Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9916735, 17 pages
https://doi.org/10.1155/2021/9916735

Research Article

Reliable Reputation Review and Secure Energy Transaction of Microgrid Community Based on Hybrid Blockchain

Zilong Song, Xiaohong Zhang, and Miaomiao Liang

School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 341000, China

Correspondence should be addressed to Xiaohong Zhang; xiaohongzh@jxust.edu.cn

Received 3 March 2021; Accepted 10 June 2021; Published 22 June 2021

Academic Editor: Yuanlong Cao

A growing number of prosumers have entered the local power market in response to an increase in the number of residential users who can afford to install distributed energy resources. The traditional microgrid trading platform has many problems, such as low transaction efficiency, the high cost of market maintenance, opaque transactions, and the difficulty of ensuring user privacy, which are not conducive to encouraging users to participate in local electricity trading. A blockchain-based mechanism of microgrid transactions can solve these problems, but the common single-blockchain framework cannot manage user identity. This study thus proposes a mechanism for secure microgrid transactions based on the hybrid blockchain. A hybrid framework consisting of private blockchain and consortium blockchain is first proposed to complete market transactions. The private blockchain stores the identifying information of users and a review of their transactions, while the consortium blockchain is responsible for storing transaction information. The block digest of the private blockchain is stored in the consortium blockchain to prevent information on the private blockchain from being tampered with by the central node. A reputation evaluation algorithm based on user behavior is then developed to evaluate user reputation, which affects the results of the access audit on the private blockchain. The higher a user's reputation score is, the more benefits he/she can obtain in the transaction process. Finally, an identity-based proxy signcryption algorithm is proposed to help the intelligent management device with limited computing power obtain signcryption information in the transaction process to protect the transaction information. A system analysis showed that the secure transaction mechanism of the microgrid based on the hybrid blockchain boasts many security features, such as privacy, transparency, and imtamperability. The proposed reputation evaluation algorithm can objectively reflect all users' behaviors through their reputation scores, and the identity-based proxy signcryption algorithm is practical.

1. Introduction

The Energy Internet (EI), a distributed sharing network that combines the Internet and distributed energy resources (DER), can connect many kinds of distributed energy nodes to achieve the two-way flow of energy. Energy is used to provide light, heat, power, and other necessities to human beings. With continual scientific and technological progress, a variety of devices are now available to easily convert electric energy into various kinds of energy needed for human production and living. Therefore, the two-way flow of electric energy will form the core of future research on EI.

Currently used forms of primary energy include fossil energy, light energy, wind energy, and water energy [1], whereas electric energy needs to be obtained through conversion from primary energy. The traditional method of conversion is thermal power generation, that is, generating electricity through the combustion of fossil fuels. However, this method is inefficient and causes serious environmental pollution. In 2010, carbon dioxide emissions from energy production, such as the production of electricity, accounted for 76% of global emissions [2]. Considering the importance of environmental protection, research on new methods of conversion has gained momentum. Renewable energy sources (RES) such as light, wind, and water are widely used in the world through primary energy conversion devices. By the end of 2018, the installed capacity of hydropower in China was 352 GW, that of wind power was 184 GW, and that of solar power was 174 GW [3]. In addition, as the number of residential and industrial users who can afford DER

deployment, in the form of solar photovoltaic panels, biomass generators, microwind turbines, and diesel engines, grows each year, a growing number of DER are being deployed at the industrial and residential scales [4]. Although DER has the characteristics of low loss, little pollution, and good system economy, it still has problems that need to be solved. First, the distributed generator (DG) that uses the RES for power generation has a small capacity and is limited by external conditions, because of which the electricity generated by it is intermittent and random. This significantly reduces the reliability of the power supply [5]. Moreover, when a large number of invisible and uncontrollable power generated by DER directly flow into the power grid, the overall power supply line is prone to overshooting the power flow, which jeopardizes the safety and reliability of the power system [6]. Finally, the relationship between supply and demand in the power market is a major obstacle to the development of the DER, and consumers' acceptance of DER power generation needs to be considered.

To solve the above problems of DER, two technologies have been proposed: the virtual power plant (VPP) and the microgrid (MG) [7]. The VPP leverages advanced coordinated control technologies, smart metering technologies, and information and communication technologies to interact with participants in EI, thus making full use of the large-scale and multiregional DER. Due to the limitation of the available power transmission technology, long-distance power transmission causes partial power loss. For industrial and residential users who have DG installed, close-range MG technology is a better choice. MG focuses on regional balance of distributed load and power supply to achieve energy autonomy. VPP focuses on realizing the maximum benefit of the main body and has the derivative function of participating in the power market and auxiliary service market [8]. Liu et al. [9] have provided a distributed robust energy management scheme for a system composed of multiple MGs. Uncertain factors in the operation of the MG have been dealt with by tunable robust optimization technology to optimize the total operating cost of the MG, and studies have verified the effectiveness of the method in a four-MG system. Zhang et al. [10] proposed a networked physical–social system for DER management in the MG that has the capability of parallel learning and can promote the emergence of high-quality DER optimization strategies through human–computer interactive learning. A case study was used to show that this technique can yield a DER optimization strategy more quickly than other heuristic algorithms. Ranjbar et al. [11] proposed an MG protection method in which the short-time Fourier transform (STFT) is used to pretreat the voltage waveform within a period, and the features of disturbance are extracted accordingly. These features are fed to a decision tree algorithm to identify fault events in the MG. The results of simulations showed that depending on the type of event, only two or six features were needed to detect any fault.

The above literature has mainly focused on solving the technical and economic problems of the MG, but it needs to be further developed to solve issues with its management. The prevalent mode of energy operation mostly uses centralized third-party management organization to manage transactions. This mode of management has the following problems: First, with an increase in the number of DER transactions within its jurisdiction, the operating cost of the trading center increases, transaction efficiency is significantly reduced, and it is difficult to ensure the effective operation of the microgrid in real time. Second, in the energy trading process, the trading center and the trading side cannot achieve complete trust, which imposes a significant annual cost on the trading centers to maintain trust. Moreover, there is no open and transparent trading and information platform in the MG, because of which the security and effectiveness of the transaction cannot be guaranteed, and its cost is high. Finally, the centralized trading center is prone to a single point of failure; that is, the trading center causes the entire system to collapse once it is attacked, and the disclosure or tempering of trading information damages the property and violates the privacy of both parties to the transaction.

Since 2016, Bitcoin, a decentralized digital currency, has gained considerable attention from the financial community due to an increase in its economic value. Academics have found that in addition to the economic value of Bitcoin itself, its core supporting technology, namely, the blockchain, has significant research value. The blockchain has the characteristics of decentralization, trustlessness, openness, and transparency. With progress in research, the scope of applications of the blockchain is no longer limited to the financial field. Adding blockchain technology to the transaction process of the MG may provide a new solution to the above-mentioned management problems. Research on combining the microgrid energy market with blockchain technology is still in its preliminary stage. To prove the feasibility of this combination, many scholars have carried out a series of studies, and the results show that the blockchain has the ability to support energy transactions within a certain range [12–14]. Based on this assessment of theoretical feasibility, a growing number of papers have been published in the area. Di Silvestre et al. [15] discussed the loss in the distribution of energy transactions of blockchains when applied to the MG and proposed two indicators of loss distribution to solve this problem. The feasibility of these indicators was verified in two operating scenarios of a medium-voltage microgrid. Di Silvestre et al. [16] considered the provision of voltage regulation technology based on the blockchain for the MG, mainly by solving for reactive power optimization power flow and reactive power compensation. The former was intended to ensure optimal economic planning in reactive power production and the latter to evaluate the contribution of voltage regulation. Hassan et al. [17] proposed an energy transaction auction mechanism called differential privacy auction to provide moderately costly but secure and private energy auctions for the MG based on consortium blockchain. Experimental comparisons showed that this mechanism was superior to the VCG mechanism. van Leeuwen et al. [18] designed an integrated energy management platform based on the blockchain that is composed of three parts: a physical layer, economic layer, and information layer. It can facilitate the trade of energy in the microgrid community through a bilateral transaction mechanism and optimize energy flow by solving optimal power flow problems. Meeuw et al. [19]

studied the impact of limitations of hardware and the communication infrastructure of applications on the blockchain system. Based on the conditions of the Swiss blockchain-based Walenstadt microgrid, the researchers artificially adjusted the bandwidth between nodes to simulate the bandwidth of the communication infrastructure. They found that a communication network with a bandwidth of less than 1000 kbit/s leads to insufficient system throughput. To solve the problems of default risk and demand uncertainty in designing a renewable energy microgrid based on the blockchain, a method based on robust two-type fuzzy programming was proposed by Tsao et al. [20], and its effectiveness was proved by a case study. The above literature has examined the blockchain-based microgrid system from different technical aspects, but a safe method to protect energy transactions in the MG remains elusive.

In this paper, a secure microgrid transaction mechanism based on the blockchain is proposed. The main contributions are as follows:

(1) Blockchain-based microgrid trading platforms can solve the problems of trust and transparency in microgrid energy trading, but most schemes proposed in the literature are based on a single blockchain. In application, a single blockchain struggles to provide effective user identity management, and this makes it easier for malicious actors to infiltrate the system. This paper proposes a microgrid energy transaction framework based on the hybrid blockchain containing a trading consortium blockchain and N private blockchains for identity management, where N is the number of microgrids in the network. Only users verified by the private blockchain can conduct transactions on the consortium blockchain

(2) To ensure good market trading behavior, a reputation evaluation algorithm based on user behavior is proposed. Because there are two kinds of identities, buyer and seller, in energy trading, this algorithm contains separate algorithms to assess buyer and seller behaviors. Whether a user can be authenticated by the private blockchain depends on their own reputation: when the reputation has a score of zero, the user cannot use the energy transaction function. In addition, the energy in the consortium blockchain is mainly auctioned by using the continuous double auction algorithm based on reputation. The higher the reputation score of a user is, the more benefit from the transaction they can draw

(3) When users participate in energy transactions, they need to communicate with the microgrid continuously. To ensure the security of the information shared during transaction-related communication, an identity-based proxy signcryption algorithm is proposed that is suitable for users with smart home manager. Proxy signcryption allows the smart home manager with a limited amount of computing power and storage to delegate its data processing rights to the powerful energy manager to participate in energy trading. The identity-based proxy signcryption algorithm solves the defect whereby the typical proxy signcryption algorithm needs to store a large number of certificates

The remainder of this paper is arranged as follows: Section 2 introduces some preliminary information, and the system as a whole and its detailed framework are introduced in Section 3. In Section 4, we describe the steps of implementation of the proposed scheme, such as details of the buyer and seller reputation evaluation algorithms, the identity-based proxy signcryption process, and the process of generation of new blocks. Section 5 is devoted to a performance analysis and evaluation of the proposed scheme, and we summarize our findings in Section 6.

