

DOI: 10.32604/iasc.2023.037875 *Article*





A Distributed Power Trading Scheme Based on Blockchain and Artificial Intelligence in Smart Grids

Yue Yu¹, Junhua Wu^{1,*}, Guangshun Li¹ and Wangang Wang²

 ¹Qufu Normal University, Rizhao, 276800, China
²Shandong Zhongsheng Data Co., Ltd., Rizhao, 276800, China
*Corresponding Author: Junhua Wu. Email: shdwjh@163.com Received: 19 November 2022; Accepted: 15 February 2023

Abstract: As an emerging hot technology, smart grids (SGs) are being employed in many fields, such as smart homes and smart cities. Moreover, the application of artificial intelligence (AI) in SGs has promoted the development of the power industry. However, as users' demands for electricity increase, traditional centralized power trading is unable to well meet the user demands and an increasing number of small distributed generators are being employed in trading activities. This not only leads to numerous security risks for the trading data but also has a negative impact on the cost of power generation, electrical security, and other aspects. Accordingly, this study proposes a distributed power trading scheme based on blockchain and AI. To protect the legitimate rights and interests of consumers and producers, credibility is used as an indicator to restrict untrustworthy behavior. Simultaneously, the reliability and communication capabilities of nodes are considered in block verification to improve the transaction confirmation efficiency, and a weighted communication tree construction algorithm is designed to achieve superior data forwarding. Finally, AI sensors are set up in power equipment to detect electricity generation and transmission, which alert users when security hazards occur, such as thunderstorms or typhoons. The experimental results show that the proposed scheme can not only improve the trading security but also reduce system communication delays.

Keywords: Smart grids; blockchain; artificial intelligence; distributed trading; data communication

1 Introduction

With the rapid development of power transmission, information, sensing, and other technologies, the smart grid (SG) industry is prospering and has become a key area with broad development prospects. Artificial intelligence (AI) technology is also being widely used for data processing and storage in SGs [1]. In traditional centralized trading, consumers and producers indirectly trade through numerous intermediary third parties and retailers. To maintain the normal operation of trading markets, high-cost regulatory systems are utilized [2]. However, the integrity and security of third



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

parties cannot be guaranteed, which may lead to various issues, such as low market transparency and fairness. The two-way flow of power and information in SGs allows users to freely choose their identities according to their own needs. Distributed trading schemes accommodate consumers, producers, and users with multiple identities and are conducive to ensuring the balance between power supply and demand [3]. Therefore, SGs integrate procedures necessary for power trading, including bidding, negotiation, and contract execution between participants, allowing buyers and sellers to directly trade without relying on any intermediaries [4]. However, with the increase in the market size, the growth in the number of users leads to many potential risks to the trading data and electrical security. In this situation, AI plays an essential role.

AI is a research and development technology that is used to simulate and expand people's theories and applications. It plays an important role in every SG application, such as grid planning, grid construction, daily inspection, and fault diagnosis [5]. AI can not only realize reasonable long-distance power transmission but also intelligently monitor equipment via daily inspection and maintenance, thus improving productivity and considerably contributing to the development of SGs [6]. Therefore, AI sensors are essential in our scheme to ensure the stable and secure transmission of power.

In addition, SGs have many unsolved challenges. Since they are employed in many fields, such as home furnishing, transportation, and urban construction, their vulnerability to cyber attacks can seriously affect the society and not just the power system. Therefore, a correct and efficient encryption mechanism should be employed for SGs for identity authentication to ensure that unauthorized opponents from outside the system cannot access or tamper with any data and to strengthen the protection of the users' identity information and trading data [7]. Moreover, the system should be equipped with a reliable monitoring mechanism to detect and record users' behaviors in real time to enhance the transparency between entities and maintain the normal operation of the market [8]. However, in highly decentralized trading markets, most of the existing supervision and claim mechanisms necessitate high management costs and may even lead to serious data privacy risks.

Blockchains originated from the underlying framework of the Bitcoin system, and they integrate many technologies, such as encryption, consensus, and smart contracts. They have the characteristics of decentralization, openness, and tamper-proof [9]. Blockchains are maintained and stored by many entities in a network without a credible third party, considerably improving the overall transparency and security of the system [10]. Thus, they have many advantages that traditional centralized systems do not have when encountering system failures and network attacks, and they realize the transformation of the traditional trading mode, as shown in Fig. 1. Therefore, owing to the growing demand for power trading, this study combines blockchain with AI in distributed trading scenarios, which can not only flexibly and efficiently trace trading records but also realize effective market supervision and security monitoring [11].

