A Secure Microgrid Power Transaction Scheme Based on Hyperledger Fabric

Shuihai Zhang[1], Haoyi Sun[1], Bei Pei[2], and Chunli Lv[1](✉)

[1] College of Information and Electrical Engineering, China Agricultural University, Beijing, China
lvcl@cau.edu.cn

[2] The 3rd Research Institute of the Ministry of Public Security, Shanghai, China

Abstract. As part of the smart grid, distributed power trading based on clean energy generation has attracted a lot of attention and investment in recent years. This paper adopts the Hyperledger Fabric blockchain as the underlying framework, combined with key technologies such as smart contracts, blockchain oracles, bilateral auction mechanisms, and multi-signatures, and proposes a secure microgrid power transaction scheme based on Hyperledger Fabric. Different from the existing schemes, this paper considers the security and integrity issues that may arise in the transaction process. In terms of power trading, this scheme proposes two trading modes that can be carried out simultaneously and don't affect each other, that is, trading based on predicted power and trading based on reserved power. In terms of transaction protection, the user credit and proof of work algorithm are introduced into the continuous double auction mechanism to solve the possible malicious bidding problem. In addition, the multi-signed address wallet is used to ensure the transaction security of users without a trusted center. Finally, the security and feasibility analysis of the paper proves the effectiveness of the scheme.

Keywords: Blockchain · Power Trading · Smart Grid · Smart Contract · Multiple Signature

1 Introduction

Energy is an important material basis for the national economy, and the future destiny of a country depends on the development and effective utilization of energy. In recent years, clean energy, led by solar energy, wind energy, and nuclear energy, has accounted for an increasing proportion of power generation. In Beijing, clean energy has replaced coal as the main energy source in this international metropolis, accounting for 46.7% of the city's energy consumption. Furthermore, as more and more people choose to install solar panels in their homes, the current energy structure is also characterized by a tendency

This work was supported by the Key Laboratory of Information and Network Security, Ministry of Public Security, the Third Research Institute of the Ministry of Public Security (C19605).

W. Meng and W. Li (Eds.): BlockTEA 2022, LNICST 498, pp. 49–65, 2023.
https://doi.org/10.1007/978-3-031-31420-9_4

to be decentralized. The distributed trend is conducive to solving the problem of energy loss due to the long physical distance of power transmission through the community-level microgrid [1]. Prosumers of clean power are allowed to trade power with others or to sell it to higher-level grids for subsidies in the microgrid. However, in the past, the transactions between prosumers were characterized by a large number of orders, small scale and fragmentation. Therefore, how to build a suitable trading platform and supervision mechanism is the focus of the current electric power research.

1.1 Related Works

Thanks to features of decentralization, tamper resistance, trustworthiness, and anonymity [2], blockchain technology is widely used in energy transactions in microgrids. Blockchains are shared and distributed ledgers of data that securely store digital transactions without the use of centralized nodes [3]. In recent years, the combination of blockchain technology and community-level microgrid power trading has been widely researched and applied pilots [4]. The Brooklyn Microgrid is the first energy blockchain project in the world to be put into practice. It adopts P2P direct energy trading without going through a third-party power supplier. The project is deployed on the Ethereum blockchain platform, and integrates the smart contract function of the Ethereum blockchain at the bottom of the smart meter for data collection. However, the experimental scale of this project is small, limited to 10 participating users, and further verification is required for larger-scale project implementation. Nonetheless, The Brooklyn Microgrid has served as a good example for energy blockchain projects around the world, driving the development of related P2P distributed electricity transactions [5].

In the academic field, there has also been a lot of discussion about energy blockchain in recent years. One of the first systematic reviews in this field was made by Andoni et al. [6]. By analyzing the existing use cases of energy blockchain, it discusses the advantages and limitations of blockchain applications in this field. Mengelkamp et al. analyze seven market components that may be required to build a blockchain microgrid energy market and analyzed and discussed the world's first energy blockchain project, the Brooklyn Microgrid [5]. Lüth et al. analyze the value of batteries in local peer-to-peer energy trading schemes and market designs for battery systems at the customer level and community level, respectively [7]. Zhao et al. designed a blockchain-based multi-microgrid energy transaction double-layer framework, which considers transactions between multiple microgrids in addition to transactions within microgrids [8]. In addition, some researchers focus on the use of cryptography to realize the protection of user privacy and transaction security in the microgrid energy trading market. Aitzhan et al. use blockchain technology, multi-signature, and anonymous encrypted information flow respectively to realize the security verification of the decentralized energy trading system [9]. Gai et al. focus on how to prevent attackers from exploiting data mining algorithms to obtain user privacy from transaction data stored in the blockchain [10]. Yao et al. introduce the lightweight WireGuard VPN technology that has been widely used in recent years based on the blockchain platform to protect users' communication privacy [11]. Furthermore, Wang H et al. [12] and Wang H.Z et al. [13] focus on research on accurate forecasting techniques for renewable energy generation to ensure a reliable environment for electricity trading.

