Research on Green Electricity Certificate Trading Based on Alliance Blockchain

Bo Ning[1], Hao Zhang[1], Junhong Guo[1], Shengnan Zhang[2], Zhen Liu[1], Qianxin Ma[3*]
973376984@qq.com, 1431185715@qq.com, 13349009652@163.com, BBiika@163.com, 1305220192@qq.com, *maqianxin57@163.com

[1]Jibei Power Exchange Center Co, Ltd Beijing, China,

[2]Beijing Power Exchange Center Co, Ltd Beijing, China,

[3]School of Economics and Management North China Electric Power University Beijing, China

Abstract—To further promote the healthy development of renewable energy and enhance the credibility and traceability of the renewable energy consumption process, this paper proposes a green electricity certificate transaction matching and circulation model based on blockchain. With the advantages of blockchain, such as equality and mutual trust, non-tampering, openness, and transparency, the issuance and transaction process of green electricity certificate can be completely recorded on the blockchain, which can effectively reduce the cost of trust between users, simplify the traceability and audit of green electricity certificate, and improve the transaction and circulation efficiency of green electricity certificate.

Keywords-green electricity certificate; blockchain; transaction matching; smart contract

1 INTRODUCTION

Aiming at the interactive consumption and value certification of the virtual power plant and green energy, it is urgent to break through the green value traceability technology that satisfies the participation of virtual power plant, realize the evaluation and traceability of green value, and ensure the credible collection and transmission of green energy production data [1]. Based on blockchain technology, all renewable energy consumed by virtual power plants can be traced back to green. The value of flexible resources of virtual power plants can be matched with point-to-point renewable energy consumption [2].

2 GREEN ELECTRICITY CERTIFICATE AND BLOCKCHAIN

2.1 Green electricity certificate

China's industrial support for renewable energy mainly depends on financial subsidies [3]. However, with the continuous expansion of the scale of new energy, subsidies for renewable energy are unsustainable, and the funding gap for new energy subsidies is increasing. To improve green power consumption, promote new energy consumption, and coordinate

ICICA 2022, December 02-04, Chongqing, People's Republic of China

DOI 10.4108/eai.2-12-2022.2328048

environmental pollution, China has introduced a green electricity certificate system and established a long-term mechanism for renewable energy development [4].

2.2 Introduction of Blockchain Technology

Blockchain technology originates from a cryptology-based digital currency bitcoin. It is a decentralized electronic accounting technology that shares information in distributed nodes. In the accounting system using blockchain technology, every transaction recorded is broadcast to everyone, and everyone's books are public. By using cryptographic methods to package a specific number of bills into blocks, and then linking these different blocks in chronological order, a blockchain containing a large amount of bill information is formed [5]. All nodes in the blockchain network are involved in the maintenance of the system [6].

2.3 Alliance Blockchain Enables Green Certificate Trading

The blockchain network links all parties involved in the issuance and trading of green certificates in a distributed manner to build an environment of equality and mutual trust, thereby completing the full life-cycle management of green certificates, ensuring the transparency and non-tamperability of all parties' data, solving the problem of anti-counterfeiting and traceability of green certificates, and enhancing the credibility of green certificates.

3 GREEN ELECTRICITY CERTIFICATE TRANSACTION MATCHING AND CIRCULATION MODEL BASED ON BLOCKCHAIN

The model of green certificate transaction matching and circulation based on blockchain is shown in Figure 1, which aims to match buyers and sellers to complete green certificate transactions in a fast, safe and credible way.

This paper studies the way of blockchain solves the defects of traditional centralized transaction matching systems, and puts forward the matching and circulation model of green certificate transactions based on blockchain, which makes the transaction directly face the buyers and sellers of the green certificate, and automatically completes the matching and ownership transfer of green certificate by smart contract [7], without the participation of intermediaries, effectively reducing the intermediate links and improving the processing efficiency and credibility in the transaction process. The sequence number in Figure 1 represents the process order of the model.