2. Preliminaries

In this section, we review some preliminary knowledge, such as the structure of the microgrid, the nature of the bilinear pairing involved, and the principle of proxy signcrytion.

2.1. Microgrid. The earliest concept of the microgrid was proposed by the United States Consortium for Electric Reliability Technology Solutions (CERTS) [21] and remains the most authoritative one. The CERTS microgrid assumes that the set of loads and DER operate as a single system. A critical feature is that it can autonomously exist in the distribution system as a self-controlling entity. In other words, it is impossible to distinguish the MG from legitimate customer sites in the grid. The initial work by the CERTS was based on small-scale micropower sources with a capacity lower than 500 kW, and the basic structure of the MG developed by the CERTS is shown in Figure 1.

The power system in the diagram consists of three feeders (A, B, C) and a set of loads. The entire power supply network has a radial shape. In terms of load distribution, both feeders A and B contain sensitive loads while feeder C contains traditional loads. The installation of micropower supply is based on the user's load demand and only in case of sensitive loads are the microsources installed on the feeder. This system contains two kinds of microsources for installation: a microturbine and a fuel cell. The microturbine is installed on feeder A, and two kinds of microsources are installed on feeder B. The fuel cell can produce electric energy as well as a large amount of heat energy when burning, which endows feeder B with the ability of cogeneration. To adjust the power and feeder flow of the microsources, each is equipped with a power and voltage controller managed by the energy manager of the MG or the local system of users.

In addition, the microgrid shown in the figure has two operating modes: the networking mode and the island mode [21]. When the distribution network is disturbed, feeders A and B can use a separation device to separate themselves from the power grid, thereby minimizing interference in the inductive load. If local power generation is not sufficient to meet the demand of sensitive loads, the islands are rendered meaningless. Feeder C is left in the interference, mainly to eliminate the interference trip caused by traditional loads.

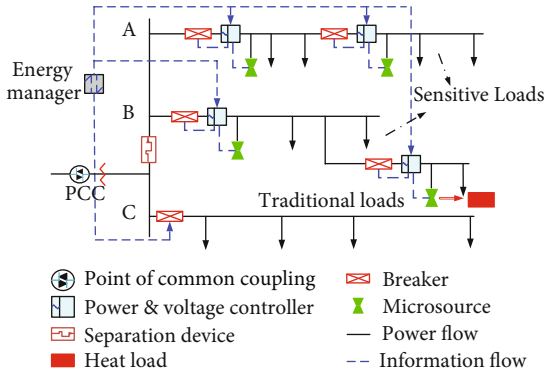

Figure 1: The basic structure of the microgrid proposed by CERTS.

With the development of power electronic equipment, microsources that can be installed in the MG are no longer limited to the two mentioned above, and the micropower supply based on clean energy, such as solar and wind energy, has been widely incorporated into the MG. The control strategy of the MG has improved, and the most commonly used one is hierarchical control. The hierarchical control strategy is divided into three layers. The first layer consists of DER and the local self-control of loads, the second layer consists of the management control of the MG, and the third layer features distribution network management control. Through the hierarchical architecture, the electrical magnitudes of the MG at different time scales can be controlled.

2.2. Bilinear Pairing. Suppose there are three cyclic groups G_1, G_2, and G_3. The order of the cyclic group is p, and the generator of the cyclic group is g. Based on bilinear pairing, there is a mapping relationship among these three cyclic groups called $e : G_1 \times G_2 \longrightarrow G_3$ that satisfies the following properties:

(i) Bilinearity: For any generators $g_1 \in G_1, g_2 \in G_2$, and $x, y \in Z_p^*$, there always exists $e(xg_1, yg_2) = e(g_1, g_2)^{xy}$

(ii) Nondegeneracy: There always exists $g_1 \in G_1, g_2 \in G_2$, such that $e(g_1, g_2) \neq 1$

(iii) Computability: There is an algorithm that renders $e(g_1, g_2)$ computable under the condition $\forall g_1 \in G_1$, $g_2 \in G_2$

This is an asymmetric bilinear pairing. The commonly used bilinear pairing is symmetric, that is, $G_1 = G_2$. Furthermore, the bilinear pairing commonly referred to is based on the prime order. The composite-order bilinear pairing proposed by Boneh et al. [22] is still undergoing improvement. For a detailed classification of bilinear pairing, the interested reader can see Ref. [23].

2.3. Proxy Signcrytion. In 1999, Gamage et al. [24] proposed proxy signcryption as a cryptographic primitive that is generated on the basis of signcryption [25] and the proxy signature [26] and inherits the characteristics of both. In the proxy signcryption scheme, the owner of the original data can entrust the authority for processing them to a person, that is, the proxy signcrypter; then, the agent can replace the owner of the original data to perform the signcryption operation. In a computation-constrained smart device, it would be a significant burden for the intelligent device to constantly consume computing power to perform signcryption. Proxy signcryption can solve this problem. It entrusts the signcryption operation to the agent with strong computing power to relieve the computing pressure on intelligent devices. The proxy signcryption scheme consists of five parts: system setup, key generation, delegation generation, proxy signcrypt, and proxy unsigncrypt. The process is as follows:

System Setup: Given a security parameter λ, the algorithm outputs the system parameter params.

Key Generation: Given system parameters params, the algorithm outputs the public/private key pairs (PK_o, SK_o) of the original data owner, pair (PK_p, SK_p) of the proxy signcrypter, and the pair (PK_r, SK_r) of the message receiver.

Delegation Generation: Given system parameters params, the data owner's private key is SK_o, and the warrant is ω; the algorithm outputs a delegation σ_ω and sends (ω, σ_ω) to the proxy signcrypter.

Proxy Signcrypt: Given system parameters params, the warrant ω, the delegation σ_ω, the proxy signcrypter's private key SK_p, the receiver's public key PK_r the message M, and the algorithm output ciphertext σ.

Proxy Unsigncrypt: Given system parameters params, warrant ω, ciphertext σ, the receiver's private key SK_r, data owner's public key PK_o and the proxy signcrypter's public key PK_p, if the ciphertext σ is legal, the algorithm outputs message M, otherwise, outputs the error symbol $\perp$.

3. System Model

In this section, we laid out the structure of the hybrid blockchain, where the private blockchain is responsible for identity authentication, and the consortium blockchain is responsible for energy transactions.

3.1. Data Storage and Sharing Model of MG Based on Hybrid Blockchain. The blockchain can be divided into public blockchain, consortium blockchain, and private blockchain according to the different modes of participation of its nodes [27–29]. The public blockchain allows all nodes to participate in the network and has the highest security. However, its deployment comes at the cost of a large amount of resources, and its characteristics of low extensibility and weak data throughput do not support the application of the public blockchain to commercial transactions involving large amounts of data. The private blockchain has the disadvantage of too high a degree of centralization, which renders it suitable only for information sharing within a single entity but not for storing transaction information involving multiple entities. The consortium blockchain is a compromise between the public and the private blockchains. It retains their advantages and is free of their major disadvantages. The consortium blockchain is the most commonly used blockchain in applications.

In the design considered in this paper, we use the consortium blockchain as the transaction blockchain to store

transaction data and call it the transaction consortium blockchain (TCB). In contrast to other literatures, we set up an identity chain outside the trading chain to authenticate and manage the identities of traders. During the operation of the MG, an MG community can be regarded as an entity, and transactions are usually carried out within it so that each MG community can establish its own identity chain to manage traders. Based on the characteristics of operation of the MG, we use the private blockchain as the identity chain of managing traders and call it the identity private blockchain (IPB). Therefore, the overall framework of this paper is a $1 + N$ hybrid blockchain framework; that is, it contains a transaction consortium blockchain and N identity private blockchains, and N is determined by the number of MGs. The framework is shown in Figure 2.

As is shown in Figure 2, the MG community communicates with the authority for verification off the blockchain. Once the verification has passed, each MG community generates an exclusive IPB that is responsible for authenticating the user's identity, assessing their reputation, and storing the corresponding identity information. When users in the MG community want to conduct energy transactions, those participating in the transactions need to communicate with the MG and send their demands to it. According to the different needs of each user, participants in the transaction can be divided into prosumers and consumers. Prosumers are users that have DER installed and can sell their surplus electricity. Consumers are regular users who need to purchase electricity to meet their needs. When the total remaining electricity among prosumers in the MG is not enough to meet the demand of the consumers, the MG purchases the required electricity from the power trading center. When the total amount of electricity left over by prosumers in the MG exceeds the total electricity demand of the community and the storage is full, the MG sells the excess electricity to the power trading center. Because power transactions involve the transfer of user property, all transactions occur on the TCB, and, accordingly, transaction data are stored on it. The TCB is jointly maintained by all network nodes and has only a TCB, which can provide adequate security for the TCB. To ensure that users have acceptable market transaction behavior, the MG uses the reputation-based auction algorithm to auction energy. The user reputation required by the auction is stored in the IPB while the algorithm used to assess the user's reputation requires the user transaction data stored on the TCB. Based on this scenario, we allow the TCB and IPB to interact with each other through smart contracts. The degree of centralization in a private blockchain is too high, and the data stored on it are at risk of being tampered with by the central node. Therefore, we store the hash digest of the IPB on the TCB to ensure the security of data in the private blockchain by relying on the security of the consortium blockchain.

3.2. Identity Authentication Model Based on IPB. When a user wants to make an energy transaction, he needs to be authenticated on the IPB. Only an authenticated user can obtain the transaction license; otherwise, he cannot use the MG power transaction platform. Community users who are new to the platform first need to register their identity so that they can join the IPB. The process of building and joining the IPB is shown in Figure 3.

Figure 3 shows seven steps, which 1–3 show of the construction of the IPB and 4–7 show the joining process of nodes. In the construction process, in step 1, the MG manager sends an IPB build request to the authority that contains the identity of the MG community, maximum power limit, and the jurisdiction to be divided. After receiving the MG's application, the authority reviews it and, after approving it, returns the information to the MG and invites it to build an IPB exclusively for its community, as in step 2. In step 3, the MG and the authority jointly set up a private blockchain. Once the IPB has been built, users of the community can apply to join the private blockchain. In the first step of the joining process, namely, step 4, community users need to send registration information to the authority. Different from consumers, the registration information of prosumers contains their identity information as well as detailed information on the deployed DER. Upon receiving the registration information from community users, the authority verifies the information, and if verified, authority will encrypt and upload the information to the private blockchain of the community to which the given user belongs. After that, the authority will generate the exclusive key for the user and distribute it. Steps 5 and 6 show this process. As shown in step 7, when a user receives a private key, they can officially join the IPB to which they belong according to this key.

Successfully joining the IPB does not mean that energy transactions can be conducted on the MG energy trading platform. Energy transactions can be officially conducted only on the TCB after obtaining a trading license on the IPB. To obtain a trading license, a user's identity must be authenticated out on the IPB. A flowchart of identity authentication is shown in Figure 4.

