Hindawi
Security and Communication Networks
Volume 2021, Article ID 6524594, 11 pages
https://doi.org/10.1155/2021/6524594

Research Article

Renewable Energy Certificate Trading via Permissioned Blockchain

Dong Wang[1,2] **Jiaxing Xuan**[1,2] **Zhiyu Chen**[3] **Da Li**[1,2] **and Rui Shi**[3]

[1]*State Grid Electronic Commerce Co., Ltd., Beijing 100053, China*
[2]*State Grid Blockchain Technology (Beijing) Co., Ltd., Beijing 100053, China*
[3]*State Grid Information and Telecommunication Branch, Beijing 100761, China*

Correspondence should be addressed to Dong Wang; wangdong@sgec.sgcc.com.cn and Zhiyu Chen; zhiyu-chen@sgcc.com.cn

Received 18 June 2021; Revised 29 September 2021; Accepted 27 October 2021; Published 25 November 2021

Academic Editor: Qingqi Pei

With the continuous advancement of the green certificate trading mechanism, information verification needs to span multiple departments, which causes the application process cumbersome and human errors. In order to solve problems of cumbersome issuance process of the renewable energy certificate (REC) and the inflexible pricing mechanism, in this paper, a hybrid REC trading system was proposed based on an permissioned blockchain technology (BT), which combined advantages of the BT and the continuous double auction (CDA). The operation process of the system was introduced in detail, and the view change protocol in the Practical Byzantine Fault Tolerance algorithm was revised according to the characteristics of the system to improve the system stability. The continuous double auction rule was also introduced in the system. And corresponding bidding strategies were designed to maximize the revenue of users (buyer and seller) and transaction probability. The simulation experiment proves that the bidding mechanism can flexibly adjust the REC price according to the supply and demand relationship. At the same time, the effectiveness and feasibility of trading rule and bidding strategy were also verified.

1. Introduction

The REC is an electronic certificate issued to the qualified producer of renewable energy power. It is a recognition of the renewable energy generation capacity of power generator and a certificate for consumer to consume green power. The REC is a market-based instrument that certifies the producer who owns one megawatt-hour (MWh) of electricity generated from a renewable energy resource. Once the power provider has fed the energy into the grid, the REC can then be sold on the open market as an energy commodity. The REC represents environmental benefits of certain actions that help to mitigate greenhouse gas emissions. The REC arbitrage is a green power procurement strategy used by electricity consumers to simultaneously meet two objectives: (1) decrease the cost of renewable electricity use and (2) substantiate renewable electricity use and carbon footprint reduction. The strategy is used by consumers installing self-financed renewable electricity projects or consumers who directly purchase renewable electricity from a renewable electricity project.

China started the voluntary subscription of RECs in 2017. Firstly, the "Renewable Energy Medium and Long-Term Development Plan" requires that renewable energy consumption should account for more than 15% of the total energy consumption by 2020 [1]. For consumers, purchasing the REC is an important way to accomplish this goal. Secondly, the REC is a powerful way of attracting investment in the wind power project [2]. Thirdly, the REC transaction can promote adjustment of energy structure to support clean energy in a more market-oriented manner [3]. After China initiated the REC subscription, the purchase volume on the market did not meet expectations [4]. Before the verification and issuance of the REC were introduced [5], companies need to submit audit materials to various departments for review if they want to apply for the REC. Such cumbersome processes consume a lot of labour costs and other resources. Besides, the traditional approach cannot avoid human error.

Recently, most RECs were traded on the trading platform through listed sales. This transaction method not only brings about the problem of unequal information between the two parties of the transaction but also fails to fully reflect market demand, resulting in the REC price not changing in time. Therefore, an efficient REC issuance and a trading system are needed.

Satoshi Nakamoto proposed that using the BT to build the distributed database is suitable for all transactions in P2P network, which has the characteristics of decentralization, security and credibility, and data traceability [6–8]. With the rises of bitcoin and other cryptocurrency, the potential value of the BT in other fields is gradually reflected. The BT is widely used in finance, supply chain, health, education, and other fields [9]. A sharing scheme of blockchain-enabled secure data was proposed based on BT in mobile-edge computing [10]. Especially, the BT is promoting the development of information interaction in the direction of energy interconnection due to its decentralized nature that makes the system more robust without data loss [1,11–13]. For example, a 3-layer energy trading framework based on the BT was designed, and problems and challenges faced by the application of blockchain were also analysed in energy trading [14]. A market-oriented transaction of distributed power generation based on the BT was proposed, and the corresponding transaction mechanism, settlement mechanism, and reward and punishment mechanism were constructed [15]. The BT was also applied to build the logistics supply chain system, and its operation mode was analysed [16]. Kang et al. [17] introduced the BT into the power energy transaction of rechargeable cars and used BT to complete operations such as power energy transaction, price setting, and transaction record. The application of the blockchain in the energy industry has achieved good results. However, the above models are all researched in the simulated environments.

A trading method of the renewable energy and green certificate based on quota system was proposed [18]. This method only analyses the dynamic process of the relationship between price and supply and does not give specific transaction cases. A distributed energy trading model based on blockchain was proposed [19], but it does not comply with China's relevant policies. The implementation of the renewable energy system and the difference between fixed electricity prices and renewable energy quotas were summarized [20]. Zhou et al. [21] analysed the impact of transmission congestion on electricity prices and constructed a model for minimizing transmission congestion costs based on the nodal electricity price method. Xie et al. [13] described the application of blockchain in the interactive trading market and analysed the computing performance, storage capacity, and potential problems in practical applications. These studies focus on the impact of the renewable energy quota mechanism and REC trading, but the details of the specific transaction method need to be further studied. A lightweight protocol based on blockchain was proposed to solve the problem of low throughput [22]. But the security of data interaction cannot be guaranteed. A green certificate transaction technology was proposed based on Hyperledger Fabric 1.1, which improves the security level of transaction information [12]. However, this method has some shortcomings in transaction timeliness.

On the basis of existing researches, we introduced the BT in the green certificate transaction and aimed to solve problems of cumbersome green certificate issuance process and opaque information. We used the BT in the process of the REC issuance and trading to make the REC data collation and review easier and improve the efficiency of issuance and the transparency of information.

The double auction is that multiple buyers and multiple sellers bid to buy and sell items, and the CDA enables buyers and sellers to adjust their bids in real time, which more accurately reflects market demand [23–26]. At present, the CDA has been widely used in market transaction such as stocks and futures. For example, the CDA was used in document to price cloud computing service, and a bidding strategy was proposed to maximize the interests of buyers and sellers [27]. Therefore, the CDA can be considered to implement the REC transaction. In this way, the market can adjust prices to promote the formation of supply and demand relationship and further activate the trading market. In addition, the CDA model can force some backward green power companies to make technical improvement to achieve the purpose of reducing transaction cost. In this paper, we also introduced the CDA in order to promote more market-oriented REC transaction, to improve the efficiency of REC transaction and realize the flexible adjustment of the supply-demand relationship and price customization.

