IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 19, 2019, accepted September 30, 2019, date of publication October 11, 2019,
date of current version October 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2946794

A Privacy Protection Scheme of Microgrid Direct Electricity Transaction Based on Consortium Blockchain and Continuous Double Auction

SHAOMIN ZHANG[1], **MIAO PU**[1], **BAOYI WANG**[1], **AND BIN DONG**[2]

[1]School of Control and Computer Engineering, North China Electric Power University, Baoding 071003, China
[2]Affiliated Hospital of Hebei University, Hebei University, Baoding 071000, China

Corresponding authors: Shaomin Zhang (zhangshaomin@126.com) and Bin Dong (dongbin@hbu.edu.cn)

This work was supported by the Fundamental Research Funds for the Central Universities under Grant 2018ZD06.

ABSTRACT Low cost, high efficiency, price transparency, and timely settlement of transactions are required for direct transactions between electricity providers and consumers in the microgrids. So the blockchain technology and the continuous double auction mechanism for direct electricity trading have always been a hot topic in the field of microgrids.In order to further reduce the transaction cost of blockchain and increase the transaction efficiency, and to solve the problem of lack of privacy protection for continuous double auction in the existing scheme, a privacy protection scheme of microgrids direct electricity transaction based on consortium blockchain and the continuous double auction is proposed. In it, the combination of consortium blockchain technology and continuous double auction mechanism is applied to reduce costs and improve the efficiency of transactions. In the meanwhile, pseudonyms and pseudonym certificates are generated by fair blind signature technology to realize identity privacy in the continuous double auction. And decentralization and user identity traceability are achieved by using (t, n) threshold secret sharing technology which distributes and recovers the private key of a trusted third party. The theoretical security analysis shows that the privacy protection scheme has higher security. The simulation experiment shows that the consortium blockchain technology has lower cost and higher efficiency in this scheme.

INDEX TERMS Microgrid electricity trading, consortium blockchain, fair blind signature, (t, n) threshold secret sharing, privacy protection.

I. INTRODUCTION

Microgrid is a modular and decentralized power supply network based on distributed generation technology and combined with end-user power quality management and cascade utilization of energy. A microgrid is a collection of distributed power sources, energy storage units, loads, and monitoring and protection devices.Distributed power supplies have the characteristics of small storage capacity and inconvenient long-distance transmission. Therefore, the traditional centralized power supply scheduling method increases the complexity of the system, resulting in low efficiency and high cost of the microgrid.With the gradual deepening of the development and construction of microgrid, microgrid groups can be formed between adjacent microgrids. Meanwhile, the improvement of market mechanism gives microgrid the opportunity to participate in bidding transactions in the power market.Distributed power supplies and users can complete transaction matching through bidding in the microgrid energy market, and establish a direct and open power trading information flow system between distributed power supplies and users. Distributed power supplies sell surplus power to neighboring energy consumers in a point-to-point manner [1]. In this way, not only users in the microgrid can purchase local power at a lower price, distributed power supplies sell excess power at a higher price, but also improve resource utilization of distributed power sources. All kinds of entities in microgrid need to measure, interact, control and make decisions in the distributed environment, but these entities are difficult to realize mutual trust as distributed participation nodes.As an emerging distributed and decentralized value transfer protocol, blockchain is a very good research direction to solve such problems.

Currently, the research on how to apply blockchain technology to energy trading has become a hot topic. The specific application form of blockchain technology in energy

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaochun Cheng.

internet is proposed in the literature [2]. For the current energy market, a trading framework based on blockchain technology in paper [3]. The application of blockchain technology to large-user direct-purchasing and decentralized distribution network transactions are proposed in papers [4], [5]. Although decentralized transactions are realized, there are no market trading mechanism compatible with blockchain. The application of blockchain technology and multi-signature proposed in paper [6] enables peers to negotiate energy prices anonymously and execute transactions securely, but lacks a flexible pricing scheme.The continuous double auction (CDA) mechanism in paper [7] is introduced into the microgrid to achieve pricing and balance of transactions. Combining the market trading mechanism with the blockchain technology to solve the microgrid distributed electricity trading in the literature [8], which uses the continuous double auction. The mechanism is considered to be the most suitable market model for distributed energy trading [9], which maximizes social welfare and enables more producers and users to participate. However, the cost of establishing a blockchain in a microgrid with limited energy is too high, which requires the shortcoming of the transaction speed caused by the consensus of all nodes.

Continuous double auctions are used to match transactions on electricity generated in the next hour or hours. Bidders' identities and bidding information all contain users' electricity consumption in the next one to several hours. Criminals can calculate whether users are at home from users' electricity consumption information and then carry out theft [10] and other behaviors when they are not at home. Therefore, it is also very important to protect bidders' identities and bidding information.Privacy protection problem in the process of auction has aroused people's concern. The first attempt in the literature [11] to conduct a secure continuous double auction mechanism achieves the anonymity of bidders. However, its marketing manager has a pseudonym and a real identity correspondence, which is likely to cause the bidder's privacy to leak. Based on the literature [11], a new scheme based on group signature CDA was proposed in paper [12], which not only enables secure anonymity but also adds and removes bidders in bids without affecting the auction process.The electronic auction scheme based on group signature and partial blind signature was proposed in paper [13], which reduced the dependence on trusted third parties. However, [12], [13] all have the problem that group administrators have the supreme right of identity tracking, and it is possible that administrators abuse their power to expose users' privacy [14]. The British electronic auction scheme based on the revocable ring signature proposed in [15] can achieve conditional privacy but requires multiple repeated bilinear operations to achieve traceability [16]. The scheme of public auction based on blind signature is proposed in [17], which improves efficiency but does not have traceability.