The system first checks whether the user node ID exists in the blacklist BL; if it does, the user is denied the use of the energy transaction function and can otherwise continue to the next step. The user node then selects the roles it plays on the TCB, where only seller and buyer roles are available. When it chooses to be a seller, the system checks whether the user node has a DER certified by the given authority. If not, the system returns to the previous step, and the user node reselects its role. In this case, the system checks the seller reputation value R_j of the user to whom the node belongs. If the reputation value is zero, the node reenters the role selection process. If the reputation value is not zero, the node is issued a seller license. When selecting a buyer, the system needs to only check the buyer reputation value R_i of the user to whom the node belongs. If the reputation value is zero, the user ID is added to the BL, and the user node is denied energy transactions. If the reputation value is not zero, a buyer license is issued to the user node. Finally, users with seller or buyer licenses can use them to trade energy on the TCB. Prosumers can choose to trade as either sellers or buyers. So, in each round of trading, the IPB provides identity authentication for each user only once. After the transaction, the system recalculates the reputation score of each node based on its performance in the transaction. All new nodes

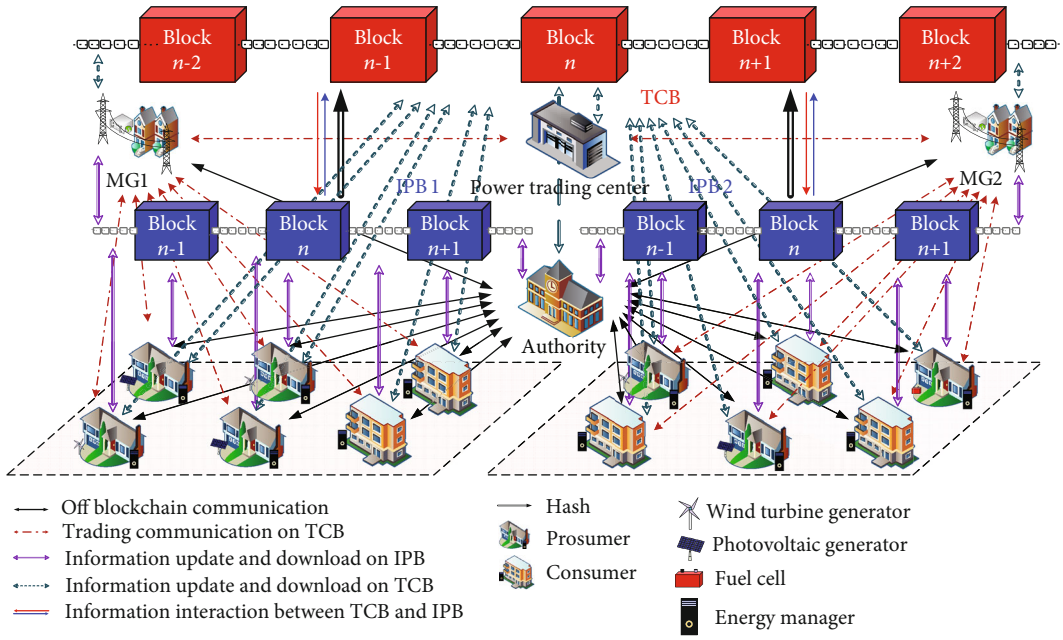

Figure 2: Data storage and sharing model of microgrid based on the hybrid block chain.

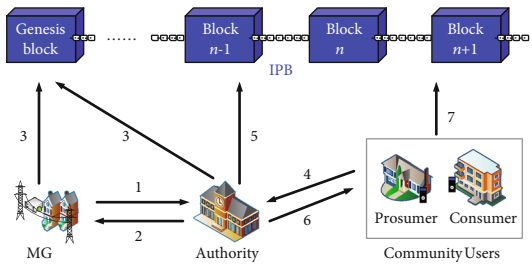

Figure 3: Flowchart of building and joining the IPB.

are assigned the same initial reputation score by the system, and each node has the reputation scores of the seller and the buyer, but only prosumers can use the former score. Prosumers with a seller reputation of zero cannot conduct energy transactions on the TCB as sellers and can only purchase energy as ordinary consumers. Users in the blacklist cannot reregister with the authority to obtain a new node identity. The means of obtaining another transaction authority is formulated by the given authority.

3.3. Secure Trading Model Based on TCB. Forms of DER energy trading on the MG energy trading platform can be divided into two types: P2P trading and centralized clearing. A P2P transaction is a direct transaction between individuals that is executed automatically according to the corresponding contract. However, such a transaction is disordered and can easily affect the power system. Centralized clearing requires a third-party platform for unified trading under optimized scheduling to reduce the risk of system disorder. Due to the problem of trust of the third-party platform, the mode of transaction of centralized clearing has been criticized. The emergence of the blockchain provides a new solution to the problem of trust. The TCB uses continuous double auction (CDA) as method for transactions, where this is a kind of centralized clearing. The CDA allows both parties to a contract to modify their quotations continuously during the auction to maximize the interests of the traders [30]. The secure transaction model is shown in Figure 5.

The traditional CDA has only three trading entities: the auctioneer, buyer, and seller. In our model, MG is the auctioneer, the prosumer is the seller, and the consumer is the buyer. Besides, the model features another power trading center acting as an energy balancer. The greater the number of nodes in the blockchain network is, the stronger the security of the blockchain is. For security-related reasons, we should deploy as many nodes as possible in the blockchain network. The block is the basic unit in the formation of a blockchain and collection of data. Each block is composed of a header and a body [31]. The block header contains a transaction information hash, a block hash, and a time stamp while detailed transaction information is stored in the block body. The byte size of the block header is smaller than that in the block body. Therefore, nodes that store only block header information are called light nodes, and those that store information on the entire block are called full nodes. For the smart home manager or the DER with limited computing and storage capabilities, being a light node in the blockchain network can not only reduce its own storage pressure but also enhance the security of the network. As for the problem of limited computing power, the pressure can be shared by an energy manager with powerful computing power, which exists in the form of a full node in the network. As a result, the buyers in this scheme can be accurate to smart home managers such as smart appliances, smart lighting and smart windows, and doors, while the sellers are the DER devices deployed by prosumer.

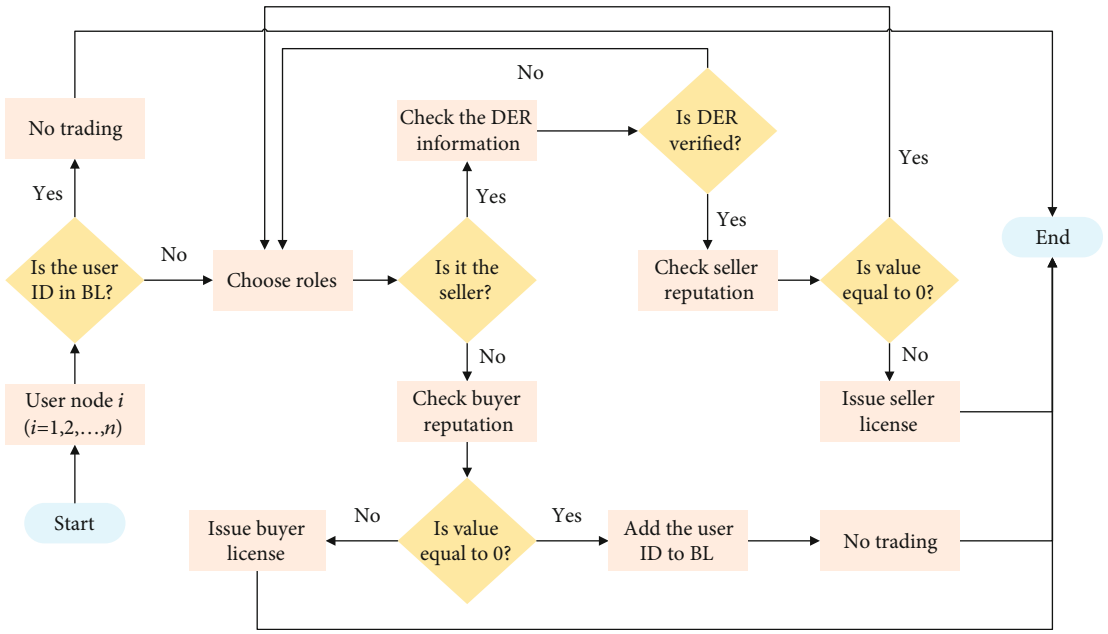

Figure 4: Flowchart of identity authentication.

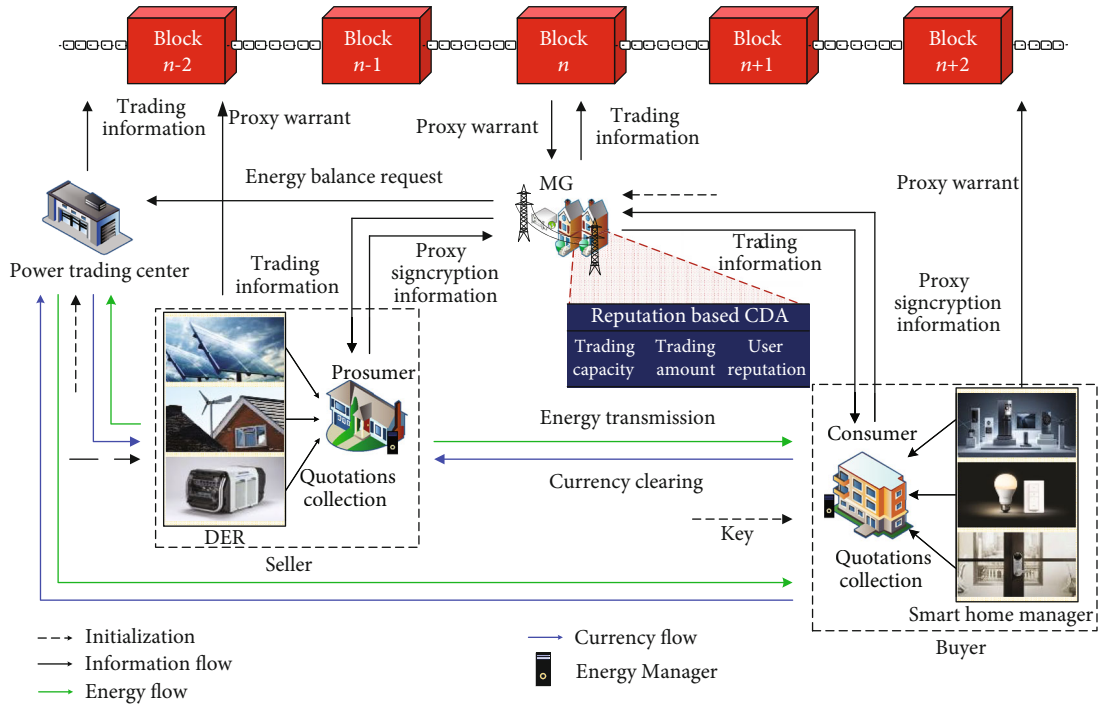

Figure 5: Secure trading model based on the TCB.

