2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) | 978-1-6654-1658-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/TRUSTCOM53373.2021.00218

A Renewable Energy Certificate Trading System Based on Blockchain

1st Ming Gao
State Grid Zhejiang Ninghai Power Supply Co., Ltd.
Zhejiang, China
396455769@qq.com

2nd Xiaokun Yu
State Grid Blockchain Technology (Beijing) Co., Ltd.
Beijing, China
yuxiaokun1@sgec.sgcc.com.cn

3rd Lei Ren
State Grid Zhejiang Ninghai Power Supply Co., Ltd.
Beijing, China
396455769@qq.com

4th Hongxiang Cai
State Grid Zhejiang Ninghai Power Supply Co., Ltd.
Zhejiang, China
396455769@qq.com

5th Zhiyong Wang
State Grid Blockchain Technology (Beijing) Co., Ltd.
Beijing, China
15771341236@163.com

6th Yuyang Zhou
Beijing University of Posts and Telecommunications
Beijing, China
ammo@bupt.edu.cn

***Abstract*—At present, the cumbersome issuing process of renewable energy certificate (REC) and inflexible pricing mechanism consume a lot of manpower and material resources. In order to solve this problem, this paper proposes a hybrid REC trading system based on Consortium Blockchain. The paper introduces the operation mode of the system in detail and changes the view replacement protocol in the Practical Byzantine Fault Tolerance (PBFT) Algorithm to improve the stability of the system. It also introduces the bidding rules of Continuous Double Auction (CDA) used in the system, and designs the bidding strategies to maximize the user's profit and the success rate of transaction. Finally, ARIMA model is also used to forecast the price of RECs to provide guidance for both buyers and sellers.**

***Index Terms*—REC transaction, Consortium Blockchain, Continuous Double Auction, ARIMA**

I. Introduction

Renewable energy Certificate (REC) is an electronic certificate issued by the state to renewable energy producers that meet the requirements. China started the voluntary subscription policy of REC in 2017. According to *The Medium and Long-Term Development Plan for Renewable Energy*, the proportion of renewable energy in total energy consumption should reach more than 15% by 2020. The purchase of RECs is an important way for renewable energy consumers to achieve this goal. From the experience of other countries, REC trading can indeed promote the energy structure and support the development of renewable energy in a more market-oriented mean.

Since China started the voluntary subscription of RECs, the situation is not optimistic. The paper introduces the approval and issuance process of RECs. The issuance of RECs needs to be examined by various departments after the enterprise submits relevant materials. This way consumes a lot of manpower and material resources. The process is cumbersome, inefficient and prone to human errors. Most of the REC transactions are listed on the trading platform. The information that both parties get is not equal, and the listing sales can not better reflect the market demand, which makes the price of RECs unable to adjust in time with the market changes. Therefore, it is very important to design an efficient REC issuing and trading system.

Satoshi Nakamoto first proposed blockchain technology in his literature. With the rise of bitcoin and other cryptocurrencies, people realize the potential value of blockchain technology in other fields, especially in the field of energy trading. The blockchain technology is used in the market-oriented distributed transaction of power, and help construct the transaction mechanism, settlement mechanism, reward and punishment mechanism. The issuance and transaction of RECs can also be carried out on the blockchain. With the traceability and unforgeability of blockchain data, the audit of data will become easier, and the efficiency of REC issuance will be improved. In addition, decentralization makes the system more robust without worrying about data loss.

Double Auction (DA) is a process in which multiple buyers and sellers bid to buy and sell goods. Continuous Double Auction (CDA) enables buyers and sellers to adjust their bids in real time, which can better reflect market demand and has higher efficiency. CDA has been widely used in stock, futures and other market-oriented transactions. This paper proposed a bidding strategy to maximize the interests of buyers and sellers. The market can adjust the price, improve the relationship between supply and demand, and activate the trading market. CDA has high requirements for real-time performance, but blockchain is difficult to meet its requirements. We propose a Hybrid REC Trading System based on Consortium blockchain (HRECTS-CBC), which utilizes the advantages of blockchain and CDA.

ARIMA model is used to predict the price in the system. ARIMA, also known as ARIMA (p, d, q), is one of the most common statistical models used for time series prediction.