By analyzing the privacy protection schemes proposed in [11]–[17], this paper summarizes the following basic characteristics of the privacy protection scheme for the continuous double auction process.

1) Anonymity: No one can identify the true identity of the user who participated in the auction throughout the auction.

2) Unforgeability. Users or organizations cannot participate in bidding by forging other users.

3) Non-repudiation. Two-way authentication between users and authorities.

4) Traceability. The true identity of users who are involved in the auction can be tracked.

5) Robustness. Even if any authority or two authorities are attacked, the privacy of the user cannot be undermined.

In this paper, the privacy protection scheme of microgrid direct transaction based on consortium blockchain and continuous double auction is proposed to solve the problems of high blockchain cost, slow speed and lack of privacy protection for continuous double auction. The combination of consortium blockchain technology and continuous double auction mechanism is applied to reduce transaction cost and improve transaction efficiency, pseudonyms and pseudonym certificates are generated by fair blind signature technology to realize identity privacy in continuous double auction, and decentralization and user identity traceability are realized by using (t, n) threshold secret sharing technology which distributes and recovers the private key of a trusted third party.

The rest of this article is organized as follows. The second part introduces the knowledge of the consortium blockchain, continuous double auction mechanism, fair blind signature and secret sharing used in the implementation of the scheme. The third part firstly describes the scheme model of this scheme, and then describes the working process of microgrid power direct transaction.The fourth part describes in detail the implementation process of the solution in this paper. The fifth part analyzes the scheme of this paper from two aspects of performance and security. The sixth part summarizes the paper and points out the potential research direction.

II. RELATED TECHNOLOGY

A. UNION BLOCKCHAIN

The consortium blockchain is a special blockchain. It is built on a certain number of pre-selected authentication nodes. The consensus algorithm is executed by these pre-selected nodes instead of all nodes in the whole network, which can greatly reduce energy costs and improve consensus efficiency. As a semi-centralized blockchain, the consortium blockchain also has the characteristics that trading data can be trusted, traceable and stored in the distributed system without tampering [18]. Moreover, only authorized nodes can join the blockchain trading platform, which can achieve a good balance between supervision and user privacy.

Compared with the public blockchain, the consortium blockchain has fewer consensus nodes, higher system operating efficiency, lower cost and faster transaction speed, etc., which are more suitable for power trading of micro grid.

B. CONTINUOUS DOUBLE AUCTION MECHANISM

Continuous double auction is a public auction in which there are multiple buyers and sellers in the market and the buyers and sellers can submit their offers at any time during the trading cycle and adjust their offers by observing others' offers. The seller and the buyer are sorted according to the principle of "price first, time first". The buyer's price is sorted from high to low, while the seller's price is sorted from low to high. Once the price matches, the transaction can be completed.

The continuous double auction mechanism is suitable for energy trading in the microgrid with sufficient flexibility and efficiency.

C. FAIR BLIND SIGNATURE TECHNOLOGY

Chaum first proposed a blind digital signature scheme [19] in 1983. In this scheme, signers sign without knowing the specific contents of signed messages. The sender can extract the valid signature of messages from the blind signed messages, and signers cannot match the signing process with the final signature. A fair blind signature adds a feature to blind signatures by establishing a trusted center through which the signer can track the signature.

The fair blind signature has the characteristics of protecting the privacy of the user and realizing the traceability of the user's real identity. It is fully applicable to the microgrid users requesting anonymous transactions, and traces the identity of dishonest users in the transaction process.

D. SECRET SHARING

The secret sharing technique is to share the secret S among many participants P. Currently, in most schemes, (t,n) threshold secret sharing is applied, that is, S is divided into n parts and then distributed to n participants. At least t members of the participants can reconstruct the secret S, while any member less than t cannot reconstruct the secret S [20].

(t,n) threshold secret sharing technology saves the private key of trusted third party separately to realize decentralization. The user's identity can be traced by obtaining the complete private key using key recovery technology.

III. DESCRIPTION OF PRIVACY PROTECTION SCHEME

A. WORKING PROCESS OF MICROGRID POWER DIRECT TRANSACTION

The microgrid electricity direct transaction model based on the consortium blockchain and continuous double auction mechanism is designed for users in a microgrid. There are two types of entities involved: power producers and power consumers. Power producers and power consumers continuously adjust their quotations during the trading cycle through a continuous double auction mechanism to complete the transaction matching. The transaction settlement is carried out through the consensus process of the consortium blockchain, thereby realizing direct transactions of users within the microgrid. The basic execution process consists of the following three parts. 1) Users register to generate the transaction certificate. 2) Users complete the electricity transaction matching through the continuous double auction mechanism. 3) The consortium blockchain local aggregator nodes complete the consensus. Flow diagram of direct power trading process in microgrid is shown as Fig.1.

