Journal of Universal Computer Science, vol. 25, no. 10 (2019), 1240-1260
submitted: 3/12/18, accepted: 29/5/19, appeared: 28/10/19

Research on Fair Trading Mechanism of Surplus Power Based on Blockchain

Zhuoqun Xia, Jingjing Tan, Jin Wang[1], Runnong Zhu
Hongguang Xiao
(School of Computer and Communication Engineering
Changsha University of Science and Technology
Changsha, China
xiazhuoqun@csust.edu.cn, 1436931299@qq.com, jinwang@csust.edu.cn
zrnong@outlook.com, 2273444019@qq.com)

Arun Kumar Sangaiah
(Vellore Institute of Technology, Vellore632014, India
arunkumarsangaiah@gmail.com)

Abstract: The development of blockchain technology is very rapidly. As a decentralized distributed technology, the blockchain has become one of the most promising Internet applications, and its application in the power balance trading platform has also received extensive attention. In view of the information asymmetry between the trading center and the margin trading users in the power balance trading platform, it is difficult to guarantee the fairness of the transaction and affect the actual income of the production consumers. First, we analyze the trading mechanism of the power surplus market.Then we designed a smart contract for multi-party bidding power resources based on blockchain technology, and achieved the decentralized power trading decision to ensure the information is symmetric and fair.At the same time, the credibility model is established by analyzing the user's recent transaction records, and we design a corresponding punishment mechanism to strengthen the constraint on the execution of offline point-to-point power transactions.
Key Words: blockchain, smart contract, power margin trading, fairness
Category: J.7

1 Introduction

Nowadays, there are appropriate and relevant contributions on intelligent computing applications in various fields of life such as smart grid, traffic, business, government, etc[Wang, 17][Wang, 17].

The market-oriented trading of distributed generation has received great attention, and many distributed power sources will be integrated into the grid. Accessing a high proportion of distributed power within the distribution network has transformed many traditional users of electricity into new production consumers who are both producers and consumers, the so-called producers . Such

[1] Corresponding author

users generally adopt a mode of self-use and surplus power. With the continuous increase of distributed power sources, the surplus energy generated by the production-type consumers has increased significantly. Since the on-grid price of surplus electricity is less than the sales grid, they hope to sell the power surplus in the market, sell it to surrounding users, and increase revenue [Vogt, 10][Ilic, 12][Lampropoulos, 10].

The key issue in power margin trading is how to ensure the security, transparency and information symmetry of the transaction process. The existing research analyzes the composition of participants in the energy trading system and the needs of all parties, and puts forward some ideas about the system architecture and trading methods [Sajjadi, 16][Apostolopoulou, 16][Kristov, 16]. Most of them believe that the power surplus trading still needs to rely on the regional trading center to execute, adopt a centralized trading auction and settlement method. However, the trading pattern of power surplus is quite different from the traditional power system characteristics: the number of users participating in the transaction is huge, but the size of a single transaction is usually small, and the quotation strategy has strong uncertainty and difference. Therefore, the centralized trading center faces two major problems: First, a large number of small-scale trading requests will seriously consume the system resources of the trading center, increase the operating cost of the trading center, and result in low efficiency of transaction settlement; Second, there is information asymmetry between the trading center and the users of power surplus trading, which is difficult to guarantee the fairness of transactions and weaken the actual income of production consumers [Masiello, 16].

In order to ensure the safe and efficient operation of the transaction, a blockchain technology with decentralization characteristics can be introduced in the power balance trading network system [Chen, 17]. Blockchain technology is a new type of distributed database technology that can support peer-to-peer transactions of a large number of users, thus solving the problems of high cost, low efficiency and insecure data storage of traditional centralized organizations. Providing a low-cost, open and transparent platform for the trading of power surplus [Nakamoto, 17][Yuan, 16]. In recent years, the energy industry has been regarded as one of the most promising areas of blockchain technology, and it is very promising to become a supporting technology for future energy market trading platforms [Kim, 16][Ning, 16]. Blockchain technology plays a role in different aspects of energy Internet in different aspects such as measurement and certification, market transactions, and collaborative organization [Bo, 19][Ke, 18]. The core advantage of an application based on blockchain technology is that it can provide a decentralized information interaction mode, which enables the trust between the various entities in the decentralized system to be solved. In the distributed structure network, let each The nodes reach a consensus, and

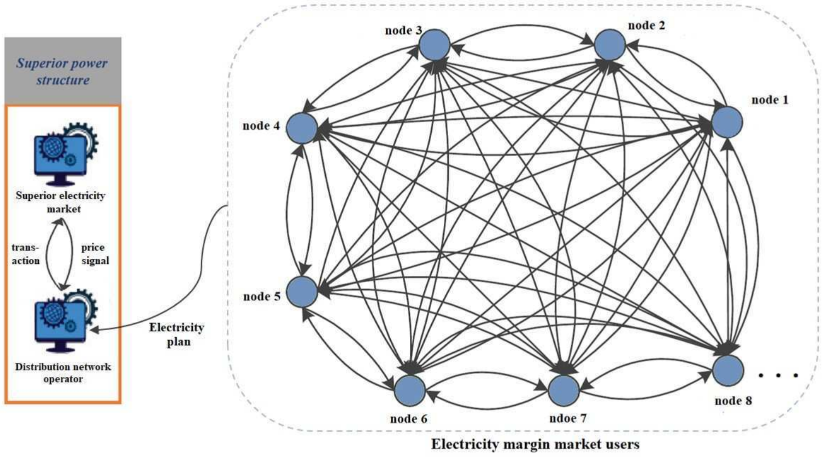

Figure 1: Decentralized power network diagram.

the various forms of distributed power in the energy Internet contain different subjects, which are like nodes in a distributed network. Energy Internet emphasizes information interaction and rapid decision-making. It can realize mutual trust and information interaction security among various entities by means of blockchain network. The information involved in the energy Internet is very complicated. At present, its integration with blockchain technology is at an early stage. As a forward-looking study, we simplifies the application scenario and considers how to use blockchain technology for information in power networks. Interaction. A power trading model based on blockchain combined with smart contract is proposed. As shown in Figure 1, in this trading mode, the user's power information is sent and received through smart meters and other smart devices. The participants in the power trading market are equal. , decentralized, and implement trusted transactions under the conditions of going to the trading center. After the decision to be traded is completed in the form of a smart contract, a peer-to-peer transaction between users is performed. At the same time, in order to guarantee the implementation of point-to-point power trading after the transaction is reached, we design a mechanism for punishing fraud based on the credibility model for users participating in the power surplus market. Strengthened the constraints of offline transactions.