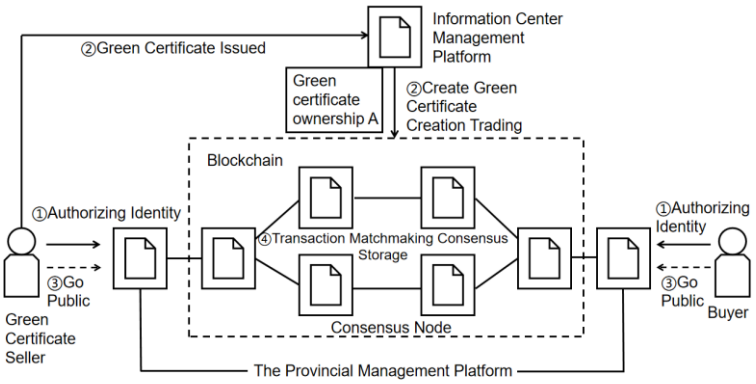

Figure 1. Green certificate trading matching and circulation model based on blockchain

1)The seller and buyer of green certificates first need to complete unified identity authentication on the blockchain to ensure the authenticity, integrity, and non-repudiation of the green certificate issuance and trading process, while reducing the authentication cost of the trading subject.

2)The Seller may apply to the Information Center Management Platform for green certificate issuance at any time. The information center management platform uses the grid metering equipment to complete the verification of renewable energy power and issue the green certificate to the applicant. The green certificate issued will be stored as a creation transaction on the chain consensus, and its information can indicate the current institution or user of the green certificate.

3)The seller and the buyer of the green certificate can submit the electricity sale order and the electricity purchase order to the provincial management platform for listing. The power selling order includes the number of green certificates, power type, project information, quotation, and other information. The power purchase order includes information such as the number of green certificates expected to be purchased, the budget amount, and the type of electricity.

4)The blockchain will regularly elect transaction matchmaking nodes, and the matchmaking nodes will match the current order to complete the matching of green card transactions. The results of the green certificate transactions will be agreed upon across the network, and the transaction settlement and transfer of ownership of the green certificate will be automatically completed by the smart contract and recorded on the blockchain distributed ledger.

4 RESEARCH ON KEY TECHNOLOGIES

4.1 Unified identity authentication based on blockchain

In the blockchain, the user uses the public and private key pairs (P_k, S_k) in the asymmetric cryptographic algorithm to represent the identity, and the registration authority (RA) sends the public key representing its identity to the blockchain through the smart contract. The blockchain's public key is stored through the blockchain consensus and cannot be tampered

with, so identity authentication has strong credibility. At the same time, because the blockchain is a distributed system, it can also effectively avoid problems such as system paralysis caused by a single point of collapse, and loss of user identity data caused by malicious attacks, and enhance the stability and reliability of the system.

4.1.1 User Identity Registration

The information center is faced with the problems of heavy workload and difficulty in authentication when the green certificate seller and the purchaser are authenticated. With the help of distributed qualification examinations, the workload can be dispersed to various places, and the provinces can complete the certification of their jurisdictions. The provincial management platform acts as RA to complete the user's real-name authentication and chain the user's public key. The blockchain does not store the user's real name information, but stores the public key representing the user's anonymous identity, and finally realizes anonymous and trusted unified identity sharing among the peer nodes of the blockchain. The specific user identity registration process is shown in Figure 2.

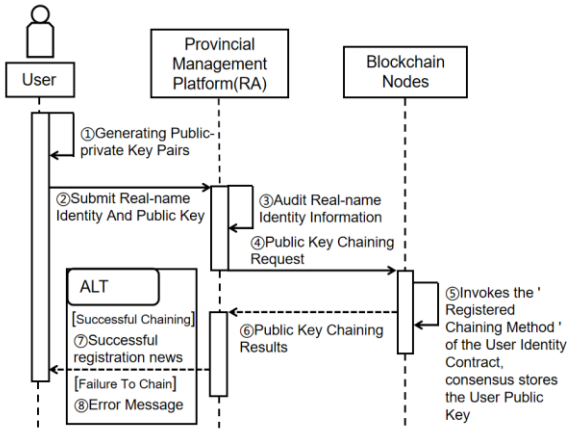

Figure 2. User identity registration timing process

1)Users use relevant registration tools to generate user public and private key pairs (P_k,S_k) representing their identity.