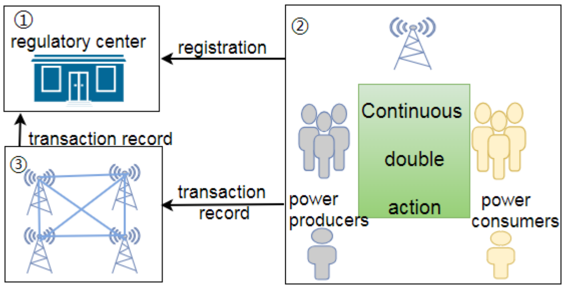

FIGURE 1. Flow diagram of direct power trading process in microgrid. There are three stages: user registration, user participation in auction and node consensus on transaction records.

The basic process of microgrid direct power trading is as follows.

① Users who participate in power transactions register in the regulatory center to obtain pseudonyms and pseudonyms trading certificates for transaction matching.

② After matching between consumers and producers through a continuous double auction mechanism, consumers confirm the authenticity of the accounts and electricity bills sent by producers and create transaction records.

③ Power producers send electricity charges and transaction records to a local aggregator, which encrypts the transaction records and packages them into blocks that broadcast validation to each aggregator node. After the consensus process of the consortium blockchain, a new block is generated to join the consortium blockchain. The transaction records in the consortium blockchain shall not be tampered with and are highly transparent for user nodes to query.

B. PRIVACY PROTECTION PLAN

In this paper, a privacy protection scheme is designed to prevent unnecessary losses caused by the leakage of users' electricity information during the direct transaction of microgrid based on consortium blockchain and continuous double auction mechanism. The basic system architecture of this privacy protection scheme based on a microgrid design. The privacy protection scheme involves four types of entities: microgrid users (U_i), Registration Management Center (RM), Market Management Center (MM), and Trace Center (TC). Users generate pseudonyms in RM and pseudonym certificates corresponding to pseudonyms in MM. Users only need pseudonyms and pseudonym certificates to participate in subsequent auctions without real user identity information to achieve fair auction. The TC is used to track the true identity of the user when necessary. Privacy protection scheme system architecture is shown as Fig.2.

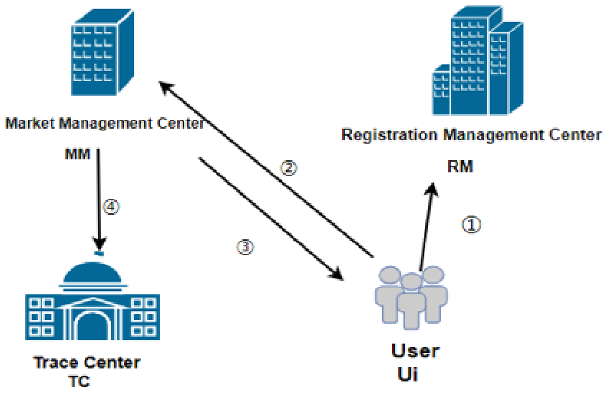

FIGURE 2. The system architecture of the privacy protection scheme. The privacy protection scheme involves four types of entities: microgrid users (U_i), Registration Management Center (RM), Market Management Center (MM), and Trace Center (TC).

The basic implementation process of this privacy protection is as follows.

① Users who participate in the auction register first, and generate the corresponding pseudonym after verifying the user's identity through RM using fair blind signature.

② Users apply to MM for pseudonym certificates.

③ MM generates the pseudonym certificate required by the user to participate in the power auction.

④ Trusted third party–Trace Center (TC). TC's private key is kept separately by using (t, n) threshold secret sharing technology to ensure that no trusted institution can generate the corresponding relationship between the user's real identity and pseudonym in this process. Meanwhile, key recovery can also be used to realize the traceability of users who back out halfway.

IV. PRIVACY PROTECTION PROGRAM IMPLEMENTATION

A. THE IDEA OF PRIVACY PROTECTION SCHEME

1) The private key of the TC is stored separately through the secret sharing of (t, n) thresholds, which is not vulnerable to attack and achieves robustness.

2) User pseudonym and transaction certificate are generated by fair blind signature. During the generation process, the user and the RM and MM are authenticated in both directions to achieve the anonymity, unforgeability and non-repudiation of the scheme.

3) The recovery of the TC private key is through the (t, n) threshold secret sharing technology, then the TC tracks the true identity of the user to achieve traceability of the solution.

B. IMPLEMENTATION PROCESS

1) SYSTEM INITIALIZATION AND PARAMETER SETTINGS

Before participating in the power transaction, the node joining the blockchain of the alliance connects to a local aggregator and sends its account to the local aggregator. Local aggregator nodes store complete blockchain transaction data [21] for users to query and verify transactions, while ordinary nodes participating in power transactions store part of the data and the form of hash chain composed of each block head in blocks, thus effectively reducing the total data storage and the overall storage overhead. On the other hand, it lowers the performance threshold of joining nodes and promotes more and poorer nodes to join the consortium blockchain.