2 Related works

At present, there are many studies on block connections, but research on energy trading is still in its infancy. Alam et al. [Alam, 15] mainly analyzed the feasibility of blockchain technology for energy trading in smart grids. Aitzhan et al. [Aitzhan, 16] discussed the security of electrical energy transactions in smart grids. In the decentralized smart grid based on blockchain, it is proposed to use a multi-signature and anonymous encrypted message flow to spread energy without relying on third parties. Transaction information, a program that guarantees the security of energy transactions. Claudia et al. [Pop, 18] proposed a decentralized solution for managing demand response in the context of smart grids. Security is an important consideration for smart grids [Xia, 18]. Wu Zhengquan et al. [Zhenquan, 17] proposed a smart grid data security storage system based on the alliance blockchain, so that the perceived data is stored securely in a decentralized manner. Potential security risks for centralized data storage. HU Jian-Li et al. [Jian-Li, 09] proposed the residual market model of energy local area network and its basic transaction flow, and analyzed the significance of using blockchain technology for the margin market.

Based on the blockchain technology, J Ping et al. [Ping, 17] designed a decentralized power multilateral bidding trading mechanism for distribution networks. But it is more focused on building a decentralized distribution network trading mechanism, and does not explore the structure of the blockchain system and the details of the smart contract. At the same time, in the decision-making process of the transaction, in order to prevent the quotation leakage from multiple users, the solution adopted is to divide the process of the buyer's bidding into two stages. The first stage passes a real quote hash encryption to the smart contract. The ciphertext, then the second stage of the transaction logic, determine the winning bidder, at this point the smart contract no longer accepts the ciphertext, and the user passes the real quote to it, and verifies whether the real quote is matched with its corresponding ciphertext string. This prevents the leakage of bidding information, but it affects the efficiency of trading decisions.

Ethereum is one of the most mature blockchain technologies available today. It provides a Turing-complete programming environment. On the Ethereum platform, developers can write smart contracts of any kind. Once the encoding is complete, the smart contract is uploaded to the block-connected network, and other users who have synchronized the block to the network view the contents of the contract and can send information to it for interaction. A smart contract is not just a computer program that can be executed automatically, it is also a system participant. Accounts in the Ethereum network are divided into two categories: external accounts and contract accounts. The external account corresponds to the transfer address, created by the user, and can initiate a transaction, such as transferring an Ether or triggering a contract code. A smart contract can be called a contract account. It also has its own account address. It is created by Ethereum Virtual Machine (EVM) based on the contract address in Ethereum. It cannot initiate transactions but could be transmitted with other users and smart contracts[Dienelt, 16], as well as passively triggering the execution of the contract code.

We analyzes the demand for power surplus trading, and believes that the decision of energy trading can be completed by multi-party bidding [Menniti, 09], and the decision of trading is settled by generalized second-order auction (GSP) [Edelman, 07]. In this method, the last amount that the successful bidder needs to pay is only a little higher than the second place in the bidding order, and can receive less influence from the game between the bidding users. Based on the smart contract technology,we design the multi-party bidding power surplus trading intelligent contract to realize the decentralized trading mode, which ensured the fairness and transparency of the transaction, and solved the problem that high transaction cost and low decision-making efficiency of the trading center.

We use blockchain technology in power surplus trading, which solves some shortcomings of traditional trading methods, but because of its decentralized nature, no third party supervises the execution of the transaction, which causes users to conduct transaction fraud behavior. In response to this phenomenon, we design a user reputation model and a penalty mechanism for fraudulent users to reduce the possibility of fraud.

3 Fair trading mechanism for power surplus market

3.1 Credit model in the trading market

Although we apply the blockchain technology to the energy surplus transaction and achieve the decentralization of the transaction which ensure the transaction data is transparent and not falsified,it is not possible to constrain the execution of the transaction after the transaction is completed. By setting the trading margin, the offline transaction can be restricted, and the user will deduct the pre-submitted guarantee as a penalty after the fraud default. However, in this method, the margin is usually represented by a Virtual currency(token) in the blockchain, and thus it will involves the exchange transaction between the legal currency and the virtual currency . Exchanges between the two currencies will have exchange rate fluctuations, there are many uncertainties, and the criteria for punishing fraud cannot be accurately measured.

Therefore, we design the credit model of the honest transaction of the two sides of the transaction, examines the behavior of the multi-party users participating in the transaction in the transaction process, and takes corresponding rewards and punishments according to the specific behavior of the user. At present, when the transaction in the market is delivered, it is required to go to the buyer to pay, and then the seller is shipping, and we set this kind of delivery as the study background. In this model, the factors affecting the seller's reputation value mainly include single transaction amount and historical transaction.

At the same time, we use the Ethereum platform as the technical basis to realize the power surplus trading. Since the Ethereum platform has not provided an API for external application queries to obtain historical data, therefore, when querying the transaction history data stored on the blockchain, only the query one by one in the blockchain in turn. In order to balance the transaction efficiency and the accuracy of the reputation value, we set the scope of adoption of the data of the credibility model, and only count the latest n transactions into the construction of the credibility model.