1.2 Contribution

Most of the existing distributed energy trading schemes have the following three problems. First, most current energy blockchain designs are based on public chains such as Ethereum. However, the confidentiality of transaction information is one of the important attributes for electricity transactions in smart grids. As a consortium chain, Hyperledger Fabric can better meet privacy and permission requirements than public chains. Second, most schemes fail to consider the potential attacker's damage to the transaction process, and cannot well meet the security requirements of the system. Finally, due to the volatility and other characteristics of clean energy power generation, the corresponding transaction methods are based on the predicted energy and based on reserve energy. But many studies have considered only one of them.

This paper proposes a distributed power trading system based on Hyperledger Fabric, which fully considers the security and integrity issues that may arise in the trading process. The main contributions of this paper are described as follows:

1) In view of the possible electricity trading situations in reality, we have designed two trading models based on predicted power and based on reserve power.
2) In order to curb the malicious bidding behavior of users and encourage the honest behavior of participants, we designed a bilateral continuous bidding mechanism based on credit behavior and proof of work algorithm.
3) We use multi-signature technology to protect the smooth delivery of funds during the transaction process without a trusted center.

The remainder of this paper is organized as follows. We introduce the main technologies used in the distributed power trading system in Sect. 2. The user model, framework design, and core components of the scheme are elaborated in Sect. 3. In Sect. 4, We describe the process of distributed electricity trading in detail. In Sect. 5, we analyze the effectiveness of this scheme from two aspects of safety and feasibility. Finally, we summarize the overall work in Sect. 6.

2 Preliminary

2.1 Hyperledger Fabric

Blockchain, also known as distributed ledger technology, is essentially a decentralized distributed ledger database [14]. Cryptography and consensus algorithms enable multiple peer nodes in a blockchain network to replicate, synchronize and share the same ledger. They ensure the consistency of ledger data, and also make the blockchain have the characteristics of decentralization, tamper-proof, trustworthiness, and traceability [15]. Depending on the way users of the network participate, blockchains can be divided into permissionless and permissioned. In permissionless blockchains, such as Bitcoin and Ethereum, nodes are free to participate without any permission, and transactions are completely transparent. Anyone can access the data. Correspondingly, permissioned blockchains only allow authorized users to join the network and have the ability to control data access. Furthermore, transactions on permissioned blockchains are not transparent.

Permissioned blockchains can be further divided into consortium blockchains and private blockchains. Different from the private blockchain, each node of the consortium blockchain usually has a corresponding entity organization, which can only join and exit the network after authorization. Various institutions and organizations form stake-related alliances to jointly maintain the healthy operation of the blockchain.

Hyperledger Fabric is a type of consortium blockchain, launched by the Linux Foundation in 2015 for developing applications or solutions with a modular architecture. Compared with public blockchain platforms. The biggest differences in Fabric compared to Bitcoin and Ethereum are privacy attributes and permission attributes. Fabric registers and records all members through the member management module, and gives them corresponding access rights. The Fabric architecture is shown in Fig. 1, and its modular and versatile design can satisfy a wide range of industrial use cases.

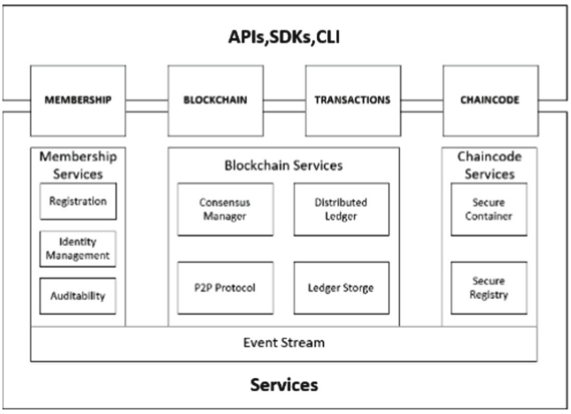

Fig. 1. The Architecture of Hyperledger Fabric.

2.2 Blockchain Oracle

A major limitation of blockchain technology is that it can't interact with the "outside world", only by manipulating the data on the blockchain to calculate and reach a consensus on the calculation results [16]. In addition, smart contracts usually require relevant information from the outside world as input (or meet certain conditions) in order to execute the agreement [17]. Therefore, how to realize the interaction between smart contracts and external resources is a practical problem that must be faced by the scheme design. The blockchain oracle is a consensus mechanism that incorporates external data into the blockchain [18]. It is a trusted entity that can collect, verify and transmit data from external sources [19]. Oracles need to provide reliable and valid information to ensure the consistency and validity of smart contract execution [20].

2.3 Proof of Work

As a consensus algorithm, Proof of Work (PoW) is widely used in most public chains and virtual currencies to ensure the consistency of distributed ledgers [21]. The effectiveness

of this algorithm has been extensively demonstrated. Its process can be summarized as: by searching for a suitable random number *nonce*, the Hash value of the content obtained after the data x is spliced with the *nonce* is less than or equal to the target hash value T. The hash value T is determined by the difficulty value n. The probability of finding a suitable nonce for a given target T is given by the following formula.

$$P(Hash(x||nonce) \leq T) = T/\left(2^{256}\right) \tag{1}$$

In this scheme, the broadcast of each quotation of a trader needs to meet the requirements of the PoW algorithm. That is, the appropriate *nonce* is calculated so that the transaction data x satisfies $Hash(x||nonce) \leq T$. In a transaction cycle, the difficulty value n of the PoW algorithm is the smallest at the beginning and increases with the increase of the number of quotations. In addition, the initial value of n is related to the user's credit value, and well-behaved users will likely have more bidding opportunities.

