PoS), are the most mature and generally accepted methods to finish the consensus in the blockchain. However, for the PoW, it is computation consuming and high latency. For the PoS, it lacks randomness that will bring about the one with a larger stake always win the package right. They are not suitable for our B-ET ecosystem because it requires low latency and security. Thereby, we proposed a credit-based PoW consensus mechanism, which overcomes the high latency in PoW and a lack of randomness in PoS.

In the aforementioned contract, it exists an interaction between the agent and DES before launching a new electricity trading, where the agent offers a unit price to purchase electricity from DES, then DES responds it with the amount of electricity they are willing to sell. Here, we take combined cooling, heating, and power (CCHP) system [8] as an instance of DES. In a city, each DES's utility consists of two parts: one is to serve the residents living in its community by providing them with the energy needed for life, and the other is sold electricity to the APG of its corresponding city for gaining revenues. The agent's utility is the profit gain from buying electricity at a lower price and selling it at the retail price. To encourage the DESs to sell more electricity, the AGP should offer them a higher price. But like this, it has the potential to make less profit because of this higher cost. Thus, this is a dilemma. Then, due to the multilevel decision-making processes of APG and DESs in a city, we formulate a Stackelberg game to model the bargain between them, where the AGP is leader and DESs are followers. The leader offers a price for buying electricity from followers, such that its profit based on the optimal responses from DESs can be maximized. The properties of this Stackelberg game are analyzed in this article, and we prove the Stackelberg equilibrium (SE) exists and is unique. Because the responses of DESs are unpredictable in advance, we propose a distributed algorithm that is guaranteed to reach the unique SE by limited information interactions. Finally, we conduct numerical simulations to model our B-ET ecosystem, verify the correctness of our proposed utility functions and feasibility of our proposed algorithm.

The remainder of this article is organized as follows. Section II discusses the state-of-the-art work. Section III introduces the B-ET ecosystem and CCHP system and defines utility functions. Section IV presents our blockchain design. Section V analyzes the Stackelberg game, distributed algorithm, and security. Section VI conducts numerical simulations. Section VII concludes this article.

II. Related Work

The distributed energy system has been studied intensively, especially for how to integrate DES into the power grid. Cecati *et al.* [9] exploited DES to make the cost of power delivery minimized by the use of an efficient smart grid management system. Georgilakis and Hatziargyriou [1] summarized the optimally distributed generation placement problem systematically and analyzed current and future research about it. Zhang *et al.* [10] considered microgrid as a local energy supplier for domestic buildings by utilizing DES and studied optimal scheduling of energy consumption through mixed-integer programming. To deal with the transaction security issues in P2P energy trading, many latest works about it adopt the blockchain technology. Kang *et al.* [11] put forward a localized P2P electricity trading pattern based on consortium blockchain among plug-in hybrid electric vehicles. Liu *et al.* [12] designed an adaptive blockchain-based charging scheme to reduce power fluctuation in the grid and cost of electric vehicle users. Aggarwal *et al.* [13] proposed an EnergyChain that permits energy trading between grid and home in a secure manner, including miner choice, transaction verification, and block adding. Zhou *et al.* [14] considered the scenario of vehicle-to-grid and developed a secure energy trading mechanism based on a consortium blockchain. Even though that, our ecosystem is novel and more realistic. Besides, they did not consider some of the inherent flaws in the traditional blockchain.

A Stackelberg game is suitable to model the interactions in energy trading. Maharjan *et al.* [15] addressed the demand response management problem by means of establishing a Stackelberg game between multiple utility companies and customers to maximized the profit of each company and utility of each customer. Meng and Zeng [16] studied a Stackelberg game between an electricity retailer and customers. They adopted genetic algorithms for the retailer to maximize its profit and developed an analytical solution for customers to minimize their bills. Bu and Yu [17] considered a real-time pricing problem for the electricity retailer in the demand-side management, proposed a four-stage Stackelberg game, and solved it by a backward induction process. Tushar *et al.* [18] proposed an energy management scheme and formulated a Stackelberg game between residential units and the shared facility controller that can buy energy from residential units or grids. Other researches about game theory in energy trading and management are shown in [19]–[21].

III. Ecosystem

Consider a smart city, it can be divided into a number of smart communities, each of which is equipped with a DES for supplying multiple energies, especially electricity, to these residents living in this community. In this city, there is an agent representing the power grid company that collects electricity from all DESs appertained to this city. Given a smart city S_i, the structure of this smart city is shown in Fig. 1, and the entities in this smart city are shown as follows.

1) *Agent:* There is an agent delegated by the power grid associated with this city S_i, which is denoted by APG_i. The APG_i is a monopoly of the energy market that purchases electric energy generated by DESs in those communities that belong to this smart city.
2) *DESs:* The city S_i can be partitioned into disjoint smart communities, denoted by set $\{C_{i1}, C_{i2}, \ldots, C_{ij}, \ldots, \}$. In community C_{ij}, there is a distributed energy station DES_{ij} supplying energies to the residents living in this

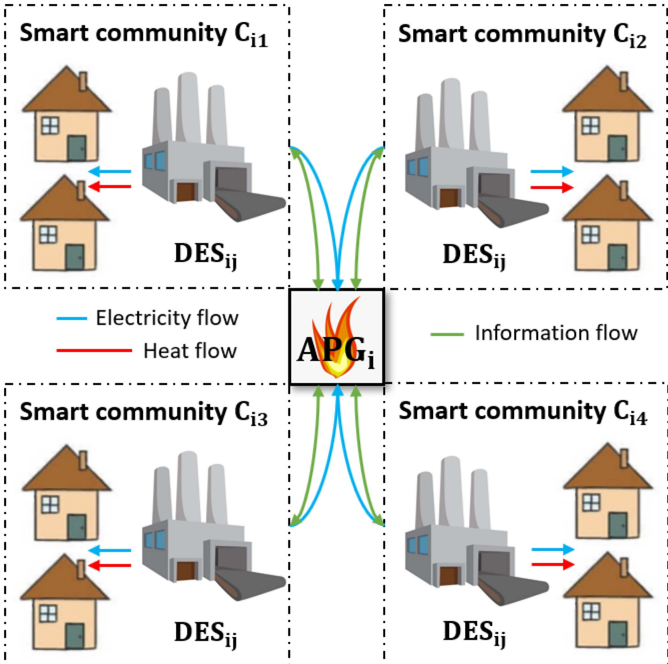


Fig. 1. Structure of smart city S_i.

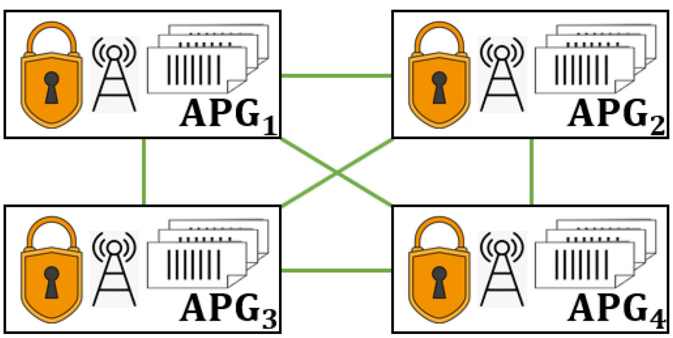


Fig. 2. Instance of B-ET ecosystem that is composed of four smart cities (a P2P network among all agents in the ecosystem).

community. Besides, DES_{ij} is able to sell surplus electric energy to the corresponding APG_i in order to make revenues.