Setting z denote the transaction amount of the current single transaction, and $s(z)$ denote the increase value of the reputation value after the seller transaction is successfully executed. When the transaction amount is larger, the increase in the reputation value will be correspondingly larger, which is conducive to encouraging the seller to make large transactions. z_i indicates the size of the transaction amount of the i-th $(1 \leq i \leq n)$ that has recently been considered. n is the number of transactions the seller has recently conducted, that is, the value of the reputation is measured using only the value of the last n transactions. z_0 is the adjustment factor of the change in the reputation of the merchant. As the amount of successful transactions increases, the value of the reputation value should increase, so the calculation formula of $s(z)$ is obtained:

$$s(z) = \frac{z}{\sum_{i=1}^{n} |z_i|} + z_0 \tag{1}$$

Using $f(z)$ to indicate the penalty function of the system for the reputation score after the transaction fails. Let m be the most recent m transactions included in the scoring range, and agree: when the transaction is successful, $f(z) = 0$; when the transaction fails, different degrees of punishment will be taken according to the specific fraudulent behavior of the malicious seller. Because the greater the amount of fraudulent transactions, the greater the penalty, so the formula for the penalty function $f(z)$ is obtained:

$$f(z) = \frac{|z|}{\sum_{i=1}^{m} |z_i|} + z_0 \tag{2}$$

In the course of the transaction, there is usually a situation in which the seller accumulates a higher credit value with a small transaction when his reputation value is low, and then uses this as a bait to conduct fraud in a large transaction. In order to reduce this fraud, we introduces a penalty coefficient $c(n)$ to adjust the penalty for fraud. Where n is the cumulative number of fraudulent transactions performed by the merchant until the most recent transaction, and $c(n)$ varies non-proportionally with the cumulative number of fraudulent transactions.

Since $c(n)$ changes rapidly with the cumulative number of fraudulent transactions, when the seller first obtains a certain amount of credit value through multiple small transactions, and then waits for a large amount of fraudulent transactions, then the seller will successfully trade in the next small amount. The reward points obtained in the competition are drastically reduced; at the same time, when the seller repeats the same fraudulent trading behavior again, the system will gradually increase its punishment.In this way, the feasibility and probability of occurrence of the above fraudulent transaction scheme can be greatly reduced. At the same time, in order to prevent the seller from re-entering the market transaction after changing the identity ID due to the reputation problem, the initial credit value of the new user is specified as 0.

In summary, the seller's reputation model can be formalized as:

$$R_n^s = \frac{s(z) + k_1}{c(n)f(z) + k_2} R_{n-1}^s \tag{3}$$

Where R_n^s represents the reputation value of the seller after the n-th transaction, and k_1,k_2 are constants.

For the buyer, if the buyer does not pay for fraud after winning the bid, who will not have any income, and the damage caused to the seller is limited. Assume that L is the profit coefficient of the transaction. If the buyer does not pay for fraud in the transaction, the loss caused by it is L times the amount of the transaction ($0 < L < 1$), and the loss is $L * z$. Set $p(z)$ to indicate the buyer's penalty function for fraudulent non-payment, its reputation score, let k be the last k transactions included in the score consideration, and agree: when the transaction is successful, $p(z) = 0$; Then there is a calculation formula of $p(z)$:

$$p(z) = \frac{L * z}{\sum_{i=1}^{k-1} |z_i| + L * z} \tag{4}$$

In order to encourage both buyers and sellers to conduct good faith transactions, the seller's sell orders in the trading market can be treated fairly by the buyer, and the new sellers of low-credit sellers are not allowed to issue large sales orders. Use $q(z)$ to represent the reputation value growth function. When the transaction is reached, the reputation value will increase as long as the buyer makes the payment. In order to encourage the buyer to participate in the large-value transaction with relatively low creditworthiness of the seller, the growth rate is related to the creditworthiness of the seller. Assuming $s(z)$ is the seller's credit transaction, its reputation value increases by $q(z)$ formula:

$$q(z) = L * s(z) \tag{5}$$

In summary, the buyer's reputation model can be formalized as:

$$R_n^b = \frac{p(z) + t_1}{c(n)q(z) + t_2} R_{n-1}^b \tag{6}$$

Where R_n^b represents the reputation value of the seller after the n-th transaction, and t_1, t_2 are constants.

At the same time, we designs a penalty mechanism for both users who are fraudulent during the execution of the transaction. For such users, they will be prohibited from entering the market on the following trading days. Use d to indicate the date the transaction is forbidden. Then there are:

$$d = \frac{c(n)}{R_n^t}, (t = s, b) \tag{7}$$

As the number of user default fraud increases, the time of punishment will increase exponentially, thus showing the deterrent of punishment. And the user's breach of contract fraud will be recorded in the log of the blockchain, which cannot be falsified and open to the public.

3.2 Smart contract for trading in the surplus electricity market

We designs a multi-party bidding energy trading smart contract, through the smart contract to complete the decision-making process in energy trading. S-mart contract carries the data information of the energy transaction, including: the publisher's account address, the amount of energy transactions, the public key of the quoted encryption, the status of the transaction, and the quotation information. Users who are synchronized to the blockchain network can view the transaction details and ensure the transparency and fairness of the energy transaction.

In the course of the transaction, the price of the transaction is determined by the form of the bid, and the smart contract will accept the offer from multiple users. Due to the characteristics of the blockchain distributed storage, the information of the user participating in the quotation is visible to all the people in the network, and the actual situation requires the bidder not to know the quotation amount and other information of other people when submitting the quotation.

Therefore, in the quotation phase, the bidding user needs to encrypt the real quotation. The ellipsis encryption algorithm is used to encrypt the quotation to generate ciphertext. The ciphertext is presented in the form of a point pair. Then the account address of the ciphertext and the quotation user is stored in the smart contract in the form of key-value, so that each quotation Traceable source. In the trading decision stage, the smart contract decrypts the ciphertext to generate a real quotation, and uses a generalized second-order auction (GSP) to make a logical decision to determine the winning bidder.