3 Smart Microgrid Power Trading System Based on Consortium Blockchain

In Hyperledger Fabric, the channel is a very important concept. It's a private atomic broadcast channel divided and managed by ordering nodes [22]. Its function is to isolate the information in the channel so that users outside the channel can't access the distributed ledger in the channel. The transaction in the channel satisfies privacy. To meet the practical needs of the two transaction modes proposed in this paper, namely forecast energy transaction and real-time reserve energy transaction, we have established two sets of application channels to ensure that they can be performed simultaneously without affecting each other. The design of channels and tissues in this protocol is shown in Table 1. Channel 1 is used to predict power trading, and Channel 2 is used to Stored power trading.

Table 1. Channel and organizational design in the scheme.

Channel	Channel 1	Channel 2
Organization 1	Prosumers	Prosumers with battery
Organization 2	Consumers	Consumers
Organization 3	Grid Operators	Grid Operators

In the microgrid power transaction based on predicted power, there may be three roles based on whether the power generation capacity is available. They are prosumers, consumers, and upper-level grid operators. Prosumers refer to community users who own clean energy output devices such as solar photovoltaic panels or wind turbines, and they can buy and sell power. Consumers refer to traditional electricity users who can't generate power. Since it is difficult to achieve a complete balance between the generation and

consumption of microgrids, the upper-level grid operators will participate in microgrid market transactions to regulate power.

In the microgrid power transaction based on reserve power, there may also be three roles: prosumers with energy storage devices, consumers, and upper-level grid operators. They are divided by whether they have the ability to store energy. Users in the microgrid can freely choose to purchase clean energy or fossil energy. They can also buy fossil fuels to meet demands when clean energy production is insufficient. Likewise, the prosumer can also sell the power he produces to the grid operator. The overall frame diagram of the system is shown in Fig. 2.

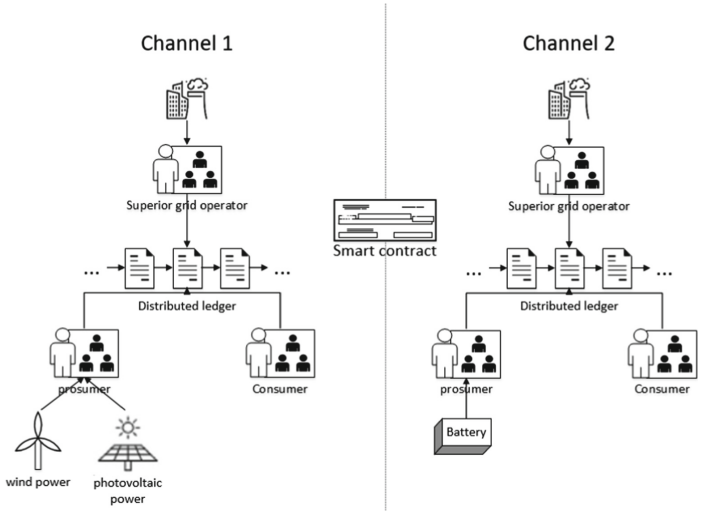

Fig. 2. The overall frame diagram of the system.

3.1 User and Node Definitions

Certificates are the basis of authority management in Fabric, and any entity or organization has its own unique identity certificate. The scheme adopts the asymmetric encryption algorithm based on ECDSA to generate the public key and private key, and the certificate format adopts the X.509 specification. When community users join the network for the first time, they need to verify the authenticity of their identities, and then the Fabric CA project will generate corresponding certificates for them. In addition, for the need of confidential communication outside the network, the ECDSA algorithm will additionally generate a pair of public key and private key for the user. The public-private key pair used to prove identity is denoted as pk, sk, and the public-private key pair used for secure communication is denoted as pk', sk'. In addition, credit should be used as an important indicator to evaluate users, which reflects whether users comply with the rules of network operation. Record the user's credit level as c. In this scheme, tokens are used to conduct virtual electricity transactions in the network. However, it is not a

virtual currency like Bitcoin, but is regarded as a kind of points obtained by exchanging or recharging legal currency. The user's token balance is recorded as a. The increase in the token balance can only be done in two ways: transaction or fiat currency exchange. The basic attributes of the node account A_i of user i in this scheme can be expressed as:

$$A_i = <pk_i, sk_i, pk_i', sk_i', c_i, a_i> \tag{2}$$

In fact, the above information of the node account is not completely public. For privacy reasons, the token balance recorded in the distributed ledger will be encrypted by pk_i, and the encrypted token balance will be recorded as a_i', as shown in the following formula.

$$a_i' = ENG_{pk_i}(a_i) \tag{3}$$

The encrypted token balance a_i' can only be unlocked by the private key sk_i. Therefore, all users in the network have no right to view the number of other users' tokens. This effectively protects the privacy of users. Build a structure for storing accounts in smart contracts. Record the mapping of node account A_i in the ledger as A_i'. Its structure is shown in the following formula.