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

Then, consider a larger ecosystem, it is composed of a number of smart cities. For instance, a country is a typical energy ecosystem. Here, the ecosystem $\mathbb{S}$ is denoted by $\mathbb{S} = \{S_1, S_2, \ldots, S_i, \ldots,\}$, where $S_i = \{\{APG_i\}, \{C_{i1}, C_{i2}, \ldots, C_{ij}, \ldots,\}\}$ is a smart city in this ecosystem. For convenience, the notation DES_{ij} can be considered equivalent to C_{ij}. Our B-ET ecosystem is established on such an ecosystem, where all APGs are interconnected with each other to form a P2P network called "blockchain network." An instance of the B-ET ecosystem that is composed of four smart cities is shown in Fig. 2. In order to support secure trading between the agent and DESs, we adopt consortium blockchain to construct our B-ET ecosystem. In

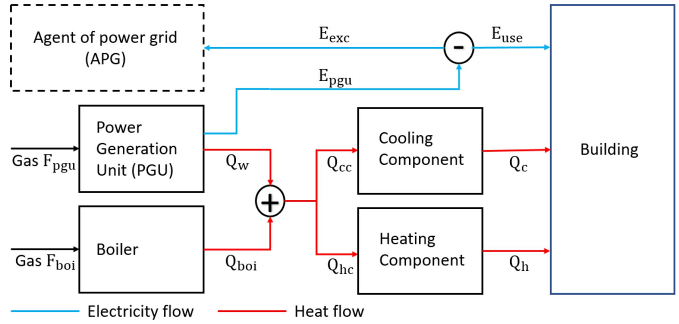


Fig. 3. CCHP system.

the traditional blockchain, the consensus process is carried out by all participants. But the blockchain in the B-ET takes all agents in the ecosystem as authorized participants, and they are charged with storing the whole blockchain and performing the consensus process. Each agent 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 agents is reached, then stored in all agents permanently.

A. Combined Cool, Heat, and Power System

In this article, the aforementioned DES is implemented by the CCHP system, which is the most common and widely used technique of distributed energy utilization. The CCHP system consumes natural gas to generate electricity and exploits the recoverable waste heat generated by the power generation unit (PGU) for the purpose of space cooling, heating, and hot water. The process is shown in Fig. 3. The gas is fed into the PGU which will generate electricity E_{pgu} and emit high-temperature waste heat Q_w. Then, the E_{use} is used to supply electricity to the community for lighting, electronic equipment, etc., and E_{exc} is sold to the APG. For the heat energy, when the waste heat Q_w is insufficient for supply to buildings, it can be replenished by the input of the boiler. Here, $Q_w + Q_{\mathrm{boi}}$ can be split into two parts, where Q_{cc} is fed into the cooling component to generate cool (air conditioning) Q_c and Q_{hc} is fed into the heating component to generate heat Q_h.

Shown as Fig. 3, the total electricity produced by PGU is $E_{\mathrm{pgu}} = E_{\mathrm{use}} + E_{\mathrm{exc}}$. Measured in days, the units of E_{pgu}, E_{use}, E_{exc}, Q_w, Q_{boi}, Q_{cc}, Q_{bc}, Q_c, and Q_h are J/day. The PGU fuel consumption F_{pgu} (m^3/day) is

$$F_{\mathrm{pgu}} = E_g/(q \cdot \eta_{\mathrm{pgu}}) = Q_w/(q \cdot (1 - \eta_{\mathrm{pgu}})) \tag{1}$$

where q ($\mathrm{J/m}^3$) is the calorific value of fuel, hence the total energy generated by F_{pgu} is $q \cdot F_{\mathrm{pgu}}$. The η_{pgu} is the conversion efficiency of PGU, percent energy that transferred from heat to electricity. Given a specific PGU, its conversion efficiency is assumed to be a constant. Consider the heat energy supplied by the boiler, we have

$$F_{\mathrm{boi}} = Q_{\mathrm{boi}}/(q \cdot \eta_{\mathrm{boi}}) \tag{2}$$

where η_{boi} is the thermal efficiency of the boiler. To handle the cooling load, the input of thermal energy Q_{cc} to cooling component can be defined as $Q_c = \mathrm{COP}_{cc} \cdot Q_{cc}$, where Q_c is the cooling load and COP_{cc} is the coefficient of performance of chiller. Similarly, to handle the heating load, the input of thermal energy Q_{hc} to heating component can be defined as $Q_h = \eta_{hc} \cdot Q_{hc}$, where Q_h is heading load and η_{hc} is the thermal efficiency of coil. By the heat balance, we can know that $Q_w + Q_{\mathrm{boi}} = Q_{cc} + Q_{hc}$ definitely.

However, it is complex to determine how to distribute the total thermal energy $Q_r + Q_{\mathrm{boi}}$ to cooling component Q_{cc} and heating component Q_{hc}. For example, in summer, the cooling load is significantly heavier than in other seasons due to the hot weather; but in winter, heating demand is higher because of the demand to heat the space of buildings. Apart from this, in different regions, such as tropical or temperate regions, even at different times of the day, the requirements for cooling and heating are different as well. Thus, the allocation of total thermal energy to the cooling and heating component depends more on experience. For simplicity, we consider the cooling and heating load as a whole, that is, $Q_{\mathrm{com}} = Q_c + Q_h = \eta_{\mathrm{com}} \cdot (Q_r + Q_{\mathrm{boi}})$, where Q_{com} is the sum of cooling load and heating load and η_{com} is its comprehensive thermal efficiency such that $\eta_{\mathrm{com}} \in [\min\{\mathrm{COP}_{cc}, \eta_{hc}\}, \max\{\mathrm{COP}_{cc}, \eta_{hc}\}]$. It can be determined by historic records of cooling and heating load, and we assume it to be a constant.

The total fuel consumption can be denoted by F, which is $F = F_{\mathrm{pgu}} + F_{\mathrm{boi}}$. Thereby, we define two dispatching factors $\alpha, \beta \in [0, 1]$ for this CCHP system, where $\alpha = F_{\mathrm{pgu}}/F$ is the fuel dispatching factor and $\beta = E_{\mathrm{use}}/E_{\mathrm{pgu}}$ is the electricity 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 that is able to meet the DES's requirement. Given a smart city S_i and a community $C_{ij} \in S_i$, the energy relationship in the CCHP_{ij} of C_{ij} can be defined, that is

$$E^{ij}_{\mathrm{use}} = \alpha^{ij} \cdot \beta^{ij} \cdot \eta_{\mathrm{pgu}} \cdot \left(qF^{ij}\right) \tag{3}$$

$$E^{ij}_{\mathrm{exc}} = \alpha^{ij} \cdot \left(1 - \beta^{ij}\right) \cdot \eta_{\mathrm{pgu}} \cdot \left(qF^{ij}\right) \tag{4}$$

$$Q^{ij}_{\mathrm{use}} = \left(\alpha^{ij}\left(1 - \eta_{\mathrm{pgu}}\right) + \left(1 - \alpha^{ij}\right)\eta_{\mathrm{boi}}\right) \cdot \eta_{\mathrm{com}} \cdot \left(qF^{ij}\right). \tag{5}$$

The CCHP_{ij} can determine the amount of heat that used in this community by adjusting α^{ij} and the amount of electricity that sold to APG_i by adjusting β^{ij} for making revenue.