2324-9013/21/$31.00 ©2021 IEEE
DOI 10.1109/TrustCom53373.2021.00218

II. The Model and Method

A. System Construction

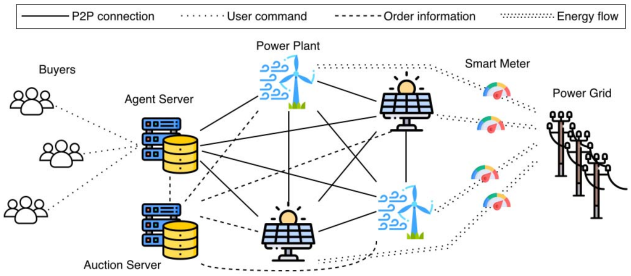

Fig. 1. HRECTS-CBC System Structure

The structure of HRECTS-CBC trading system proposed in this paper is shown in Figure 1. In the figure, the power plant and agent server are nodes in the network. They are connected to form a blockchain system. The seller and the buyer publish the order information on the auction server. When the price is agreed, the RECs are traded in the form of the smart contract. Individuals, organizations and enterprises can only act as buyers and use proxy servers as agents for transactions. Smart meter records the power consumption the amount of energy production for each power plant. The smart contract automatically checks the power generation and distributes the RECs.

At present, the most successful application of blockchain is bitcoin. Based on the development of public chain, it has the advantages of completely open, decentralization and preventing data tampering, but it is not suitable for the current business. The first is that renewable energy power plants are qualified for network access only after they are approved by authoritative institutions (such as the government), which does not meet the characteristics of the completely open public chain. The second is that nodes in the public chain will not trust each other. They keep accounts after using mechanisms such as proof of work (POW) to reach consensus, which not only causes a lot of waste of computing power and other resources, but also leads to low transaction efficiency. At present, it takes about 10 minutes to generate a new block, which means that it takes 10 minutes for a transaction to be confirmed by the whole network.

Consortium Blockchain is a technology to form a network between authorized nodes. The simulation experiment shows that the confirmation time of Consortium Blockchain using the practical Byzantine Fault Tolerant algorithm (PBFT) is less than 1s, and the throughput can reach 50K transactions per second. Although the performance will be reduced in the real complex situation, it can still meet most of the transaction situation, so this paper uses the Consortium Blockchain to build the chain trading system.

B. Mode of Operation

The operation of the system includes system initialization, REC issuing, sales of RECs, purchase of RECs, bidding transaction, transaction packaging and block consensus. Table I illustrates the mathematical symbol.

TABLE I
Variable Description

Symbol	Definition
ID_i	The identification for energy plant when registering
PK_i	Public key for energy power plant or seller i
SK_i	Private key for energy power plant or seller i
WA_i	Wallet address for energy power plant or seller i
$Cert_i$	Certificate for energy power plant i
$SMID_i$	Smart meter ID
$REC_{j,rid,...}$	The REC whose ID is rid and be sold by seller j
P_{ask}	Selling unit price
P_{bid}	Purchase unit price

System Initialization: The renewable energy power plant will receive the identification ID_i after audit, and the power plant can join the chain system by registering in the transaction information release module. When joining the chain system for the first time, the system will assign public key (PK_i), private key (SK_i), wallet address (WA_i), certificate ($Cert_i$), among which the certificate includes the basic information of the power plant, such as company name, address, installed capacity, smart meter ID ($SMID_i$), etc. After distributing the above information, the new power plant node downloads the account book through the surrounding nodes, and becomes the node in the network after synchronization. After the buyer completes the registration in the transaction information publishing module of the proxy server, the system assigns the public key, private key and wallet address to the buyer. The user can log in to the system with the public key and his own password.

REC Issuing: The Smart Contract of REC issuing on the chain runs regularly. The REC issuing module issues the REC for the power plant by calculating the data of the smart meter and other necessary information. According to the regulations, a REC is issued for 1MWh. The smart contract issues the REC to the wallet address of the power plant in the form of transaction. Each renewable energy certificate can be expressed as follow.

$$REC = \{ID, t, c, m\} \tag{1}$$

In which ID is the number of REC, t is the issuing time, c is the type of green power, the identification of wind power, photoelectric and other types. m is some additional information, including the enterprise, project number and other information.