$$A_i' = <pk_i, pk_i', c_i, a_i'> \tag{4}$$

Smart meter is an intelligent meter with microprocessor application and network communication technology as the core, and has the capabilities of automatic metering/measurement, data processing, two-way communication and function expansion. In this scheme, the smart contracts in Fabric will be highly integrated with the smart meter, and will be installed and executed on the smart meter. Users participating in the transaction need to install smart meters with integrated smart contracts. Smart meters can statistically analyze users' power consumption or generation in real time, and make predictions and preparations for users to participate in power transactions in the network. For prosumers, power analysis helps them master power consumption and generation. Excess power can be sold for profit under the premise of meeting their own availability. For consumers, mastering power consumption is conducive to purchasing the right amount of energy during the transaction phase, without causing excess or shortage of energy. We assume that the smart meter is sealed and tamper-proof. In addition, all smart meters installed by users participating in the microgrid in the community have the same model and computing power.

3.2 Smart Contract and Blockchain Oracle Design

In blockchain, smart contracts automate the process of transactions. The smart contract is a self-validating, self-executing, tamper-proof program executed on blockchain platform. It is defined as a program that digitally facilitates, verifies, and executes a contract between two or more participants on blockchain. Smart contracts are event-driven, which means they can be activated when predefined conditions are met [23]. In Fabric, smart contracts are called chaincodes, which are programs that can run independently in docker

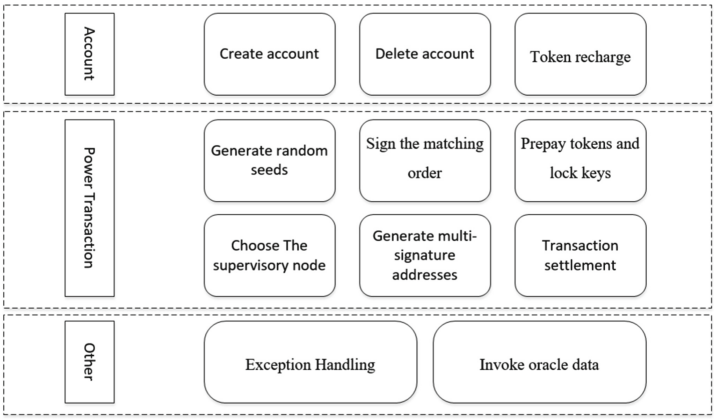

Fig. 3. Smart Contracts Design of Distributed Electricity Trading System.

containers. The main interfaces and functions of the smart contract designed in this scheme are shown in Fig. 3.

In this scheme, the oracle is designed to transmit local power generation and consumption data to the blockchain. Additionally, oracles complete transactions by interacting with smart contracts. Blockchain oracles will collect data from the physical world, including user electricity consumption information recorded in electricity meters and the power generation of clean energy power generation equipment under different conditions. The oracle will be installed in the smart meter along with the smart contract, and the smart meter is sealed and immutable.

The collection and upload of oracle data is designed in a "$Request - Response$" mode. This is because the user's data is too large to be completely stored in the blockchain. In addition, the smart contract only needs a part of the data per operation. "$Request - Response$" mode will initiate requests for oracle data by smart contracts on the blockchain. The off-blockchain infrastructure (the smart meter) will be used to monitor requests and retrieve data.

3.3 PCDA Algorithm

In transactions with multiple sellers and buyers, such as electricity transactions, the continuous double auction (CDA) mechanism is widely used [24]. When the auction starts, both buyers and sellers can make multiple bids. The transaction is completed when the prices of both parties match [25]. However, unrestricted offers from users can lead to increased processing burden on the system and even lead to DDoS attacks. In order to prevent traders from making multiple bids maliciously, this scheme introduces a credit-based PoW algorithm on the basis of CDA. c is the user's credit value, and x is the quotation order. num is the number of bids in the current trading cycle, and $nonce$ is a random number that satisfies the PoW algorithm. The process of Algorithm PCDA $(x, c, num, t) \rightarrow nonce$ is as follows.

1) At the beginning of the transaction phase, the user executes smart contracts to obtain the random seed t of the transaction period. The content of t is shared by all nodes in the network and is only valid within this period;
2) Calculate the required hash value $T \leftarrow f(c, num)$;
3) Traverse to find the random number $nonce$ to satisfy $Hash(x||t||nonce) < T$;
4) Output target $nonce$.

Correspondingly, each quotation order will be checked whether the nonce meets the requirements of the PCDA algorithm, such as formula 5.

$$Hash(x||t||nonce) < T \leftarrow f(c, num) \tag{5}$$

Any cheating behavior of the user will make the bid verification fail, and the calculation used to find the nonce of the random number will be in vain, which will further increase the difficulty of bidding. Therefore, it can be concluded that honest and curious nodes will consciously abide by the PCDA algorithm when bidding transactions. Malicious multiple bidding will not occur.

4 Distributed Power Transaction Process

This paper uses the concept of channels in Fabric to design two different power trading modes for forecast power and reserve power, respectively. This section will describe their detailed designs and processes.