The basic flow of the secure trading model is as follows:

(1) Initialization: Once users of the community have passed IPB authentication, they can conduct identity transactions on the TCB according to their identity licenses. Users with the seller's license act as sellers, and those with the buyer's license act as buyers. The MG manager node acts as auctioneer, and the keys required for the transactions are generated by the authority

(2) Quotation collection: Although the smart home manager or DER, as a light node, can generate the quotation and signcrypt it to the MG manager node by itself, frequent signcrypts require a large amount of computing power. In addition, multiple energy quotes may belong to the same entity in the auction list, which increases the workload of the auction and causes unnecessary waste. As a full node, the energy manager can first integrate the quotation

information of the user's home manager, signcrypt this information through the identity-based proxy signcryption algorithm, and send the signcrypted information to the MG manager node. In this way, the effect of the light node's participation in the transaction can be obtained and problems incurred by this participation can be solved

(3) Energy auction: After receiving the signcryption information from buyers and sellers, the MG manager node decrypts them. Auction matching is then carried out according to the bidding price. To increase the user's attention to reputation, the CDA auction mechanism based on reputation is used for auctioning; it divides users' grades according to their scores. The higher the grade is, the wider is the range of options to which the corresponding user can match. The matching rule of "price first, reputation first, time first" is used. At the end of the auction, if energy balance has not been attained within the MG community, an energy transaction is conducted with the power trading center as is appropriate

(4) Transaction and clearing: Community users who have been successfully matched check the transaction information and then conduct energy transaction according to the confirmed transaction contract. During the transaction, the default users are punished financially, and default behaviors will lead to a decline in their reputation scores. Transaction clearing needs to be carried out through the unique energy coin of the system that is generated by the power trading center. When each user joins the TCB for the first time, they can get a certain value of energy coin for free through their IDs. Each ID can be collected only once

4. System Implementation

To implement the secure transaction model of the MG proposed here, the most important factors to consider are the reputation evaluation of users, secure collection of quotations required for MG auction, and generation of new blocks on the blockchain. The section is thus composed of three parts, namely, a reputation evaluation algorithm based on user behavior, an identity-based proxy signcryption algorithm, and a data block generation algorithm. These three parts correspond to the implementation of the above functions. The variables involved in system implementation are shown in Table 1.

Table 1: Symbol definitions.

Symbol	Definition
$\eta(T)$	Time adaptive weight parameter
P	The peak period of power consumption
A	The average period of power consumption
V	The valley period of power consumption
$R_{i/j}^{\text{con}}$	Buyer/seller's contract reputation
$R_{i/j}^{C}$	Buyer/seller's consensus reputation
R_{i}^{DR}	Buyer's demand response reputation
R_{j}^{F}	Seller's feedback reputation
$R_{i/j}$	Buyer/seller's reputation
R_{MG}	MG's reputation
GP	System global parameters
MSK	System master key
PK_{ori}, SK_{ori}	Original signcrypter's public and private keys
PK_{proxy}, SK_{proxy}	Proxy signcrypter's public and private keys
PK_{MG}, SK_{MG}	MG's public and private keys
PSK_{op}	Proxy key
ω	Warrant
M	Plaintext information
σ	Proxy signcryption information

4.1. Reputation Evaluation Algorithm Based on User Behavior. In the traditional centralized power supply mode, users' power consumption behavior changes with time and leads to the emergence of peak and valley periods of power consumption. The peak period refers to the duration when the power consumption is concentrated and the power supply is limited. The valley period is the opposite duration, when there is less activity and supply is plentiful. The detailed peak–valley time is divided according to the local season and when the peak–valley load appears. The peak–valley time varies slightly in different regions; therefore, only the peak P, average A, and the valley V are defined in this paper, and no detailed time division is given. To better control the user's trading behavior, we define a time-adaptive weight parameter $\eta(T)$ according to the peak–valley interval.

$$\eta(T) = \begin{cases} 1.5, & T \in P, \\ 1.25, & T \in V, \\ 1, & T \in A. \end{cases} \tag{1}$$

In the formula, regardless of whether the trading time T is in the peak or the valley period, its weight is greater than the weight of the average period. This is done to enhance users' attention to the two periods and reduce the probability of poor trading behavior.

4.1.1. Algorithm to Assess Reputation of Buyer Based on Behavior. Buyers in the MG community are mainly composed of consumers who need to buy energy. When prosumers have a seller reputation score of zero or the DER power supply cannot meet their needs, they are also buyers. In the algorithm to assess the reputation of the buyer, three reputation events affect the buyer's reputation: default events, demand response events, and block generation events.

When the buyer and the seller reach the intention to engage in a transaction through an auction and sign a contract, the seller begins to transmit electricity to the buyer.

When the electricity consumption of the buyer in the agreed time slots exceeds the agreed transaction capacity, the seller's interests are undermined because the number of coins stipulated in the contract is fixed.

Therefore, this paper uses the default contract as an evaluation index for the buyer's reputation. The buyer's contract reputation R_i^{con} is assessed as shown in Formula (2):

$$R_{i,t-1}^{con} = \begin{cases} -\eta(T_i), & Q_{ij}^i > Q_{ij}^{\text{con}}, \\ 0, & Q_{ij}^i \le Q_{ij}^{\text{con}}, \end{cases} \tag{2}$$

where $R_{i,t-1}^{\text{con}}$ is the contract reputation of buyer i at the end of round $t-1$, T_i is the transaction time of buyer i, Q_{ij}^i is the electricity consumption of i in the trading time slot, and Q_{ij}^{con} is the amount of electricity agreed in the contract. When the buyer violates the contract, they must compensate the seller according to the price of electricity of the power trading center.

A demand response event is used to balance the energy demand of the power supply system when power is in short supply. Each MG issues the demand of reducing energy consumption to its community and announces the total value by which the energy consumption needs to decrease. Buyers who are qualified to respond reduce their electricity consumption according to the agreed response amount. The buyer's demand response reputation R_i^{DR} is shown in Formula (3).

$$R_{i,t-1}^{\text{DR}} = \begin{cases} \dfrac{T_{i,d.5\%} + 0.7T_{i,d.5\%\sim25\%} + 0.5T_{i,d.25\%\sim50\%}}{T_{i,t-1}^{\text{DR}}}, & r = 1, \\ -0.5, & r = 0, \end{cases} \tag{3}$$

where $R_{i,t-1}^{\text{DR}}$ is the demand response reputation of buyer i at the end of round $t-1$, $T_{i,d.5\%}$ indicates the time when the deviation between the response capacity and the agreed capacity of buyer i is less than 5%, $T_{i,d.5\%\sim25\%}$ indicates the time when the deviation is in the range 5% ~25%, $T_{i,d.25\%\sim50\%}$ indicates the time when the deviation is in the range 25% ~50%, and $T_{i,t-1}^{\text{DR}}$ indicates the total time buyer i needs to respond in round $t-1$ of the transaction. If r is 1, i responds as required, and if r is 0, i does not respond.

The generation of blocks is inseparable from the consensus algorithm. To encourage nodes on the network to participate in the consensus process, the system assigns a certain reputation to nodes that participate in the consensus process. The consensus reputation R_i^C is calculated as follows:

$$R_{i,t-1}^C = k_i\alpha, \tag{4}$$

where $R_{i,t-1}^C$ is the consensus reputation of buyer i at the end of round $t-1$, and k_i represents the number of times that buyer i participates in the consensus process in round $t-1$. α is always greater than zero, and its value depends on the rate of block generation. The two are inversely proportional.

To sum up, before the buyer prepares to conduct a transaction in round t, we calculate their reputation according to Formula (5):

$$R_{i,t} = \begin{cases} 50, & t = \text{init}, \\ R_{i,t-1} + R_{i,t-1}^{\text{con}} + RR_{i,t-1}^{\text{DR}} + R_{i,t-1}^C, & t \ne \text{init}, \end{cases} \tag{5}$$

where $R_{i,t}$ is the reputation of buyer i at the end of round $t-1$, $R_{i,t-1}$ is the reputation of i in round $t-1$, and R is a judgment function. When i is qualified to respond, R is 1 and is otherwise 0. When buyer i is participating in the transaction for the first time, their initial reputation is 50.

4.1.2. Algorithm to Assess Reputation of Seller Based on Behavior. In the MG community, only prosumers can be sellers. The algorithm to assess their behavior as seller uses three reputation events as indicators: a default event, a feedback event, and a block generation event.

When the supply of electricity provided by the seller fails to reach the trading capacity agreed with the buyer in the contract, the buyer needs to purchase electricity from the power trading center to meet their electricity demand. The price of electricity offered by the power trading center is often higher than the transaction price in the MG community and causes losses for the buyer.

Therefore, whether a contract is default can be used as an evaluation index to assess the seller's reputation, the buyer's contract reputation R_j^{con} is as shown in Formula (6).

$$R_{j,t-1}^{\text{con}} = \begin{cases} -\eta(T_j), & Q_{ij}^j < Q_{ij}^{\text{con}}, \\ 0, & Q_{ij}^j \ge Q_{ij}^{\text{con}}, \end{cases} \tag{6}$$

where $R_{j,t-1}^{\text{con}}$ is the contract reputation of seller j at the end of round $t-1$, T_j is the transaction time of j, and Q_{ij}^j is their electricity consumption in the trading time slot. When seller j defaults, they compensate buyer i for the extra cost of purchasing electricity from the power trading center.

A feedback event is one where after a transaction between buyer i and seller j, and i needs to provide feedback to j on the quality of the power supply service, which is expressed by F_{ij}. The range of F_{ij} is [-0.5,0.5], and the seller's feedback reputation R_j^F is shown in Formula (7):

$$R_{j,t-1}^F = \frac{\sum_{i=1}^{L}(F_{ij}E_i)}{\sum_{i=1}^{L}E_i}. \tag{7}$$

In the formula, $R_{j,t-1}^F$ is the feedback reputation of seller j at the end of round $t-1$, L is the number of buyers who give feedback to seller j, and E_i is the feedback equilibrium function used to balance the feedback value.