The public key (N_u, e_u) and private key d_u generated by the user through the RSA algorithm. The public key (N_{RM}, e_{RM}) and private key d_{RM} generated by the RM via the RSA algorithm. MM generates a public key (N_{MM}, e_{MM}) and a private key d_{MM} via the RSA algorithm. The TC generates a public key (N_{TC}, e_{TC}) and a private key d_{TC} via the RSA algorithm. The public keys of RM, MM and TC are published on the bulletin board managed by MM, and the private keys of RM and MM are kept by themselves.

2) USING THE (T,N) THRESHOLD SECRET SHARING TO REALIZE TC PRIVATE KEY DISTRIBUTION

After TC private key is generated by RSA algorithm, the private key is stored in n participants separately according to (t,n) threshold secret sharing scheme. The private key distribution process is as follows.

① The share of the sub-private key owned by each participant is selected. In order to improve the efficiency, the share selected is incremental while ensuring that the share of each participant is not the same.

② Construct the n-order polynomial $F(x)$ using Lagrangian interpolation.

$$F(x) = d_{TC} + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{n-1} x^{n-1} \quad (1)$$

The first term is the initial obtained private key d_{TC}, and a_1, a_2, a_3, …, a_{n-1} are the coefficients of the polynomial. The electricity of the polynomial represents the share of the child private key obtained by the participant.

③ The contents of the sub-private key obtained by each participant are obtained by substituting the share and private key information obtained by each participant into the polynomial calculation results.

3) GENERATE USER PSEUDONYMS AND TRANSACTION CERTIFICATES USING FAIR BLIND SIGNATURE TECHNOLOGY

At this stage, the users participate in the public electric energy auction anonymously by generating pseudonyms and pseudonym certificates, as shown in Fig.3. The basic execution process is divided into the following six steps.

① $U_i \rightarrow RM : \{ID_u, S_U\}$

The user sends the ID_u that identifies the user's identity to RM, as well as S_U. where

$$S_U = ID_{RM}^{d_u} \ mod \ N_u \quad (2)$$

② $RM \rightarrow U_i : \{ID_{RM}, S_{RM}\}$

The RM verifies the user signature, and if the authentication is successful, agrees to generate a pseudonym and sends ID_{RM} and S_{RM} to the user.

$$S_{RM} = \left[(ID_{RM} \| ID_u \| \ ts)^{d_{RM}} \ mod \ N_{RM} \right]^{e_u} mod \ N_u \quad (3)$$

where *ts* is a valid timestamp.

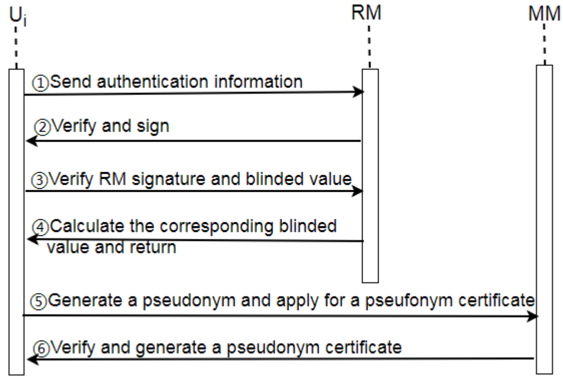
Ui
RM
MM
①Send authentication information
②Verify and sign
③Verify RM signature and blinded value
④Calculate the corresponding blinded value and return
⑤Generate a pseudonym and apply for a pseufonym certificate
⑥Verify and generate a pseudonym certificate

FIGURE 3. **The process of pseudonym transaction certificate generation. Mainly divided into six steps, involving three types of entities.**

③ $U_i \rightarrow RM : \{B_i\}$

After receiving the message, the user decrypts using the user's private key, and then uses the public key of the RM to verify that it is the RM signature, selects the random number $x_i, y_i \in Z_N^*$, and calculates the blind value.

$$B_i = y_i^{e_{RM}} x_i \tag{4}$$

④ $RM \rightarrow U_i : \{Z_i, w_i\}$

After receiving the $B - i$, the RM calculates

$$z_i = \left(y_i^{e_{RM}} x_i \cdot (i \,\| ID_u \|\, ts)\right)^{d_{RM}} \tag{5}$$

$$w_i = \left((i \,\| ID_u \|\, ts)^{e_{TC}}\right)^{d_{RM}} \tag{6}$$

Then sends z_i and w_i to the user.

⑤ $U_i \rightarrow MM : \{(ID_{RM} \,\|\, \{ID_{u'} \,\|\, s_{1,i} \,\|\, s_{2,i} \,\|\, e_{u'} \,\|\, N_{u'} \,\|\, S_{u'}\})^{e_{MM}}\}$

User verified RM signature. If the verification is successful, the process of blindness is as follows.

$$s_{1,i} = z_i / y_i \tag{7}$$

$$s_{2,i} = s_{1,i}^{e_{TC}} / w_i \tag{8}$$

Generate the pseudonym as follows:

$$ID_{u'} = x_i \cdot (i \,\| ID_u \|\, ts)\, x_i^{e_{TC}} \tag{9}$$

Send the message $C_{u'}$ to MM.The message is generated as follows:

$$C_{u'} = (ID_{RM} \,\|\, \{ID_{u'} \,\|\, s_{1,i} \,\|\, s_{2,i} \,\|\, e_{u'} \,\|\, N_{u'} \,\|\, S_{u'}\})^{e_{MM}} \tag{10}$$

where $S_{u'}$ is the temporary signature of the user U with the temporary private key $d_{u'}$.