This study proposes a secure and efficient distributed power trading scheme based on blockchain and AI. The main study contributions are as follows:

- 1. Credibility-based power trading: To protect the legitimate interests and rights of both buyers and sellers, a trading scheme based on the credibility is proposed to effectively restrain users' dishonest behaviors. In addition, blockchain can realize the traceability of trading records and low-cost market supervision.
- 2. Weighted communication tree (WCT) construction algorithm: A WCT construction algorithm is proposed based on nodes' trust value and communication capability. It constructs a communication topology suitable for the blockchain network to achieve superior data

transmission. Thereby, the blockchain transaction confirmation is accelerated and the power trading efficiency is improved.

3. Smart sensors are set up in the power equipment to monitor users' power generation and transmission, which has high economic benefits. This practice can effectively reduce the occurrence of security accidents.



Figure 1: Distributed management mode

This paper is structured as follows: Section 2 introduces the related work. Section 3 presents the details of the distributed power trading scheme based on blockchain and AI, including the credibility-based power trading and WCT construction algorithm. Section 4 describes the performance analysis of the proposed scheme. Section 5 presents the conclusions.

2 Related Work

In recent years, many researchers have suggested schemes for distributed power trading and the application of AI in SGs. The relevant technologies are summarized as follows.

Guo et al. [12] and Xia et al. [13] designed reliable trading schemes using Stackelberg game and Bayesian game theory, respectively. In the distributed chain with incomplete shared information in their scheme, the optimal pricing maximizes the utility and ensures the power trading security. Hassan et al. [14] and AlAshery et al. [15] realized secure and reliable energy trading by combining blockchain with the auction mechanism. Hassan et al. used differential privacy technology to ensure the security and privacy of the auction and used a consortium chain to reduce the computational complexity of the nodes. AlAshery et al. integrated the trading framework comprising bilateral contracts, e-commerce platform, two-way auction Vickrey Clarke Groves (VCG) mechanism, and trading capacity with the main power grid. Through these multi-layer mechanisms, various trading preferences and attributes of power generation and consumption can be adapted. Simultaneously, the VCG mechanism eliminates the possibility of exercising any market power by encouraging participants to make real bids. Furthermore, Pee et al. [16] created a point-to-point (P2P) system that uses blockchain to ensure the immutability and transparency of energy trading while generating ERC20 tokens based on smart contracts; this enables the automatic execution of trades without third-party intervention and enables the scaling to various trading conditions. To manage the demand-response in the vehicle-to-grid environment, Aggarwal et al. [17] and Kang et al. [18] designed a P2P energy trading mechanism between electric vehicles (EVs) and service providers and between local plugin hybrid EVs, respectively. Their mechanisms can achieve balance between demand and response

through incentive measures and can solve the energy pricing and trading volume in demand-response through a two-way auction mechanism to maximize social welfare. Combined with federated learning and edge computing, Fan et al. [19] proposed a blockchain-based hybrid resource trading system. To avoid the overheads of interregional blockchain data synchronization, their system allows requesters and edge devices to interact with public and consortium chains and uses smart contracts to integrate payment channels into the public chain to enable efficient and reliable payments between requesters and edge nodes. Baza et al. [20] designed a generic linkable prefix, anonymous authentication scheme that blockchains can identify if EVs simultaneously submit multiple bookings or offers. They also introduced an anonymous, blockchain-based efficient payment system to further protect the privacy of EV drivers.

To solve the problems of accuracy, range, and speed required by indoor positioning technologies in SG applications, Cheng et al. [21] proposed a real-time indoor positioning system for SG based on ultra-wideband and AI technology. Since their system has a short duration of radio frequency pulse and wide bandwidth, it can minimize the influence of multipath interference. Thus, it is suitable for real-time positioning in SGs. Neto et al. [22] proposed that with the increasing use of SGs to improve the energy efficiency, smart meters and other devices have accumulated considerable information flows, which can be analyzed to help power system controllers in decision making. Using an adaptive neuro-fuzzy inference system based on AI, they obtained better performance of outlier correction than the techniques based on artificial neural network and linear interpolation. Tong et al. [23] proposed a lightning fault prediction method for an SG distribution system based on AI and introduced selfbalancing dynamic lightning protection to assist in the self-healing of the SG distribution network. This method provides a comprehensive lightning protection solution for SGs and improves the system reliability.