The value of E_i can be only 0 or 1. To use E_i, the average value F_a and standard deviation F_{sd} of the buyer's feedback

need to be calculated first. They are calculated, respectively, by Formulae (8) and (9):

$$F_a = \frac{\sum_{i=1}^{L} F_{ij}}{L}, \tag{8}$$

$$F_{sd} = \sqrt{\frac{\sum_{i=1}^{L} \left(F_{ij} - F_a\right)^2}{L}}. \tag{9}$$

Then, the equilibrium parameter ε is obtained from F_a and F_{sd} as shown in Formula (10):

$$\varepsilon = F_a - F_{sd}. \tag{10}$$

Finally, E_i is assigned a value by Formula (11).

$$E_i = \begin{cases} 1, & F_{ij} \geq \varepsilon, \\ 0, & F_{ij} < \varepsilon. \end{cases} \tag{11}$$

The block generation events of the seller and the buyer are identical, and the seller's consensus reputation R_j^C is calculated as follows:

$$R_{j,t-1}^C = k_j \alpha, \tag{12}$$

where $R_{j,t-1}^C$ is the consensus reputation of seller j at the end of round $t-1$, and k_j represents the number of times that seller j participated in the consensus process in round $t-1$.

We can then obtain the seller's reputation in round t:

$$R_{j,t} = \begin{cases} 50, & t = \text{init}, \\ R_{j,t-1} + R_{j,t-1}^{\text{con}} + R_{j,t-1}^F + R_{j,t-1}^C, & t \neq \text{init}, \end{cases} \tag{13}$$

where $R_{j,t}$ is the reputation of seller j at the end of round $t-1$, and $R_{j,t-1}$ is their reputation in round $t-1$. When j participates for the first time in the transaction, their initial reputation is 50.

For both buyers and sellers, the range of values of the reputation score is [0, 100]. Therefore, after calculating the reputation of the user for participating in a given round using the above formulae, their reputation score should be recalculated through Formula (14) to restrict the range of reputation scores:

$$R_{i/j,t} = \begin{cases} 100, & R_{i/j,t} > 100, \\ R_{i/j,t}, & 0 \leq R_{i/j,t} \leq 100, \\ 0, & R_{i/j,t} < 100, \end{cases} \tag{14}$$

where $R_{i/j,t}$ is the reputation of the buyer/seller in round t. When the seller's reputation is zero, they can participate only in the transaction as a buyer. When the buyer's reputation is zero, they are blacklisted and forbidden from participating in round t.

4.2. Identity-Based Proxy Signcryption Scheme. The identity-based proxy signcryption (IDPSC) algorithm [32] is an improvement over the proxy signcryption algorithm. The core idea is the same; that is, the right to signcryption of the data can be entrusted to the proxy signcrypter, who can then signcrypt the data instead of the original signcrypter. After receiving the proxy signcryption data, the receiver can regard the proxy signcrypter as the original signcrypter, who becomes responsible for the data. The original proxy signcryption algorithm uses traditional public key facilities and encounters the problem of authenticating the user's identity when using the key generated by this facility to communicate. It thus needs a trusted third party to issue the user's identity certificate. When there are too many users, the problem of certificate management becomes significant. The IDPSC does not encounter this problem and thus is more efficient.

In the MG community, the auctioning algorithm is often used for transaction matching. It involves a large number of communication processes. To ensure the confidentiality and nonrepudiation of the communicated information, the information needs to be signcrypted. In the proposed model, the participants are DER installed by prosumers and smart home manager installed by consumers, but these are unsuitable for data signcryption because of their hardware. To solve this problem, we propose a secure IDPSC algorithm for MG energy trading consisting of five subalgorithms: those for system setup, key generation, proxy key generation, proxy signcryption, and unsigncryption. The program description is as follows:

4.2.1. System Setup. The primary function of the phase is that the government initializes the system in order to provide basic conditions for the operation of subsequent phases. The core algorithm of this phase is $\text{Setup}(1^\ell) \longrightarrow (\text{GP}, \text{MSK})$, which is controlled by the authority. The authority first enters the security parameter ℓ into the system, which generates two additive cyclic groups G and G_T of order p according to the parameter ℓ, and defines four hash functions $H_1 : \{0,1\}^* \longrightarrow G$, $H_2 : \{0,1\}^* \longrightarrow Z_p^*$, $H_3 : G_T \longrightarrow \{0,1\}^n$, and $H_4 : \{0,1\}^n \times G_T \longrightarrow Z_p^*$, where n is the byte length of message M. For the cyclic group G, g is the generator; G and G_T satisfy the bilinear mapping relation $e : G \times G \longrightarrow G_T$. The authority then randomly selects element $\lambda \in Z_p^*$ as the system's master key and computes the system's public key $\text{PK}_{\text{pub}} = \lambda g$. Finally, the master key MSK and the system global parameter GP are output:

$$\begin{cases} \text{MSK} = \lambda, \\ \text{GP} = \left\{n, e, g, \text{PK}_{\text{pub}}, H_1, H_2, H_3, H_4\right\}. \end{cases} \tag{15}$$

MSK is kept secret by the authority while GP is published to the entire network. All nodes can access this information.

4.2.2. Key Generation. The primary function of the phase is to generate public and private key pairs for users, and the core algorithm is $\text{KGen}(\text{GP}, \text{MSK}, \text{ID}) \longrightarrow (\text{PK}_{\text{ID}}, \text{SK}_{\text{ID}})$. The

algorithm needs input a user ID; the authority audits it. If ID fails to pass the audit, the authority refuses to generate the key for the user. If the audit is passed, the authority outputs the public–private key pair $(\mathrm{PK}_{\mathrm{ID}}, \mathrm{SK}_{\mathrm{ID}})$ corresponding to the ID:

$$\begin{cases} \mathrm{PK}_{\mathrm{ID}} = H_1(\mathrm{ID}), \\ SK_{\mathrm{ID}} = \lambda \mathrm{PK}_{\mathrm{ID}}. \end{cases} \tag{16}$$

During the key generation process, each user can obtain multiple public–private key pairs. The energy managers and smart home managers deployed in the consumers' houses obtain exclusive public–private key pairs. In addition to obtaining exclusive public–private key pairs for the energy managers and smart home managers, prosumers also obtain public–private key pair for the DER deployed by them. To better explain our scheme, we define the public–private key pair of the smart home manager and DER as $(\mathrm{PK}_{\mathrm{ori}}, \mathrm{SK}_{\mathrm{ori}})$, which is the key of the original signcrypter. The key of the energy manager is $(\mathrm{PK}_{\mathrm{proxy}}, \mathrm{SK}_{\mathrm{proxy}})$, which is also the key of the proxy signcrypter. The recipient's key is represented by the public–private key pair $(\mathrm{PK}_{\mathrm{MG}}, \mathrm{SK}_{\mathrm{MG}})$ of the MG.

4.2.3. Proxy Key Generation. This phase is the core of IDPSC algorithm, and its main function is to entrust the data signcryption right to the proxy signcrypter, which is represented by $\mathrm{PKGen}(\mathrm{GP}, \omega, \mathrm{SK}_{\mathrm{ori}}, \mathrm{SK}_{\mathrm{proxy}}) \longrightarrow \mathrm{PSK}_{\mathrm{op}}$. The process of proxy key generation is performed by the user and can be divided into three steps. The first step is performed by the original signcrypter, such as smart home manager and DER, who uploads a warrant $\omega_{\mathrm{ori}} \in (0,1)^*$ (which records the proxy expiration date, proxy content permissions, and the identities of the original signcrypter and the proxy signcrypter) to the consortium blockchain. At this time, the MG needs to update the value of ω_{ori} of each node in the storage list in real time to verify the validity of the information during unsigncryption.

The second step is to generate the delegation D_ω. Both the private key $\mathrm{SK}_{\mathrm{ori}}$ of the original signcrypter and the private key $\mathrm{SK}_{\mathrm{proxy}}$ of the proxy signcrypter belong to the same user. In this step, the user can choose for the delegation to be generated by either the original signcrypter or the proxy signcrypter (energy manager). When the user has too many original signcrypters, it is recommended that the original signcrypter generate the delegation D_ω. The process is as follows:

$$\begin{aligned} s &= H_2(\omega_{\mathrm{ori}}), \\ D_\omega &= s\mathrm{SK}_{\mathrm{ori}}. \end{aligned} \tag{17}$$

In the third step, the proxy signer generates the proxy key.

$$\mathrm{PSK}_{\mathrm{op}} = \mathrm{SK}_{\mathrm{proxy}} + D_\omega. \tag{18}$$

The informational interaction between the proxy signcrypter and the original signcrypter takes place on the home LAN, and so there is no need to verify the information with the original signer.

4.2.4. Proxy Signcryption. In this phase, signcryption is performed on plaintext, the result of which is the ciphertext after signature and encryption, and the core algorithm is $\mathrm{PSigc}(\mathrm{GP}, \omega_{\mathrm{proxy}}, \mathrm{M}, \mathrm{PK}_{\mathrm{MG}}, \mathrm{PSK}_{\mathrm{op}}, \mathrm{SK}_{\mathrm{proxy}}) \longrightarrow \sigma$. When a user wants to participate in an auction, their proxy signcrypter needs to collect the quotation information $M \in (0,1)^n$ from the original signcrypter and organize it. The proxy signer randomly selects an element $x \in Z_p^*$ and computes the symmetric encryption key K:

$$K = H_3\left(e\left(\mathrm{PK}_{\mathrm{pub}}, \mathrm{PK}_{\mathrm{MG}}\right)^x\right). \tag{19}$$

Then, the proxy signer calculates the symmetric encrypted ciphertext C.

$$C = K \oplus M. \tag{20}$$

The proxy key $\mathrm{PSK}_{\mathrm{op}}$ is then used to perform the proxy signcryption.

$$\begin{cases} V = e\left(g, \mathrm{PK}_{\mathrm{pub}}\right)^x, \\ \mu = H_4(C, V), \\ S = x\mathrm{PK}_{\mathrm{pub}} - \left(\mu \mathrm{SK}_{\mathrm{proxy}} + \mathrm{PSK}_{\mathrm{op}}\right). \end{cases} \tag{21}$$

Finally, the proxy signcrypter outputs the proxy signcryption information $\sigma = (\omega_{\mathrm{proxy}}, \mu, C, S)$ and sends it to the MG. ω_{proxy} represents the original signcrypter's warrant forwarded by the proxy signcrypter. Placing ω_{proxy} in the proxy signcryption information σ helps the MG quickly find the original signcrypter corresponding to the proxy signcryption information.