2)Users sign their authentication-related material information and public key and submit them to the provincial management platform.

3)After the provincial management platform receives and verifies the identity registration request submitted by the user, the submitted real-name information is reviewed.

4)After the audit is passed, the provincial management platform encapsulates the user's public key P_k into a public key chaining request and signs the request with its private key.

5)Each blockchain node receives a public key on-chain request, triggers the user identity contract call, verifies the provincial RA signature, and consensus stores the public key.

6)The provincial management platform returns the registration result to the user according to the execution of the blockchain node. If the blockchain node is successfully executed, the registration is successfully returned, otherwise, the corresponding error information is returned.

4.1.2 User authentication

The user's public key stored in the blockchain trusted storage will be used to verify the signature of the user's operation to ensure that the operation is indeed issued by the user, and the user himself cannot deny it. The user authentication timing process is shown in Figure 3, including three stages: user signature, public key query, and signature verification.

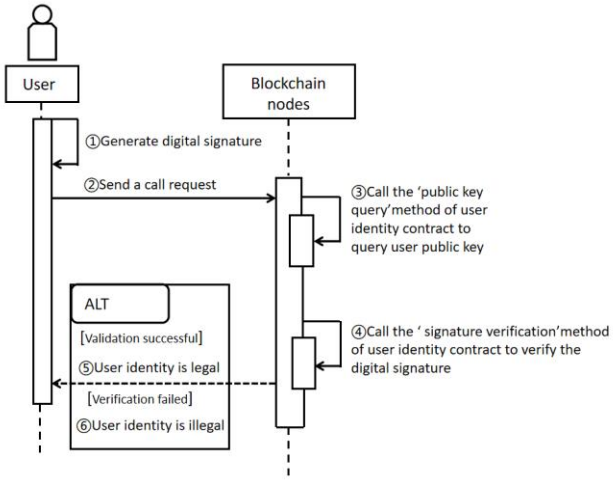

Figure 3. User authentication timing process

1)The user signs the original data m and the public key P_k using the private key S_k to obtain a digital signature for the current operation.

2)The user sends the public key P_k, the original data *m*, and the obtained signature *sig* to the blockchain node.

3)Invoke the registration chain method of the user identity contract, and the blockchain node queries the ledger for the existence of the corresponding user public key P_k. If it does not exist, the user identity is illegal.

4)By calling the signature verification method of the user identity contract, the blockchain node uses the user's public key P_k and the received raw data *m* to verify whether the user's signature *sig* is correct, and if the verification is passed, the user's identity is considered legal.

4.2 Transaction matching model

4.2.1 Matching node selection

Trade matching, as a timing task, is proactively triggered by only one node in the blockchain (the matching node) at any one time. To avoid a single point of failure and ‘ central authority ’, the matching node is not always held by a certain node but is determined by a specific node rotation method. The rotation time interval is *t*. Considering that the matching process is not particularly frequent, *t* can be measured in minutes. In each rotation interval, each node calculates the next time to initiate a matching transaction *e* and the matching node serial number *d* according to the recorded last transaction matching time *s*. Due to the influence of network factors, it is difficult to ensure the real-time consistency of s recorded in each node’*s* ledger. Therefore, the next transaction matching time *e* cannot be simply obtained by way $\mathrm{e} = s + t$, but should use the system time *c* (the error with the standard time is $\triangle t$ and $\triangle t \ll t$) and be calculated by the following formula :

$$\begin{aligned} &\mathrm{e} = \min(\{x > c \mid x = s + kt, k_i \in N_+\}) = \\ &\left\{\begin{matrix} c + t - c \bmod t, (t - c \bmod t) > \triangle t \\ c + 2t - c \bmod t, (t - c \bmod t) \le \triangle t \end{matrix}\right\} \end{aligned} \tag{1}$$

Although different nodes *s* and *c* will lead to different values of k_i, the time point of transaction matching is determined in the form of *t*, *2t*, *3t*, and the time error of each node is kept in a small range, which can ensure the consistency of the matching time *e* calculated by Equation (1).