The analysis of the above schemes shows that the most popular scheme is the use of a double auction mechanism to promote power trading. This discrete fast-trading algorithm helps to accurately predict the electricity consumption and generation, allowing users to make more flexible choices and reducing the power waste due to inaccurate predictions. The common feature of the above trading schemes is that most of them mainly focus on the optimization of social welfare and economic utility, but they seldom consider the possible reliability problems of the users themselves. Consequently, few effective accountability mechanisms have been provided for malicious behaviors, and the potential threats of loopholes in the market supervision mechanism to the users' interest are ignored. Moreover, due to the limited transaction confirmation speed of traditional blockchain, the improvement of power trading efficiency is hindered.

3 Distributed Power Trading Scheme Based on Blockchain and AI

The scheme proposed in this study is mainly divided into two parts: credibility-based power trading and WCT construction algorithm. To make the trading records traceable and effectively restrain the dishonest behaviors of users, a management center (MC) is employed to maintain the private chain and manage multiple data aggregators (DAs) for collecting, packaging, and verifying trading information. After receiving a trading request, the MC verifies the user's identity and assists them in accomplishing a credibility-based power trading. To prevent accidents, AI sensors are used to detect whether extreme weather or equipment failure occurs, which are unsuitable for power transmission. Then, the DAs select the accounting node and determine the communication route for block verification by the WCT to optimize the transaction confirmation speed on the chain. Finally, DAs store the trading information in the private chain. The system framework is shown in Fig. 2.



Figure 2: System framework

3.1 Credibility-Based Power Trading

The relevant symbols and descriptions used in this section are listed in Table 1.

| Symbol | Description |
|-----------|---|
| ID | Identity of buyers or sellers |
| Cert | Certificate of buyers or sellers |
| Credit | Credibility of buyers or sellers |
| volume | Power demand |
| W | User's wallet |
| price | Intended price of sellers |
| wallet | Shared wallet |
| pk | Public key generated by the MC for the shared wallet |
| sk | Private key generated by the MC for the shared wallet |
| Token | Token generated by the MC for buyers |
| Sign | Signature |
| Timestamp | Current timestamp |
| balance | Current balance of the buyer's account |
| t | Validity period of the shared wallet |
| date | Payment period |
| record | Previous consumption records |
| PRE | Consumption compliance record |
| S | Number of timely payments |
| f | Number of untimely payments |

| Table 1: | List of related symbols |
|----------|-------------------------|

1) Initialization and Registration

The MC initializes the system and generates an initial WCT for data communication. To obtain certificates, users register with the MC using their real identity.

- 2) Request
 - The buyer B_i sends a power request to the MC:

$$B_i \to MC: RE = \left\{ ID_i || \left\{ W_{B_i,k} \right\}_{k=1}^k || Cert_i || Credit_i || volume_i \right\}$$

where $\{W_{B_i,k}\}_{k=1}^k$ represents all the used wallet addresses of B_i and $Cert_i$ denotes the buyer's certificate, which binds the users registration information to a unique node.

- When the MC receives a request, it checks the certificate validity. Then, it downloads the records related to this user in the blockchain and queries the trading history to obtain the capital flow according to $\{W_{B_i,k}\}_{k=1}^k$. After calculating the current wealth of B_i , the MC broadcasts the request if the asset of B_i is non-empty.
- Sellers who want to trade in the system send a request to the MC: $S_i \rightarrow MC$: $RE = \{ID_i || Cert_i || Credit_i || price_i\}$
- The MC checks the validity of the sellers' certificates after receiving their requests and records their credibility.
- 3) Respond
 - The MC creates a shared wallet and sends the sellers' identities, credibility, and respective pricing as well as the key pair of the shared wallet to the buyer.
 - The buyer receives a response:

$$MC \rightarrow B_i: RES = \left\{ \left(pk_{mc}^i, sk_{mc}^i \right) \mid \left\{ ID_j \right\}_{j=1,2,\dots} \mid \left\{ Credit_j \right\}_{j=1,2,\dots} \mid \left\{ price_j \right\}_{j=1,2,\dots} \right\}$$
$$\mid |Token_i| \mid Sign_{sk_{mc}} \left(Token_i \right) \mid |Timestamp \right\}$$

where pk_{mc}^{i} and sk_{mc}^{i} are the public and private keys generated by the MC for the shared wallet, and $Sign_{sk_{mc}}$ (*Token_i*) is the signature of the MC on *Token_i*. $Token_{i} = \{balance_{i}||t_{i}||Cert_{mc}^{i}||volume_{i}||date_{i}||record_{i}||Timestamp\}$