4.2.5. Unsigncryption. The primary function of this phase is to help the information receiver recover the real and effective plaintext information from the ciphertext. The algorithm is expressed as $\mathrm{UnSigc}(\mathrm{GP}, \sigma, \mathrm{SK}_{\mathrm{MG}}, \mathrm{PK}_{\mathrm{MG}}, \mathrm{PK}_{\mathrm{ori}}, \mathrm{PK}_{\mathrm{proxy}})$. When the MG conducts an energy auction, it needs the quotation information M from the original signcrypter, which exists in the received proxy signcryption information σ. The MG thus needs to perform the unsigncryption process. If the warrant ω_{proxy} in the proxy signcryption information σ is inconsistent with that sent by the original signcrypter, an error symbol $\perp$ is returned. Otherwise, the MG performs the following tasks to check the validity of the ciphertext C in the proxy signcryption information σ:

$$\begin{cases} s = H_2(\omega_{\mathrm{ori}}), \\ V' = e(g, S)e\left(\mathrm{PK}_{\mathrm{pub}}, \mathrm{PK}_{\mathrm{proxy}}\right)^{\mu+1} e\left(\mathrm{PK}_{\mathrm{pub}}, \mathrm{PK}_{\mathrm{ori}}\right)^s. \end{cases} \tag{22}$$

Only when $\mu = H_4(C, V')$ is true does the MG receive the ciphertext C; it then calculates the symmetric encryption key:

$$K' = H_3\left(e(S, \mathrm{PK}_{\mathrm{MG}})e\left(\mathrm{PK}_{\mathrm{proxy}}, \mathrm{SK}_{\mathrm{MG}}\right)^{\mu+1}e\left(\mathrm{PK}_{\mathrm{ori}}, \mathrm{SK}_{\mathrm{MG}}\right)^{s}\right). \tag{23}$$

Finally, the MG obtains the original signcrypter's quotation information $M = K' \oplus C$. If the content of M does not fall within the scope specified in the warrant ω_{ori}, the algorithm outputs an error symbol $\perp$.

4.2.6. Proof of Correctness. We prove the correctness of this scheme by proving the correctness of V' and K'.

First, we prove the correctness of V'.

$$\begin{aligned}
V' &= e(g, S)e\left(PK_{pub}, PK_{proxy}\right)^{\mu+1}e\left(PK_{pub}, PK_{ori}\right)^{s} \\
&= e(g, S)e\left(\lambda g, PK_{proxy}\right)^{\mu+1}e(\lambda g, sPK_{ori}) \\
&= e(g, S)e\left(g, \lambda PK_{proxy}\right)^{\mu}e\left(g, \lambda PK_{proxy}\right)e(g, s\lambda PK_{ori}) \\
&= e(g, S)e\left(g, \mu SK_{proxy}\right)e\left(g, SK_{proxy}\right)e(g, sSK_{\mathrm{ori}}) \\
&= e(g, S)e\left(g, \mu \mathrm{SK}_{\mathrm{proxy}} + \mathrm{SK}_{\mathrm{proxy}} + D_{\omega}\right) \\
&= e\left(g, x\mathrm{PK}_{\mathrm{pub}} - \left(\mu \mathrm{SK}_{\mathrm{proxy}} + \mathrm{PSK}_{\mathrm{op}}\right)\right)e\left(g, \mu \mathrm{SK}_{\mathrm{proxy}} + \mathrm{PSK}_{\mathrm{op}}\right) \\
&= e\left(g, x\mathrm{PK}_{\mathrm{pub}}\right) = e\left(g, \mathrm{PK}_{\mathrm{pub}}\right)^{x} = V.
\end{aligned} \tag{24}$$

Then, we can prove the correctness of K'.

$$\begin{aligned}
K' &= H_3\left(e(S, \mathrm{PK}_{\mathrm{MG}})e\left(\mathrm{PK}_{\mathrm{proxy}}, \mathrm{SK}_{\mathrm{MG}}\right)^{\mu+1}e\left(\mathrm{PK}_{\mathrm{ori}}, \mathrm{SK}_{\mathrm{MG}}\right)^{s}\right) \\
&= H_3\left(\begin{array}{c} e(S, \mathrm{PK}_{\mathrm{MG}})e\left(\mathrm{PK}_{\mathrm{proxy}}, \lambda \mathrm{PK}_{\mathrm{MG}}\right)^{\mu} \\ e\left(\mathrm{PK}_{\mathrm{proxy}}, \lambda \mathrm{PK}_{\mathrm{MG}}\right)e(s\mathrm{PK}_{\mathrm{ori}}, \lambda \mathrm{PK}_{\mathrm{MG}}) \end{array}\right) \\
&= H_3\left(e(S, \mathrm{PK}_{\mathrm{MG}})e\left(\lambda \mathrm{PK}_{\mathrm{proxy}}, \mathrm{PK}_{\mathrm{MG}}\right)^{\mu}e\left(\lambda \mathrm{PK}_{\mathrm{proxy}}, \mathrm{PK}_{\mathrm{MG}}\right)e(s\lambda \mathrm{PK}_{\mathrm{ori}}, \mathrm{PK}_{\mathrm{MG}})\right) \\
&= H_3\left(e(S, \mathrm{PK}_{\mathrm{MG}})e\left(\mu \mathrm{SK}_{\mathrm{proxy}}, \mathrm{PK}_{\mathrm{MG}}\right)e\left(\mathrm{SK}_{\mathrm{proxy}}, \mathrm{PK}_{\mathrm{MG}}\right)e(\mathrm{sSK}_{\mathrm{ori}}, \mathrm{PK}_{\mathrm{MG}})\right) \\
&= H_3\left(e(S, \mathrm{PK}_{\mathrm{MG}})e\left(\mu \mathrm{SK}_{\mathrm{proxy}} + \mathrm{SK}_{\mathrm{proxy}} + D_{\omega}, \mathrm{PK}_{\mathrm{MG}}\right)\right) \\
&= H_3\left(e\left(x\mathrm{PK}_{\mathrm{pub}} - \left(\mu \mathrm{SK}_{\mathrm{proxy}} + \mathrm{PSK}_{\mathrm{op}}\right), \mathrm{PK}_{\mathrm{MG}}\right)e\left(\mu \mathrm{SK}_{\mathrm{proxy}} + \mathrm{PSK}_{\mathrm{op}}, \mathrm{PK}_{\mathrm{MG}}\right)\right) \\
&= H_3\left(e\left(x\mathrm{PK}_{\mathrm{pub}}, \mathrm{PK}_{\mathrm{MG}}\right)\right) \\
&= H_3\left(e\left(\mathrm{PK}_{\mathrm{pub}}, \mathrm{PK}_{\mathrm{MG}}\right)^{x}\right) = K
\end{aligned} \tag{25}$$

The $e(.,.)$ in all of the above formulas refers to the bilinear algorithm in Section 2.2.

4.3. Generation of Data Blocks. In the blockchain network, the generation of blocks is closely related to the consensus algorithm used on the blockchain, where consensus algorithms used by different types of blockchains are different. The system used in this paper is a $1 + N$ hybrid blockchain system, which is essentially a transaction consortium blockchain and N identity private blockchains. Because there are two different types of blockchains, this system uses two consensus algorithms to generate blocks at the same time, namely, the Raft consensus algorithm [33] and the PBFT consensus algorithm [34].

4.3.1. Consensus Algorithms of IPB. The private blockchain built by the MG itself is highly centralized and has central nodes, which coincides with the strong leadership of the Raft consensus algorithm. We thus use the Raft consensus algorithm on identity private blockchain. The strong leadership of the Raft consensus algorithm is mainly manifested in the fact that all log entries flow only from the leader server to the backup server, which simplifies the management of replicated logs [33]. There are three identities of the leader, candidate, and follower in the Raft consensus mechanism. In the identity private blockchain constructed by the MG, the leader is a node chosen by the MG from among its manager nodes, other unselected MG manager nodes and authority nodes are candidates, and followers are community user nodes in the identity private blockchain. A candidate is a candidate for leader. When the leader fails to operate normally, a new leader is selected from among the candidates. Only when all MG manager nodes fail does the authority node temporarily act as leader. The process of generating blocks using the Raft consensus algorithm can be simplified into three steps. In the first step, the leader node reviews the reputation data of the community users. Once the review is passed, it is sent to the energy manager nodes of each community user for reinspection. In the second step, the energy manager node reinspects the data sent by the leader node and returns the result to the leader node. In the third step, the leader node packages the data passed by both validation and revalidation into blocks and uploads them to the local private blockchain. To prevent the MG manager node on the private blockchain from tampering with the data, the hash value of the blocks on the private blockchain is uploaded to the trading consortium blockchain. In addition, the Raft consensus algorithm does not affect the user's reputation.

4.3.2. Consensus Algorithms of TCB. The PBFT consensus algorithm is used in the transaction consortium blockchain. A modified form of the original is used in this paper by changing the mechanism of establishing the consensus committee. In the original algorithm, the consensus committee is composed of preselected consensus nodes, the number of nodes in the consensus committee is fixed, and the consensus nodes do not change. In our modified PBFT algorithm, the consensus nodes that form the consensus committee are constantly changing. At the beginning of each round of transaction, the system selects the consensus nodes to form a new consensus committee, and the working time of each consensus committee is one trading cycle as planned by the system. To encourage MG trading platforms to maintain good internal trading behavior, the system constructs a consensus committee according to the principle of "reputation first, quantity first." The essence is to select the highest ranked MG community according to the selection principle. Reputation first in the selection rules refers to the selection of the MG community with the highest reputation score. Reputation depends on its internal users and is calculated as follows:

$$R_{\mathrm{MG}} = \frac{\sum_{i=1}^{l} R_i + \sum_{j=1}^{m} R_j}{l + m}, \quad (l + m) > H, \tag{26}$$

where l represents the number of buyers in the MG community at the time, m represents the number of sellers, and H is the fixed number of nodes of the consensus committee. The community with more users is preferred if two MG communities have the same reputation score. The same MG community cannot be selected consecutively; when this happens, the second-ranked MG community is responsible for block production.

Once the consensus committee has been built, members of the committee follow the same consensus process as in the original PBFT consensus algorithm to generate the blocks, as shown in Figure 6.

The distributed consensus process is divided into five stages: request, preprepare, prepare, commit, and reply. At the beginning of the request phase, the authority sends the client's request to the MG manager node. After receiving the request, the algorithm enters the preprepare phase; this stage requires the MG manager node to broadcast the sequence of execution of the transaction to the user node inside the consensus committee. In the prepare stage, the user node has two behaviors for the received information: one is to receive and forward the received information to the nodes, and the other is to do nothing. Nodes in the second state are called Byzantine nodes, such as producer 2 in Figure 6. The trigger for the commit phase is to receive $(H - f)$ identical requests for information. If this condition is satisfied, the commitment information is broadcast to the entire network. f is the number of Byzantine nodes in the consensus committee and needs to meet the condition $f \leq (H-1)/3$. In the reply phase, the consensus nodes also collect $(H-f)$ identical commitment information items before feeding it back to the authority. The verified information is packaged into blocks and uploaded to the trading consortium blockchain. Except for the MG manager node, all consensus nodes can receive reputation rewards after the block has been generated.

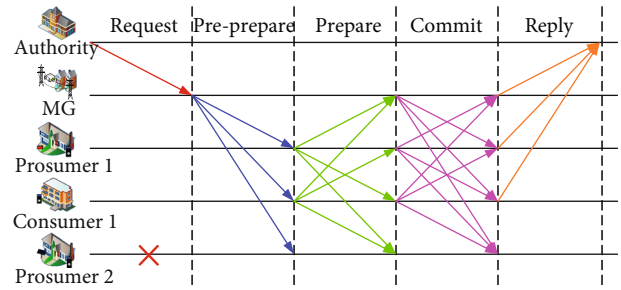

Figure 6: Consensus flowchart of the simplified PBFT algorithm.