B. Utility Functions

Consider a smart city S_i, the agent in this city APG_i offers a unit price p^i_e to collect surplus electricity generated by $\mathrm{DES}_{ij} \in S_i$, where the units of p^i_b are coin/J. For each $\mathrm{DES}_{ij} \in S_i$, it is risk averse in the energy market. If DES_{ij} chooses the dispatching factors α^{ij}, β^{ij} and consume natural gas F^{ij}, its utility function is

$$\begin{aligned} U^{ij}\left(\alpha^{ij}, \beta^{ij}, F^{ij}\right) = {} & k^{ij}_1 \cdot \ln\left(1 + b^{ij}_1 E^{ij}_{\mathrm{use}}\right) \\ & + k^{ij}_2 \cdot \ln\left(1 + b^{ij}_2 Q^{ij}_{\mathrm{use}}\right) + p^{ij}_b \cdot E^{ij}_{\mathrm{exc}} \end{aligned} \tag{6}$$

where k^{ij}_1, b^{ij}_1, k^{ij}_2, and b^{ij}_2 are adjustable parameters. The utility function U^{ij} is composed of three items. The first item is the utility of electricity used for electricity demand in its community. The second item is the heat used for cooling and heating demand in its community, and it consists of waste heat from PGU and boiler. The third item is the revenue from selling electricity to the APG_i at the price of p^i_b.

Unfortunately, the utility $U^{ij}(\alpha^{ij}, \beta^{ij}, F^{ij})$ is a multivariate function and cannot be guaranteed to be concave because of involving two variables in the first item. This causes great difficulty for our follow-up mathematical analysis processing. Thereby, we need to analyze the actual situation carefully and simplify this utility function. In (6), we neglect the cost of natural gas since we assume the price p^i_b offered by APG_i is always greater than this cost. If not, there is no electricity trading between the agent and DESs, and this is meaningless. For each $\mathrm{DES}_{ij} \in S_i$, it will produce electricity as much as possible, because of the fact that it is always profitable to sell them to the APG_i. At this time, to maximize its utility, each CCHP system will run at full capacity. Here, for each CCHP_{ij}, we define its maximum production capacity (maximum gas consumption) per day as F^{ij}_m. In addition, we suppose the waste heat Q_w at full capacity is enough to supply heat to satisfy its community if dispatching all fuel F^{ij}_m to PGU. Therefore, the utility $U^{ij}(\alpha^{ij}, \beta^{ij}, F^{ij}_m)$ can be denoted by $U^{ij}(\beta^{ij})$, where F^{ij}_m is considered as a constant and $\alpha^{ij} = 1$.

Remark 1: After here, we default $F^{ij} = F^{ij}_m$ and $\alpha^{ij} = 1$. Moreover, we denote $X^{ij} = \eta_{\mathrm{pgu}} \cdot (qF^{ij}_m)$ and $Y^{ij} = (1 - \eta_{\mathrm{pgu}}) \cdot \eta_{\mathrm{com}} \cdot (qF^{ij}_m)$.

From (6), the natural logarithmic functions were adopted to characterize the satisfaction of consuming electricity and heat. This method has been used in [18], [22], and [23]. But it exists a drawback to this utility function that logarithmic function does not have an asymptote. Thus, we add an adaption parameter b^{ij}_1 such that $\ln(1 + b^{ij}_1 x) \in [0, 1]$ and use it to model the satisfaction of electricity used in the community. This parameter b^{ij}_1 is to control the variation range of term $\ln(1 + b^{ij}_1 x)$ and avoid growing infinitely. Our objective is to have $\ln(1 + b^{ij}_1 x) = 1$ if $\beta^{ij} = 1$, then the utility of the first item in (6) reaches the maximum value. That is

$$b^{ij}_1 = \left(1/X^{ij}\right) \cdot (1 - e); \;\; b^{ij}_2 = \left(1/Y^{ij}\right) \cdot (e - 1). \tag{7}$$

For the agent in this city, it has no power of pricing because the retail price of electricity is usually regulated by the government. Thereby this retail price can be considered as a constant. To make revenue, the APG_i wishes to purchase electricity from those $\mathrm{DES}_{ij} \in S_i$ at a price as low as possible. Based on (6), if it offers a lower p^i_b, the DESs tend to increase their electricity dispatching factor β, namely, sell less and use more electricity to serve themselves. They consume more electricity to improve the quality of life, or simply reduce power generation, results in the revenue of APG_i is reduced. In contrast, if it offers a higher p^i_b, even approached to retail price p_s, the profit per unit of electricity will be small. Therefore, it is important for the APG_i to offer a valid price p^i_b, not only encourage DESs to sell more electricity but also ensure to have sufficient profitability. Usually, $p^i_b \in (p_m, p_c)$, where p_c is the cost price of generating electricity by itself, where the grid needs to generate electricity at a cost price p_c when the electric energy

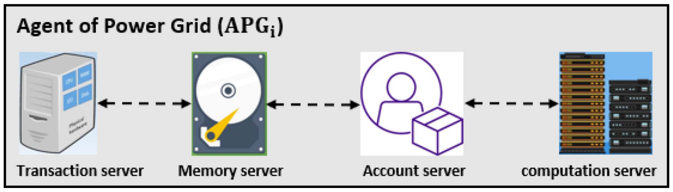


Fig. 4. Four major component in an APG.

collected from DESs is not enough to meet the requirement. If APG_i offer a price p_b^i, its profit function can be defined as

$$L^i(p_b^i) = (p_s - p_b^i) \cdot \left(\sum_{C_{ij} \in S_i} E_{\text{exc}}^{ij}\right) + (p_s - p_c) \cdot \left(R_i - \sum_{C_{ij} \in S_i} E_{\text{exc}}^{ij}\right) \quad (8)$$

where R_i is the electric load of APG_i, and we assume $R_i \geq \sum_{C_{ij} \in S_i} X^{ij}$. The profit function $L^i(p_b^i)$ is composed of two items. The first item is the profit of selling the electricity bought from all DESs. The second item is the profit of selling the electricity generated by itself.

IV. Blockchain Design

Generally speaking, our B-ET ecosystem is made up of IoE subsystems and blockchain subsystem. A smart city $S_i \in \mathbb{S}$ is an IoE subsystem, which is composed of an APG_i and a number of $DES_{ij} \in S_i$. It mainly realizes information interactions and finishes energy transactions between the APG and DESs in this city. Shown as Fig. 1, there is an information channel and an electrical transmission path between the APG and each DES in this city. The blockchain subsystem consists of all APGs in the ecosystem $\mathbb{S}$, where all APGs are connected by P2P communication shown as Fig. 2. Apart from the effect described above in the IoE subsystem, it needs to verify and record those energy transactions between APGs and DESs in a secure and trusted manner. The workflow of electricity trading in the B-ET ecosystem is as follows: first, a transaction between the APG and DESs is initiated and finished in an IoE subsystem; then this transaction can be verified and stored permanently in the blockchain subsystem.

A. IoE Subsystem

For each $APG_i \in S_i \in \mathbb{S}$ in the ecosystem, there are four major components: 1) a transaction server; 2) an account server; 3) a memory server; and 4) a computation server, which is shown in Fig. 4. The transaction server is a central controller, which is mainly responsible for offering a price, collecting the responses from DESs in its city, adjusting trading strategy, and decide whether to trade. All entities, including APG and DESs in the S_i, have a personal account in the APG_i's account server, which stores personal transaction records. Besides, there is a wallet associated with each personal account, and the digital assets of each entity are stored in its wallet in the form of energy coin [11]. For privacy protection, the true address of the wallet is hidden by a public key (random pseudonym), and the mapping relationships between the personal accounts and the public keys of their associated wallets are stored in this account server. Moreover, the memory server and computation server are mainly used in the later blockchain subsystem, we will introduce in the next section.

Next, our core problem is how to protect privacy during information interaction and how to ensure security during trading. Here, we design a smart contract to solve this problem. The smart contract empowers credible transactions without third parties based on blockchain technology, which can ensure transactions to be trackable and irreversible, but reduce time and cost at the same time. In a city S_i, a smart contract is launched by the agent APG_i and one of the DESs $DES_{ij} \in S_i$ together, which is denoted by $\text{Contract}(APG_i, DES_{ij}, \text{STime})$. Then, the procedure to execute this contract is demonstrated as follows.