It includes the current balance of the buyer's account $balance_i$, the validity period of the shared wallet t_i , the shared wallet's certificate $Cert^i_{mc}$, the power purchase volume $volume_i$, the payment period $date_i$, the previous consumption records $record_i$, and the current timestamp.

$$record_i = \{PRE_i (s_i, f_i) || Hash (TX_i)_{i=1,2,...,h} \}$$

It includes the consumption compliance record and the credibility-based consumption record.

- 4) Payment
 - The buyer B_i selects the trading object S_j and completes the payment through the blockchain with the shared wallet:

$$B_i \rightarrow S_j$$
: $Pay = \{ Token_i | | price_j | | Cert_i | | Cert_{mc}^i | | Sign_{sk_{R_i}} (Token_i) | | Timestamp \}$

 B_i pays S_j , and S_j checks the validity of $Cert^i_{mc}$ and $wallet^i_{mc}$ and checks the balance in the shared wallet.

• The seller verifies the balance in the shared wallet; transmits the power to the buyer on the premise that the AI sensors verify the security; and sends *Token_i*, the bill of this trading, the address of the wallet used to receive the payment, and the signature of all the above information to the MC:

$$S_j \rightarrow MC$$
: $Bill = \left\{ Token_i || Cert_j || Bill_j || W_{S_j} || Pay_i || Sign_{sk_{S_i}} (Pay_i) || Timestamp \right\}$

The buyer sends a confirmation to the MC after receiving power from S_i .

- The MC validates the received *Token*_i and transfers the balance from the shared wallet to *W*_{si} after receiving the confirmation from *B*_i.
- After the trading is completed, the MC updates the balance in *wallet*^{*i*}_{*mc*} and *Token*_{*i*}, adds its signature to *Token*_{*i*}^{*new*}, and sends it to *B*_{*i*}. The DA selected by WCT as the accounting node packages the bill and *Token*_{*i*} into the block.
- The MC recalculates and updates the credibility of both the buyer and seller:

 B_i receives $Token_i^{new}$, which contains the hash of all payment records using $Token_i$. If B_i completes the payment within $date_i$, s_i adds one; otherwise, f_i adds one. The buyer's credibility is calculated as

 $Credit_{n+1}^{i} = Credit_{n}^{i} - w \cdot volume_{i}$

where *w* is a constant greater than zero.

If the MC receives a confirmation of B_i within the specified time, s_j adds one; otherwise, f_j adds one. The seller's credibility is calculated as

 $Credit_{n+1}^{j} = Credit_{n}^{j} - w \cdot volume_{i}$

where *w* is a constant greater than zero.

• If a user has a trust-breaking record, they must pay a certain number of fines. If their credibility is below a specific limit, the MC adds the user to the blacklist and broadcasts the blacklist to all users in the system. Fig. 3 displays the trading process.



Figure 3: Credibility-based power trading

3.2 WCT Construction Algorithm

As the accounting and verification nodes in the blockchain, DAs periodically collect trading records, build them into blocks, and upload them to the private blockchain. For the block verification, a WCT construction algorithm is proposed based on the nodes' trust value and their communication ability. The communication structure of nodes in the blockchain network is simulated in a tree shape, and the comprehensive performance of a node is calculated according to the number of forwarding tasks and its success rate. Nodes with high integrity and low communication overheads are located in the upper layer of WCT and they undertake more data forwarding tasks, while those nodes in the bottom layer of WCT are only responsible for receiving and verifying. This structure ensures the data communication security and improves the transaction confirmation efficiency.