Sales of RECs: The power plant will pledge the RECs in the smart contract, mark the selling price, and send it to the trading smart contract address and the trading information release module. The message can be expressed as follow.

$$sellOrder =< (REC_{j,rid...}), P_{ask}, t > \tag{2}$$

In which $(REC_{j,rid...})$ is the REC whose ID is rid and that be sold by seller j. P_{ask} is the selling price, t is the time of registration. At the same time, the order information and digital signature, that is, $< sellOrder, sign_{SK_j}(MD5(sellOrder)) >$ will be sent to the bidding server under the chain. The bidding management module in the bidding server will render it and return it to the user through the front-end.If all the RECs are not sold successfully after a period of time, the smart contract will return the remaining RECs to the seller.

Purchase of RECs: The buyer publishes the purchase price and quantity in the transaction information release module, and pledges the required currency in the bidding transaction smart contract, which expressed as follow.

$$buyOrder =< P_{bid}, d, Coin, t > \tag{3}$$

In which P_{bid} is purchase unit price, d is the purchase quantity, $Coin = P_{bid} * d$ is the amount of currency pledged to the contract, and t is the registration time. The order information and digital signatures are sent to the bidding server under the chain, that is, $< buyOrder, sign_{SK_i}(MD5(buyOrder)) >$. The bidding management module on the bidding server renders it and returns it to the user through the front-end. If sufficient RECs cannot be purchased after a period of time, the smart contract will return the remaining currency to the buyer.

Bidding Transaction: The system uses CDA mechanism in matching module to match the buyers and sellers under the chain. The traditional client-server mode is adopted in the bidding system. The auction and transaction rules can be designed according to the actual demand, which can refer the stock and futures trading system. The successful matching transaction is represented by the order and digital signature of both parties as follow.

$$\begin{aligned} matchedOrder = < sellOrder,& \\ & sign_{SK_j}(MD5(sellOrder)), \\ & buyOrder, sign_{SK_i}(MD5(buyOrder)) > \end{aligned} \tag{4}$$

The bidding server will update the transaction information after sending $matchedOrder, sign_{SK_{as}(MD5(matchOrder))}$ to the proxy server, in which SK_{as} is the private key of the bidding server. The proxy server will send the information to the smart contract in the blockchain. After the smart contract verifies the validity of the transaction information, it will use the pledged currency and RECs of both parties for transactions.If the RECs of the seller can not be completely sold in this transaction, the smart contract will generate a new order with the same price for the remaining RECs, and give a new time stamp for publishing. If the buyer can not purchase enough RECs in this transaction, the smart contract will generate a new order with a new time stamp for the remaining currency and the required number of RECs.

Transaction Packaging: The master node collects all the transactions generated in a period of time, locally verifies the validity of the transactions, and then packages them into a block. Similar to Bitcoin block, a block includes a block header and a block body. In the block body, transaction information is stored in the form of Merkle tree. In addition, the block header also includes the hash value, version, timestamp of the previous block. We do not use workload proof, so the block header does not need to contain random numbers.

Block Consensus: PBFT is used as the consensus mechanism. In PBFT, when the primary node fails, the view is updated according to the view replacement protocol, that is, a new primary node is selected. The master node is responsible for generating blocks and leading consensus, so it should have higher stability and performance. The proxy 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 and run by a professional team. Therefore, it has higher stability and performance than the machines in the power plant, and is less likely to be manipulated maliciously.

Considering the above situation, we decided to change the policy of view replacement protocol. We set the number of the proxy server in the blockchain system on the chain to 0, and the other nodes are numbered as $1, 2, ..., N - 1$. The way to generate the master node is: $p = ((v \bmod 2)\lceil v/2 \rceil) \bmod N$, where mod is the modular operation, $v \in N$ is the number of the new view and $v = v_{pre} + 1$. v_{pre} is the number of the previous view, $\lceil \quad \rceil$ is the rounding up operation, and p is the new master node.