⑥ $MM \rightarrow U_i : \{Cert_{u'}\}$

The MM verification blind signature process is as follows.

$$\begin{aligned} s_{1,i}^{e_{RM}} &= (z_i/y_i)^{e_{RM}} = \left(x_i \cdot (i \,\| ID_u \|\, ts)^{d}_{RM}\right)^{e_{RM}} \\ &= x_i \cdot (i \,\| ID_u \|\, ts) \end{aligned} \tag{11}$$

$$\begin{aligned} s_{2,i}^{e_{RM}} &= \left(s_{1,i}^{e_{TC}}/w_i\right)^{e_{RM}} = \left((z_i/y_i)^{e_{TC}}/w_i\right)^{e_{RM}} \\ &= \left(\left(x_i^{d_{RM}}\right)^{e_{TC}}\right)^{e_{RM}} = x_i^{e_{TC}} \end{aligned} \tag{12}$$

If the validation is successful, MM generates auction certificate F1 to the user.

$$C_{u'} = ID_{MM} \| ID_{u'} \| ts \| e_{u'} \| N_{u'} \| S_{MM} \tag{13}$$

4) USERS PARTICIPATE IN CONTINUOUS DOUBLE AUCTION TO ACHIEVE TRANSACTION MATCHING

①The user completes the registration and obtains the transaction certificate.Within the trading cycle,users submit the bidding message offer, $Cert_{u'}$ and $Sig^{u'}_{d_{u'}}(offer)$. Where$offer = \{ID_{u'}, bid\ m, time\ stamp, transaction\ electricity\}$, $Cert_{u'}$ is the pseudonym certificate of the bidder as shown in Formula (13), and $Sig^{u'}_{d_{u'}}(offer)$ is u' digital signature of the bid price. A positive amount of trading power is expressed as a seller, and a negative amount of trading power is expressed as a buyer.

② Judge whether the bid price meets the market requirements according to the trading rules. If it meets the requirements, the bidder's price will be accepted; otherwise, the bidder will be required to resubmit the bid. Once the buyer's price is higher than the seller's price, the highest price of the buyer is matched with the lowest price of the seller.Similarly, the transaction price is the average price of both parties. At the same time, the market trading information is released, including the transaction price, the number of transactions and the bid information of unfinished transactions.

③ After submitting a round of quotations, the user re-selects the random number to generate the corresponding blinded value and pseudonym. It is then sent to MM for a new pseudonym certificate for the next round of auction bidding. Start a new trade match until the trading cycle expires and the market closes.

5) LOCAL AGGREGATOR NODES CONSENSUS TO GENERATE NEW BLOCKS TO JOIN THE CONSORTIUM CHAIN

After the user participating in the electricity transaction is matched, the electricity supply user sends his account information and electricity bill to the electricity user, and the electricity user confirms the authenticity of the account and creates a transaction record. Then, the electricity user sends the electricity cost and transaction record to the local aggregator. The local aggregator encrypts the transaction record and packs it into blocks, and broadcasts to each aggregator node to perform the consensus process of the consortium blockchain. Proof of Work (POW) is the consensus algorithm in the most secure public blockchain, but it is too inefficient to complete the user's real-time requirements, and there are too many computational resources. Proof of Stake (POS) and Delegated Proof of Stake (DPOS) reduce computing resource consumption relative to POW, but there is a problem of over-concentration.

Practical Byzantine Fault Tolerance (PBFT) used in consortium blockchain is adopted to implement consensus process for selected local aggregator nodes. When $n \geqslant 3f + 1$, n is the total number of local aggregator nodes participating in the consensus in the consortium blockchain, and f is the

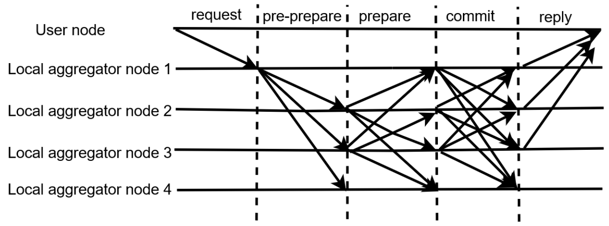

FIGURE 4. Consensus flow chart for local aggregator nodes. The local aggregator nodes 1, 2, 3, and 4 are participating in the consensus node, and the local aggregator 4 is the faulty node.

number of nodes that are allowed to fail. The consensus process is shown in Fig.4.

The consensus process between nodes is as follows [22].

① The user node sends an authentication request to the local aggregator node to invoke the service operation.

② The local aggregator node sends a broadcast request to other local aggregator nodes.

③ All local aggregator nodes execute the request and send the results to the user node, which waits for at least $f + 1$ results from different local aggregator nodes. If the result is the same, it is the final result of the request.

After the transaction record is added to the consortium blockchain through the consensus process, all records are stored in the blockchain for users to query and trace.

6) RECOVERING WITH (T,N) THRESHOLD SECRET SHARING TECHNOLOGY

The buyer of the winning bid has not paid the same amount of currency as the winning bid, or the seller has not paid the buyer the same amount of electricity as the winning bid. The trace center TC can recover the key through the (t, n) threshold secret sharing method [23] to obtain the private key.