The blockchain communication network is abstracted as a graph $G = \{N, E, T, W, L\}$, where N is the set of nodes, E is the set of edges, T is the set of nodes' trust value, W is the matrix of communication overheads, and L is the set of the maximum linking number of nodes:

$$N = \{v_1, v_2, \dots, v_i, \dots, v_n\}$$
$$E = \{(v_1, v_2), \dots, (v_i, v_j), \dots, (v_{n-1}, v_n)\}$$
$$T = \{t_1, t_2, \dots, t_i, \dots, t_n\}$$
$$L = \{l_1, l_2, \dots, l_i, \dots, l_n\}$$

Here, $w(v_i, v_j)$ represents the communication overheads between v_i and v_j . For the convenience of subsequent search, the communication overheads between nodes are constructed as a matrix:

$$W_{n \times n} = \begin{bmatrix} 0 & \cdots & w(v_1, v_n) \\ \vdots & \ddots & \vdots \\ w(v_n, v_1) & \cdots & 0 \end{bmatrix}$$

Trust value, communication overheads, and the maximum linking number are all important indicators for measuring some aspects of a node's performance, which significantly impact the node position in the WCT constructed by the algorithm.

During the communication, the trust value of different nodes is evaluated based on the legality of the trading information provided and the success rate of the data forwarding; it is recorded as t_i and $0 \le t_i \le 1$. Let the credit threshold be t_{thre} and the communication overheads threshold be w_{thre} . If the trust value of a node is less than t_{thre} , it is considered unreliable and its position in WCT is moved down. If the communication overhead between two nodes is greater than w_{thre} , data forwarding should not be performed between these two nodes. The WCT construction process is as follows:

• Examine the initial node set N and confirm the trust value t of each node. If the trust value of v_i is less than the threshold t_{thre} , move the node v_i to the end of the sequence. After the traversal, record the serial number of the last node with a trust value greater than t_{thre} as j to obtain a new node sequence.

$$N' = \{v_1, v_2, \ldots, v_j, \ldots, v_n\}$$

In the sequence N', if $k \leq j$, then $t_k \geq t_{thre}$, and if k > j, then $t_k < t_{thre}$.

• The score for each node in the sequence is calculated based on its trust value *t*, the maximum linking number *l*, and their respective weighted proportions w_t and w_l . $Score_i = w_t * t_i + w_l * l_i$ where $i = \{1, 2, ..., j\}$. Then, rank the nodes according to their scores from high to low to obtain a new ordered set.

 $N'' = \{v_1, v_2, \ldots, v_i, \ldots, v_j, \ldots, v_n\}$

• Examine the first *j* nodes and query the communication overheads between nodes in the matrix *W*. If the communication between v_1 and v_i is very expensive, namely $w(v_1, v_i) > w_{thre}$, then insert the node v_i after the node v_j to obtain the final node sequence. $N^* = \{v_1, v_2, \dots, v_i, v_i, \dots, v_n\}$

Then, N^* is the WCT construction sequence.

• Let v_1 be the root node of the WCT, and $T = \{v_1 | v_1 \in N^*\}$ $N^* - T = \{v_2, \dots, v_i, \dots, v_n | v_i \in N^*\}$ $E_T = \emptyset$

Set $m = l_1$, and successively connect the first *m* nodes in $N^* - T$ to node v_1 so that $T = T \cup \{v_2, \ldots, v_i, \ldots, v_{m+1} | v_i \in N^*\}$

$$E_T = E_T \cup \{(v_1, v_2), (v_1, v_3), \dots, (v_1, v_i), \dots, (v_1, v_{m+1}) | v_i \in N^*\}$$

• If there are nodes in $N^* - T$ that have been not added into the WCT, take the next adjacent node of the current root node as the new root and repeat the last step until all nodes are included in the WCT.

The data communication process between nodes is shown in Fig. 4, and Algorithm 1 describes the WCT construction process.



Figure 4: WCT data communication

Algorithm 1: WCT construction algorithm

Input: Node sequence $N = \{v_1, v_2, \dots, v_i, \dots, v_n\};$ **Output:** WCT sequence $T = \{v_1, v_2, ..., v_i, ..., v_n\};$ 1: for $i \in [1, n]$ do if $t_i < t_{thre}$ then 2: 3: Move v_i to the end of the sequence; 4: end if 5: end for 6: Record the last node serial number with a trust value greater than t_{thre} as *j*; 7: for $i \in [1, j]$ do Calculate *Score*_i = $w_i * t_i + w_l * l_i$; 8: 9: end for 10: Rank the resulting sequences by scores from high to low; 11: for $i \in [1, i]$ do 12: if $w(v_1, v_i) > w_{thre}$ then Insert the node v_i behind the node v_i ; 13: 14: end if 15: end for 16: Get the final node sequence N^* : 17: p = 1; 18: while $N^* - T$ is non-empty do 19: v_n as the root node, $v_n \in N^*$; $T = T \cup \{v_p\};$ 20: 21: $m = l_n;$ 22: for $k \in [1, m]$ do 23: $T = T \cup \{v_k | v_k \in N^* - T\};$ 24: $E_T = E_T \cup \{(v_1, v_k) | v_k \in N^* - T\};$ 25: end for 26: p = p + 1;27: end while