The traditional BT application based on on-chain model cannot meet the real-time requirements of the CDA. On-chain transactions refer to cryptocurrency transactions which occur on the blockchain and depend on the validity of the blockchain. All such on-chain transaction occurrences are considered to be valid only when the blockchain is modified to reflect these transactions on the public database record. Then, an efficient model of off-chain processing was proposed [28]. The off-chain transactions refer to those transactions occurring on a cryptocurrency network, which move the value outside of the blockchain. Due to their zero/low cost, the off-chain transactions are gaining popularity, especially among large participants. Based on the off-chain model, we proposed a hybrid REC trading system for the off-chain bidding and on-chain transaction, which combined advantages of the BT and CDA and was based on permissioned blockchain (HRECTS-PBC). In order to make the paper more readable, all abbreviations and their spelt-out forms are listed.

2. System Architecture and Operation

2.1. System Components. The structure of the HRECTS-PBC trading system is shown in Figure 1. This system includes a power plant, agent server, auction server, buyer, seller, smart meter, and power grid. The power plant and agent server were nodes in the network, and they were connected to each other to form a blockchain system. The seller and the buyer can use the agent server to conduct transaction without bearing the pressure of communication and computing on the network.

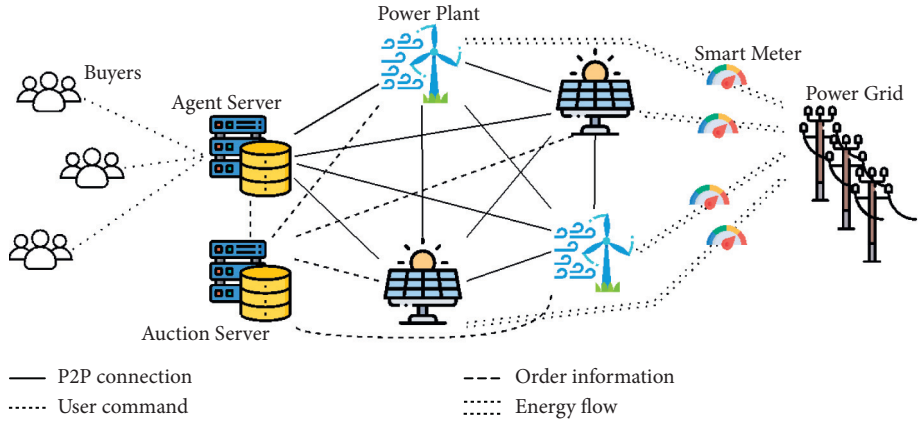

Figure 1: Structure of the HRECTS-PBC system.

The order information was published on the auction server. After the price reached an agreement, the REC was traded in the form of a smart contract. The smart contract was the code that was stored on a blockchain and automatically executed when predetermined terms and conditions were met. They were typically used to enforce some type of agreement so that all participants could be certain of the outcome without an intermediary involvement. The smart meter recorded the power consumption of each power plant and the amount of green electricity provided to the grid. The smart contract automatically verified the power generation status of the power plant based on the records of the meter and issues of the REC.

Currently, the application model based on the public chain is widely developed, but it still has some disadvantages. It is mainly reflected in the following. (1) Renewable energy power plants have to be qualified for network access after being reviewed by authoritative agencies, such as the government, which does not satisfy the completely open nature of the public chain. (2) Nodes in the public chain do not trust each other, and the work proof and other mechanisms are used to account after reaching a consensus, which not only causes a lot of waste of computing power and other resources but also leads to the low transaction efficiency. It currently takes about 10 minutes to generate new blocks, meaning that a transaction takes 10 minutes before being confirmed by the whole network [29]. The alliance chain is a network composed of authorized nodes. The trust between nodes is weak, but the trust confirmation can be completed using mutual communication confirmation method, which can improve the transaction efficiency. The simulation experiments conducted by Knezevic indicate that the confirmation time of the alliance chain block using the practical byzantine fault tolerance algorithm (PBFT) is less than 1s, and the throughput reach 50 k/s [30]. The PBFT algorithm solves the problem of low efficiency of the BFT algorithm and reduces the algorithm complexity from exponential to polynomial, making the PBFT feasible in practical applications. Although the performance will be reduced in real complex situations, it can be well applied to the alliance chain and can accommodate not only faulty nodes, but also malicious nodes. Therefore, a hybrid trading system based on alliance chain is proposed Figure 2.

2.2. Operation Model

(1) System initialization: after the renewable energy power plant received an identification IDi after review, the power plant *i* joined the on-chain system by virtue of the IDi. And then the system allocated public key (decryption key, PKi), private key (encryption key, SKi), wallet address (bank account, WAi), and certificate (Certi) to it for the first time. The certificate included the basic information of the electricity plant connected to the network, such as company name, address, installed capacity, smart meter ID, and other information. The newly added power plant node downloaded the database through the surrounding nodes after distributing the above information. After the synchronization was completed, the power plant officially became a node in the network. After the buyer completed the registration in the system, the public key, private key, and wallet address were assigned. The buyer could log into the system with the public key or the private key.

(2) Approval of the REC: based on the smart contract on the chain, the REC was regularly issued for the power plant by calculating the power meter of the power plant according to the regulations of 1MWh. The smart contract issued the REC to the wallet address of the power plant in the form of a transaction. Each REC was expressed as REC = { ID, *t*, c, *m* }, where ID, *t*, and *c* are the REC number, issuance time, and the type of green electricity, respectively, and *m* is some additional information, such as the affiliated company and project number.

(3) Sale of the REC: the power plant pledged the REC to be sold in the auction transaction smart contract and marked the sale price. The message was expressed as sellOrder = 〈(RECj, rid, ...), Pask, *t* 〉, where (RECj, rid, ...) is the REC with IDrid to be sold by seller *j*. Pask is the sale price. T is the time for pending order. At the same time, the order information and digital signature were sent to the off-chain bidding server, which was expressed by 〈 sellOrder, signSKj (MD5 (sellOrder))〉. After the server was verified,