1) System Initialization: First, all entities, including APG and DESs, need to register on a trusted institution, e.g., a department authorized by the government, to become legitimate entities. For each $DES_{ij} \in S_i$, it will be assigned with a unique identification ID_{ij}, public/private key pair (PK_{ij}, SK_{ij}), and a personal account Account_{ij}. That is

$$\{ID_{ij}, PK_{ij}, SK_{ij}, \text{Account}_{ij}\} \leftarrow \text{register}(DES_{ij})$$

where there is a wallet address mapping to this account, $\text{Account}_{ij} \leftarrow \{\text{Address}_{ij}, \text{Balance}_{ij}\}$. Similarly, the registration information of the APG_i is denoted by $\{ID_i, PK_i, SK_i, \text{Account}_i\}$ as well, but there is a credit value in its account, that is, $\text{Account}_i \leftarrow \{\text{Address}_i, \text{Balance}_i, \text{Credit}_i\}$. This credit reflects its reputation in the ecosystem. Here, the public/private key pair can be achieved by some existing asymmetric encryption algorithms, such as elliptic curve digital signature [24], lattice-based signature [25], and anti-quantum signature [26]. Given a message msg encrypted by DES_{ij}, we have $\text{Hash(msg)} = PK_{ij}(SK_{ij}(\text{Hash(msg)}))$.

2) Creation: In a city S_i, the agent APG_i offers a price p_b^i to buy electricity from communities in its city, then each $DES_{ij} \in S_i$ responds it with the amount of electricity E_{exc}^{ij} that can be sold to APG_i. Like this, a new smart contract $\mathit{Contract}(APG_i, DES_{ij}, \text{STime})$ is generated by signing with their private key, respectively. Then, this contract will be copied in its memory server and broadcasted to all agents (authorized participants) in the ecosystem $\mathbb{S}$. After reaching a consensus, this smart contract will be deployed and executed automatically. The $\text{Contract}(APG_i, DES_{ij}, \text{STime})$ is associated with several variables, they are account information on both sides $(\text{Account}_i, \text{Account}_{ij})$, offered price p_b^i, traded amount of electricity E_{exc}^{ij}, expected transaction time TransTime, and timestamp STime. To guarantee this contract can be executed successfully, it needs to verify whether the APG_i has sufficient balance such that $\text{Balance}_i \geq p_b^i \cdot E_{\text{exc}}^{ij}$ and whether DES_{ij} has enough production capacity E_{exc}^{ij}.

3) Execution: The $\mathit{Contract}(APG_i, DES_{ij}, \mathit{STime})$ will be executed if current time $t \geq \mathit{TransTime}$ after reaching a consensus among agents in blockchain network. From now on, it begins to trade energy and finish the payment. The smart meter in APG_i verifies whether the electricity has been transported to the designated location. Then, fed this result from the smart meter into the smart contract, if yes, it will execute the payment process automatically, that is

$$\left(\mathrm{APG}_i, \mathrm{Balance}_i - p_b^i \cdot E_{\mathrm{exc}}^{ij}\right);\ \left(\mathrm{DES}_{ij}, \mathrm{Balance}_{ij} + p_b^i \cdot E_{\mathrm{exc}}^{ij}\right).$$

If this smart contract is executed successfully, the APG_i's credit value Credit_i will be increased by 1. It achieves the digital currency and energy exchange specified by contract between participants in a secure manner.

B. Blockchain Subsystem

As mentioned above, it will be broadcasted to all APGs in the ecosystem when a transaction is produced. All agents will verify whether their received transactions are valid. Those valid transactions will be stored in their memory server temporarily and packaged into a block later. The whole blockchain is stored in every memory server as well. Then, a consensus process is necessary to be performed among all agents in the ecosystem so as to ensure the consistency of blockchain. In our design, we develop a credit-based PoW mechanism. This is a novel combination of PoW and PoS, which can overcome the shortcomings of high latency in PoW and lack of randomness in PoS.

1) Miner and Block Production: The consensus process is executed round by round, where all agents are authorized participants, also called "consensus nodes." The first step in a round is to select a miner from all consensus nodes by solving a computational puzzle. Based on PoW, all consensus nodes attempt to find a nonce and compute the hash value of its packaged block that contains this nonce. The one who acquires such a hash value less than a predefined threshold first is elected as the miner, and then it can broadcast its block. Thereby those nodes that have more sufficient computing power will become the miner easily by finding the correct nonce faster. Due to a credit value Credit_i associated with each $\mathrm{APG}_i \in \mathbb{S}$, we can use it to improve the PoW mechanism. For the different nodes, the difficulty of their corresponding hashing puzzles is different. The agent with a higher credit statistic has an easier hashing puzzle and a better chance of winning the election. This credit-based miner election mechanism can be formalized as

$$\mathrm{Hash}(\mathrm{ID}_i, \mathrm{Block}, \mathrm{PHash}, T, \mathrm{Nonce}) \leq f(\Delta_i(T), D) \quad (9)$$

where *PHash* is the pointer that links to the previous block, T is the timestamp (round), and D is the predefined difficulty of this blockchain subsystem. All agents in this ecosystem are given by the same difficulty D. Now, let us look at the $\Delta_i(T)$ defined in (9). We denote by $\mathrm{Credit}_i(t)$ the credit of APG_i at round t and $\mathrm{Credit}_i(t) = \mathrm{Credit}_i(t-1) + \theta_i(t)$, where $\theta_i(t)$, called credit increment, is the number of transactions finished by APG_i and DESs in its city successfully at round t. Then, $\Delta_i(T)$ can be defined as $\Delta_i(T) = \mathrm{Credit}_i(T) - \mathrm{Credit}_i(T-\delta)$ given a round interval δ that is the credit's variation of APG_i during the previous δ rounds. It represents the number of successful trades that are completed by APG_i from $T-\delta$ to T. The more number of times a node has successfully traded during the recent rounds, the more credible we think it is. This is an incentive for the agents to participate in more electricity tradings as well. Given a difficulty D, threshold function f increases as the $\Delta_i(T)$ increases. We consider $f(0, D)$ as the baseline of the threshold. If $\Delta_i(T) > 0$, we have $f(\Delta_i(T), D) > f(0, D)$ but cannot be larger than $(1+\gamma)\cdot f(0, D)$ as $\Delta_i(T)$ increases, where γ is an adjustable parameter and $\gamma \in (1, 7)$ generally. If the trading system is more active, the more nodes frequently participate in the trading, the better the robustness of the system, and the overall difficulty of mining will be reduced. It is based on the assumption that the more successful transactions a node makes over a period of time, the more credible it is. We make those credible nodes less difficult to win the election, which increases the security of this system and reduces the latency to reach consensus. In this process, the computational power is from computation servers of agents.

2) Distributed Consensus: Once some node wins the miner, it will broadcast its blocks to the blockchain network. After receiving the new block from the miner, the remaining consensus nodes requires to verify the miner's identity, nonce, and the block. If the number of consensus nodes in the ecosystem that agree to accept it satisfies the condition of consensus ($\geq 51\%$), then this new block will be added into the blockchain. Once finishing the consensus, those smart contracts contained in this new block will be executed automatically. On condition that receiving more than one block, it should follow the longest chain principle where other forks are discarded eventually.

C. Security Analysis

For each APG in the ecosystem, it is not only an entity that participating in the transaction in the IoE subsystem but also a node that stores the blockchain and executes the consensus process in the blockchain subsystem. Different roles are played by different servers, and these servers work together but work independently. Thus, our B-ET ecosystem inherits the characteristics of the blockchain, shown as follows.