4 Performance Analysis

The proposed scheme is mainly divided into two parts: credibility-based power trading and WCT construction algorithm. Through the combination of blockchain and AI, secure and efficient power trading can be realized in SGs. Therefore, security analysis and experimental numerical analysis are conducted to analyze the security and efficiency of the proposed scheme.

4.1 Security Analysis

First, in the proposed scheme, the decentralized feature of the blockchain combined with the digital signature ensures that no opponent can pretend to be a legitimate node to destroy the network. This is because the opponent cannot forge the digital signature of any node or gain control of most of the network resources. Opponents controlling one or more nodes do not know any information about the original data; thus, they cannot forge the audited and stored data in the blockchain, guaranteeing the security of the data in the chain. In addition, when verifying a block, the nodes in the network determine the accounting node and data communication route through the WCT structure. Hence,

the nodes with high integrity and low communication cost are located in the upper layer of WCT and participate in data forwarding. The nodes in the lower layer of WCT are only responsible for receiving and verifying, which ensures the security and efficiency of the data communication.

Moreover, trading records are verified and maintained jointly by all DAs. The data transparency of the blockchain makes all the trading history publicly traceable. Users rely on digital signatures to prove the ownership of their assets. Before each trading, the MC determines the account balances of users by checking their trading history and fund flows, which effectively prevents double spending.

Finally, AI sensors are used to ensure stable power transmission. When trading is not in progress, the AI sensors can detect and record the electricity consumption and generation in real time. During the power trading process, the AI sensors can monitor the weather, transmission lines, and other environmental problems, thus reducing the generation cost of suppliers and improving the security of power supply.

4.2 Experimental Analysis

The experiments are conducted on a 64-bit computer equipped with the Win10 system. The relevant experimental code is implemented on PyCharm 2020 and the system interpreter is Python3.8.

Fifty nodes are set up in the system and their average transaction confirmation time (ATCT) is recorded. The following is assumed: the nodes with the maximum linking number of 3, 2, and 1 account for 5%, 15%, and 80%, respectively; the ratio of honest to malicious nodes is 8:2; the trust value of honest nodes is above 0.8; and the weight ratios of the node trust value to the maximum linking number are 1:1 and 3:2.

First, the transaction confirmation speed of the proposed scheme, the traditional blockchain, and schemes proposed in [8] and [17] are compared. Fig. 5 displays the experimental results. The ATCT of the traditional public blockchain is about 60 min; thus, in 1 h, regardless of the number of transactions generated in the system, each node can only confirm one transaction on average. The energy blockchain proposed in [8] uses the consortium chain and a specific consensus mechanism to reduce ATCT. It takes about 10 min to confirm a transaction on average, and each node can confirm up to 6 transactions in 1 h. The scheme proposed in [17] uses the Proof of Activity (PoA) consensus and consortium chain, and its ATCT is around 6-7 min. However, because the WCT constructed by our algorithm greatly improves the block verification efficiency, the ATCT of the proposed scheme is only about 6 min. Clearly, the transaction confirmation performance of the proposed scheme is superior to the other three schemes considered.

Next, the performance of the WCT construction algorithm is evaluated by comparing it with two single-performance-optimal algorithms through the following three groups of experiments, and the evaluation is performed based on three metrics: the overall trust value, the concurrent communication time, and the node concurrency. For a WCT with *n* nodes, its overall trust value is calculated from the number of forwarding tasks $task_i$, node trust value t_i , and the number of forwarding n - 1, i.e.,

$$T = \frac{\sum_{i=1}^{n} task_i * t_i}{n-1} \tag{1}$$



Figure 5: Average transaction confirmation speed

A high trust value of a WCT indicates that the forwarding reliability is high and the data communication is stable; in contrast, a low trust value denotes that the reliability and stability are poor. The concurrent communication time describes the time consumed by all nodes from receiving data to completing the entire communication. It is the most important parameter for measuring the communication efficiency. The node concurrency denotes the maximum number of data forwarded by all nodes at a time, which can be understood as the maximum forwarding capability of the communication tree. In Figs. 6–8, the trust value and the maximum linking number have the same weight proportion in (a), while the weight ratio of the two indicators is 3:2 in (b).