When the current master node is 0, if the trigger condition of the original PBFT view replacement is met, the new master node is selected by the above formula to replace the view. When the current master node is not 0, if the trigger condition of the original PBFT view replacement is met, or when the master node receives the confirmation message from the 0 node in the commit phase of the k consecutive consensus process, the new master node is selected according to the above formula to change the view. Except for the way of selecting the master node, other operations in the view replacement protocol remain unchanged. In order to make the system run in an efficient state, we let the proxy server node act as the main node most of the time, which will greatly increase the stability of the system, and also reduce the burden of the power plant machine.

The platform operation mechanism is shown as Figure 2.

III. Price Forecast of RECs

The price forecast of RECs can provide some advice for producers and buyers when they trade RECs. REC price forecasting is a process of quantitative analysis of energy market. At present, the main research methods are modern statistical methods, such as time series analysis, trend extrapolation, exponential smoothing and artificial intelligence methods. Among various quantitative analysis methods, time series analysis is the most classic one. When building a time series model, we first extract the historical trading price of RECs as a series, then put the data into the model, and finally train the model, and use the trained model to predict the future REC price. This paper selects the price of RECs in recent 2

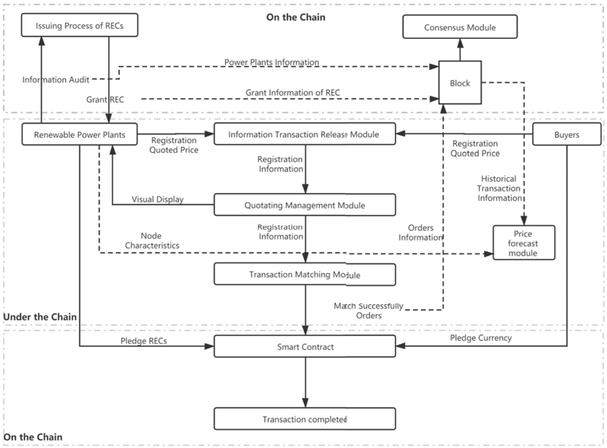

Fig. 2. Mode of Operation

years, through the ARIMA model to predict the trend of REC price, to study the short-term change rule of REC price.

A. Introduction of ARIMA

ARIMA Model (Auto Regressive Integrated Moving Average Model) is constructed by Auto Regressive Model and Moving Average Model. The formula of Auto Regressive is shown as follow.

$$y_i = \mu + \sigma_{i=1}^{p}\gamma_i y_{t-i} + \theta_t \tag{5}$$

In which y_i is the current value, p is the auto regressive Order, γ_i is coefficient of auto correlation, θ_t is the error term that is independent and identically distributed.

The auto regressive model describes the relationship between the current value and the historical value of the series, that is, the historical data, as an independent value, is used to predict the future. The auto regressive model needs the stationary series as the training data. Moving Average Model (MA) is illustrated as follow.

$$y_i = \mu + \sigma_{i=1}^{q}\epsilon_i\theta_{t-i} + \theta_t \tag{6}$$

For Moving Average model, it mainly deals with the error term in the autoregressive model. By accumulating the error term, the Moving Average can better predict the random fluctuation in the error term. The input of ARIMA model should be non-stationary data, and I represents the difference. The non-stationary data is differentiated and transformed into stationary data. The three parameters of ARIMA model are p, q and d. p is the order of autoregression, q is the number of moving average terms, and d is the difference times when non-stationary data is transformed into stationary data.

ARIMA model has the following properties about autocorrelation coefficient and partial autocorrelation coefficient in Table II. PACF is used to determine the order of AR model, that is p. ACF is used to determine the order of MA, that is q.

TABLE II
ORDER PROPERTIES OF ARIMA MODEL

Model	ACF	PACF
$AR(p)$	Reduce to 0	Truncate after order p
$MA(q)$	Truncate after order q	Reduce to 0
$ARMA(p,q)$	Reduce to 0 after order q	Reduce to 0 after order p

When estimating the parameters of ARIMA model, we could refer to the above properties. When p and q satisfy the above description in ACF diagram and PACF diagram, it can be considered that this parameter is more suitable for ARIMA model, and truncation means falling into the confidence interval.