1) *Decentralization:* The electricity trades between the APG and DESs in a smart city are carried out in a P2P manner, and the bookkeeping process is finished among APGs without a third trusted intermediary.
2) *Privacy Protection:* Each DES uses its public key to communicate with the APG in its city, and this public key is shared among the APGs to be verified without disclosing true identity. Besides, the wallets of DESs are hidden by pseudonyms and can only be accessed by corresponding key and certificate, which avoiding malicious attacks against a specific entity.
3) *Authentication:* All transactions need to be audited and verified publicly in the consensus process by all APGs in the ecosystem. It is extremely hard to dominate the majority of APGs to create an unreal block because of the difficulty of credit-based PoW.
4) *Integrity:* Any block that newly added into blockchain contains the hash of the previous block, and its subsequent block contains its hash. A malicious attacker that attempts to modify a transaction must create a new chain after the block this transaction is in by dominating the majority of computational power and credit, this

is impossible. Besides, every transaction in the block is encrypted, it is hard to be decrypted without the private key.

5) *Transparency:* The nature of decentralization requires the blockchain to be saved in all memory servers of APGs. Thus, it is transparent to every entity, and DESs are able to check and confirm those transactions that they participate in easily.
6) *No Double-Spending:* The blockchain provides all entities with a public ledger of transactions in the ecosystem, which avoids double-spending potentially.

V. Electricity Trading: Stackelberg Approach

A noncooperative 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 [27]. In this section, we formulate a Stackelberg game to model the interactions in the above smart contract between the APG and DES. Consider a smart city S_i, the Stackelberg game $\mathbb{G}$ is formally defined by its strategic form as

$$\mathbb{G} = \left\{S_i, \mathbb{P}, \mathbb{D}, \{L^i\}, \{U^{ij}\}_{C_{ij}\in S_i}\right\} \tag{10}$$

where the components are shown as follows.

1) *Players Set S_i:* The agent APG$_i$ acts as a leader and offers a price p_b^i to the DESs in this city. Then, DES$_{ij} \in S_i$ act as followers and decide on the amount of electricity they want to sell according to this offered price.
2) *Strategy Spaces $\mathbb{P}$ and $\mathbb{D}$:* Let $\mathbb{P} = [p_m, p_c]$ be the strategy space of the agent, where we say $\{p_b^i\} \in \mathbb{P}$ is a feasible strategy of APG$_i$. Then, let $\mathbb{D} = \times_{C_{ij}\in S_i}\{[0, 1]\}$ be the strategy space of all DESs in this city, and we have $\{\beta^{ij}\}_{C_{ij}\in S_i} \in \mathbb{D}$ is a feasible strategy of DESs.
3) *Utility Functions $\{L^i\}$ and $\{U^{ij}\}_{C_{ij}\in S_i}$:* Each player in this game aims to maximize its utility or profit, which reflects the quality of strategy that this player chooses. $\{L^i\}$ is the profits of the agent, defined in (8); and $\{U^{ij}\}_{C_{ij}\in S_i}$ are the utilities of DESs, defined in (6).

A. DESs (Followers) Side Analysis

Given a price p_b^i offered by APG$_i$ in city S_i, each DES$_{ij} \in S_i$ responds it with the amount of electricity E_{exc}^{ij} that sold to the agent by controlling its dispatching factor β^{ij}. Thus, the objective of DES$_{ij}$ can be defined, that is

$$\max_{\{\beta^{ij}\}} U^{ij}\left(\beta^{ij}\right) \quad \text{s.t.,} \ \beta^{ij} \in [0, 1]. \tag{11}$$

Then, its first-order derivative is

$$\frac{\partial U^{ij}}{\partial \beta^{ij}} = X^{ij} \cdot \left(\frac{k_1^{ij} b_1^{ij}}{1 + b_1^{ij} X^{ij} \beta^i} - p_b^i\right). \tag{12}$$

The maximum utility can be obtained by solving its first-order differential condition $\partial U^{ij}/\partial \beta^{ij} = 0$, so we have

$$\beta_{\diamond}^{ij} = \frac{1}{X^{ij}} \cdot \left(\frac{k_1^{ij}}{p_b^i} - \frac{1}{b_1^{ij}}\right) \tag{13}$$

which is the DES$_{ij}$'s optimal response according to p_b^i. However, the choice of k_1^{ij} must be in a valid range such that $\beta_{\diamond}^{ij} \in [0, 1]$ given offered price $p_b^i \in [p_m, p_c]$. Or else, this utility function is monotone, and it is meaningless to adjust its dispatching factors. Based on (7) and (13), we have

$$X^{ij} \cdot (p_c)(e - 1)^{-1} \le k_1^{ij} \le X^{ij} \cdot (e \cdot p_m)(e - 1)^{-1} \tag{14}$$

where it assumes $p_c \le e \cdot p_m$, or else no such k_1^i can keep $\beta_{\diamond}^i \in [0, 1]$ satisfied. Thereby the optimal $\beta_{\diamond}^{ij}$ is proportional inversely to the offered price p_b^i, and the DES$_{ij}$ tends to sell more electricity by decreasing β^{ij} for a higher offered price.

B. Agent (Leader) Side Analysis

After receiving the optimal responses E_{exc}^{ij} from all DESs in S_i, the APG$_i$ needs to make a decision such that maximizing its profit by offering a reasonable price. Thus, the objective of APG$_i$ can be defined, that is

$$\max_{\{p_b^i\}} L^i\left(p_b^i\right) \quad \text{s.t.,} \ \ p_b^i \in [p_m, p_c]. \tag{15}$$

Substituting (13) into (8), we have

$$\begin{aligned} L^i\left(p_b^i\right) = (p_c - p_b) \sum_{C_{ij}\in S_i} \cdot \left(X^{ij} - \left(\frac{k_1^{ij}}{p_b^i} - \frac{1}{b_1^{ij}}\right)\right) \\ + (p_s - p_c) \cdot R_i. \end{aligned} \tag{16}$$

Then, its first-order derivative is

$$\frac{\partial L^i}{\partial p_b^i} = \sum_{C_{ij}\in S_i} \left(\frac{k_1^{ij} p_c}{{p_b^i}^2} - \left(X^{ij} + \frac{1}{b_1^{ij}}\right)\right). \tag{17}$$

The maximum profit can be obtained by solving its first-order differential condition $\partial L^i/\partial p_b^i = 0$, so we have

$$\hat{p}_b^i = \sqrt{\frac{p_c \sum_{C_{ij}\in S_i} k_1^{ij}}{\sum_{C_{ij}\in S_i}\left(X^{ij} + \left(b_1^{ij}\right)^{-1}\right)}} \tag{18}$$

which shows that the temporary optimal price $\hat{p}_b^i$ is affected by the number of DESs and their properties. From (18), we can see that this optimal price is interfered with by the cost price p_c as well. With the increase of p_c, the optimal price increases theoretically. In order to make the profit maximized, the agent has to offer its price according to (18). But based on (15), $p_b^i \in [p_m, p_c]$, the optimal strategy of APG$_i$ can be shown as follows:

$$\bar{p}_b^i = \begin{cases} p_c, & \text{if } \hat{p}_b^i \ge p_c \\ p_m, & \text{if } \hat{p}_b^i \le p_m \\ \hat{p}_b^i, & \text{if } p_m < \hat{p}_b^i < p_c. \end{cases} \tag{19}$$

Because the profit function is concave which will be proved later, $L^i(p_c)$ is the maximum value when $\hat{p}_b^i \ge p_c$. Similarly, $L^i(p_m)$ is the maximum value when $\hat{p}_b^i \le p_m$. Now, we can discuss whether they can reach an SE.