Table 2: Comparison of security features.

Security features	Ref. [35]	Ref. [36]	Ref. [37]	Our scheme
Privacy	√	×	×	√
Confidentiality	×	×	×	√
Transparency	√	√	√	√
Traceability	√	√	√	√
Imtamperability	√	√	√	√
Nonrepudiation	√	×	×	√

5. Analysis and Evaluation

5.1. Analysis of System Performance. To verify the security of the MG energy trading mechanism based on the hybrid blockchain, we theoretically analyzed the implementation of various security features of this scheme. We also conducted a feature comparison with some proposals in the literature, and the results are shown in Table 2. It is clear that the proposed scheme outperformed the other schemes.

(1) Privacy and confidentiality: In this paper, two types of blockchains, the transaction consortium blockchain and the identity private blockchain, were used to store information. The user's identity-related information is stored in the identity private blockchain. When the user transacts in the trading consortium blockchain, the attacker cannot learn their identity from the transaction information. To ensure the confidentiality of the transaction information, we use an identity-based proxy signcryption algorithm in which the quotation submitted by users is encrypted with a symmetric encryption key. Nodes in the consortium blockchain cannot understand the quotation information contained in the ciphertext without obtaining the symmetric encryption key

(2) Transparency and traceability: As blockchain is a shared ledger, all nodes share the same data, and the transaction records generated by each node are public. The generation of blocks in the blockchain also follows transparent consensus rules. The consensus node processes the transaction information and generates new blocks according to the specific consensus to render the data transparent. Blocks on the blockchain are generated in chronological order, and all transactions are open due to the transparency of the blockchain. When there is doubt about a transaction, the information on it can be traced according to the above conditions

(3) Imtamperability: The difficulty of data tampering on the blockchain is related to the consensus algorithm used. In this paper, the Raft consensus algorithm was used on the private blockchain and the PBFT consensus algorithm on the consortium blockchain. The central node of the private chain is powerful. To prevent the central node from tampering with the data, we store the block digest of the private blockchain in the consortium blockchain. Therefore, the scheme's resistance to being tampered with is implemented by the PBFT consensus algorithm on the consortium blockchain. The PBFT algorithm is the most commonly used consensus algorithm on the consortium blockchain because of its high scalability and low power consumption. When it is used, the system can still work normally even if 33% of the nodes in the system are Byzantine nodes [38]. In

addition, the consensus nodes in this paper were selected from among nodes with good reputation, which yield more benefits. It is unrealistic for more than a third of nodes with good reputation to go against their own interests to jeopardize the stability of the system

(4) Nonrepudiation: The nonrepudiation of information is realized by a digital signature that is broadcast and verified between nodes before being stored in the blockchain. When a trade dispute arises, the nonrepudiation of the given trade can be realized by tracing the trade signature in the blockchain. The identity-based proxy signcryption scheme used in this paper can not only encrypt the information but can also sign it. Because the transaction entity does not have enough computing power to carry out frequent signcryption, we entrust the right of signcryption of the data to a proxy signcrypter with strong computing power. The signcryption information of the proxy signcrypter is identical to that of the original signcrypter

5.2. Analyzing Validity of Algorithm to Assess Reputation Based on User Behavior. Algorithms to assess reputation based on user behavior can be divided into those based on buyer behavior and seller behavior. The validity of the algorithm considered here thus needs to be analyzed from the perspectives of both the buyer and the seller. Because the contract reputation scores of the buyers and sellers are closely related to the peak and trough periods of trading time, this paper used the peak–valley period division table as shown in Table 3 for a more concise analysis of the validity of the algorithm. Each trading cycle is 30 minutes long.

5.2.1. Analyzing the Validity of Algorithm to Assess Buyer Behavior. To verify the validity of the algorithm to assess buyer behavior, we considered a scenario in which three buyers performed different behaviors over 24 hours. As Figure 7 shows, when the buyer did not trigger a reputation event, their score remained the same. From 3:00 to 3:30, buyer A triggered a default event; as this was a valley period, buyer A's score dropped by 1.25. From 6:00 to 6:30, buyer C triggered a default event. At this was the average period, buyer C's score dropped by 1. From 8:00 to 11:00, the user entered the peak period of electricity consumption. When power consumption was in short supply during the peak period, the MG issued a demand response event. Both buyers A and C activated the demand response event in this period. From 8:00 to 10:00, buyer A continuously activated four demand response events and maintained a capacity deviation of less than 5%. Buyer A thus added 4 scores in total in this period. From 8:30 to 10:30, buyer C also activated four demand response events in a row, but the capacity deviation the first two times was in the range of 5%–25% and was less than 5% for the last two instances. Buyer C thus added 3.4 scores in total. From 10:00 to 10:30, the MG community was selected to lead the block generation process, and buyer C successfully triggered the block generation event and earned a score of 0.45. From 14:30 to 15:00, buyer C triggered the default event again, in the average period, and lost

Table 3: Peak and valley time division.

Period (hour)	Peak period	Average period	Valley period
(0-6]	0	0	1
(6-8]	0	1	0
(8-11]	1	0	0
(11-16]	0	1	0
(16-21]	1	0	0
(21-22]	0	1	0
(22-24]	0	0	1

1: current time belongs to this period; 0: current time does not belong to this period.

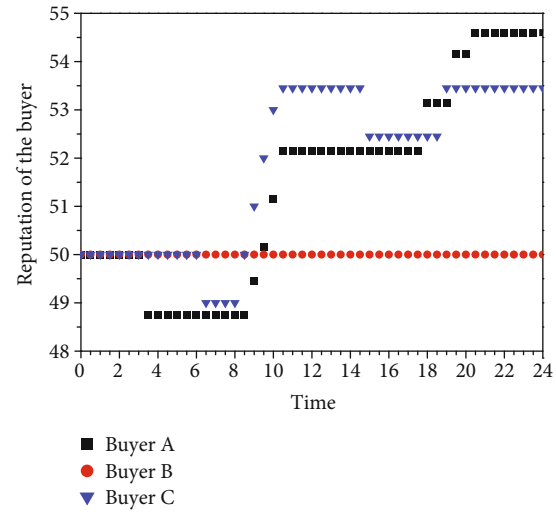

Figure 7: Reputation scores of three buyers.

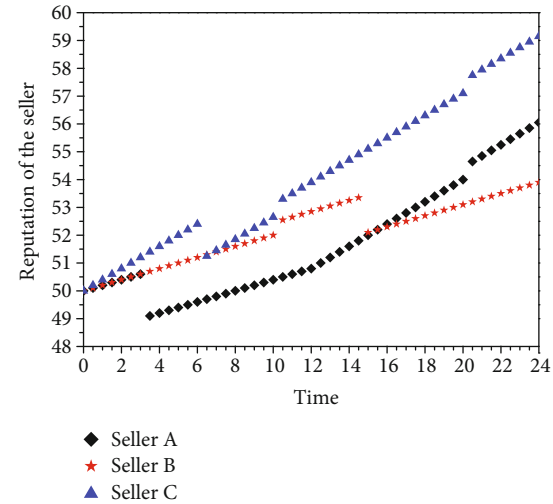

Figure 8: Reputation scores of three sellers.

1 point again. From 16:00 to 21:00, during the peak period of electricity consumption, buyer A activated demand response events two times, from 17:30 to 18:00 and from 19:00 to 19:30 and obtained 2 scores; buyer C activated only once, from 18:30 to 19:00, and earned 1 reputation score.

Table 4: Comparison of computational overheads.

Scheme	PKGen	PSigc	UnSigc	Total
Ref. [39]	$2T_M$	$5T_M + T_E$	$T_M + T_E + 5T_P$	$8T_M + 2T_E + 5T_P$
Ref. [40]	$2T_M + T_E + T_P$	$3T_M + T_E$	$T_M + T_E + 4T_P$	$6T_M + 3T_E + 5T_P$
Ref. [41]	$2T_E + 2T_P$	$T_M + 2T_E$	$4T_P$	$T_M + 4T_E + 6T_P$
Our scheme	T_M	$2T_M + 2T_E$	$4T_E + 2T_P$	$3T_M + 6T_E + 2T_P$

T_M: time needed for scalar multiplication operation on G; T_E: time needed for exponential operation on G_T; T_P: time needed for bilinear pairing operation.

From 20 : 00 to 20 : 30, the MG community was again eligible for block generation, and buyer A triggered this block generation event to obtain 0.45 scores. Buyer B neither initiatively triggered the default event nor the demand response event. When the MG community obtained the block generation qualification, buyer B's reputation was not among the top H-1; so, B could not trigger the block generation event, and its reputation score remained unchanged at the initial value of 50. The results show that all behaviors of buyers are objectively reflected in their reputation scores.

5.2.2. Analyzing the Validity of Algorithm to Assess Seller Behavior. To verify the validity of the algorithm to assess seller behavior, we considered another scenario in which three sellers performed different behaviors in 24 hours. As Figure 8 shows, assuming sellers A and B had the same quality of power supply service, and seller C supplied better service than them, and when the seller did not trigger a default event, the reputation scores of 0.1 were obtained for A and B by the feedback event at the end of each round. C obtained 0.2 reputation points through the feedback event. When the seller triggered the default event, both A and B lost 0.25 reputation points for the feedback event and C lost 0.15 reputation points. The occurrence of consensus events did not affect the score of the feedback events. From 3 : 00 to 3 : 30, seller A triggered a default event; as this was a valley period, seller A's score dropped by 1.5. From 6 : 00 to 6 : 30, seller C triggered a default event in the average period, and his/her score dropped by 1.15. From 10 : 00 to 10 : 30, the MG community was selected to dominate the block generation process, sellers B and C triggered the block generation event together, and seller B scored 0.55 while seller C scored 0.65. At 12 : 00, and seller A updated the equipment. Following this, A and C had the same quality of service, and the reputation scores provided by the feedback event were identical to those for C. From 14 : 30 to 15 : 00, seller B triggered the default event in the average period, and his/her reputation score decreased by 1.25. From 20 : 00 to 20 : 30, the MG community was again eligible for block generation, and A and C triggered block generation events together; both received 0.65 points. The results show that all behaviors of sellers were objectively reflected in their reputation scores.