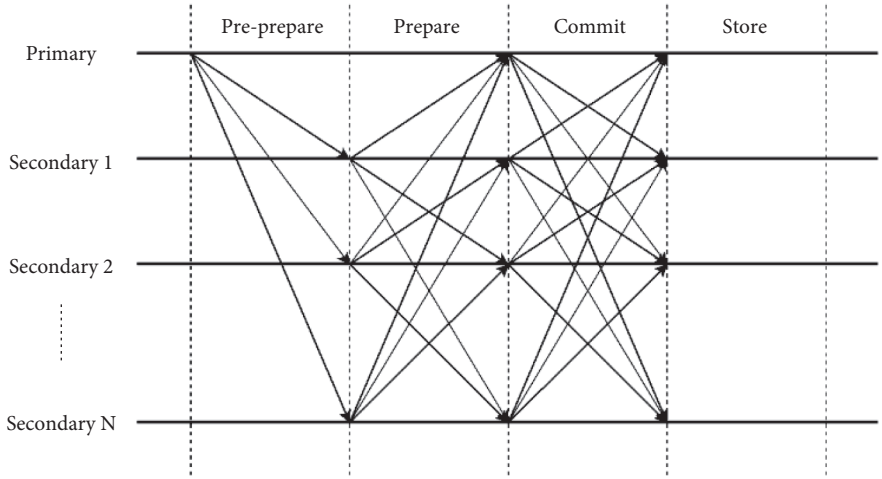

Figure 2: PBFT consensus process.

the corresponding information was displayed in the sale list. If not all of the sale was completed after a period of time, the smart contract returned the remaining REC to the seller.

(4) Purchasing the REC: the buyer published the purchase price and quantity in the auction system and pledged the required currency in the auction transaction smart contract, that is, sent buyOrder = 〈 buyer ID, Pbid, d, Coin, t 〉 to the transaction smart contract address; Pbid is the purchase unit price, d is the purchase quantity, Coin = Pbid × d is the amount of money pledged into the contract, and t is the time of the pending order. The order information was sent to the bidding server with the digital signature, that was buyOrder = 〈 buyOrder, signSKi (MD5 (buyOrder)) 〉 . After the server was verified, the corresponding information was displayed in the purchase list. If a sufficient number of the REC was not purchased after a period of time, the smart contract returned the remaining currency to the buyer.

(5) Transaction: bidding transactions applied a two-way auction mechanism to match transactions in off-chain bidding servers. The bidding system adopted the traditional client-server model and displayed the order status in real time through the visual interface. The auction and closing rules were introduced in detail in Section 3. Successfully matched transactions were marked with both orders and digital signatures of parties, that is, matchedOrder = 〈 sellOrder, signSKj (MD5 (sellOrder)), buyOrder, signSKi (MD5 (buyOrder)) 〉 . Bidding server sent 〈 matchedOrder, signSKas (MD5 (matchedOrder)) 〉 to the agent server and updated the transaction information on the server. SKas is the private key of the bidding server. The agent server sent the information to the bidding transaction smart contract in the blockchain. After the smart contract was verified, the validity of the transaction information, the pledged currency, and the REC were used to conduct the transaction. If the REC of the seller cannot be fully sold in the transaction, the smart contract generates a new order for the remaining REC at the same price and issues a new time stamp for release. If the buyer fails in this transaction after purchasing enough RECs, the smart contract also generates a new order and issues a new time tamp for release.

(6) Transaction packaging: the primary node collected transactions for a period of time and then packed them into a block after verifying the validity of the transaction locally. Similar to the Bitcoin block, a block included a block header and a block body. The block body was transaction information, which was stored in the form of a Merkle tree, and the hash value of the Merkle root was stored in the block header. The block header also includes the hash value, version, and time stamp of the previous block. Because we did not use the proof of work information, the block header did not need to contain random numbers.

(7) Consensus: the application of PBFT was considered as a consensus mechanism [31]. There were N nodes in the system, and the number of failed nodes was f. If $N \geq 3f + 1$, the system reached agreement through PBFT. The consensus process is shown in Figure 2. In the pre-preparation stage, the primary node broadcasted a message to the slave node; the message format was 〈 〈 PREPREPARE, v, n, d 〉 , m〉 . Among them, m is the newly generated block, v is the view number, n is the message sequence number in the current view, and d = MD5(m) is abstract of m. After receiving the message from the node, the system verified the correctness of v, n, d. The node sent the preparation message 〈 PREPREPARE, v, n, d, i 〉 to all other nodes. I is the number of the current node in the system. When a node received at least 2f preparation messages from other nodes, and v, n, d were the same as the received prepreparation message, it entered the commit phase. The node checked the validity of the

transaction in the block and the correctness of the block header. After the check was passed, a confirmation message 〈 COMMIT, v, n, MD5(m), i 〉 was generated and sent to all other nodes. When the node received at least 2f +1 identical confirmation information (including its own confirmation information), it entered the store stage, which wrote the block to the local block chain, and the consensus process was completed.

2.3. View Replacement. In PBFT, when the primary node fails, the view is updated according to the view replacement protocol, and the new primary node is reselected. In the basic PBFT, there is no need to consider the stability of the node, because the selection of node is indiscriminately selected in turn (primary node $p = v \bmod \mathrm{N}$). V = vpre +1 is the new view number. P is the number of the new primary node. Because the primary node has the function of generating blocks and leading consensus, it needs higher stability and performance. The agent server of the system on the chain is not only a node in the blockchain network, but also a portal server for other users to log in. They are operated by a professional team, so they will have higher stability and performance than the machines in the electricity plant. It is also less likely to be maliciously manipulated. Considering the above situation, some view replacement strategies need to be changed.

We set the number of the blockchain system of the agent server on the chain to 0 and sequentially number other nodes as 1, 2, . . ., N-1. The method of generating the primary node is

$$p = \left((v \bmod 2)\frac{v}{2}\right) \bmod N, \qquad v = v_{\mathrm{pre}} + 1. \tag{1}$$

where mod is modulo operation, $v \in \mathbb{N}$ is the number of the new view, $[\cdot]$ is the rounding up operation, and v_{pre} is the number of the previous view. When the current primary node was 0 and the trigger condition for PBFT view replacement was met, then a new primary node for view replacement was selected according to (1). When the current primary node was not 0 and the trigger condition for PBFT view replacement was met, or the primary node received the confirmation message from node 0 in the commit phase of the consensus process for k consecutive times, a new primary node was selected according to the view change operation. Except for the change in the method of selecting the primary node, other operations in the view replacement protocol were unchanged. In order to make the system run in an efficient state, we let the agent server node act as the primary node most of the time, which reduced the burden on the power plant machines.

3. CDA Rules and Bidding Strategies

This section mainly introduces the continuous double auction rules and transaction rules used in the bidding stage. We also designed alternative bidding strategies for users based on the auction rules to maximize the probability of transaction and user benefit.