C. Stackelberg Equilibrium

In a smart city, the purpose of APG (resp., DES) is to maximize its profit (resp., utility) by adapting its corresponding trading strategy. The optimal solution of this game can be obtained when the APG_i get the maximized profit by offering a price $\tilde{p}_b^i$ given the DESs' optimal responses. In other words, none of them, including the leader and followers, can get a larger profit and utilities through altering their strategies unilaterally. At this time, the SE is formulated, which is defined as follows.

Definition 1 (SE): Given a Stackelberg game $\mathbb{G}$ defined in (10), we say a set of strategies $(\tilde{p}_b^i, \{\beta_*^{ij}\}_{C_{ij}\in S_i})$ reaches an SE of game $\mathbb{G}$ if and only if the following inequalities are met:

$$U^{ij}\left(\tilde{p}_b^i, \left\{\beta_*^{il}\right\}_{C_{il}\in S_i}\right) \geq U^{ij}\left(\tilde{p}_b^i, \beta^{ij}, \left\{\beta_*^{il}\right\}_{C_{il}\in S_i\setminus C_{ij}}\right) \quad (20)$$

$$L^{i}\left(\tilde{p}_b^i, \left\{\beta_*^{il}\right\}_{C_{il}\in S_i}\right) \geq L^{i}\left(p_b^i, \left\{\beta_*^{il}\right\}_{C_{il}\in S_i}\right) \quad (21)$$

where $\{\beta_*^{il}\}_{C_{il}\in S_i}$ is the optimal responses defined in (13) according to their previous leader's price.

Now, neither the leader and the followers can improve their utilities by changing their strategies, respectively, when the SE $(\tilde{p}_b^i, \{\beta_*^{ij}\}_{C_{ij}\in S_i})$ is reached. However, it is possible for the noncooperative game with pure strategies that the point of equilibrium does not exist [27]. Hence, we want to know whether our proposed game $\mathbb{G}$ exists an SE.

Theorem 1: Between the APG and DESs in city S_i, it exists a unique SE in our Stackelberg game $\mathbb{G}$.

Proof: For each $\mathrm{DES}_{ij} \in S_i$, based on the first-order derivative of U^{ij} defined in (12), we have

$$\frac{\partial^2 U^{ij}}{\partial {\beta^{ij}}^2} = -k_1^{ij} \cdot \left(\frac{b_1^{ij}X^{ij}}{1 + b_1^{ij}X^{ij}\beta^{ij}}\right)^2 < 0. \quad (22)$$

The utility function U^{ij} defined in (6) is strictly concave with respect to β^{ij}. Thus, regardless of offered price p_b^i, each $\mathrm{DES}_{ij} \in S_i$ exists a unique dispatching factor $\beta_\diamond^{ij}$ selected from $[0, 1]$ that maximizing DES_{ij}'s utility function. An SE can be reached when the APG and DESs have their maximum profit and utilities, respectively. Because the optimal response $\beta_\diamond^{ij}$ for $\mathrm{DES}_{ij} \in S_i$ is unique, we have that the game $\mathbb{G}$ reaches an equilibrium only if the APG_i is capable of offering the best price $\tilde{p}_b^i$ depended on the optimal responses from DESs. Based on (16) and (17), we have

$$\frac{\partial^2 L^i}{\partial {p_b^i}^2} = -\frac{2p_c}{{p_b^i}^3} \cdot \sum_{C_{ij}\in S_i} k_1^{ij} < 0. \quad (23)$$

The profit function L^i defined in (16) is strictly concave with respect to p_b^i. The APG_i can acquire the maximum profit by offering the uniquely optimal price $\tilde{p}_b^i$. Therefore, our proposed game $\mathbb{G}$ exists a unique SE definitely. ∎

D. Distributed Algorithm

From (18) and (19), the APG_i can obtain its optimal offering price $\bar{p}_b^i$ that maximize its profit easily if it can acquire complete information about those parameters, such as k_1^{ij}, b_1^{ij}, and X^{ij} for each $\mathrm{DES}_{ij} \in S_i$. However, in the real situation, it seems unrealistic that complete information about the parameters setting of all DESs can be accessed by the agent in a direct way because of their flexibility or out of privacy protection. Thereby the complete information about DESs is not available for the APG. Instead of a centralized manner, a distributed algorithm needs to be designed, where the APG is not required to know the complete parameter information of DESs in its city, but only receives the amounts of electricity DESs plan to sell. Consider a smart city S_i, the APG_i and all $\mathrm{DES}_{ij} \in S_i$ can reach the unique SE of Stackelberg game $\mathbb{G}$ in an iterative manner by use of limited communications between the leader and followers, which is shown in Algorithm 1.

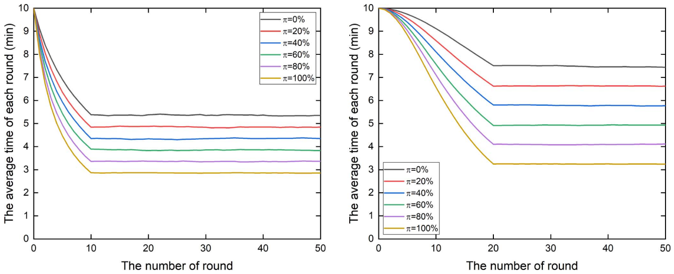
Algorithm 1 Finding SE

Initialize: $\tilde{p}_b^i := p_m$, $L_*^i := (p_s - p_c)R_i$
for each $\mathrm{DES}_{ij} \in \mathrm{S}_i$ **do**
  Initialize: $\beta_*^{ij} = 0$
end for
for the offering price p_b^i from p_m to p_c **do**
  for each $\mathrm{DES}_{ij} \in \mathrm{S}_i$ **do**
    DES_{ij} decides on its dispatching factor $\beta_\diamond^{ij}$ according to $\beta_\diamond^{ij} = \frac{1}{X^{ij}} \cdot \left(\frac{k_1^{ij}}{p_b^i} - \frac{1}{b_1^{ij}}\right)$
  end for
  The APG_i computes its profit L^i based on the response $\beta_\diamond^{ij}$ for each $\mathrm{DES}_{ij} \in \mathrm{S}_i$ according to
  $$L^i = (p_c - p_b) \sum_{\mathrm{DES}_{ij}\in \mathrm{S}_i} \left(X^{ij}(1 - \beta_\diamond^{ij})\right) + (p_s - p_c)R_i$$
  if $L^i \geq L_*^i$ **then**
    $\tilde{p}_b^i := p_b^i$, $L_*^i := L^i$
    $\beta_*^{ij} := \beta_\diamond^{ij}$ for each $\mathrm{DES}_{ij} \in \mathrm{S}_i$
  end if
end for
return $(\tilde{p}_b^i, \{\beta_*^{ij}\}_{\mathrm{C}_{ij}\in \mathrm{S}_i})$

According to Algorithm 1, in each iteration, the APG_i in city S_i offers a price $\tilde{p}_b^i$ which is initialized by $\tilde{p}_b^i := p_m$ first, then each $\mathrm{DES}_{ij} \in S_i$ decides on its best dispatching factor $\beta_\diamond^{ij}$ according to (13) based on the current price $\tilde{p}_b^i$ offered by APG_i and sends it back to the APG_i. After receiving all the optimal responses $\{\beta_\diamond^{ij}\}_{C_{ij}\in S_i}$ from DESs, the agent is able to compute its current profit L^i according to (8). If this profit L^i is larger than the maximum profit got before, it updates the global variables $\tilde{p}_b^i$ and L_*^i. The result $(\tilde{p}_b^i, \{\beta_*^{ij}\}_{C_{ij}\in S_i})$ returned by Algorithm 1 satisfies the definition of SE shown as (20) and (21), thus the game $\mathbb{G}$ reaches the SE. Here, the interval $[p_m, p_c]$ can be split at any step length.