B. Data acquisition and preprocessing

We obtained the price of RECs from August 2018 to August 2020 through China REC Subscription Trading Platform. Because the subscription of RECs has not been popularized in China, the amount of data is small and the data is discrete. In order to make the price data series more in line with the time series input of ARIMA model, we calculate the transaction price of RECs weekly.

First of all, the paper tests the stationarity of the data. By observing Figure 3, we can see that the moving average and standard deviation of the data are relatively stable.

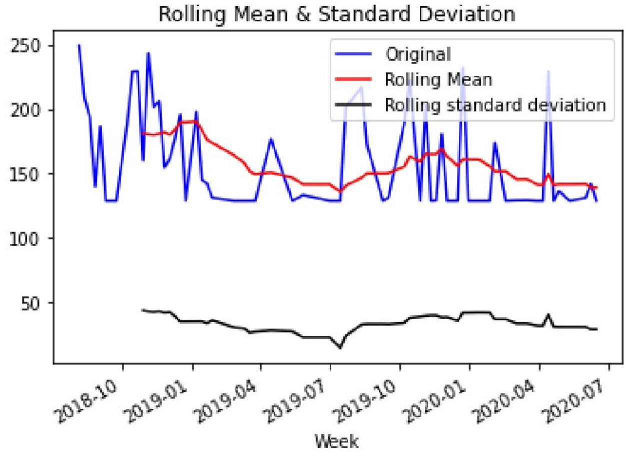

Fig. 3. The Moving Average and Standard Deviation of REC Price Data

Then the paper test the stationarity by Dickey-Fuller Test. In statistics, the Dickey–Fuller Test tests the original hypothesis that a unit root is present in an autoregressive model. In this experiment, we assume that the REC price data is unstable. Table III shows the result of Dickey-Fuller Test.

The value of $p-value$ is very small, so we can reject the original hypothesis of Dickey–Fuller Test and think that the price data of RECs is stable. So we can use these data for ARIMA model.

After checking the stability of the data, we need to determine the order of the model, that is, to determine p and q.

TABLE III
THE RESULT OF DICKEY-FULLER TEST

Test Statistic	-6.534065e+00
p-value	9.707336e-09
Number of Observations Used	6.400000e+01
Critical Value (1%)	-3.536928e+00
Critical Value (5%)	-2.907887e+00
Critical Value (10%)	-2.591493e+00

Figure 4 is the ACF and PACF of price data. We find that both autocorrelation coefficients and partial autocorrelation coefficients are tailed, and they have obvious first-order correlation, so we set $p = 1$, $q = 1$.

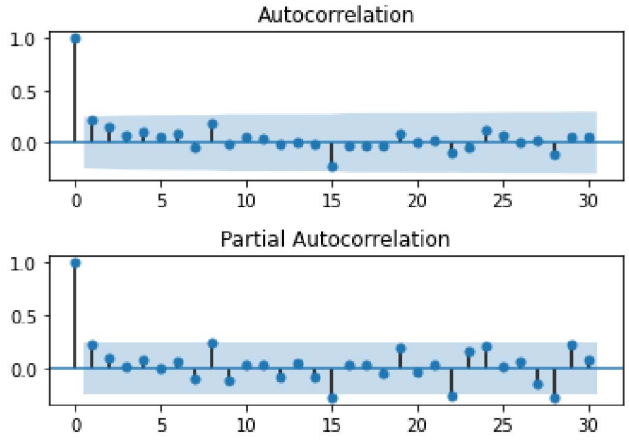

Fig. 4. ACF and PACF of RECs Price Data

Finally, we use ARIMA model to fit the historial price and predict future price. We use root mean square error (RMSE) to evaluate the effectiveness of the model. Figure 5 shows the original price curve and prediction price curve. This paper also uses the model to forecast the REC price in the future.