5.3. Assessing the IDPSC Algorithm. The computational cost of the proxy signcryption algorithm consists mainly of three operations: proxy key generation, proxy signcryption, and unsigncryption. In this section, our scheme is compared with those proposed in Refs. [39–41] from the perspective of computational cost, and the results are shown in Table 4. Many key parameters in the IDPSC algorithm can be used all the time after one calculation. These parameters are calculated in advance by the system and thus are not included in the comparison of computational costs of the algorithms considered here. In Table 4, T_M represents the duration of operation of scalar multiplication on G, T_E represents that of the exponential operation on G_T, and T_P represents the time required for the bilinear pairing operation. To show the computational cost of each scheme more clearly, we refer to the operation time defined by He et al. [42] for calculation; that is, the time required for the scalar multiplication operation on G was 13.405 ms, that for exponential operation on G_T was 2.249 ms, and the time required for the bilinear pairing operation was 32.713 ms.

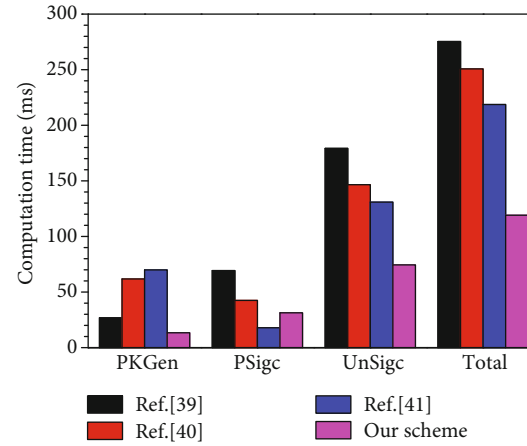

Figure 9: Comparison of computational overhead.

Figure 9 shows a comparison of the calculation costs of the proposed scheme with certain other schemes. It is clear that our scheme delivered the best performance on the proxy key generation algorithm and the unsigncryption algorithm. In the proxy signcryption algorithm, although our scheme was not the best, only the one proposed by Yu et al. [41] was superior to it. In terms of overall overhead, our method was the best. Our overall overhead accounts for 43.27% of Ref. [39], 47.51% of Ref. [40], and 54.62% of Ref. [41]. In general, it was more useful in practical application scenarios.

6. Conclusion

To address the problems of data storage and identity management and transaction in the microgrid, this paper proposed a secure transaction mechanism for it based on a

hybrid blockchain. A combination of the identity private blockchain and the transaction consortium blockchain is used to store users' identity information and trade information separately to guarantee user privacy. Blockchain-based features such as transparency and traceability provide a transparent and open energy trading platform for users of the MG community. In the process of energy transactions in the microgrid community, both parties to the transaction may have dishonest behaviors, and the occurrence of dishonest behaviors will result in property losses, which will reduce the participation of users. A reputation evaluation algorithm based on user behavior is used to constrain users' MG trading behavior on the identity private blockchain and is committed to creating a favorable atmosphere for the energy trading market. The smart home manager or DER, as a light node, cannot afford the computing power required for frequent signcryption. This paper proposes an identity-based proxy signcryption algorithm to guarantee the confidentiality of user quotations and the nonrepudiation of transactions. A system analysis showed that the reputation evaluation algorithm proposed here can objectively reflect all the behaviors of users, and the identity-based proxy signcryption scheme has advantages over competitors in data sharing.

Data Availability

The authors approve that data used to support the finding of this study are included in the article.

Conflicts of Interest

The authors declare no conflict of interest.

Authors' Contributions

Conceptualization was done by Z. S. and X. Z. Algorithm and simulation were done by Z. S. Writing-original draft and review were done by Z. S and X. Z. Security analysis was done by X. Z. Paper polish, editing, and revision were done by M. L. Visualization was done by Z. S. and X. Z.

Acknowledgments

This work is jointly supported by the National Natural Science Foundation of China (Nos. 61763017, 51665019, and 61901198), Scientific Research Plan Projects of Jiangxi Education Department (No. GJJ150621), the Program of Qingjiang Excellent Young Talents, Jiangxi University of Science and Technology (No. JXUSTQJYX2020019), and the Innovation Fund for Graduate Students in Jiangxi Province (Grant No. YC2020-S443).

References

[1] W. A. Hermann, "Quantifying global exergy resources," *Energy*, vol. 31, no. 12, pp. 1685–1702, 2006.

[2] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, and M. Kraft, "Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application," *Applied Energy*, vol. 209, pp. 8–19, 2018.

[3] D. Han and H. Xie, "China Renewable Energy Development Report 2018," *Water Power*, vol. 45, no. 8, p. 46, 2019.

[4] A. Y. Saber and G. K. Venayagamoorthy, "Plug-in vehicles and renewable energy sources for cost and emission reductions," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 4, pp. 1229–1238, 2011.

[5] A. Ahmad and J. Y. Khan, "Real-Time load scheduling and storage Management for Solar Powered Network Connected EVs," *IEEE Transactions on Sustainable Energy*, vol. 11, no. 3, pp. 1220–1235, 2020.

[6] W. Shao, W. Xu, Z. Xu, B. Liu, and H. Zou, "A grid connection mechanism of large-scale distributed energy resources based on blockchain," in *2019 Chinese Control Conference (CCC)*, pp. 7500–7505, Guangzhou, China, July 2019.

[7] A. Khanjanzadeh, S. Soleymani, and B. Mozafari, "A decentralized control strategy to bring back frequency and share reactive power in isolated microgrids with virtual power plant," *Bulletin of the Polish Academy of Sciences-Technical Sciences*, vol. 69, no. 1, article e136190, 2021.

[8] M. Royapoor, M. Pazhoohesh, P. J. Davison, C. Patsios, and S. Walker, "Building as a virtual power plant, magnitude and persistence of deferrable loads and human comfort implications," *Energy & Buildings*, vol. 213, article 109794, 2020.

[9] Y. Liu, Y. Li, H. B. Gooi et al., "Distributed robust energy management of a multimicrogrid system in the real-time energy market," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 1, pp. 396–406, 2019.

[10] X. Zhang, T. Yu, Z. Xu, and Z. Fan, "A cyber-physical-social system with parallel learning for distributed energy management of a microgrid," *Energy*, vol. 165, pp. 205–221, 2018.

[11] S. Ranjbar, A. R. Farsa, and S. Jamali, "Voltage-based protection of microgrids using decision tree algorithms," *International Transactions on Electrical Energy Systems*, vol. 30, no. 4, article 2274, 2020.

[12] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017.

[13] G. Kim, J. Park, and J. Ryou, "A study on utilization of blockchain for electricity trading in microgrid," in *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 743–746, Shanghai, China, January 2018.

[14] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: a case study: the Brooklyn microgrid," *Applied Energy*, vol. 210, pp. 870–880, 2018.

[15] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino, and G. Zizzo, "A technical approach to the energy blockchain in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4792–4803, 2018.

[16] M. L. Di Silvestre, P. Gallo, M. G. Ippolito et al., "Ancillary services in the energy blockchain for microgrids," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 7310–7319, 2019.

[17] M. U. Hassan, M. H. Rehmani, and J. Chen, "DEAL: differentially private auction for blockchain-based microgrids energy trading," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 263–275, 2020.

[18] G. van Leeuwen, T. AlSkaif, M. Gibescu, and W. van Sark, "An integrated blockchain-based energy management platform with bilateral trading for microgrid communities," *Applied Energy*, vol. 263, article 114613, 2020.

[19] A. Meeuw, S. Schopfer, A. Woerner et al., "Implementing a blockchain-based local energy market: Insights on communication and scalability," *Computer Communications*, vol. 160, pp. 158–171, 2020.

[20] Y. C. Tsao and V. V. Thanh, "Toward blockchain-based renewable energy microgrid design considering default risk and demand uncertainty," *Renewable Energy*, vol. 163, pp. 870–881, 2021.

[21] R. Lasseter, A. Akhil, C. Marnay et al., *Integration of distributed energy resources. The CERTS Microgrid Concept*, Lawrence Berkeley National Lab.(LBNL), Berkeley, CA (United States), 2002.

[22] D. Boneh, E. J. Goh, and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," in *Theory of Cryptography. TCC 2005. Lecture Notes in Computer Science, vol 3378*, J. Kilian, Ed., pp. 325–341, Springer, Berlin, Heidelberg, 2005.

[23] D. Freeman, S. Michael, and T. Edlyn, "A taxonomy of pairing-friendly elliptic curves," *Journal of Cryptology*, vol. 23, no. 2, pp. 224–280, 2010.

[24] C. Gamage, J. Leiwo, and Y. Zheng, "An efficient scheme for secure message transmission using proxy-signcryption," in *The Twenty Second Australasian Computer Science Conference*, pp. 18–21, Auckland, New Zealand, 1999.

[25] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption)," in *Advances in Cryptology — CRYPTO '97. CRYPTO 1997. Lecture Notes in Computer Science, vol 1294*, B. S. Kaliski, Ed., pp. 165–179, Springer, Berlin, Heidelberg, 1997.

[26] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 79, no. 9, pp. 1338–1354, 1996.

[27] G. Sun, M. Dai, F. Zhang, H. Yu, X. Du, and M. Guizani, "Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7868–7882, 2020.

[28] X. Zhang and D. Wang, "Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain," *IEEE Access*, vol. 7, pp. 97281–97295, 2019.

[29] 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 Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[30] P. Wang, Y. Li, S. Zhao, H. Chen, Y. Jin, and Y. Ding, "Key technologies of distributed energy trading based on blockchain," *Automation of Electric Power Systems*, vol. 43, no. 14, pp. 53–64, 2019.

[31] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium Blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.

[32] H. Zhu, Y. Wang, C. Wang, and X. Cheng, "An efficient identity-based proxy signcryption using lattice," *Future Generation Computer Systems*, vol. 117, pp. 321–327, 2021.

[33] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14)*, pp. 305–319, Philadelphia, PA, USA, June 2014.

[34] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *the Third Symposium on Operating Systems Design and Implementation (OSDI'99)*, pp. 173–186, New Orleans, Louisiana, USA, 1999.

[35] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[36] W. Zhao, J. Lv, X. Yao et al., "Consortium blockchain-based microgrid market transaction research," *Energies*, vol. 12, no. 20, article 3812, 2019.

[37] Z. Xu, D. Yang, and W. Li, "Microgrid group trading model and solving algorithm based on bockchain," *Energies*, vol. 12, no. 7, article 1292, 2019.

[38] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.

[39] C. Zhou, "Identity based generalized proxy signcryption in standard model," *Journal of Cryptologic Research*, vol. 3, no. 3, pp. 307–320, 2016.

[40] H. Yu, Z. Wang, J. Li, and X. Gao, "Identity-based proxy signcryption protocol with universal composability," *Security and Communication Networks*, vol. 2018, 11 pages, 2018.

[41] H. Yu and Z. Wang, "Construction of certificateless proxy signcryption scheme from CMGs," *IEEE Access*, vol. 7, pp. 141910–141919, 2019.

[42] D. He, H. Wang, L. Wang, J. Shen, and X. Yang, "Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices," *Soft Computing*, vol. 21, no. 22, pp. 6801–6810, 2017.