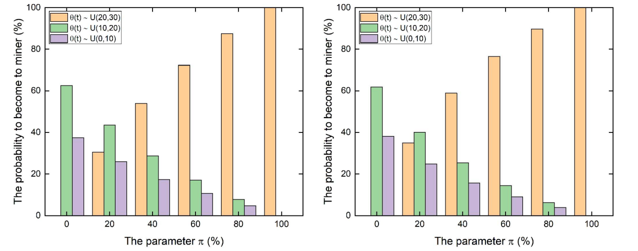
VI. Numerical Simulation

In this section, we will test the efficiency of our credit-based PoW mechanism and conduct several simulations to model the interactions between the APG and DESs in a smart city.



(a) (b)

Fig. 5. Average time to generate a new block under the different π and threshold functions. (a) $\delta = 10$, linear model. (b) $\delta = 20$, quadratic model.



(a) (b)

Fig. 6. Probability of consensus nodes with different credit increments to win the miner election at round 50. (a) $\delta = 10$, linear model. (b) $\delta = 20$, quadratic model.

A. Simulation Setup

To test our credit-based PoW mechanism, we give a blockchain network with 100 APGs (consensus nodes) with the same computational power and there are at most k communities in each city. It implies that an APG can finish at most k transactions with the DESs in its city at each round. Then, we need to define the threshold function $f(\Delta_i(T), D)$. Under the difficulty D and $f(0, D)$, the average time to generate a new block among these 100 consensus nodes is given by 10 min generally. During the previous δ rounds, each agent can finish at most $k\delta$ transactions with its DESs. Under the linear model, we define $f(\Delta_i(T), D)$ as

$$f(\Delta_i(T), D) = \left(1 + \frac{\Delta_i(T)}{k\delta} \cdot \gamma\right) \cdot f(0, D). \tag{24}$$

And under the quadratic model, we have

$$f(\Delta_i(T), D) = \left(1 + \left(\frac{\Delta_i(T)}{k\delta}\right)^2 \cdot \gamma\right) \cdot f(0, D) \tag{25}$$

where $\Delta_i(T) = \text{Credit}_i(T) - \text{Credit}_i(T-\delta)$. If $T - \delta \leq 0$, we have $\text{Credit}_i(T-\delta) = 0$. When $\Delta_i(T) = k\delta$, $f(\Delta_i(T), D)$ reaches its maximum value $(1+\gamma) \cdot f(0, D)$.

To model the interactions between the APG and DESs in a smart city, we give this city $S = \{\{\text{APG}\}, \{C_1, C_2, \ldots, C_n\}\}$ and denote the number of communities in this city by n. Typically, the calorific value of natural gas is 3.6×10^7 J/m^3 at the standard atmosphere and the measure for electricity is kW $\cdot$ h, where 1 kW $\cdot$ h $= 3.6 \times 10^6$ J. According to the latest U.S., retail price of electricity, that is, 0.2 dollar/kW$\cdot$h, hence, we can set $p_s = 5.5 \times 10^{-8}$ dollar/J. In our B-ET ecosystem, it can be considered as $p_s = 5.5 \times 10^{-8}$ coin/J equivalently. We assume the cost price $p_c = 4 \times 10^{-8}$ coin/J because the cost price should be less than retail price. Besides, for these DESs in this city, we assume their maximum gas consumption $F_m^j = 200$ m^3 for $C_j \in S$ and $\eta_{\text{pgu}} = 1$ for simplicity, because these settings does not affect the properties of our objective functions. From (14), we have $p_c \leq e \cdot p_m$, thus we are able to assume $p_m = 2 \times 10^{-8}$ coin/J, $k_1^j \in [167.6093, 227.8046]$, and $k_2^j = 0$ for $C_j \in S$. Thereby we have the range of variables, that is, $\beta^j \in [0, 1]$ for each DES and $p_b \in [2 \times 10^{-8}, 4 \times 10^{-8}]$ for the APG.

TABLE I
DISTRIBUTION OF CREDIT INCREMENT FOR AGENT AT $\pi = 20\%$

$\theta(t) \sim$ at each round	$U(20, 30)$	$U(10, 20)$	$U(0, 10)$
# Nodes	20	40	40

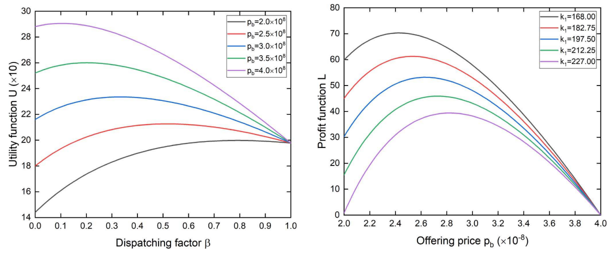
B. Simulation Results

First, we show the performance analysis and security analysis of our credit-based PoW mechanism as follows.

1) *Performance Analysis:* We default the maximum number of transactions (maximum credit increment) for an agent at each round is $k = 30$ and define a parameter $\pi \in [0, 1]$ to show the percentage of nodes whose credit increment at each round is high. Take $\pi = 20\%$ as an example, there are 20% consensus nodes whose number of completed transactions at each round $\theta_i(t)$ is sampled from [20, 30] uniformly and remaining nodes is split into two parts half and half distributed in [0, 10] and [10, 20] uniformly. The distribution at $\pi = 20\%$ is shown in Table I. Fig. 5 draws the average time to generate a new block under different settings. Shown as Fig. 5, the average time to reach the consensus reduces as the number of consensus increases until reaching the stationary point, which is equal to δ. After reaching the stationary point, we can see that the average time decreases with the increase of π because the proportion of nodes with high credit increments increases, which results in the falling of difficulty of their hash puzzles. Thereby it reduces latency for reaching a consensus.
2) *Security Analysis:* As mentioned early, we have a basic assumption that the more transactions have been completed by an agent during the previous δ rounds, the more credible this agent is. Fig. 6 draws the probability of consensus nodes with different credit increments to win the miner election. At the $\pi = 40\%$, the probability of nodes with $\theta(t) \sim U(20, 30)$ to win the miner should be equal to 40% under the classic PoW mechanism. However, shown as Fig. 6(a), this probability soars to 53.93%, which implies that those more credible nodes have a better chance to win the miner. Thereby it improves the security of our B-ET ecosystem.

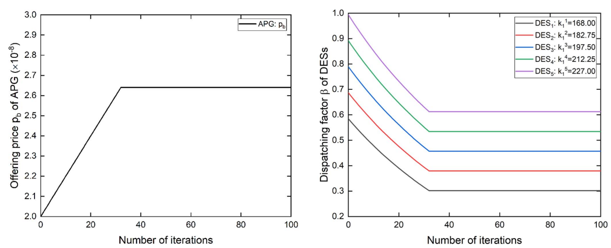
Then, we demonstrate the interactions between the APG and DESs and SE in a smart city as follows.

1) *Concavity of Functions:* Consider a city S that has only one community, we define the DES's parameter



(a) (b)

Fig. 7. Objective function of entities, including APG and DES, in the city S under the different parameter settings. (a) DES's utility U. (b) APG's profit L.