In the private key recovery phase, the scheme sets the participant's collection to $A = \{P_1, P_2, P_3, \ldots, P_n\}$, requiring t participants to participate in order to recover the private key.The specific recovery process is as follows.

① Among the t participants participating in the recovery of the private key, each participant must obtain information about the private key.

② Each participant uses its own sub-private key share to calculate the sub-private key content. The result of the calculation is passed to the private key generator or to another participant who summons the recovery private key.

③ When the private key is recovered, Lagrange interpolation method is used to substitute the sub-private keys of each participant into the reconstruction polynomial. The calculation result of F(0) in Formula (1) restores the shared private key.

$ID_{u'}$ is derived from Formula (13), and $x_i^{e_{TC}}$ can be calculated from the above Formula (9). x_i is calculated by the recovered private key d_{TC}, and then the user's real identity ID_u is calculated. The restored users are subject to economic penalties or blacklists that prevent them from continuing to participate in consecutive double auctions.

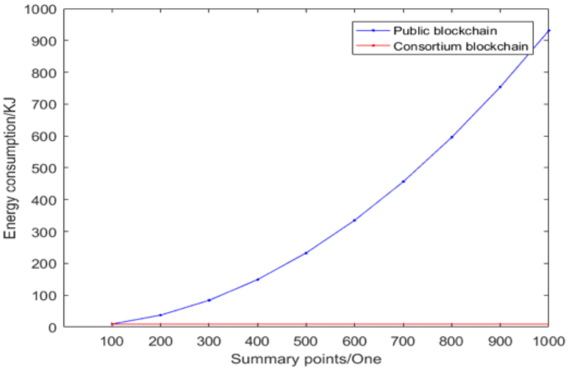

FIGURE 5. Comparison of consumption cost of public chain and alliance chain. The consortium blockchain is not affected by the summary points.the public blockchain increases dramatically as the number of summary points increases in broadcast and verification consumption.

V. PROGRAM ANALYSIS

In this paper, a privacy protection scheme of microgrid direct transaction based on consortium blockchain and continuous double auction is designed to realize user privacy protection by using fair blind signature and (t, n) threshold secret sharing technology.The following analysis of the program from both performance and security.

A. PERFORMANCE ANALYSIS

The consortium blockchain in this scheme has lower storage cost and consumption compared with the public blockchain. The main block energy consumption of the consortium blockchain adopts the PBFT consensus algorithm is the broadcast data operation between the authorized nodes and the inter-node verification operation. $n^2 + n - 2$ broadcast operations and $n^2 + 2n - 2$ verify operations are required between n authorized nodes [24]. Each node requires $0.9J$ of energy to perform a broadcast operation and $0.03J$ of energy for a verification operation. Comparison of consumption cost of public chain and alliance chain is shown in Fig.5.

The Fig. 5 shows that with the increase of the total number of nodes in the consortium blockchain and the blockchain, in the consortium blockchain with the authorization node of 100, each consensus consumes about 9.6KJ, and is not affected by the summary points. In contrast, the public blockchain, which requires a consensus of the total nodes of the entire network, increases dramatically as the number of summary points increases in broadcast and verification consumption.

The consortium blockchain in this scheme is broadcast and verified by selecting limited authorized nodes.Verification time t is related to block size(S), number of authorized nodes(n) and network bandwidth(B). According to multivariate linear fitting, t = 253.763 + 520.603S + 0.414n − 23.877 B [25]. According to the above calculation method, the simulation experiment was carried out with Matlab in 2.40 GHz CPU, 8 GBRAM, Windows 7 environment. The amount of transactions per second in the coalition chain as a function of the number of consensus nodes is shown in Fig.6.

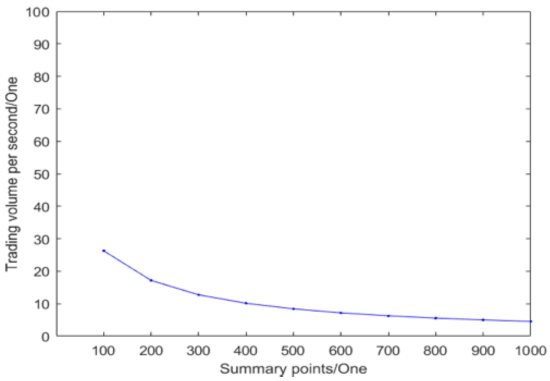

FIGURE 6. The amount of transactions per second in the coalition chain as a function of the number of consensus nodes.

The Fig.6 shows that when the number of authorized nodes is 100, the consortium blockchain can achieve 26 transactions per second, which is easier to land in the microgrid electricity transaction.

B. SECURITY ANALYSIS

Security analysis of consumers in the process of continuous double auction:

1) Anonymity: Firstly, the known information of RM includes ID_u, ts, $y_i^{eRMx_i}$, z_i and w_i. Since $x_i, y_i \in Z_N^*$ is a random number selected by the user, RM cannot derive x_i, y_i from $y_i^{eRMx_i}$, and thus cannot obtain the Formula (9). Secondly, the known information of MM includes ID_u, $s_{1,i}$, $s_{2,i}$, ts, $e_{u'}$ and $N_{u'}$. Since MM does not trace the private key of TC center, the user's real identity ID_u cannot be obtained according to $s_{1,i}$, $s_{2,i}$ and the Formula (9). Thirdly, the known information of the remaining producers participating in the auction includes $ID_{u'}$, ts, e'_u, $N_{u'}$ in the pseudonym certificate. Since the private key d_{TC} of the center TC is not traced, it cannot be obtained according to the Formula (9).