In the distributed power transaction based on predicted power, namely channel 1, time is divided into time periods of length T in days. Due to the strong dependence of photovoltaic power generation on the environment and climate, the power generation in different cycles has great differences. Therefore, the division of cycles is necessary. Trade matching for predicted power will only take place at a fixed time before the start of a cycle, while trade settlement will take place at the end of the cycle. The difference is that in the distributed transaction based on reserve power, namely channel 2, the transaction is no longer divided into time periods or stipulated transaction time. Traders will be allowed to publish orders and trade at any time. The specific process of distributed power transaction is shown in Fig. 4.

The distributed power transaction processes are as follows:

Step 1: The smart meter statistically analyzes the user's electricity consumption and power generation in each cycle, and provides a reference for the user's quotation;
Step 2: Entering the trading stage, users generate eligible quotation orders and broadcast them through the p2p network. Nodes participating in the transaction establish a distributed order matching database locally to match the orders of buyers and sellers;
Step 3: Users can quote multiple times by executing the PCDA algorithm, and the successfully matched quote orders are submitted to the smart contract;
Step 4: The two parties of the successfully matched order will further confirm and sign the contract through the smart contract;
Step 5: After the contract is signed, the buyer prepays tokens and the seller delivers the electricity usage rights. The transaction result is written to the blockchain.

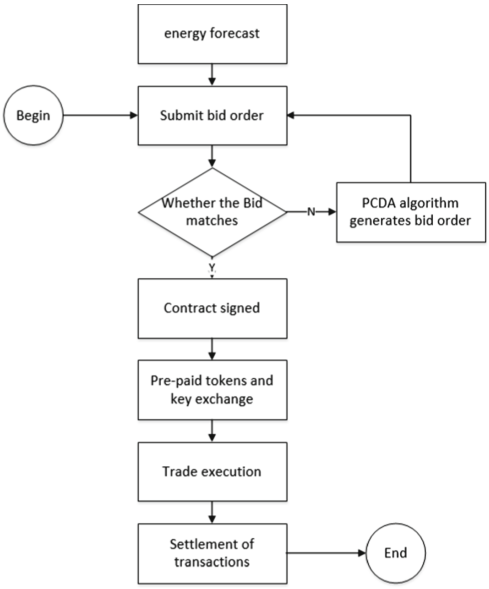

Fig. 4. The specific process of distributed power transaction.

Step 6: At the end of the order execution cycle, the smart contract reads the meter data of the transaction party and settles the transaction.

4.1 Publish Bid Order

In distributed electricity transactions, both prosumers and sellers have the right to issue orders. However, any prosumers who want to sell power will need to prove to the smart contract its ownership of the declared pre-sale power before publishing bid order. Take prosumer b as an example, generate b_α and b_β and store them in blockchain.

$$b_\alpha = Hash(pk_b||E_b||Time) \tag{6}$$

$$b_\beta = Hash(b_\alpha||RandomNumber) \tag{7}$$

E_b is the pre-sold electricity of prosumer b, and pk_b is its identity public key. b_α represents the ownership of the sellable power E_b by the prosumer b, and b_β is used for locking to prevent double payment for the power E_b. If b_β is not locked during the transaction, then b may sell the same power multiple times to other consumers.

For power trading based on forecasted power, quoting and matching of orders is only allowed during the order-issuing phase. The content of quotation order M^1 in channel 1 is shown in Eq. 8.

$$M^1 = <pk, S, E, P, c, num, nonce, Time> \tag{8}$$

Among them, pk represents the identity public key of the publisher, and S represents the type of quotation order issued (selling power or purchasing power). E is the amount

of electricity the bidder wants to trade. P is the unit price of power. c represents the credit rating of the publisher. *Time* is the order generation time. *num* represents the number of bids, and the initial value is 0. *nonce* is a random number that satisfies the condition calculated by the publisher through the *PCDA*. In addition, in order to prevent malicious attackers from forging or tampering with communication information, the publisher will use the communication private key $sk^{'}$ to sign the content M and broadcast it together.

For channel 2, bid orders to buy energy or sell energy are allowed to be issued at any time. Bid orders are recorded as M^2. Compared with M^1, M^2 adds transaction execution time t. This is because the transaction in channel 1 has the regulation of the transaction cycle, while channel 2 needs to manually set the duration and end time of the transaction. Similarly, the publisher will use $sk^{'}$ to sign the content M^2 and publish it.

$$M^2 = <pk, S, E, P, t, c, num, nonce, Time> \tag{9}$$

When nodes in the network receive the broadcasted bid order, the verification algorithm will be executed to verify whether the order is legal. Denote the signature of M as $M^{'}$. The algorithm $BidVerify(M, M') \rightarrow True/False$ process are as follows.

1) Verify the authenticity of order M and its signature M';
2) If M is a power sale order, verify whether there are matching power ownership certificates b_α and b_β in blockchain;
3) Verify whether the order meets the requirements of the PCDA algorithm according to *num* and c;
4) Returns *True* if the content is correct, otherwise returns *False*.