Figure 6: Trust value of the three communication trees



Figure 7: Concurrent communication time of the three communication trees



Figure 8: Node concurrency of the three communication trees

The analysis of the experimental results shows that the linking-number-first communication tree (LFT) algorithm preferentially places the node with the highest communication performance on the top of the communication tree; consequently, its communication performance is optimal, but its reliability cannot be guaranteed. While the trust-value-first communication tree (TFT) algorithm first considers the trust value of nodes and does not emphasize on indicators such as forwarding ability and communication overheads. Therefore, its overall trust value is optimal, but the communication tree efficiency is low. The two algorithms adopt the greedy idea when constructing a communication tree and pursue the optimization of a single performance. However, in practice, the reliability and efficiency cannot reach the optimal state at the same time. Thus, our algorithm comprehensively considers the influences of the nodes' trust value and their communication performance. The credibility of the WCT is clearly better than that of the LFT, as illustrated in Fig. 6. The communication delay of the WCT

is smaller than that of the TFT, as shown in Fig. 7. The accuracy of the values in Fig. 6 is verified using Eq. (1), and the experimental data well fit the results calculated using Eq. (1). For the LFT and WCT algorithms, the concurrent communication time does not sharply increase with the number of nodes, but it remains stable under small increases. This is because the concurrent communication mechanism and linking number are introduced and nodes with strong communication ability are preferentially selected to join the communication tree. Therefore, during the data communication, the node concurrency is high and the concurrent communication time does not sharply increase. In addition, as the proportion of trust value increases, the curves of WCT tend closer to those of TFT as a whole.

Fig. 8 displays the node concurrency of the three communication trees. The concurrency of all three communication trees markedly increases with the number of nodes. The communication tree constructed by the LFT algorithm and the proposed WCT algorithm is obviously better than that constructed by the TFT algorithm due to the superior communication performance of the upper nodes. The advantages of WCT are more prominent especially for large numbers of nodes.

The performance comparison of the communication trees constructed by the three algorithms is illustrated in Table 2. The advantages and disadvantages of the three different communication trees are shown in terms of communication efficiency and concurrent communication capability. Since both the LFT and TFT algorithms use the greedy idea, they can reach the optimal level of a single performance, but they ignore other performance aspects. The WCT algorithm simultaneously considers multiple metrics; therefore, although performance of the WCT algorithm is suboptimal on a single metric, it is still at a high level. Notably, the WCT algorithm has no obvious shortcomings. Thus, its comprehensive performance is superior.

| Algorithm | LFT | TFT | WCT |
|--------------------|-----------------------------------|-----------------------------|-----------------------------------|
| Priority index | Efficiency | Security | Efficiency and security |
| Reliability | Poor | Excellent | Good |
| Time performance | Excellent | Poor | Good |
| Concurrent ability | Excellent | Poor | Good |
| Optimization goal | Enhance communication reliability | Shorten communication delay | Improve comprehensive performance |

Table 2: Performance comparison of the three communication trees

5 Conclusion

This study proposed a secure and efficient scheme for distributed power trading based on blockchain and AI in SGs. The credibility-based scheme is adopted to limit the untrustworthy behavior of users and protect the legitimate benefits of the buyers and sellers. Simultaneously, the topology structure of node communication in the blockchain network is constructed using a WCT. By improving the security and efficiency of data transmission, the speed of transaction confirmation is accelerated. Finally, security analysis demonstrated that the combination of blockchain and AI ensures the security of data, equipment, and personnel during power transmission. The experimental results showed that the use of blockchain makes the trading records traceable and the WCT algorithm makes the system run efficiently. Therefore, the proposed scheme can realize secure and efficient distributed power trading in SGs.

In the future, the combination of blockchain and AI is expected to bypass the traditional gridstyle energy supply and locally produced and distributed energy is expected to serve local consumers through microgrids. However, the operation of a decentralized energy system needs to have strong information collection and utilization capabilities to be able to conduct multi-party coordination, make timely information contributions, and optimize pricing according to the statistical data. Eventually, this model will expand the scope of power circulation and promote the use of renewable energy generation.