3.1. CDA Rules. The market trading mechanism includes the market trading subjects, trading time, price mechanism, and the disclosure way of market information. Continuous two-way auction refers to the transaction form in which buyers and sellers can submit bids at any time during the trading cycle when market participants exist in many-to-many form, and once the prices match, the transaction can be concluded. In the continuous two-way auction mechanism, the buyers and sellers are sorted according to the principle of "price first, time first". The buyer's price is sorted from high to low, while the seller's price is sorted from low to high. In the case of the same price, the order is sorted according to the time before and after the submission of the offer. Under this auction mechanism, the buyer's highest price is called the optimal purchase price and the seller's lowest price is called the optimal offer price. A transaction occurs when the optimal purchase price is greater than or equal to the optimal offer price. In the matching process of transaction price, the buyer with the highest bid is matched with the seller with the lowest bid, and the transaction price is the average of the two prices. And so on, a round of transaction is completed until the optimal purchase price is lower than the optimal offer price, and each round of transaction has at least one transaction. In the transaction process, market participants can check the optimal purchase price, the optimal offer price, and the transaction price and then adjust their bid continuously according to the market information using bid strategy to carry out the next round of transaction, until all the transaction prices in the market are matched or the transaction time ends.

The CDA is the process in which multiple buyers and multiple sellers bid to purchase and sell items. During the opening period of the trading day, each user can arbitrarily bid to complete the transaction [32]. The minimum time interval between two bids was set to T, and the opening time of one trading day was TD. Then, the user can have TD/T round of bidding opportunities. In this CDA rules, there are the following contents: t indicates the current bid round of user. The current maximum bid of buyer was recorded as obid. The current lowest offer of seller was recorded as oask. Buyer (i) bid in the round t was recorded as bit, and the highest acceptable price of buyer (i) was Bi. Seller (j) offer in the round t was recorded as ajt, and the lowest acceptable price of seller (j) was Aj. The act submitting price and transaction quantity to the system by user are called pending order.

According to the results researched by Wang et al. [15], the CDA trading rules are formulated.

(1) If the buyer bids, the price should be greater than or equal to the highest bid at the previous moment, and if the seller offers, the price should be less than or equal to the lowest bid at the previous moment ($b_i^t \geq o_{\mathrm{bid}}^{t-1}$ an d $a_j^t \leq o_{\mathrm{ask}}^{t-1}$). If there is no local order in the market at the moment of bidding, there will be no o_{bid}^{t-1} or o_{ask}^{t-1}. If the bid price is not subject to the above

rules, it can be arbitrarily bid. In theory, when $o_{\text{bid}}^{t-1} > B_i$, Buyer i does not bid, and when $o_{\text{ask}}^{t-1} < A_j$, Seller j does not quote.

(2) If $o_{\text{bid}}^{t} < o_{\text{ask}}^{t}$, no transaction will be completed at the time t. If $o_{\text{bid}}^{t} \geq o_{\text{ask}}^{t}$, the two parties of the transaction will trade at the price $p = o_{\text{bid}}^{t}$, and the transaction volume will be subject to the party with the smaller transaction volume reported by both parties. The remaining transaction volume of one party is still pended at the original price. If there are multiple orders with the same bid, the order with the earlier bidding time will be firstly executed.

(3) The user can cancel the order at any time after the transaction is pended order. If the pending order has not been completed after the time mT, the system will automatically cancel the order, and all unsuccessful pending orders will be withdrawn at the end of the trading day.

3.2. Bidding Strategy. According to trading rules, a bidding strategy called PP strategy was designed, which allows users to obtain higher returns and trading probabilities.

We first estimated the competitive equilibrium price p^* with the help of the past transaction price which can reflect the current supply-demand relationship. When the transaction price $p = p^*$, the current supply and demand is balanced. When $p > p^*$, the supply is less than the demand, which increases the price of goods. When $p < p^*$, the supply exceeds the demand, which decreases the price of the goods [33]. We used a moving average to estimate the current competitive equilibrium price, that is,

$$\begin{aligned} \widehat{p^*}_t &= \alpha p_t + (1-\alpha)\widehat{p^*}_{t-1}, \\ \widehat{p^*}_0 &= p_0. \end{aligned} \tag{2}$$

where $\widehat{p^*}$ is the estimated competitive equilibrium price. $\alpha \in (0, 1)$ is the smoothing factor. The smaller the a is, the smoother the estimated competitive equilibrium price is, and the less it is affected by the current transaction price. Conversely, the larger the a is, the greater it fluctuates, and the greater it is affected by the current transaction price.

In order to simulate the CDA trading market, the normal distribution was used to estimate the bid [34]. In our trading rules, the bid of buyer was greater than or equal to the current maximum bid, and the bid of seller was lower than or equal to the current minimum bid. Considering the above, we used the half-normal distribution to estimate user bids. The buyer bid and seller bid were represented by

$$b_i^t = \left(1 + hn_{\text{bid}}^t\right) o_{\text{bid}}^{t-1}, \tag{3}$$

$$a_j^t = \left(1 - hn_{\text{ask}}^t\right) o_{\text{ask}}^{t-1}, \tag{4}$$

where hn belongs to the half-normal distribution. $X \sim \mathcal{N}(0, \sigma^2)$ is a normal distribution with mean 0 and variance $\sigma 2$, and then, $hn = |X|$. The variance depends on the transaction price, that is,

$$\sigma_{\text{bid}}^t = k \exp\left(p_{t-1} - \widehat{p^*}_{t-1}\right), \tag{5}$$

$$\sigma_{\text{ask}}^t = k \exp\left(\widehat{p^*}_{t-1} - p_{t-1}\right), \tag{6}$$

where $k > 0$, and it is the scaling coefficient. When $p_{t-1} - \widehat{p^*}_{t-1} > 0$, the trading price tends to rise, and σ_{bid}^t is larger. The difference between the price obtained by (3) and $\sigma_{\text{bid}}^{t-1}$ will be relatively larger. At this time, σ_{ask}^t will be smaller, and the difference between the prices obtained by (4) and $\sigma_{\text{ask}}^{t-1}$ is smaller, which indicates that both parties of the transaction expect to make a deal at a higher price. At this time, it is the seller market, and vice versa.