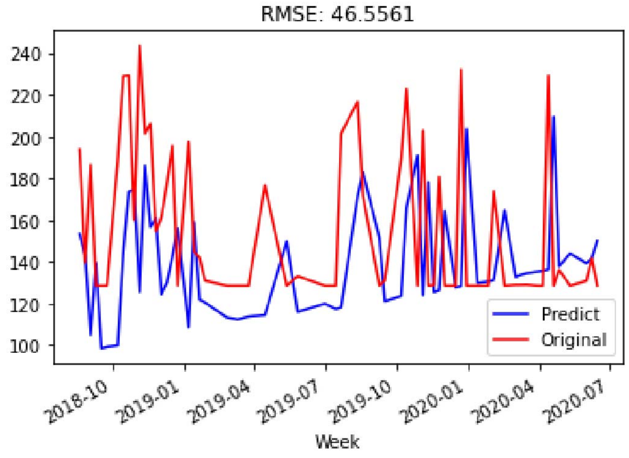

Fig. 5. The original price curve and prediction price curve

IV. CONCLUSION

The current renewable energy certificate (REC) issuance process is cumbersome. Pricing is not flexible, and users are not actively involved, based on this, a hybrid Consortium Blockchain REC trading system is proposed. The paper introduces the detailed process of the system operation, including system initialization, REC issuing, sales of REC, purchase of REC, bidding transaction, transaction packaging, and block consensus. According to the characteristics of the system, the paper changes the view replacement protocol in PBFT algorithm. We use continuous double auction to adjust the price of RECs, establish the trading rules, and predict the future price of RECs through ARIMA model. Experiments show that ARIMA model can better fit the REC price trend and predict the future price.

Due to the limitation of time and data volume, some details about the system are not considered. Developers can design based on the real business according to this paper. In the process of REC price prediction, we did not consider the characteristics of blockchain nodes, such as the price and the quantity of RECs in the past n times, the number of remaining RECs, the recent power generation of nodes, etc. Therefore, the follow-up research work can take the characteristics of blockchain nodes into account to better predict the future price of RECs, and then better guide the bidding strategy. All the above are for future research.

REFERENCES

[1] Q. Kong, F. Yin, R. Lu, B. Li, X. Wang, S. Cui, P. Zhang, "Privacy-Preserving Aggregation for Federated Learning-Based Navigation in Vehicular Fog," IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3075683.

[2] Q. Kong, R. Lu, F. Yin, S. Cui, "Blockchain-Based Privacy-Preserving Driver Monitoring for MaaS in the Vehicular IoT," IEEE Transactions on Vehicular Technology, vol. 70, no. 4, pp. 3788-3799, April 2021.

[3] Y. Xu, F. Yin, W. Xu, J. Lin and S. Cui, "Wireless Traffic Prediction With Scalable Gaussian Process: Framework, Algorithms, and Verification," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1291-1306, June 2019.

[4] F. Yin et al., "FedLoc: Federated Learning Framework for Data-Driven Cooperative Localization and Location Data Processing," IEEE Open Journal of Signal Processing, vol. 1, pp. 187-215, 2020.

[5] F. Yin, C. Fritsche, F. Gustafsson, A. M. Zoubir, "TOA-Based Robust Wireless Geolocation and Cramér-Rao Lower Bound Analysis in Harsh LOS/NLOS Environments," IEEE Transactions on Signal Processing, vol. 61, no. 9, pp. 2243-2255, May1, 2013.

[6] M. H. Eiza, Y. Cao, L. Xu, "Towards Sustainable and Economic Smart Mobility: Shaping the Future of Smart Cities," World Scientific, London, 2020.

[7] X. Zhang, Y. Cao, L. Peng, N. Ahmad, L. Xu, "Towards Efficient Battery Swapping Service Operation Under Battery Heterogeneity," IEEE Transactions on Vehicular Technology, vol.69, no.6, pp.6107-6118, June 2020.

[8] G. Cui, X. Li, L. Xu, W. Wang, "Latency and Energy Optimization for MEC Enhanced SAT-IoT Networks," IEEE Access, vol. 8, pp. 55915-55926, 2020.

[9] L. Xu, et al. "Telecom big data based user offloading self-optimisation in heterogeneous relay cellular systems," International Journal of Distributed Systems and Technologies, 8(2), pp. 27-46, April 2017.

[10] Scatasta Sara, Mennel Tim. Comparing feed-in-tariffs and renewable obligation certificates-the case of wind farming [J]. Preliminary version. 2009.

[11] Nakamoto Satoshi. Bitcoin: A peer-to-peer electronic cash system [R]. 2019.