2) Unforgeability: For RM, the user's true identity information ID_u cannot be forged. It is determined whether the RM forges user identity information by checking whether $y_i^{eRM} = (i \,\|ID_u\|\, ts)^{eTC}$ is established after the w_i is sent to the user in the transmitted message $\{z_i, w_i\}$. For users, no other user information can be forged to generate a pseudonym certificate. Since the pseudo-names of other consumer information are generated, it is necessary to satisfy the Formula (11) and (12). However, the user cannot obtain the RM private key to satisfy the above formula, so the user cannot generate the pseudonym certificate through the verification of the MM. For non-legal entities, there is two-way authentication throughout the certificate issuance process. The illegal entity cannot obtain the private key of the user and the RM, so it cannot obtain any communication information during the certificate issuance process.

3) Non-repudiation: The public and private key values between consumer, RM and MM are used to realize encryption and digital signature so that the whole certificate issuance process has two-way authentication, realizing the non-repudiation among the three.

TABLE 1. Comparison of security.

	Attributes				
	Anonymity	Unforgeability	Non-repudiation	Traceability	Robustness
Ref.[11]	✓	✗	✗	✓	✗
Ref.[12]	✓	✓	✓	✓	✗
Ref.[17]	✓	✓	✓	✗	✗
This program	✓	✓	✓	✓	✓

4) Traceability: When the successful bidder does not pay the corresponding electricity or the amount to be paid, the private key of the TC is restored based on the (t, n) threshold secret sharing method. The pseudonym $ID_{u'}$ is derived from Formula (13), and x_i^{eTC} can be calculated from the above Formula (9). x_i is calculated by the recovered private key d_{TC}, and then the user's real identity ID_u is calculated.

5) Robustness: RM only saves the real identity certificate of the user of the producer, MM only saves the pseudonym generated by the user of the producer, and the collusion of the two does not reveal the mapping relationship between the real identity and the pseudonym of the user. The private key of the tracking center utilizes the (t, n) threshold secret sharing scheme to store the private key in a distributed manner, avoiding the problem of centralized and excessive electricity. At the same time, it can avoid the failure of the tracking center to find the Real identity information of the users who renege.

The security comparison of several schemes is shown in Table 1.

VI. CONCLUSION

With the rapid development of distributed energy, traditional centralized power trading cannot meet the requirements of direct safe and efficient power trading among microgrid users. This paper proposes a privacy protection scheme for micro grid transactions based on consortium blockchain and continuous double auction mechanism. Performance analysis and security analysis show that: 1) The combination of the alliance blockchain and the continuous double auction mechanism is used to address the small-scale, low-cost, high-efficiency requirements of the microgrid. 2)The privacy protection scheme achieves anonymity, non-forgery, non-repudiation, traceability and robustness. How to carry out detailed quantitative verification of this program is a problem worthy of further study and solution.

REFERENCES

[1] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The brooklyn Microgrid," *Appl. Energy*, vol. 210, pp. 870–880, Jan. 2018. doi: 10.1016/j.apenergy.2017.06.054.

[2] N. Zhang, Y. Wang, C. Kang, and J. Cheng, "Blockchain technique in the energy Internet: Preliminary research framework and typical applications," *Proc. CSEE*, vol. 36, pp. 4011–4022, Aug. 2016.

[3] S. Cheng, B. Zeng, and Y. Z. and Huang, "Research on application model of blockchain technology in distributed electricity market," *IOP Conf. Earth Environ. Sci.*, vol. 93, Nov. 2017, Art. no. 012065. doi: 10.1088/1755-1315/93/1/012065.

[4] X. Ouyang, X. Zhu, L. Ye, and J. Yao, "Preliminary applications of blockchain technique in large consumers direct power trading," *Proc. CSEE*, vol. 37, no. 13, pp. 3672–3681, Jun. 2017.

[5] J. Ping, S. J. Chen, and N. Zhang, "Decentralized transactive mechanism in distribution network based on smart contract," *Proc. CSEE*, vol. 37, no. 13, pp. 3682–3690, Jun. 2017.

[6] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018. doi: 10.1109/TDSC.2016.2616861.

[7] J. Stanczak, W. Radziszewska, and Z. Nahorski, "Dynamic pricing and balancing mechanism for a microgrid electricity market," in *Advances in Intelligent Systems and Computing*, vol. 323. 2015, pp. 793–806.

[8] J. Wang, Q. G. Wang, and N. C. Zhou, "A novel electricity transaction mode of microgrids based on blockchain and continuous double auction," *Energies*, vol. 10, no. 12, p. 1971, Nov. 2017. doi: 10.3390/en10121971.

[9] K. Chen, J. Lin, and Y. Song, "Trading strategy optimization for a prosumer in continuous double auction-based peer-to-peer market: A prediction-integration model," *Appl. Energy*, vol. 242, pp. 1121–1133, May 2019. doi: 10.1016/j.apenergy.2019.03.094.