Based on the above assumptions, we formulated bidding strategies for both parties. For seller j, it can be traded at $a_j^t \leq o_{\text{bid}}^t$, because the buyer bid was greater than or equal to the current highest bid. The o_{bid}^t must be generated by a buyers bid at t, and the probability that the seller offer can be traded as

$$\begin{aligned} P_{\text{sell}} &= P\left(a_j^t \leq b_i^t\right) = P\left(a_j^t \leq \left(1 + hn_{\text{bid}}^t\right) o_{\text{bid}}^{t-1}\right) = P\left(hn_{\text{bid}}^t \geq \frac{a_j^t}{o_{\text{bid}}^{t-1}} - 1\right) \\ &= 1 - F\left(\frac{a_j^t}{o_{\text{bid}}^{t-1}} - 1; \sigma_{\text{bid}}^t\right) = 1 - \text{erf}\left(\frac{a_j^t - o_{\text{bid}}^{t-1}}{\sqrt{2}\,\sigma_{\text{bid}}^t o_{\text{bid}}^{t-1}}\right). \end{aligned} \tag{7}$$

where $F(x; \sigma) = erf\,(x/\sqrt{2}\,\sigma)$ is the cumulative probability density function of the half-normal distribution. Similarly, for the buyer i, the probability that the bid can be concluded is

$$P_{\text{buy}} = P\left(b_i^t \geq a_j^t\right) = P\left(hn_{\text{ask}}^t \geq 1 - \frac{b_i^t}{o_{ask}^{t-1}}\right) = 1 - \text{erf}\left(\frac{o_{\text{ask}}^{t-1} - b_i^t}{\sqrt{2}\,\sigma_{\text{ask}}^t o_{\text{ask}}^{t-1}}\right). \tag{8}$$

Generally, the buyer hopes to complete the transaction with the bid b_i^t. At this time, the buyer i can get the benefit $B_i - b_i^t$. The lower the bid is, the greater the benefit is. However, it can be seen from formula (8) that the probability of being able to trade is also smaller. In the same way, the seller wants to trade with the offer a_j^t (at this time, the specific transaction price in the rule is not considered to simplify the model solution). The profit that the seller j can obtain is $a_j^t - A_j$. It can be seen that the higher the offer is, the greater the profit is, but it can be seen from formula (7) that the probability of being able to trade is also smaller. Therefore, there is a contradiction between the revenue and the transaction probability. In order to complete the transaction as soon as possible and obtain a good profit, we multiplied the two parameters to determine the optimal bid; that is,

$$\begin{aligned} \widehat{b_i^t} &= \arg\max_{b_i^t \in [0,B_i]} \left(B_i - b_i^t\right) P_{\text{buy}}, \\ \widehat{a_j^t} &= \arg\max_{a_j^t \in [A_j,\infty]} \left(a_j^t - A_j\right) P_{\text{sell}}. \end{aligned} \tag{9}$$

Due to the influence of the nonelementary function in the above formula, it is difficult to directly calculate the optimal value. We considered that the original forms are continuously differentiable in the domain, and we applied the gradient descent method to solve it [26]. For buyers and sellers, we define the objective function as

$$PP_{\text{bid}}\left(b_i^t\right) = -\left(B_i - b_i^t\right) P_{\text{buy}}, \tag{10}$$

$$PP_{\text{ask}}\left(a_j^t\right) = -\left(a_j^t - A_j\right) P_{\text{sell}}. \tag{11}$$

We set the maximum iteration number as the target parameter according to (11) and (12):

$$\begin{aligned} b_{i,n+1}^t &= b_{i,n}^t - \eta \frac{\mathrm{d}}{\mathrm{d}b_{i,n}^t} PP_{\text{bid}}\left(b_{i,n}^t\right), \\ a_{j,n+1}^t &= a_{j,n}^t - \eta \frac{\mathrm{d}}{\mathrm{d}a_{j,n}^t} PP_{\text{ask}}\left(a_{j,n}^t\right). \end{aligned} \tag{12}$$

where η is learning rate. b_i^t and a_j^t were respectively initialized by Bi and Aj. When the maximum number of iteration N or the difference between the objective function updates is twice less than ε, renewal ends. And the current parameters are taken as the final result. In our experiments, the objective function usually had only one minimum value point in the domain, and the value at the boundary was greater than the value at the minimum value point. Therefore, the minimum value point can be guaranteed to be the smallest value point.

The optimal bid above was used as a reference, but the demand of users in the actual transaction is different. Therefore, we defined the turnover intention $\lambda \in [-1, 1]$, where the bigger λ is, the more likely users tended to close the transaction as soon as possible. The smaller the λ is, the more the benefits users wanted to gain are. Combined with transaction intention, the bidding strategy of users is as follows:

$$b_i^t = \begin{cases} \widehat{b_i^t} + \lambda\left(\widehat{b_i^t} - o_{\text{bid}}^{t-1}\right) \lambda \le 0, \\ \widehat{b_i^t} + \lambda\left(B_i - \widehat{b_i^t}\right) \lambda > 0. \end{cases} \quad a_j^t = \begin{cases} \widehat{a_j^t} - \lambda\left(o_{\text{ask}}^{t-1} - \widehat{a_j^t}\right) \lambda \le 0, \\ \widehat{a_j^t} - \lambda\left(\widehat{a_j^t} - A_j\right) \lambda > 0. \end{cases} \tag{13}$$

The formula above is valid when it satisfies $o_{\text{bid}}^{t-1} \le \widehat{b_i^t} \le B_i$, $A_j \le \widehat{a_j^t} \le o_{\text{ask}}^{t-1}$. If the constraint conditions of $\widehat{b_i^t}$, $\widehat{a_j^t}$ in the formulas (12) and (13) are not satisfied, $B_i < o_{\text{bid}}^{t-1}$ or $A_j > o_{\text{ask}}^{t-1}$. The PP strategy does not offer reference for users in the t-th round. When the buyer gets the bid by formula (15) and $b_i^t \ge o_{\text{ask}}^{t-1}$, the transaction is concluded. According to rules in Section 3.1, the price of the transaction should be b_i^t. Regardless to the number of transaction, the buyer will try to reduce the price. Therefore, the final buyer bid was further revised to

$$b_i^t = \min\left(b_i^t, o_{\text{ask}}^{t-1}\right). \tag{14}$$

The seller does not have to consider a_j^t and o_{bid}^{t-1}, because $a_j^t \le o_{\text{bid}}^{t-1}$, and the transaction price of o_{bid}^{t-1} and the seller actual income will not be affected whether or not a_j^t was modified.

At the beginning of each trading day or when one party's orders are completely consumed, there are no parameters needed to obtain the final bid. We used the following strategies. (1) At the beginning of the trading day, the first bidder used the p and p^* to calculate σ and used the last transaction price of the previous trading day p as the o. (2) If the seller order is completely absorbed at the last moment, the buyer has no enough order amount required by formula (10) o_{ask}. Similarly, if the buyer order is completely consumed at the last moment, the seller has no enough order amount required by formula (11) o_{bid}. At this point, we considered using the transaction price of the previous transaction time p_{t-1} as a corresponding o and completing calculation. In the current situation, the buyer bid is not considered in formula (14) and it directly used b_i^t as a final bid. (3) If the seller order is completely consumed at the last moment, the seller will lack the value of o_{ask}^{t-1} in formula (16). We supposed that the maximum profit ratio expected by the seller is $\mu \in (0, +\infty)$; when $\lambda = -1$, the seller shall offer in the way of maximum profit, where $a_j^t = o_{\text{ask}}^{t-1} = (1 + \mu)A_j$. In this case, we used $(1 + \mu)A_j$ to replace o_{ask}^{t-1}. Similarly, we used the $(1 - \mu)B_i$ to replace o_{bid}^{t-1}. Taking into account the market price, economic benefit, and other factors, in the follow-up experiments, the maximum return was assumed to be 20% ($\mu = 0.2$).