Table 1: User data structure

'Person' data structure	
string sCredit;	//Seller's credibility
string bCredit;	//Buyers credibility
uint[] HTransaction;	//Recent transaction history
uint PDate;	//Date of prohibition of transaction
address PurseAddress;	//Personal address

Based on the above business analysis, we simplified the trading process of the surplus power and divided the smart contract into two different contract types, namely user contract and trading business contract. The user contract (UserCon), whose main function is to store users and data types. Model-related data for user credibility is stored in the constructed user contract. The user contract is similar to a user agent, and each user has a user contract. The user contract contains information about the user, such as the user's wallet address, historical transaction status, personal credit, etc., which are stored in a custom data structure, as shown in Table 1, and then stored in the form of a Map.

When the user conducts a transaction publishing service, the PDate attribute in the information is checked. As mentioned earlier, if the smart contract acquires data from an external service, the data acquisition process is repeated and independently performed by each node. Therefore, we hereby clarify the penalty result obtained by the user for fraudulent default in the form of date instead of the number of days. When reviewing before the transaction, simply compare the current date with the PDate attribute to determine whether the user is qualified. If the number of days is recorded, the user contract will periodically obtain the date data from the external service and update this attribute, which will increase the system overhead and affect the transaction efficiency.

The trading business contract is mainly used to realize the bidding decision in the power trading, and it stores the selling information, the quotation encryption algorithm and the data type. Due to the current limitations of Ethereum's performance, we completed the trading business by setting up two contracts (OrderCon, CryptoCon). The contract of CryptoCon encrypts and decrypts real quotes.

The contract of OrderCon is responsible for storing the details of the sell order. A Map is defined in the contract of OrderCon. The main function is to store the sell order information, and also to implement some function functions. For example, the acquisition, deletion, and insertion of the sell order information, and so on. The structure of Map is as follows:

```
Mapping(uint=>address) OrderIdInStore;
Mapping(address=>mapping(uint=>Oder)) stores;
```

Table 2: Oder data structure

'Oder' data structure	
uint id;	//Sell order ID
address publisher;	//Transaction publisher address
uint quantity;	//Sale of electricity
uint auctionStartTime;	//Bidding start time
uint auctionEndTime;	//Bidding end time
uint startPrice;	//Bidding start price
address highestBidder;	//Successful bidder address
uint highestBid;	//final price
uint secondHighestBid;	//Second highest price
uint totalBids;	//Number of bidder
productStatus status;	//Sell order status
uint publickey;	//Sell order encryption public key

We are here according to the defined mapping type. OrderIdInStores is responsible for the associated transaction sell order Id number and the user wallet address for issuing the transaction request. The stores are responsible for associating the user wallet address with its historical transaction sell order. The data structure of the transaction sell order is shown in Table 2.

The above-mentioned Map structure, data structure, general-purpose algorithm, etc. are all stored in the form of warehouse contracts, and the library contracts are included in other business contracts through the using for instruction, and then deployed to the blockchain, and the user performs the business contract by sending the transaction. When called, the warehouse contract is automatically called and the corresponding operation is completed.

In addition, smart contracts have their functional limitations. The blockchain is a consensus-based system. Only after each transaction and block has been processed, and each node reaches the same state, the smart contract can run normally, and everything must be accurate and consistent. If the nodes are ambiguous about the state of the data, the entire system cannot be trusted and stable. Smart contracts are executed independently by each node in the chain, so if the smart contract gets data from an external service, this data acquisition process is repeated and done independently by each node. Therefore, instead of sending out the external data by the smart contract, the user sends a blockchain transaction, and the required data is added to the transaction. The transaction will embed the data into the block and synchronize to each node to ensure the complete data. Consistent.

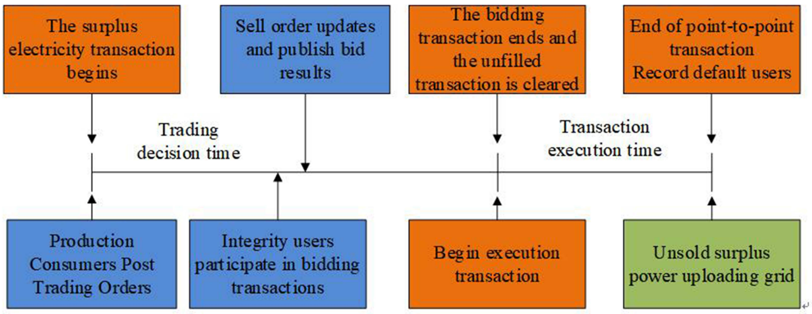

Figure 2: Surplus power market trading cycle chart.

3.3 Blockchain-based surplus power fair trading mechanism

The blockchain is the underlying technology foundation of the surplus power market architecture, consisting of a P2P network and blockchain storage devices. There are a large number of network nodes in the blockchain network, all nodes have the same status, there is no special central node and hierarchical structure, each node will assume the functions of network routing, verification data block and so on. The trading model we designed focuses on the day-to-day trading market. Production consumers determine the power usage plan before the trading day. When there is surplus power, they can initiate a transaction request and then spread to the user nodes participating in the transaction via the blockchain network.

In view of the characteristics of power surplus trading, combined with the existing margin market model and China's electricity billing mechanism [Pop, 18], the trading cycle of power surplus is divided into two stages, as shown in Figure 2. In the first phase, mainly before the trading day, the transaction information is spread in the block network, and the decision of each transaction sell order. In the second phase, the transaction order and power settlement of the transaction are implemented.