4.2 Bid Matching and Contract Signing

The bid matching stage will generate a large amount of intermediate data, which lacks the necessity of long-term storage. The blockchain has the characteristics that data cannot be tampered with and deleted. If the intermediate data of the transaction is stored in blockchain, it will inevitably cause a lot of waste of resources in the long run. Therefore, the system temporarily stores these data on all nodes in the network that participate in the transaction at this stage, which is achieved by establishing a temporary distributed order matching database locally on the node. The content of the order matching database is based on the broadcast order information. Since the predicted power transaction and the reserve power transaction are in two channels of Fabric, their transaction data and order matching database are independent of each other.

In the temporary order matching database, orders for energy sales will be ranked from lowest to highest in price, and orders for energy purchases will be ranked from highest to lowest in price. If the bid is the same, credit value and bid time will be used as the ranking basis. If $P_{buy} \geq P_{sell}$, both orders are deemed to have been matched and the energy price will be settled at P_{buy}. Both parties with successful order matching will further confirm and sign the contract through smart contracts. N is denoted as a trading contract. The processes of contract signing algorithm $Signcontract\left(M_{sell}, M_{buy}\right) \rightarrow N$ are as follows:

1) Smart contracts send trade proposals to both parties;

2) Both parties further confirm whether the transaction is executed, and sign the proposal separately if they agree;
3) Smart contracts send proposals with signatures to endorsement nodes in each organization according to endorsement policies;
4) The endorsement node verifies whether M_{sell} and M_{buy} match the quoted order of both parties, and agrees to endorse if they match;
5) Smart contracts use a random generation algorithm to select a transaction supervisor from the set of nodes participating in the endorsement;
6) Smart contracts generate the transaction contract N and writes it into blockchain by the accounting node.

The trading contract N^1 in channel 1 is shown in Eq. 11. *Value* Represents the total transaction price. *Time* Represents the time when the contract was signed. pk_{sup} Indicates the identity public key of the supervisory node of the transaction.

$$N^1 = <pk_{sell}, pk_{buy}, pk_{sup}, E_{buy}, P_{buy}, Value, Time> \tag{10}$$

$$Value = E_{buy} * P_{buy} \tag{11}$$

The transaction contract N^2 in channel 2 is shown in Eq. 12. T_{sell} represents the transaction settlement time.

$$N^2 = <pk_{sell}, pk_{buy}, pk_{sup}, E_{buy}, P_{buy}, Value, T_{sell}, Time> \tag{12}$$

Before power transmission starts, the consumer needs to prepay tokens, and the prosumers needs to lock the power ownership keys b_α and b_β stored in the blockchain. The specific algorithm $Protrade\left(pk_{sell}, pk_{buy}, pk_{sup}\right) \rightarrow RScript$ processes are as follows.

1) The smart contract sends a request for the prepaid token *Value* to the consumer.
2) After the consumer agrees to the request, the smart contract generates a (2, 3) multi-signature address *RScript*.

$$RScript = OP\_2||pk_{sell}||pk_{buy}||pk_{sup}||OP\_3||OP\_CHECKMULTISIG$$

3) The consumer hashes the *RScript* to generate a *P2SH* signature address and transfers the token worth *Value* to the corresponding address.
4) After verifying the token balance in the address, the prosumer locks the power ownership keys b_α and b_β stored in the blockchain through smart contracts.
5) After the completion of the locked key and prepaid token, the transaction will enter the physical transmission stage of power.

(2, 3) Multi-signed address wallet *RScript* means that at least 2 private keys are involved in order to use the prepaid tokens in it. Even if the consumer refuses to pay the token after the transaction is settled, the prosumer and the supervisor can also use the private key to ensure the smooth delivery of the token. Accordingly, if the prosumer refuses to process *RScript* due to violations in the physical transmission process of power, the existence of supervisor can still ensure the safety of consumers' funds.

It is important to note that if $E_{sell} > E_{buy}$, one order to sell power may be able to meet the needs of many orders to buy power. Conversely, a single order to buy power may require multiple orders to sell power to meet demand. Therefore, successful bid matching does not necessarily mean the end of the bid order, and it can continue to participate in the transaction after splitting the successfully matched electricity E. Accordingly, the power ownership key b_α will be split into multiple parts as the case may be, as shown in Formula 13.

$$b_{\alpha+1} = Hash(b_\alpha || E_{buy}/E_{sell}) \tag{13}$$

Similarly, in the fourth step of the above algorithm, the locked key is only the key $b_{\alpha+1}$ corresponding to the power E_{buy} for the transaction.

4.3 Transaction Settlement

After the transaction, the smart contract will settle the transaction based on the transaction contract N and the power (generation and consumption) data in the smart meters of both parties.

The actual power generation during the transaction or the power in the storage device is recorded as E_1'. The actual power consumption is E_2'. The power agreed in contract N is E_{buy}. c_{sell} is the credit value of the prosumer, and c_{buy} is the credit value of the consumer.

1) $E_1' < E_2^{'}$, $E_1' \leq E_{buy}$
   The actual generating power of the prosumer during the transaction period didn't reach the agreed amount of power. Prepaid tokens of the consumer were not fully used. Consumers will suffer financial losses due to the need to purchase additional power from higher grids. The smart contract will pay $Value'$ to the prosumers according to the ratio of E_1' and E_{buy}. The remaining prepaid funds will be returned to the consumer's account.
2) $E_2' \leq E_1^{'}$, $E_2' \leq E_{buy}$
   The consumer's power consumption during the transaction time doesn't reach the purchased power, and the consumer's prepaid funds are not fully used. There may be a certain amount of power waste in the microgrid. The smart contract will pay $Value'$ to the prosumers according to the ratio of E_1' and E_{buy}. The remaining prepaid funds will be returned to the consumer's account.