4. Example Analysis

4.1. New View Replacement Agreement. We compared the new view replacement protocol with the original one and assumed that there are six active nodes in the network, numbered 0, 1, ..., 5. Node 0 was the agent server. The relationship between primary node selection and view is shown in Figure 3. It can be seen that in the original view replacement protocol, each node turned to be the primary node, and node 0 in the new view replacement protocol

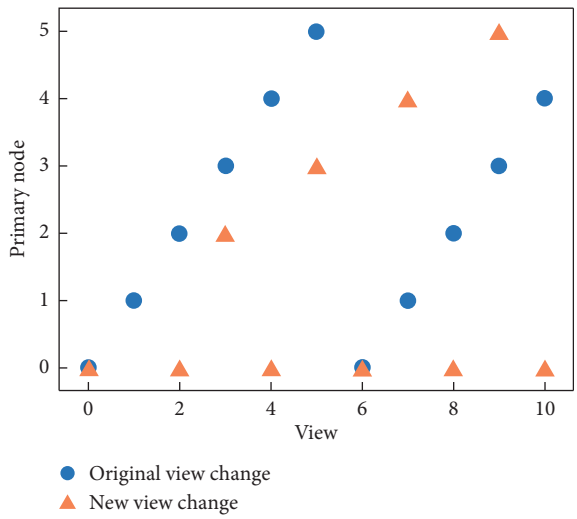

Figure 3: The relationship between primary node selection and view number.

acted as the primary node most of the time, so as to improve the stability of the system.

4.2. Optimization Objectives. The cost price A_j was supposed to 125, the current o_{bid} was 130, and the objective function (PP_{ask}) was obtained by the curve of the ask versus bid which is shown in Figure 4. In formula (5), when σ_{bid} is very small ($p - p^* \ll 0$), it indicates that it has just experienced a big decrease. Due to being uncertain whether it will continue decreasing, the bid will be close to the o_{bid} that strives for the trading success and avoids further decrease. When the bid is greater than 0.01, the bigger σ_{bid} is, the greater the value of $p - p^*$ is. That is, in the current trend of price rise, the optimal seller offer will also increase, and the seller can make more profits and have a chance to trade. We supposed that the highest price Bi acceptable to buyer i was 125, and o_{ask} was 120. The relationship between the objective function (PP_{bid}) and the bid b is shown in Figure 5. In formula (6), when σ_{ask} is very small ($p^* - p \ll 0$) , it indicates that it has just experienced a big increase. Due to being uncertain whether it will continue to increase, the offer will be close to o_{ask} that strives for trading success and avoids further increase. When σ_{ask} is greater than 0.01, the larger σ_{ask} is, the greater the value of $p^* - p$ is. That is, in the current trend of price decrease, the optimal bid of the buyer will be reduced, and the buyer can save more and have a chance to trade. When the value of σ is too large, it will be deviated from the current price seriously, which does not agree with the actual situation of the transaction. Therefore, it is necessary to reasonably select k in formulas (5) and (6). Generally, the k should be taken as a small value to ensure that σ will not be too large. Here, we only selected by experience. It can also be seen from the above two graphs that, in general, there was only one minimum value of the objective function in the definition domain, and this minimum value was also the least value. Therefore, we can ensure the convergence to the minimum point by using the gradient descent method.

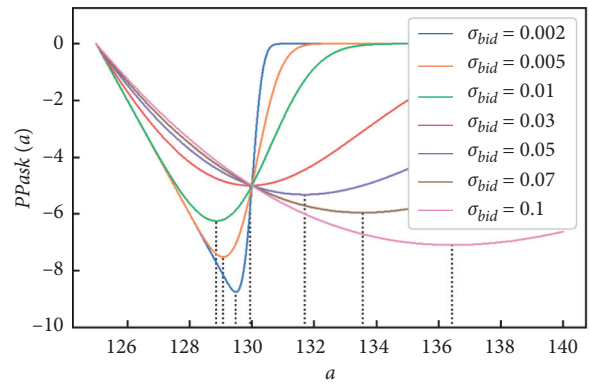

Figure 4: The objective function of seller bid.

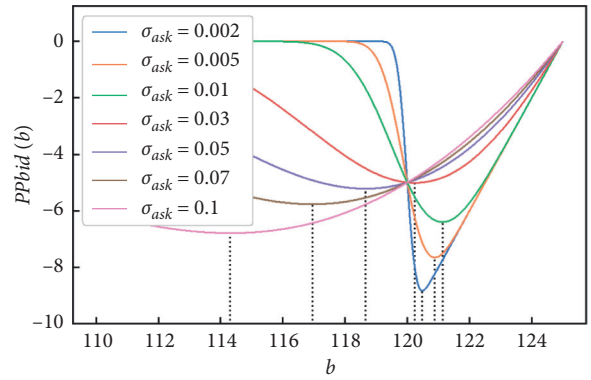

Figure 5: The objective function of buyer bid.

4.3. Transaction Simulation. We supposed that there are 5 sellers and 5 buyers in the market. Their parameters are shown in Table 1. When the market initialized, we set p and p^* both as 200, one trading day TD = 10000, and the minimum bid interval $T = 1$. The time interval for the user to bid was 10000 rounds and the transaction platform canceled the order when $m = 600$. Users did not bid every round, and the interval between two bids obeyed exponential distribution when λ was set to 1/20. In other words, the average time interval between two auctions was 20, and the number of transactions per user followed a uniform distribution between 1 and 10. In the bidding strategy of $a = 0.05$ and $k = 0.005$, the gradient fell when $N = 1000$, $\eta = 0.1$, $e = 10–8$.

We used the above parameters to conduct 10 simulation experiments and got the results in Table 2. Each income was the income from selling or purchasing a REC. The quantity of RECs provided by the seller was less than the demand of buyer, and the cost price was reasonable. Therefore, the seller can sell all RECs. Due to the high cost, s4 wanted to pursue higher income ($\lambda < 0$). Therefore, it was sometimes impossible to sell all RECs. The cost price of s2 and s5 was almost equivalent, but the selling difference of each REC was about 4.09 just because of the different λ. In the initial stage of the transaction, some sellers (s2) with low cost were eager to sell at lower price, so that some buyers with lower bids can also finish the transaction. The bidding strategy was such that the price was in the falling stage, which makes the transaction

Table 1: The information and bidding strategy parameters of buyers and sellers.