When calculating the serial number *d* of the matching node, assuming that the list of surviving nodes in the current system is *a*, the total time required for the node to complete a round of transaction matching is $len(a) \times t$, where $len(a)$ represents the number of nodes in the surviving list *a*. Therefore, $e \bmod (len(a) \times t)$ can be used to calculate the proportion of matching time *e* in a round of transaction matching, and then get the matching node serial number *d*, that is:

$$d = \frac{e \bmod (len(a) \times t)}{t} \tag{2}$$

For example, in a system, the node list is P, the number of nodes in P is 4, the rotation time of each node is 2s, the total time required for the node to complete a round of transaction matching is 4*2=8s, and the matching time is 4 seconds. Then the node number can be calculated as:

$$d = \frac{4 \bmod 8}{2} = 2$$

4.2.2 Trade matching process

For the convenience of describing the transaction matching process, it is assumed that the number of entrusted orders of the buyer and the seller is *M* and *Q*, respectively, and the buyer**’**s entrusted form is $b(I_b, n_b, p_b, t_b)$, where I_b is the buyer**’**s identity; n_b and p_b are the quantity and quotation of the green certificate to be purchased by the buyer; t_b is the creation time of the buyer**’**s order. The seller entrusts a simplex such as $s(I_s, n_s, p_s, o, t_s)$, where I_s is the seller**’**s

identity; n_s, p_s, o are the number, quotation, and the number of green certificates that the seller wants to sell; t_s is the seller's order creation time. The specific steps include 4 steps.

1)Delegate single queue creation. Buyers and sellers entrust a single order in order according to the quotation from high to low (the seller according to the quotation from low to high), entrust time from early to late, the number of the green certificate from less to more were placed in the buyer entrust a single queue and seller entrust a single queue. Assume that the buyer delegates a queue $B\ (b_1,b_2,b_3,b_4)$ and the seller delegates a queue $S\ (s_1,s_2,...,s_Q)$.

2)Delegate single queue matching. For the buy-seller order $b_i\ (I_{bi}, n_{bi}, p_{bi}, t_{bi})$ and $s_i\ (I_{sj}, n_{sj}, p_{sj}, o, t_{sj})$, if $p_{bi} \geq p_{sj}$, then I_{bi} and I_{sj} are considered to reach a transaction intention; otherwise, it indicates that the current delegated single queue cannot match, and the buyer and the seller can adjust the offer and wait for the next transaction match.

3)Delegate single queue adjustment. For I_{bi} and I_{sj}, the green certificate trading volume $v=min(n_{bi},b_{sj})$. If $n_{bi}>n_{sj}$, the order of I_{sj} is removed from the seller's order queue, and the number of green certificates n_{bi} that I_{bi} wants to buy is adjusted $n_{bi}-n_{sj}$; if $n_{bi}>n_{sj}$, I_{bi}'s order is moved out of the buyer's order queue, and the number of green certificates to be sold by I_{sj} is adjusted to $n_{sj}-n_{bi}$, and the corresponding green certificate number o is adjusted. If $n_{bi}=n_{sj}$, the delegate orders for I_{bi} and I_{sj} are moved out of the corresponding delegate order queue.

4)Order pricing. For I_{bi} and I_{sj}, whose trading intentions are reached, the green certificate transaction price is mainly determined in the form of a second-price sealed auction. Assuming that I_{bi}'s subsequent order is $b_{i+1}(I_{bi+1}, n_{bi+1}, p_{bi+1}, t_{bi+1})$, if $p_{bi+1} \geq p_{sj}$, the transaction price is p_{bi+1}; if $p_{bi+1} < p_{sj}$, the transaction price is $(p_{bi}+p_{sj})/2$. In addition, if I_{bi} is the last person in the buyer's order queue, the transaction price is also $(p_{bi}+p_{sj})/2$. When the transaction is completed on both sides of the order pricing, if the buyer and seller order queue is not empty, then re-execute 2).

4.3 Smart Contract Design

For the processes of user identity authentication, green certificate issuance, and matching transactions, it is necessary to write user identity contracts, green certificate issuance, transaction matching, and query contracts, and deploy them on the blockchain.