(1) Posting transaction information:

The production consumer issues a transaction request and needs to construct a smart contract (OrderCon) for the electricity bidding. The information of the electricity sales transaction is spread in the blockchain network in the form of a smart contract. The power amount of the transaction will be traded when the contract is initialized. Status, and other attributes are written to it. At the same time, the public key of the quoted encryption is written into the smart contract (CryptoCon), and the public key generated by the quoted encryption is shown in Figure 4. At the same time, the information on the contract is encrypted with the private key of the information publisher's account to generate a digital

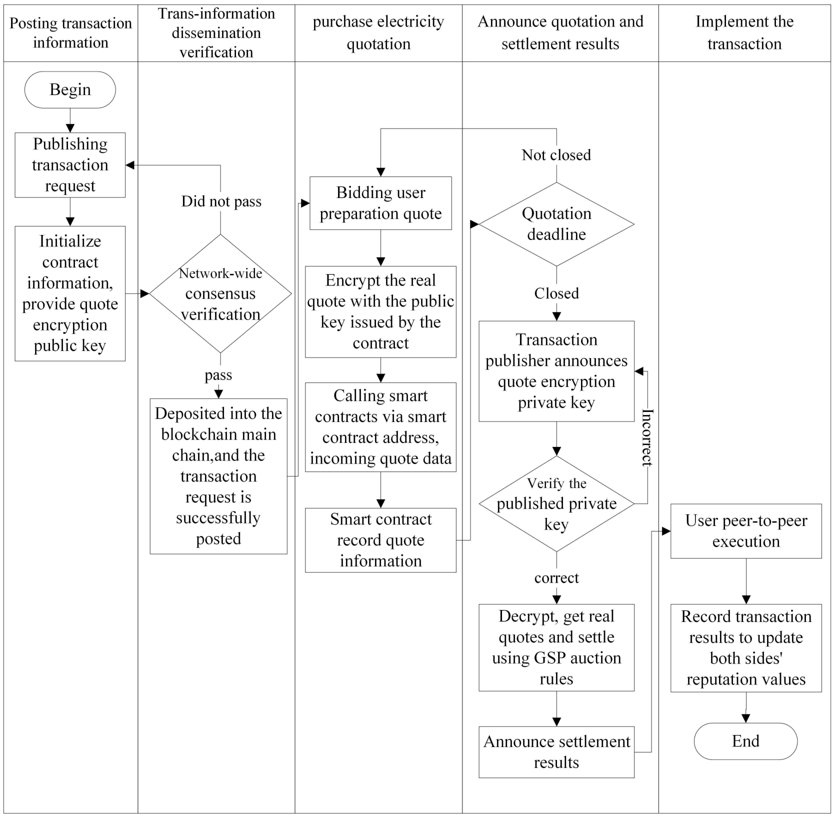

Figure 3: Flow chart of the single sell order.

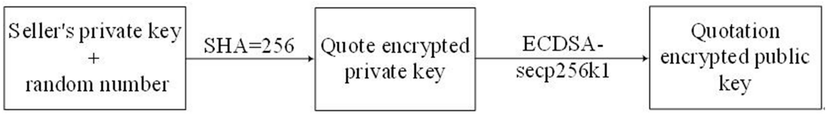

Figure 4: Key generation process for quote encryption.

signature to ensure the validity of the contract. After the bidding smart contract is concluded, it will be broadcast to the blockchain network.

(2) Transaction information dissemination verification:

When other user nodes receive the transaction information in the network, the digital signature in the transaction is first verified by the public key of the publisher account to check whether the transaction is valid. When the transaction information is verified, the node will continue to broadcast and forward the transaction information to the blockchain network. After the transaction information is reached on the whole network, the smart contract that carries the terms of the transaction will be recorded on the blockchain, and the transaction request is successfully issued. After the other user nodes synchronize the blockchain main chain information, the transaction information and its status that have been successfully published in the entire network can be queried according to the contract address.

(3) purchase electricity quotation:

Smart contracts define transaction logic and business rules for accessing state data. When a user wishes to participate in the quotation, the specific smart contract can be called through the address of the smart contract, and the quotation data (DeliveryOffer) can be transmitted. This includes the quote amount, the quote timestamp, and the quoting person's personal digital signature.

Users participating in the auction need to encrypt their real quotes during the quotation phase (EncryptedQuote). We uses the quotation encryption public key to encrypt it by the elliptic curve encryption algorithm. The encryption formula is shown in Equation 9. In this way, the quotation information will not be leaked to other bidders early, and the fairness of the transaction process is guaranteed. This operation involves modifying the internal data of the smart contract, so it needs to reach a consensus on the whole network before it can take effect.

$$C_X||C_y = Encny_{k_j}(rG||M) \tag{8}$$

Encny() is an elliptic curve encryption method, r is a random number, M is a real quotation, K_j is a quotation encryption public key, G is a relationship parameter between a private key and a public key, and the ciphertext is a point pair $(C_X||C_y)$.

(4) Announce quotation and settlement results:

The smart contract deployed on the blockchain collects the quotation information of each node of the network. After the quotation data is introduced, the address of the quotation user and the hash value encrypted by the real quotation are recorded in the form of key-value.

At the end of the sealed quotation phase, the publisher of the transaction information discloses the private key encrypted by the contract quotation, and the smart contract decrypts the previously collected sealed quotation (Decrypt), the decryption formula is as shown in Equation 10, and then uses the generalized second-order auction. (GSP) Determine the winner (Settlement). The operation of decrypting the settlement quotation involves modifying the state of the smart contract, so it is also necessary to reach a consensus on the whole network. In this process, other nodes of the blockchain network will verify whether the decrypted quotation correctly corresponds to the hash value during the bidding period.

$$M = C_y - Decny_{k_i}(C_x) \tag{9}$$

Dencny() is an elliptic curve decryption method, K_i is a private key, M is a real quote, C_X, C_y are point pairs of ciphertext.

(5) Implement the transaction:

After the transaction is reached, the two parties will implement the transaction based on the results of the game. Update the reputation values of both parties based on the results of the transaction. The transaction result records are entered into the Ethereum log through the smart contract.

4 Simulation

4.1 Simulation design

In order to verify the effectiveness of our proposed power surplus trading mechanism, this section publishes the distributed multilateral power bidding smart contract to the Ethereum private chain in the laboratory environment to simulate the distributed power multilateral trading scenario of the distribution network and perform a simulation test.