Seller ID	A	λ	Sales volume/piece
s1	187	−0.28	434
s2	181	0.84	286
s3	195	0.54	418
s4	192	−0.46	390
s5	182	−0.80	261
Buyer ID	B	λ	Purchases/piece
b1	200	−0.98	300
b2	216	0.11	394
b3	210	−0.06	307
b4	218	0.56	409
b5	207	0.29	440

Table 2: Results of 10 simulated transactions.

Seller ID	Turnover rate/%	Per revenue
s1	100.00 ± 0	9.28 ± 1.67
s2	100.00 ± 0	10.58 ± 1.34
s3	100.00 ± 0	5.89 ± 0.81
s4	99.97 ± 0.07	8.73 ± 1.87
s5	100.00 ± 0	14.67 ± 2.83
Buyer ID	Turnover rate/%	Per revenue
b1	93.70 ± 5.01	8.25 ± 0.64
b2	99.26 ± 0.92	17.00 ± 1.91
b3	99.84 ± 0.33	11.57 ± 1.59
b4	98.78 ± 2.17	17.38 ± 1.66
b5	92.32 ± 3.96	10.14 ± 0.98

The value after ± is the standard deviation.

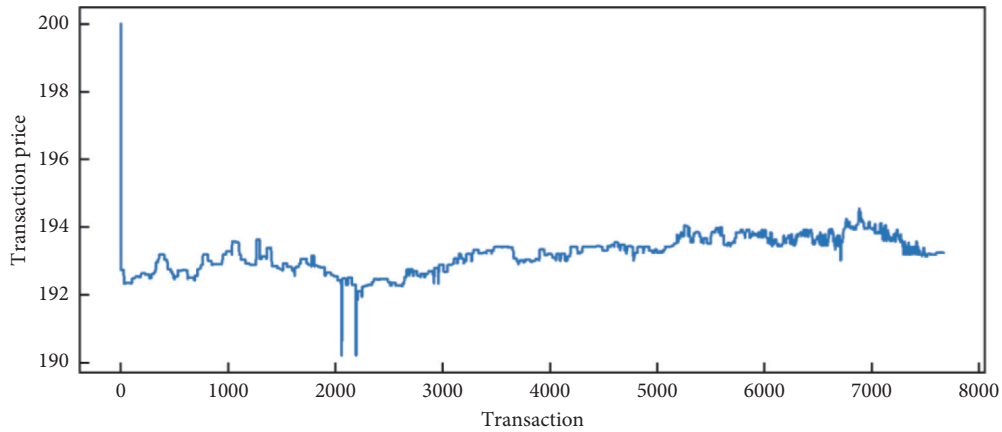

Figure 6: Transaction price when supply exceeded demand.

price at a lower level. Therefore, it can be seen from the table that the buyer income was generally higher than that of the seller. It also indicates that both sides of the transaction can complete the transaction with the help of bidding strategy and obtain good profits.

We assumed that the number of both the buyer and seller was 500, and the reserve prices were $B_i \sim \mathcal{U}(190, 210)$ and $A_j \sim \mathcal{U}(190, 210)$, respectively. The transaction willingness was $\lambda \sim \mathcal{U}(-1, 1)$. Firstly, when the situation was oversupply, the purchase volume and selling volume were taken from $\mathcal{U}(50, 60)$ and $\mathcal{U}(250, 300)$, respectively. Secondly, when the situation was such that the demand exceeded the supply, the buyer purchase was taken from $\mathcal{U}(250, 300)$. The selling volume was from $\mathcal{U}(50, 60)$. The transaction prices are shown in Figures 6 and 7. When the supply exceeded the demand, there almost were 8000 orders. When the demand exceeded the supply, there were more than 8000 orders. From the changes in the transaction prices in two figures, the market can adjust prices flexibly according to the relationship between supply and demand. The transaction price was at a low level at the beginning of the transaction and then was gradually adjusted.

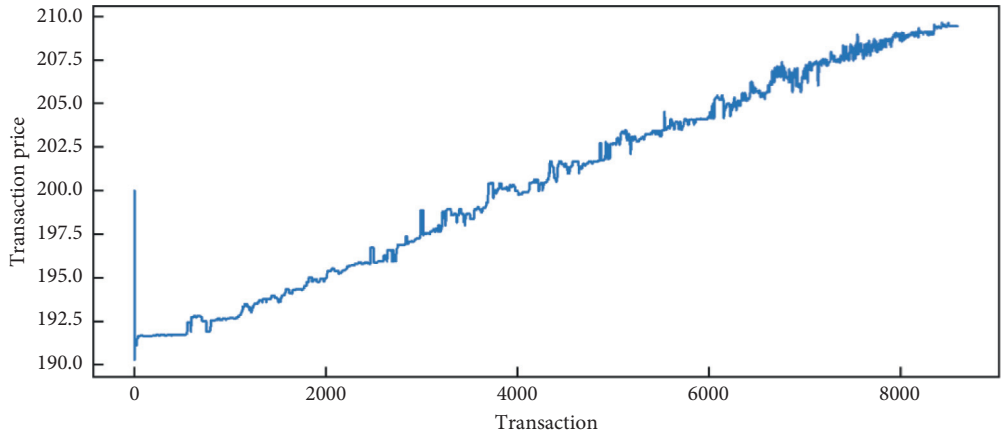

Figure 7: Transaction price when demand exceeded supply.

5. Conclusions

In this paper, we analysed the problems of the REC approval process, inflexible pricing, and low enthusiasm and proposed a hybrid alliance chain REC trading system with off-chain bidding and on-chain trading. We also introduced the detailed operation process of the system, including system initialization, REC issuance, REC sale, REC purchase, bidding transaction, transaction packaging, block consensus, and other operations. According to the characteristics of the system, the view change strategy in PBFT consensus algorithm was changed. We used the CDA to adjust the price of green certificate, formulated the corresponding trading rules, and designed a bidding strategy to maximize the user income and transaction probability. The results show that the price of REC can be adjusted according to the CDA, and the bidding strategy can make both parties obtain considerable profits.

The research in this paper shows that the proposed method can solve the problem of maintaining the consistency and security of the data ledger together by the power grid, platform operators, supervisory review agencies, and distributed entities. At the same time, the green certificate transaction mechanism based on the CDA model proposed in this paper can help the marketization of REC transactions and the healthy development of the green certificate market. Due to the limitation of research focus, some system parameter settings related to business operation have not been studied in depth. In the bidding strategy, we did not consider the number of transactions when orders were submitted, so subsequent research can take transaction volumes into account to obtain higher revenue and can try to use adaptive k which can reflect the market changes better. With the widespread popularity of mobile applications, we will carry out research on the secure data sharing based on BT in mobile-edge computing system.

Abbreviations

REC: Renewable energy certificate
BT: Blockchain technology
CDA: Continuous double auction
MWh: Megawatt-hour
HRECTS-PBC: Hybrid REC trading system based on permissioned blockchain
PK: Public key
SK: Private key
WA: Wallet address
Cert: Certificate.