4.3.1 User Identity Contract

The contract serves as the trust foundation for the platform and provides user identity chaining and validation, including the Register Identity, Query Identity, and Verify Signature functions.

When a user's identity is chained, the provincial management platform calls Register Identity to upload the user's public key to the blockchain. In the process of authentication, it is necessary to call Query Identity to query whether the corresponding user public key exists on the chain. If it exists, Verify Signature is continued to be called to verify whether the digital signature is correct by using the user's public key.

4.3.2 Green electricity certificate issuance contract

The contract is for power generation users and includes the Issue Green Certificate function. When the power generation user applies for the green certificate, it is necessary to call the Issue

Green Certificate to upload the declaration data. The function first uses the user identity contract to verify the user identity; then create a corresponding number of green certificates according to a certain proportion, and uses the hash function to generate a unique certificate number for each green certificate; finally, the green certificate and user identity are bound and coexisted in the blockchain.

4.3.3 Green Electricity Certificate Trading and Circulation Contracts

Green certificate transaction includes three stages: transaction listing, transaction matching, and transaction liquidation.

1)Trading listing stage. This stage is aimed at the buyers and sellers of green certificate transactions and provides the management function of the commission order, including the commission order creation function (Create Order), the commission order update function (Update Order), and the commission order revocation function (Delete Order). These functions verify the user's identity when executed. Buyers and sellers upload their delegate order information through the Create Order, which creates a unique delegate number for each delegate order through a hash function and binds the delegate order to the user identity.

2)Trade matching stage. This phase is implemented by the Create Order Queue function, the Match Order Queue function, the Adjust Order Queue function, and the Fix Order function according to Section Trade matching process. The method cannot be directly called by external users but is triggered by the blockchain node.

3)transaction settlement stage. This stage only includes the settlement function. The buyer's user completes the transfer of the transaction and the transfer of the green card ownership by calling the function. During the execution of the function, it will check whether the buyer's identity and the payment amount are consistent with the results of the transaction. If they are consistent, the payment will be transferred to the seller's account, the corresponding green card will be transferred to the buyer's name and the lock-in will be lifted.

5 CONCLUSION

By analyzing the challenges faced by green certificates, this paper designs a green certificate transaction matching and circulation model. This model is based on blockchain in the form of alliance chains. The blockchain ensures that the model is controllable and helps to improve its transaction processing efficiency. At the same time, the model relies on a variety of smart contracts to achieve unified user identity authentication and green certificate issuance and trading. With the help of the open, transparent, and non-tampering characteristics of the blockchain, it not only reduces the cost of user trust but also provides a strong guarantee for the traceability and audit of green certificates.

REFERENCES

[1] Lijun Zeng, Jiafeng Wang, Laijun Zhao, An inter-provincial tradable green certificate futures trading model under renewable portfolio standard policy, Energy, Volume 257,2022,12477.

[2] Liang Zhang, Dongyuan Liu, Guowei Cai, Ling Lyu, Leong Hai Koh, Tianshuo Wang, An optimal dispatch model for virtual power plant that incorporates carbon trading and green certificate trading,International Journal of Electrical Power & Energy Systems, Volume 144,2023,108558.

[3] Yu Fan, Minhui Ren, Jian Zhang, Ning Wang, Changlu Zhang, Risk identification and assessment on green product certification — Model construction and empirical analysis, Journal of Cleaner Production, Volume 370,2022,133593.

[4] Alexander Marthews, Catherine Tucker, What Blockchain Can and Can't Do: Applications to Marketing and Privacy, International Journal of Research in Marketing,2022.

[5] Zigui Jiang, Kai Chen, Hailin Wen, Zibin Zheng, Applying blockchain-based method to smart contract classification for CPS applications, Digital Communications, and Networks,2022.

[6] Lejun Zhang, Jinlong Wang, Weizheng Wang, Zilong Jin, Yansen Su, Huiling Chen,Smart contract vulnerability detection combined with multi-objective detection, Computer Networks, Volume 217, 2022,109289.

[7] Firas. H.N. Al-mutar, Osman N. Ucan, Abdullahi A. Ibrahim,Providing Scalability and Privacy for Smart Contract in the Healthcare System,Optik,2022,170077.