5 System Analysis

5.1 System Security Analysis

The main goal of this section is to evaluate and analyze the security of the proposed distributed microgrid power trading system. First of all, compared with the traditional centralized power trading system, this system doesn't have the problem of user data loss that may be caused by a single point of failure. In addition, for malicious attacks such as double-spending attacks and witch attacks that the blockchain system may suffer from, the response and description of this system are as follows.

Double-Spending Attack. There are two possible scenarios for a double-spend attack in an energy trading platform, one for power and one for tokens [26]. The power double-spend attack refers to the fact that prosumers legally sell more power in the system than they produce. For the power double-spending attack, the system requires the prosumer to upload the ownership certificates b_α and b_β of the energy E before they issue the energy sale order. The data stored in the blockchain is immutable, so it can be considered that prosumers don't have the ability to modify the data they upload. After the two parties of the transaction reach an agreement, smart contracts will lock the b_α and b_β of the prosumer stored in the blockchain. Before offer matching and contract signing, the system checks the existence and status of the power ownership proof key. Therefore, we believe that the system is resistant to power double-spend attacks.

The token double-spend attack is that consumers legitimately spend more tokens than they have in their accounts. For token double-spending attacks, consumers need to prepay tokens declared in the bid order to the multi-signature address after the transaction is successfully matched and before the power transmission starts. The prepayment behavior must require sufficient balance in the consumer's account, so the token double-spending attack is also impossible.

Sybil Attack. Sybil attack means that the attacker injecting a huge number of fake puppet nodes needs to build a private sub-network that sieges and isolates victim nodes from the rest network and can perform malicious activities on victim nodes [9]. The system is based on the Hyperledger Fabric blockchain design and has the characteristics of privacy and access permission [27]. New users will need to authenticate when joining organizations and networks, as well as check or install appropriate smart metering devices. Therefore, we believe that the system is resistant to Sybil attack.

Distributed Denial of Service Attack. In the design of previous blockchain-based distributed electricity trading schemes, most schemes did not take into account the possible DDOS attacks during the trading process. For example, during bilateral continuous bidding, one or more malicious actors may block or even destroy the system through a large number of meaningless bid orders. In this scheme, PCDA algorithm makes participants pay a certain amount of computing power for each bid, and the cost is related to the number of bids and historical credit. Any cheating behavior by the user will make the bid verification fail and further increase the difficulty of bidding. In addition, the consistency of smart meter devices owned by users ensures a fair bidding process. Therefore, it can be determined that this system can effectively reduce the possibility of DDOS attacks.

5.2 System Feasibility Analysis

This scheme designs and proposes the PCDA algorithm, and the number of users' bids within the specified time will be limited by the credit rating and computing power. Users are not able to bid unlimitedly without control. To verify the feasibility of the algorithm in practical applications, we simulate the user's behavior in the bid stage in MATLAB. The simulation results are shown in Fig. 5.

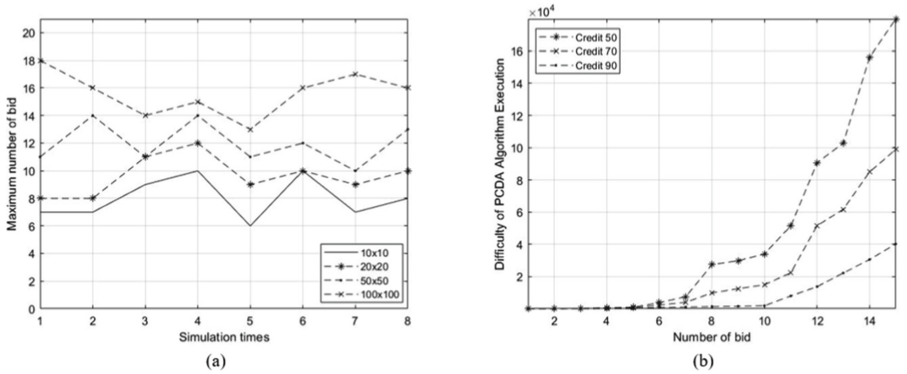

Fig. 5. Simulation of user bidding behavior, where: (a) shows the relationship between transaction size and number of quotations. (b) shows the relationship between the number of bids and the calculation cost under different user credit levels.

Firstly, we simulate the number of bids required by participants to reach a consensus on a deal under different deal sizes. The result is shown in Fig. 5a. Next, we simulate the relationship between the number of bids and the calculation cost under different credit levels. The results are shown in Fig. 5b. It can be seen that the computational cost required for bidding by users with high credit values is much smaller than that of users with low credit values. The advantage of high credit value becomes more and more obvious as the number of bids increases. We believe that the PCDA algorithm can incentivize users to participate in transactions legally while limiting malicious bids. In addition, the further deployment of the system in the future, the PCDA algorithm will also support dynamic adjustment of the computational cost.