In the actual operating environment of Ethereum, when performing write operations on the chain, each full node in the network performs the same calculation and stores the same value. This execution is expensive, in order to encourage users to The operations performed under the chain are not placed on the chain, so each time a write operation is performed on the chain, a certain fee is required, which is counted in units of gas, and each command that can be executed on the chain is setting a consumed gas value. At the same time, each block has a gas limit, which is the maximum amount of gas allowed by a single block, which can be used to determine how many transactions can be packaged in a single block. The gas limit is set for each transaction or contract call. The operation will only be executed if the amount of gas used by the operation is less than the set gas limit.

Before the simulation test, we analyzed and tested the smart contract through the solgraph tool. Solgraph can visually analyze the security process of the smart contract written by Solidity, generate DOT graphs, highlight potential security vulnerabilities and display the calling process of each function method in the smart contract.

In the DOT diagram generated using the solgraph tool, colors are used to identify the type of operation to which the function in the smart contract belongs. Black indicates normal operation, data read and write involves temporary variables, red indicates that the address of a certain information on the blockchain will be exposed to the outside, blue indicates that the blockchain data is written, and yellow indicates that only read is supported. operating.

Solgraph can only analyze a single smart contract at a time to generate a visual analysis graph, so in order to be more intuitive, we combines multiple

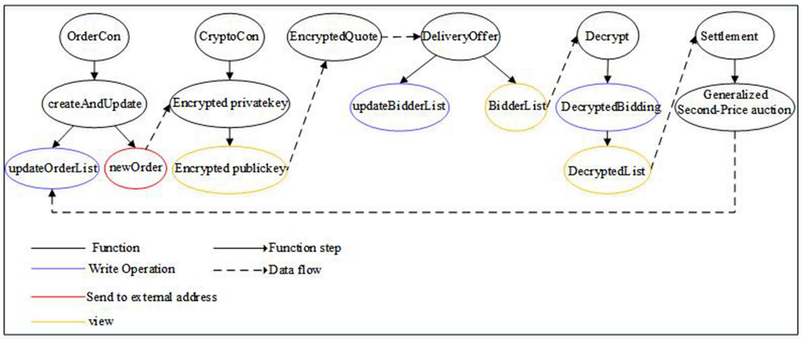

Figure 5: Smart contract function call flow chart.

analysis graphs into one. Here, the main steps are selected for display. As shown in Figure 5, there are four functional steps involved in updating and writing data on the blockchain, which will consume more resources accordingly. Therefore, the following operations will be tested and analyzed. The change in the gas value.

In this simulation, we calculated the consumption of gas value in each step of the power trading process. The consumption of gas value can reflect the consumption of system resources computer by the power surplus trading mechanism proposed in this paper.We created 40 users on the private chain and sent 126 transactions to simulate transactions across the entire power trading cycle. In Table 3, the consumption of gas for each step of operation is shown. During a single power transaction, the transaction publisher operates to generate a transaction that is only broadcast once throughout the network (in the table,transaction publisher indicated by the prefix 'S'). Users who participate in the electricity bidding at the same time (in the table with the prefix 'B' indicates the user participating in the bidding), will broadcast a transaction to the network when the offer is made. In the single power transaction process, 41 transactions will be broadcast to the blockchain network.

During the simulation test, because the total amount of gas allowed in a single Ethereum block is about 4.7 million gas, and the amount of code to implement the power trading business is too large, we have to complete the entire power transaction through two smart contracts. business. The smart contract of OrderCon is responsible for carrying the details of the transaction, recording the information of the participating bidders and the quotation, as well as the logical processing of the settlement quotation. The smart contract of CryptoCon helps the participating bidders encrypt their real quotes and is responsible for decrypting the quoted ciphertext during the settlement phase.

After the smart contract of CryptoCon is deployed, it can be repeatedly

Table 3: Gas consumption of a single power transaction

Entity:Transaction	Cost in Gas
S:OrderCon	3,779,963
S:CryptoCon	2,435,848
B:EncryptedQuote	70,112
B:DeliveryOffer	763,118
S:Decrypt	1,834,368
S:Settlement	2,490,412
Seller Total	10,540,591
SingleBidder Total	833,230
Auction transaction Total	43,036,561

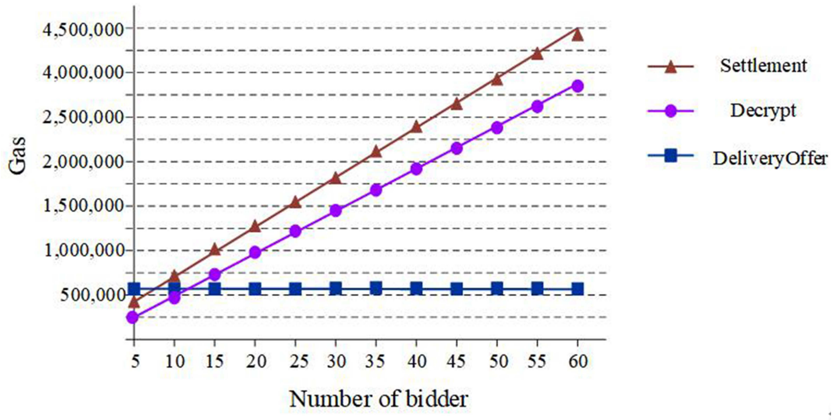

Figure 6: Gas consumption changes with the number of users.

called by the participating users. The user obtains the public key corresponding to the transaction encryption. We put the quoted ciphertext calculation process locally, which saves a lot of computing resources. It also reduces the consumption of gas. The smart contract of CryptoCon ensures that all users participating in the auction receive the correct and identical encrypted public key.

It can be seen from Table 3 that the value of gas consumed by each participating user in the bidding operation accounts for 16% of the upper limit of the gas value of a single block in Ethereum. Under the current Ethereum block setting, each block can accommodate Quotation information for 6 users. At the same time, Ethereum currently generates blockchains for a new block every 12 seconds. The quotation of 30 users can be processed every minute under the current standard.