[10] S. Zhang, T. Zheng, and B. Wang, "A privacy protection scheme for smart meter that can verify terminal's trustworthiness," *Int. J. Elect. Power Energy Syst.*, vol. 108, pp. 117–224, Jan. 2019. doi: 10.1016/j.ijepes.2019.01.010.

[11] C. Wang and H.-F. Leung, "Anonymity and security in continuous double auctions for Internet retails market," in *Proc. 37th Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2004, pp. 10–17. doi: 10.1109/HICSS.2004.1265431.

[12] J. Trevathan, H. Ghodosi, and W. Read, "An anonymous and secure continuous double auction scheme," in *Proc. 39th Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 6, p. 125b, Jan. 2006. doi: 10.1109/HICSS.2006.45.

[13] Y. Dong, B. Li, and Z. X. Zheng, "An electronic auction scheme based on group signatures and partially blind signatures," *Procedia Eng.*, vol. 15, pp. 3051–3057, Jan. 2011.

[14] S. M. Zhang, Y. Q. Zhao, and B. Y. Wang, "Certificateless ring signcryption scheme for preserving user privacy in smart grid," *Autom. Electr. Power Syst.*, vol. 42, no. 3, pp. 23–118, Mar. 2018.

[15] H. Xiong, Z. Chen, and F. Li, "Bidder-anonymous english auction protocol based on revocable ring signature," *Expert Syst. Appl.*, vol. 39, no. 8, pp. 7062–7066, Jun. 2012. doi: 10.1016/j.eswa.2012.01.040.

[16] C.-C. Chang, T.-F. Cheng, and W.-Y. Chen, "A novel electronic english auction system with a secure on-shelf mechanism," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 657–668, Apr. 2013. doi: 10.1109/TIFS.2013.2250431.

[17] C.-I. Fan, C. N. Wu, and W. Z. Sun, "Multi-recastable e-bidding game with dual-blindness," *Math. Comput. Model.*, vol. 58, nos. 1–2, pp. 68–78, Jul. 2013. doi: 10.1016/j.mcm.2012.06.003.

[18] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017. doi: 10.1109/TII.2017.2709784.

[19] M. Abe and E. Fujisaki, "How to date blind signatures," in *Proc. ASIACRYPT*, vol. 1163, 1996, pp. 244–251.

[20] H. G. Rong, J. X. Mo, B. G. Chang, and G. Sun, "Key distribution and recovery algorithm based on Shamir's secret sharing," *J. Commun.*, vol. 36, no. 3, pp. 60–69, Mar. 2015. doi: 10.11959/j.issn.1000-436x.2015083.

[21] J. H. Chen, "Research on capacity optimization model of alliance blockchain,"M.S. thesis,Dept.Computer, Dalian Maritime University, Dalian, China, 2018.

[22] X. F. Liu, "Study on performance improvement of byzantine fault-tolerant consensus based on dynamic authorization," M.S. thesis, Dept. Comput., Zhejiang Univ., Zhejiang, China, 2017.

[23] L. J. Pang and Y. M. Wang, "Threshold secret sharing scheme based on RSA cryptosystem (t, n) threshold," *Chin. J. Commun.*, vol. 26, no. 6, pp. 70–73. Jun. 2005.

[24] J. Kang, R. Yu, S. Maharjan, Y. Zhang, X. Huang, S. Xie, F. Bogucka, and S. Gjessing, "Toward secure energy harvesting cooperative networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 114–121, Aug. 2015. doi: 10.1109/MCOM.2015.7180517.

[25] K. K. Wang, Z. D. Chen, and J. Xu, "Quality, safety and effificient traceability system of agricultural products based on union blockchain," *Comput. Appl.*, vol. 38, no. 8, pp. 1–7, Jul. 2019.

SHAOMIN ZHANG received the B.S. and Ph.D. degrees from Xidian University, China, in 1988 and 2009, respectively.

She is currently a Professor with School of Control and Computer, North China Electric Power University. Her current research interests include power information and information security. Her research is supported by the Fundamental Research Funds for the Central Universities (2018 ZD06).

MIAO PU received the B.S. degree from the City College, Dalian University of Technology, China, in 2017. She is currently pursuing the master's degree with the School of Control and Computer, North China Electric Power University.

Her current research interests include data aggregation and information security. Her research is supported by the Fundamental Research Funds for the Central Universities (2018 ZD06).

BAOYI WANG received the B.S. degree from Xi'an Jiaotong University, China, in 1984, and the Ph.D. degree from North China Electric Power University, China, in 2009.

He is currently a Professor with the School of Control and Computer, North China Electric Power University. His current research interests include power information and information security. His research is supported by the Fundamental Research Funds for the Central Universities (2018 ZD06).

BIN DONG received the B.S. and M.S. degrees in information and computing science and computer science and technology from North China Electric Power University, Baoding, in 2003 and 2006, respectively, and the Ph.D. degree in optical engineering from Hebei University, Baoding, in 2012. He is currently an Advanced Engineer with the Affiliated Hospital of Hebei University. His research interests include network security and the artificial intelligent algorithm in computer vision.