6 Conclusions

This paper designs a transaction security microgrid power transaction scheme based on Hyperledger fabric. Compared with most schemes that only have the function of predictive power trading, we design two trading modes, predictive power trading and reserve power trading, which are carried out simultaneously through different channels of Fabric. In addition, this paper proposes the PCDA algorithm by introducing the user credit and proof of work algorithms into the bilateral bidding mechanism. We simulate and prove the effectiveness of the PCDA algorithm in eliminating malicious bidding behaviors, as well as the incentives for users to participate in transactions with integrity. In terms of transaction security, this paper uses the multi-signature address wallet to ensure the user's transaction security without the trusted center.

References

1. Silvente, J., Kopanos, G.M., Pistikopoulos, E.N., Espuña, A.: A rolling horizon optimization framework for the simultaneous energy supply and demand planning in microgrids. Appl. Energy **155**, 485 (2015)

2. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Bus. Inf. Syst. Eng. **59**, 183 (2017)
3. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc. (2015)
4. Zia, M.F., Benbouzid, M., Elbouchikhi, E., Muyeen, S.M., Techato, K., Guerrero, J.M.: Microgrid transactive energy: review, architectures, distributed ledger technologies, and market analysis. IEEE Access **8**, 19410 (2020)
5. Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., Weinhardt, C.: Designing microgrid energy markets: a case study: the Brooklyn Microgrid. Appl. Energy **210**, 870 (2018)
6. Andoni, M., et al.: Blockchain technology in the energy sector: a systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. **100**, 143 (2019)
7. Lüth, A., Zepter, J.M., Del Granado, P.C., Egging, R.: Local electricity market designs for peer-to-peer trading: the role of battery flexibility. Appl. Energy **229**, 1233 (2018)
8. Zhao, Z., et al.: Energy transaction for multi-microgrids and internal microgrid based on blockchain. IEEE Access. **8**, 144362 (2020)
9. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secure Comput. **15**, 840 (2016)
10. Gai, K., Wu, Y., Zhu, L., Qiu, M., Shen, M.: Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans. Ind. Inform. **15**, 3548 (2019)
11. Yao, S., Tian, X., Chen, J., Xiong, Y.: Privacy preserving distributed smart grid system based on hyperledger fabric and wireguard. Int. J. Netw. Manage. e2193 (2021)
12. Wang, H., et al.: Taxonomy research of artificial intelligence for deterministic solar power forecasting. Energy Convers. Manage. **214**, 112909 (2020)
13. Wang, H.Z., Wang, G.B., Li, G.Q., Peng, J.C., Liu, Y.T.: Deep belief network based deterministic and probabilistic wind speed forecasting approach. Appl. Energy **182**, 80 (2016)
14. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Decent. Bus. Rev. 21260 (2008)
15. Wattenhofer, R.: The Science of the Blockchain. Inverted Forest Publishing (2016)
16. Berryhill, R., Veneris, A.: ASTRAEA: a decentralized blockchain oracle. IEEE Blockchain Tech. Briefs (2019)
17. Beniiche, A.: A study of blockchain oracles. arXiv preprint arXiv:2004.07140 (2020)
18. Al-Breiki, H., Rehman, M.H.U., Salah, K., Svetinovic, D.: Trustworthy blockchain oracles: review, comparison, and open research challenges. IEEE Access **8**, 85675 (2020)
19. Ahn, J.: EdenChain: the programmable economy platform. Eden, Singapore, White Paper, vol. 1 (2018)
20. Mammadzada, K., Iqbal, M., Milani, F., García-Bañuelos, L., Matulevičius, R.: Blockchain oracles: a framework for blockchain-based applications. In: Asatiani, A., et al. (eds.) BPM 2020. LNBIP, vol. 393, pp. 19–34. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58779-6_2
21. Vashchuk, O., Shuwar, R.: Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake. Electron. Inf. Technol. **9**, 106 (2018)
22. Baliga, A., Solanki, N., Verekar, S., Pednekar, A., Kamat, P., Chatterjee, S.: Performance characterization of hyperledger fabric. In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), vol. 65. IEEE (2018)
23. Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y., Zhao, Y.: EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts. IEEE Internet Things J. **6**, 4719 (2018)
24. Zhang, S., Pu, M., Wang, B., Dong, B.: A privacy protection scheme of microgrid direct electricity transaction based on consortium blockchain and continuous double auction. IEEE Access **7**, 151746 (2019)
25. Zhong, W., Xie, K., Liu, Y., Yang, C., Xie, S.: Auction mechanisms for energy trading in multi-energy systems. IEEE Trans. Ind. Inform. **14**, 1511 (2017)

26. Zhang, S., Lee, J.: Double-spending with a sybil attack in the bitcoin decentralized network. IEEE Trans. Ind. Inform. **15**, 5715 (2019)
27. Dabholkar, A., Saraswat, V.: Ripping the fabric: attacks and mitigations on hyperledger fabric. In: Shankar Sriram, V.S., Subramaniyaswamy, V., Sasikaladevi, N., Zhang, L., Batten, L., Li, G. (eds.) ATIS 2019. CCIS, vol. 1116, pp. 300–311. Springer, Singapore (2019). https://doi.org/10.1007/978-981-15-0871-4_24