Acknowledgement: The authors would like to thank the anonymous reviewers for their insightful comments and suggestions on improving this paper.

Funding Statement: This work was supported by the National Natural Science Foundation of China with Grants 61771289 and 61832012, the Natural Science Foundation of Shandong Province with Grants ZR2021QF050 and ZR2021MF075, Shandong Natural Science Foundation Major Basic Research with Grant ZR2019ZD10, Shandong Key Research and Development Program with Grant 2019GGX1050, Shandong Major Agricultural Application Technology Innovation Project with Grant SD2019NJ007, and National Natural Science Foundation of Shandong Province Grants ZR2022MF304.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- A. Jindal, G. S. Aujla, N. Kumar and M. Villari, "Guardian: Blockchain-based secure demand response management in smart grid system," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 613–624, 2020.
- [2] M. B. Mollah, J. Zhao, D. Niyato, K. -Y. Lam, X. Zhang et al., "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2021.
- [3] A. Paudel, L. P. M. I. Sampath, J. Yang and H. B. Gooi, "Peer-to-peer energy trading in smart grid considering power losses and network fees," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 4727– 4737, 2020.
- [4] P. Zhuang, T. Zamir and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 3–19, 2021.
- [5] A. Mehmood, Z. Lv, J. Lloret and M. M. Umar, "ELDC: An artificial neural network based energyefficient and robust routing scheme for pollution monitoring in WSNs," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 1, pp. 106–114, 2020.
- [6] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE Journal on Selected Areas of Communication*, vol. 31, no. 7, pp. 1319–1330, 2013.
- [7] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani *et al.*, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.
- [8] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng *et al.*, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.
- [9] H. -N. Dai, Z. Zheng and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.
- [10] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008–1027, 2020.

- [11] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2794– 2830, 2019.
- [12] J. Guo, X. Ding and W. Wu, "A blockchain-enabled ecosystem for distributed electricity trading in smart city," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2040–2050, 2021.
- [13] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma *et al.*, "A Bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 6856–6868, 2020.
- [14] M. U. Hassan, M. H. Rehmani and J. Chen, "Differentially private auction for blockchain-based microgrids energy trading," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 263–275, 2020.
- [15] M. K. AlAshery, Z. Yi, D. Shi, X. Lu, C. Xu et al., "A blockchain-enabled multi-settlement quasi-ideal peer-to-peer trading framework," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 885–896, 2020.
- [16] S. J. Pee, E. S. Kang, J. G. Song and J. W. Jang, "Blockchain based smart energy trading platform using smart contract," in *Proc. 2019 Int. Conf. on Artificial Intelligence in Information and Communication (ICAIIC)*, Okinawa, Japan, pp. 322–325, 2019.
- [17] S. Aggarwal and N. Kumar, "A consortium blockchain-based energy trading for demand response management in vehicle-to-grid," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9480–9494, 2021.
- [18] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang *et al.*, "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.
- [19] S. Fan, H. Zhang, Y. Zeng and W. Cai, "Hybrid blockchain-based resource trading system for federated learning in edge computing," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2252–2264, 2021.
- [20] M. Baza, A. Sherif, M. M. E. A. Mahmoud, S. Bakiras, W. Alasmary *et al.*, "Privacy-preserving blockchainbased energy trading schemes for electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9369–9384, 2021.
- [21] L. Cheng, H. Chang, K. Wang and Z. Wu, "Real time indoor positioning system for smart grid based on uwb and artificial intelligence techniques," in *Proc. 2020 IEEE Conf. on Technologies for Sustainability* (*SusTech*), Santa Ana, CA, USA, pp. 1–7, 2020.
- [22] J. T. C. Neto, P. H. M. de Andrade, J. M. Vilanueva and F. A. O. Santos, "Big data analytics of smart grids using artificial intelligence for the outliers correction at demand measurements," in *Proc.*, Bento Gonçalves, Brazil, pp. 1–6, 2018.
- [23] C. Tong, Y. Cai, Z. Zhang, Q. Wang and Y. Gao, "Artificial intelligence-based lightning protection of smart grid distribution system," in *Proc.*, Natal, Brazil, pp. 279–286, 2017.