Data Availability

The experimental data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the State Grid E-commerce Special Technology Funding (1200/2021-72003B).

References

[1] J. Xu and L. Ma, "Application of blockchain technology in distributed energy transaction," *Electric Power Automation Equipment*, vol. 40, no. 8, pp. 17–22, 2020.

[2] T. Romano, T. Mennel, and S. Scatasta, "Comparing feed-in tariffs and renewable obligation certificates: the case of repowering wind farms," *Economia e Politica Industriale*, vol. 44, no. 3, pp. 291–314, 2017.

[3] X. Zhao and X. Wu, "International comparison of tradable green certificates and its enlightenment to China," *Journal of North China Electric Power University*, vol. 1, no. 3, pp. 1–8, 2019.

[4] J. Gu and Y. Lu, "Status analysis on Chinese tradable green certificate market and the optimization of trading mechanism," *Electric Power Construction*, vol. 40, no. 10, pp. 45–55, 2019.

[5] Y. Wang, "Introduction of issuing and voluntary subscription of RECs," *Applied Energy Technology*, vol. 1, no. 12, pp. 15–17, 2017.

[6] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2017, https://bitcoin.org/bitcoin.pdf [Online] Available:.

[7] J. Zhu, Q. Zhang, and S. Gao, "Research progress of blockchain key technologies and their application," *Journal of Taiyuan University of Technology*, vol. 51, no. 3, pp. 321–330, 2020.

[8] Y. Yuan and F. Wang, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[9] J. Wang, Q. Wu, and H. Cao, "Overview of research on typical application of domestic block chain," *Science & Technology and Economy*, vol. 32, no. 5, pp. 1–6, 2019.

[10] L. Liu, J. Feng, Q. Pei et al., "Blockchain-enabled secure data sharing scheme in mobile-edge computing: an asynchronous advantage actor-critic learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2342–2353, 2021.

[11] B. Li, Q. Qin, B. Qi et al., "Design of distributed energy trading scheme based on blockchain," *Power System Technology*, vol. 43, no. 3, pp. 961–972, 2019.

[12] Y. Cai, Y. Gu, G. Luo, X Zhang, and Q Chen, "Blockchain based trading platform of green power certificate: concept and practice," *Automation of Electric Power Systems*, vol. 44, no. 15, pp. 1–9, 2020.

[13] K. Xie, X. Zhang, and S. Zhang, "Application and prospect of blockchain technology in electricity trading," *Automation of Electric Power Systems*, vol. 44, no. 19, pp. 19–28, 2020.

[14] J. Cai, S. Li, B. Fan, and L. Tang, "Blockchain based energy trading in energy Internet," *Electric Power Construction*, vol. 38, no. 9, pp. 24–31, 2017.

[15] B. Wang, Y. Yan, F. Wen, and Lee Mun-Kyu, "A blockchain based distributed power trading mechanism," *Electric Power Construction*, vol. 40, no. 12, pp. 3–10, 2019.

[16] C. Yuan, "Research on the application of blockchain in logistics supply chain," *Service Science and Management*, vol. 8, no. 4, pp. 142–146, 2019.

[17] 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 Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[18] X. Zhang, Z. Chen, and Z. Ma, "Study on electricity market trading system adapting to renewable portfolio standard," *Power System Technology*, vol. 43, no. 8, pp. 2682–2690, 2019.

[19] Z. Shen, S. Chen, and Z. Yan, "Distributed energy trading technology based on blockchain," *Proceedings of the CSEE*, vol. 41, no. 11, pp. 3841–3850, 2020.

[20] Y. Jiang, H. Cao, Y. Li, F Fei, and J Li, Zhemin LIN, Mechanism design and impact analysis of renewable portfolio standard," *Automation of Electric Power Systems*, vol. 44, no. 7, pp. 187–199, 2020.

[21] X. Zhou, Q. Peng, R. Yang, HAN Zhiyong, and WANG Miao, "Power price marketing strategy of comprehensive energy-based electricity sales company participating in electricity market competition under ubiquitous environment of internet of things," *Power System Technology*, vol. 44, no. 4, pp. 1317–1324, 2020.

[22] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5799–5812, 2020.

[23] J. Wang, N. Zhou, Q. Wang, and P. Wang, "Electricity direct transaction mode and strategy in microgrid based on blockchain and continuous double auction mechanism," *Proceedings of the CSEE*, vol. 38, no. 17, pp. 5072–5084, 2018.

[24] D. Chatzopoulos, S. Gujar, B. Faltings, and P. Hui, "Privacy preserving and cost optimal mobile crowdsensing using smart contracts on blockchain," in *Proceedings of the IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 442–450, Chengdu, China, Oct. 2018.

[25] B. An, M. Xiao, A. Liu, G. Gao, and H. Zhao, "Truthful crowdsensed data trading based on reverse auction and blockchain," *Database Systems for Advanced Applications*, vol. 11446, pp. 292–309, 2019.

[26] M. Li, J. Weng, A. Yang et al., "CrowdBC: a blockchain-based decentralized framework for crowdsourcing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 6, pp. 1251–1266, 2019.

[27] Y. Zhang, K. Xu, X. Shi, Wang Haiyang, Liu Jiangchuan, and Wang Yong, "Continuous double auction for cloud market: pricing and bidding analysis," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, pp. 1–6, IEEE, Doha, Qatar, April 2016.

[28] B. Wang, Y. Li, S. Zhao, C. Hao, J. Yi, and D. Yu, "Key technologies on blockchain based distributed energy transaction," *Automation of Electric Power Systems*, vol. 43, no. 14, pp. 53–64, 2019.

[29] S. Zeng, R. Huo, T. Huang, LIU Jiang, Shuo WANG, and Wei FENG, "Survey of blockchain: principle, progress and application," *Journal on Communications*, vol. 41, no. 1, pp. 134–151, 2020.

[30] N. Knezevic, "A high-throughput byzantine fault-tolerant protocol," *IIF, Lausanne, EPFL*, , Tech. Thesis.vol. 163, 2012.

[31] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, pp. 173–186, New Orleans, USA, February 1999.

[32] P. Vytelingum, D. Cliff, and N. R. Jennings, "Strategic bidding in continuous double auctions," *Artificial Intelligence*, vol. 172, no. 14, pp. 1700–1729, 2008.

[33] M. Raberto and S. Cincotti, "Modeling and simulation of a double auction artificial financial market," *Physica A: Statistical Mechanics and Its Applications*, vol. 355, no. 1, pp. 34–45, 2005.

[34] S. Ruder, *An Overview of Gradient Descent Optimization Algorithms*, Cornell University, New York, USA, 2016.