In addition, we also analyzed the impact of changes in the number of people participating in the auction on the consumption of gas. As shown in Figure 6, we counts the cost of the operation cost of the bidding users when they are 5, 10, 15, ..., 60, etc. It can be seen that the consumption of gas by the publisher of the transaction increases linearly with the increase of the number of bidding users. This is because the increase in the number of bidding users increases the computational power of the settlement phase. The consumption of gas consumed by a single bidding user remains basically the same, indicating that the user's competition for computing power does not increase the overhead of computing resources.

4.2 Reputation model simulation

In this section, we first simulated the change in the reputation value of the fraudulent user.For this model, take $k_1 = k_2 = 1$, $z_0 = 200$, $c(n) = \{1, 2, 4, \cdots, 2^{n-1}\}$ to simulate the fraudulent transaction behavior of the merchant.Assume that a malicious merchant conducts transaction fraud in the following manner: When the credit value is lower than 7.5, the legitimate transaction is performed to obtain the transaction success bonus score; otherwise, the large transaction fraud is started. Among them, the small transaction value is 10, and the large transaction fraud is 20.The change in the reputation value obtained by simulating the behavior of the malicious merchant according to the model is shown in Figure 6.

As can be seen from Figure 7, under the condition that the amount of fraud has not changed, the penalty for the system's fraudulent behavior of bad users increases as the number of malicious operations accumulated in his history increases.Whenever a bad user maliciously operates in a new transaction, the decline in the reputation value is steeper than the previous one, so the bad user needs to conduct more honest transactions to restore the reputation value to the original level.It can be seen that the user credibility model designed for power trading can greatly curb the malicious transaction behavior of bad users. It can reflect the change of the credit status of the users participating in the transaction more realistically and objectively, and encourage users to conduct honest transactions.

4.3 Smart contract security verification

Smart contracts are executable computer code stored on a blockchain. The blockchain's non-tamperable nature guarantees the physical security of the contract code, but the logical security of smart contracts and how to develop smarter smart contracts It is the research focus of current smart contracts. We used the Oyente tool to detect the smart contract code of the power balance trading business.

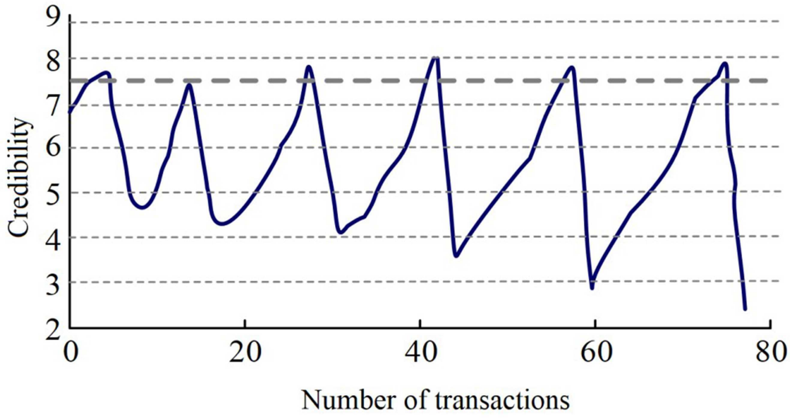

Figure 7: Changes in the reputation value of fraudulent transactions by merchants.

Oyente is embedded in the smart contract development tool Browser-solidity, which not only allows developers to write better smart contracts, avoids calling vulnerable contracts, but also provides the most common security vulnerability detection in smart contracts, such as heavy Attacks, transaction order dependencies, timestamp dependencies, misoperation exceptions, etc. As shown in FIG. 8, when an operation such as issuing transaction information and performing quotation decryption is performed, a warning message is reported. This is because when a contract calls another contract, the current execution process stops and waits for the call to end, which creates an intermediate state that can be exploited, which can lead to reentrant attack vulnerabilities.

For this analysis, we reconstructed some of the business code in the pretest smart contract. In order to avoid reentrant attack vulnerabilities, we try to avoid contracts for external calls and multi-level nested calls, and external call functions cannot share state with functions that initiate external calls.At the same time, the Checks-Effects-Interactions model is used for smart contract development. It is characterized by first judging conditions, then performing actions, and finally interacting with smart contracts.

5 Conclusions

The combination of distributed generation technology and existing grid systems is the main method to save investment, reduce energy consumption, and improve system safety and flexibility. With the increasing penetration rate of distributed energy in the power grid, the development of power network systems

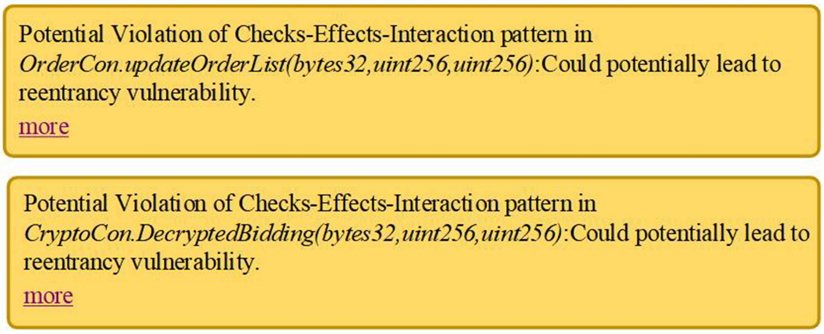

Figure 8: Trading warning information.

is inevitable. The direction will be to introduce a power surplus market trading mechanism in the grid to achieve flexible internal transactions. Based on the blockchain technology, we propose a decentralized power trading mode in which multiple parties participate in the bidding, and design a decentralized power multi-party transaction process.At the same time, considering the current limitations of blockchain technology, we designed the user credibility model and the corresponding penalty mechanism to constrain the offline point-to-point transaction after the bidding decision is completed. According to the decentralized power trading process, using Ethereum smart contract technology, we designed a smart multi-party bidding contract, providing privacy protection for users participating in the transaction, and ensuring that the bidding result can be publicly verified.