(a) (b)

Fig. 8. Process of entities in the city S converged to SE under the different parameter settings by following Algorithm 1. (a) APG's offering price. (b) DESs' dispatching factor.

as $k_1 = 197.7069$ and APG's electric load $R = 0$. Fig. 7 draws the objective function of entities in the city S. Shown as Fig. 7(a), we set DES's parameter $k_1 = 197.7069$. As β increases, these utility functions increase first and then decrease regardless of what the offered price is. It proves that the utility function U defined in (6) is concave. Furthermore, as p_b increases, the point of maximum utility moves to the left, which means that this DES tends to allocate more electricity that sold to the APG by decreasing its β in order to obtain the maximum utility. Shown as Fig. 7(b), these profit functions increase first and then decrease regardless of what the k_1 is. It proves that the profit function L defined in (16), is concave. Furthermore, as k_1 increases, the point of maximum profit moves to the right, which means that the APG has to offer a higher price to buy the electricity from DES in order to obtain the maximum profit. Here, a larger k_1 implies the electricity that used to serve community contributes much to the total utility, thus the APG has to offer a higher price.

2) *SE:* Consider a city S that has five communities, we define there DES$_j$'s parameter where $j \in \{1, \dots, 5\}$ as $k_1^1 = 168.00$, $k_1^2 = 182.75$, $k_1^3 = 197.50$, $k_1^4 = 212.25$, and $k_1^5 = 227.00$, and APG's electric load $R = 2 \cdot \sum_{C_j \in S} X^j$. Now, we can evaluate the performance of the convergence to the SE by Algorithm 1. Fig. 8 draws the process of converging to SE in the city S by following Algorithm 1. In the beginning, the price p_b offer by APG is low, the DESs are unwilling to sell their electricity to the APG, hence, their dispatching factor is very high. By interacting with DESs in this city, the APG adjusts its strategy (increases its offering price) gradually in each iteration to encourage DESs to sell more electricity in order to obtain a larger profit. After the 32nd iterations, the APG gains the largest profit at the offering price 2.64×10^{-8} coin/J, which is the point of equilibrium, thus their SE is reached.

TABLE II
APG's Profits Obtained in Centralized and Distributed Manner Under Different # of DESs in the City

n	**Centralized**		**Distributed**		**Incret**
—	$\tilde{p}_b$	Profit	$\tilde{p}_b$	Profit	——-
5	2.6300	3507.2231	2.6400	3507.2026	108%
10	2.5969	3800.6279	2.6000	3800.6236	117%
15	2.6225	4050.5182	2.6200	4050.5142	125%
20	2.6645	4255.7724	2.6600	4255.7551	131%
25	2.6656	4507.6399	2.6600	4507.6065	139%
30	2.6487	4799.9251	2.6400	4799.8273	148%

3) *Centralized Versus Distributed:* We have discussed before that the APG can acquire the optimal offering price directly in a centralized manner if all parameters of DESs in its city are known. Here, we can compare the performance of profits that are obtained in both the centralized and our proposed distributed manner. The comparison results are shown in Table II. Here, we set electric load $R = 30 \cdot X^j$ and k_1^j for $j \in \{1, 2, \dots, 30\}$ are sampled uniformly from $[167.6093, 227, 8046]$. Shown as Table II, the profits of APG at the SE of this game obtained by following our distributed algorithm are very close to that computed in a centralized manner regardless of the number of DESs in this city. The profit in a centralized manner is slightly higher than that under the distributed algorithm, thus its performance is better because of complete information. We execute 100 iterations between $[2 \times 10^{-8}, 4 \times 10^{-8}]$, thus the stride is 2×10^{-10}. To improve the accuracy of the distributed algorithm further, we can reduce the stride by increasing the number of iterations. In addition, we assess how the profit of APG changes with the different number of DESs in this city by comparing with the base profit. The base profit is computed under the circumstance that there is no DES, which is equal to $(p_s - p_c) \cdot R = 3240$. This implies that all required energy R has to be generated at the cost price. Accordingly, the base profit is lower than that involved with DESs. Next, the profit of APG increases gradually with the increase of the number of DESs in this city, because the APG is able to buy more electricity from DESs at a price lower than cost price. Thus, the profit will be increased certainly. The increment in Table II measures the performance compared to base profit because of DESs' existence, namely, quantified by actual profit divided by base profit. The effect is getting more and more significant that increasing from 108% to 147% as the number of DESs increases.

VII. Conclusion

In this article, we investigate a distributed electricity trading problem systematically. First, we propose the B-ET ecosystem to solve the privacy protection and transaction security issues in distributed electricity trading. To overcome the shortcomings of PoW and PoS, we design a smart contract for executing transactions and propose a credit-based PoW consensus mechanism. Then, we model the interactions between the agent and DESs in a smart city by Stackelberg game and take the CCHP system as an example to show this scene really. We prove that the SE between the agent and DESs in a city is guaranteed to exist and be unique, and propose a distributed algorithm that is able to reach the SE by limited iterations. Finally, the numerical simulations indicated that our model is valid and our algorithm is verified to be correct and efficient.

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] J. Matamoros, D. Gregoratti, and M. Dohler, "Microgrids energy trading in islanding mode," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Tainan, Taiwan, 2012, pp. 49–54.

[3] Y. Wu, X. Tan, L. Qian, D. H. Tsang, W.-Z. Song, and L. Yu, "Optimal pricing and energy scheduling for hybrid energy trading market in future smart grid," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1585–1596, Dec. 2015.

[4] 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.

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

[6] M. Li *et al.*, "CrowdBC: A blockchain-based decentralized framework for crowdsourcing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1251–1266, Jun. 2019.

[7] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

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

[9] 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.

[10] 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.

[11] 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.

[12] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[13] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N. Kumar, "EnergyChain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem," in *Proc. 1st ACM MobiHoc Workshop Netw. Cybersecurity Smart Cities*, 2018, pp. 1–6.

[14] 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.

[15] 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.

[16] F.-L. Meng and X.-J. Zeng, "A Stackelberg game-theoretic approach to optimal real-time pricing for the smart grid," *Soft Comput.*, vol. 17, no. 12, pp. 2365–2380, 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] 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.

[19] W. Tushar, J. A. Zhang, D. B. Smith, H. V. Poor, and S. Thiébaux, "Prioritizing consumers in smart grid: A game theoretic approach," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1429–1438, May 2014.

[20] S. Bu, F. R. Yu, Y. Cai, and X. P. Liu, "When the smart grid meets energy-efficient communications: Green wireless cellular networks powered by the smart grid," *IEEE Trans. Wireless Commun.*, vol. 11, no. 8, pp. 3014–3024, Aug. 2012.

[21] G. E. Asimakopoulou, A. L. Dimeas, and N. D. Hatziargyriou, "Leader–follower strategies for energy management of multi-microgrids," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 1909–1916, Dec. 2013.

[22] P. Samadi, A.-H. Mohsenian-Rad, R. Schober, V. W. Wong, and J. Jatskevich, "Optimal real-time pricing algorithm based on utility maximization for smart grid," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, 2010, pp. 415–420.

[23] W. Tushar, W. Saad, H. V. Poor, and D. B. Smith, "Economics of electric vehicle charging: A game theoretic approach," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1767–1778, Dec. 2012.

[24] 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.

[25] 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.

[26] 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.

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

Jianxiong Guo received the B.S. degree in energy engineering and automation from the South China University of Technology, Guangzhou, China, in 2015, and the M.S. degree in chemical engineering from the University of Pittsburgh, Pittsburgh, PA, USA, in 2016. He is currently pursuing the Ph.D. degree with the Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA.

His research interests include social networks, data mining, IoT application, blockchain, and combinatorial optimization.

Xingjian Ding received the B.E. degree in electronic information engineering from Sichuan University, Sichuan, China, in 2012, and the M.S. degree in software engineering from Beijing Forestry University, Beijing, China, in 2017. He is currently pursuing the Ph.D. degree with the School of Information, Renmin University of China, Beijing.

His research interests include wireless rechargeable sensor networks algorithm, 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, 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.