The use of blockchains in multi-party trading of power surplus within the grid is worthy of deeper research. Possible future directions includeBlockchain consensus mechanism design for power multi-party transactionsResearch on the optimal scale of power multi-party trading based on blockchain technology using multilabel learning [Edelman, 07][Shen, 18], etcimproving the comprehensive utilization of electricity in the grid system.

Acknowledgments

The paper is supported by Hunan Provincial Natural Science Foundation of China, 2019JJ40314.

References

[Aitzhan, 16] Aitzhan N Z, Svetinovic D. Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams[J]. IEEE Transactions on Dependable & Secure Computing, 2016, PP(99):1-1.

[Alam, 15] Alam M T, Li H, Patidar A. Bitcoin for smart trading in smart grid[C]// IEEE International Workshop on Local and Metropolitan Area Networks. IEEE, 2015:1-2.

[Apostolopoulou, 16] Apostolopoulou D, Bahramirad S, Khodaei A. The Interface of Power: Moving Toward Distribution System Operators[J]. IEEE Power & Energy Magazine, 2016, 14(3):46-51.

[Bo, 19] Bo Yin, Xuetao We. Communication-Efficient Data Aggregation Tree Construction for Complex Queries in IoT Applications. IEEE Internet of Things Journal,2019, 6(2):3352 - 3363.

[Chen, 17] Chen S, Liu C C. From demand response to transactive energy: state of the art[J]. Journal of Modern Power Systems & Clean Energy, 2017, 5(1):1-10.

[Dienelt, 16] Dienelt J. Understanding Ethereum. Technical Report, 2016.

[Edelman, 07] Edelman B, Ostrovsky M, Schwarz M. Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords[J]. American Economic Review, 2007, 97(1):242-259.

[Ilic, 12] Ilic D, Silva P G D, Karnouskos S, et al. An energy market for trading electricity in smart grid neighbourhoods[C]// IEEE International Conference on Digital Ecosystems Technologies. IEEE, 2012:1-6.

[Jian-Li, 09] Jian-Li H U, Quan-Yuan W U, Zhou B, et al. Robust Feedback Credibility-Based Distributed P2P Trust Model[J]. Journal of Software, 2009, 20(10):2885-2898.

[Ke, 18] Ke Gu, Linyu Wang,Bo Yin. Social Community Detection and Message Propagation Scheme based on Personal Willingness in Social Network. Soft Computing,DOI:10.1007/s00500-018-3283-x.

[Kim, 16] Kim M, Song S, Jun M S. A Study of Block Chain-Based Peer-to-Peer Energy Loan Service in Smart Grid Environments[J]. Advanced Science Letters, 2016, 22(9):2543-2546.

[Kristov, 16] Kristov L, Martini P D, Taft J D. A Tale of Two Visions: Designing a Decentralized Transactive Electric System[J]. IEEE Power & Energy Magazine, 2016, 14(3):63-69.

[Lampropoulos, 10] Lampropoulos I, Vanalme G M A, Kling W L. A methodology for modeling the behavior of electricity prosumers within the smart grid[C]// Innovative Smart Grid Technologies Conference Europe. IEEE, 2010:1-8.

[Masiello, 16] Masiello R, Aguero J R. Sharing the Ride of Power: Understanding Transactive Energy in the Ecosystem of Energy Economics[J]. IEEE Power & Energy Magazine, 2016, 14(3):70-78.

[Menniti, 09] Menniti D, Costanzo F, Scordino N, et al. Purchase-Bidding Strategies of an Energy Coalition With Demand-Response Capabilities[J]. IEEE Transactions on Power Systems, 2009, 24(3):1241-1255.

[Nakamoto, 17] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[Ning, 16] Ning Z, Yi W, Kang C, et al. Blockchain Technique in the Energy Internet: Preliminary Research Framework and Typical Applications[J]. Proceedings of the Csee, 2016.

[Ping, 17] Ping J, Chen S, Zhang N, et al. Decentralized Transactive Mechanism in Distribution Network Based on Smart Contract[J]. Proceedings of the Csee, 2017.

[Pop, 18] Pop C, Cioara T, Antal M, et al. Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids[J]. Sensors, 2018, 18(1):162.

[Sajjadi, 16] Sajjadi S M, Mandal P, Tseng T L B, et al. Transactive energy market in distribution systems: A case study of energy trading between transactive nodes[C]// North American Power Symposium. IEEE, 2016:1-6.

[Shen, 18] Shen, X, Liu, W, Tsang, IW, Sun, QS & Ong, Yew-Soon Ong:Multilabel Prediction via Cross-View Search. IEEE Transactions on Neural Networks and Learning Systems, 2018, 29(9):4324-4338.

[Vogt, 10] Vogt H, Weiss H, Spiess P, et al. Market-based prosumer participation in the smart grid[C]// IEEE International Conference on Digital Ecosystems and Technologies. IEEE, 2010:592-597.

[Wang, 17] Wang, J.; Cao J. Y.; Ji S.; Park J. H. (2017): Energy efficient cluster-based dynamic routes adjustment approach for wireless sensor networks with mobile sinks, Journal of Supercomputing, vol. 73, no. 7, pp. 3277-3290.

[Wang, 17] Wang, J.; Cao, Y. Q.; Li, B.; Kim, H.; Lee, S. (2017): Particle swarm optimization based clustering algorithm with mobile sink for WSNs. Future Generation Computer Systems, vol. 76, pp. 452-457.

[Xia, 18] Xia zhuoqun,Zhou hong,Gu ke,Yinbo,Zeng youyou,Xu ming,Secure Session Key Management Scheme for Meter-reading System Based on LoRa Technology,IEEE access,2018, 6(1): 75015-75024.

[Yuan, 16] Yuan Y, Wang F Y. Blockchain: The State of the Art and Future Trends[J]. Acta AutomaticaSinica, 2016, 14(2):43-52.

[Zhenquan, 17] Zhenquan W U, Liang Y, Kang J, et al. Secure data storage and sharing system based on consortium blockchain in smart grid[J]. Journal of Computer Applications, 2017.