energies

MDPI

Article

A Trusted Sharing Strategy for Electricity in Multi-Virtual Power Plants Based on Dual-Chain Blockchain

Wei Huang [1], Chao Zheng [2], Xuehao He [3], Xiaojie Liu [4], Suwei Zhai [2], Guobiao Lin [4], Shi Su [3], Chenyang Zhao [5,*] and Qian Ai [5]

[1] Kunming Power Dispatching Control Center, Kunming Power Supply Bureau, Yunnan Power Grid Co., Ltd., Kunming 650010, China; huangwei@yn.csg.cn
[2] Yunnan Power Dispatching Control Center, Yunnan Power Grid Co., Ltd., Kunming 650011, China; zhengchao@yn.csg.cn (C.Z.); zhaisuwei@yn.csg.cn (S.Z.)
[3] Electric Power Research Institute of China Southern Power Grid Yunnan Power Grid Co., Ltd., Kunming 650217, China; hexuehao@yn.csg.cn (X.H.); sushi@yn.csg.cn (S.S.)
[4] Dongfang Electronics Cooperation, Yantai 264010, China; 18660575203@163.com (X.L.); 15813315065@163.com (G.L.)
[5] Key Laboratory of Control of Power Transmission and Conversion, Ministry of Education, Shanghai Jiao Tong University, Shanghai 200240, China; aiqian@sjtu.edu.cn
* Correspondence: 19337128331@163.com

Abstract: Distributed power trading is becoming the future development trend of electric energy trading, and virtual power plant (VPP), as a kind of aggregated optimization scheme to enhance energy utilization efficiency, has received more and more attention for studying distributed trading among multiple VPPs. However, how to guarantee the economy, credibility, security, and efficiency of distributed transactions is still a key issue to be overcome. To this end, a multi-VPP power sharing trusted transaction strategy based on dual-chain blockchain is proposed. First, a dual-chain blockchain electric energy transaction architecture is proposed. Then, the VPP-independent operation cost model is constructed, based on which, the decision model of multi-VPP electric energy sharing transaction based on Nash negotiation theory is constructed. Again, an improved-Practical Byzantine Fault Tolerant (I-PBFT) consensus algorithm combining the schnorr protocol with the Diffie–Hellman key exchange algorithm and a smart contract for multi-VPP electricity trading are designed to realize trusted, secure, and efficient distributed transactions. Finally, the example results verify the effectiveness of the strategy proposed in this paper.

Keywords: virtual power plants; distributed transactions; blockchain; Nash negotiation; consensus algorithms; smart contracts

Academic Editor: Emanuele Martelli

Received: 28 April 2025
Revised: 22 May 2025
Accepted: 23 May 2025
Published: 25 May 2025

Citation: Huang, W.; Zheng, C.; He, X.; Liu, X.; Zhai, S.; Lin, G.; Su, S.; Zhao, C.; Ai, Q. A Trusted Sharing Strategy for Electricity in Multi-Virtual Power Plants Based on Dual-Chain Blockchain. *Energies* **2025**, *18*, 2741. https://doi.org/10.3390/en18112741

1. Introduction

In the context of deepening reforms in the power system, continuous innovations have been made to the structure and operation mode of the power system. With the rapid development of new energy technologies, clean energy sources such as photovoltaics, wind power, and energy storage have been increasingly integrated into the energy internet, leading to a growing abundance of adjustable load resources on the distribution network side [1]. Against this backdrop, the Virtual Power Plant (VPP) [2–5], an innovative energy management model, has emerged as the times require. As a new type of market entity, the VPP aggregates distributed flexible resources within its jurisdiction and participates in power trading and system regulation in a market-oriented manner. It plays a crucial

role in ensuring the safe and stable operation of the power grid and promoting the low-carbon transformation of the energy sector. Moreover, it serves as an important pillar for achieving the goals of "carbon peaking and carbon neutrality" and establishing a new power system characterized by a new-energy-dominated structure and source–grid–load–storage interaction [6].

The demand for source–network–load–storage interaction under the new power system is increasing, and with the gradual maturation of the power trading market, VPP will usher in great development, and distributed trading among multiple VPPs has gradually become a research hotspot. However, in the process of VPP participating in distributed trading, there are still problems such as high transaction costs, low execution efficiency, and lack of credibility. Therefore, it is necessary to study the distributed power trusted transaction strategy between multiple VPPs.

Currently, the optimal operation between multiple VPPs in distributed trading scenarios has been widely studied. Paper [7–9] studied the economic operation problem of multiple VPPs containing wind and photovoltaic power generation systems. Paper [10,11] proposed a multi-VPP hybrid game optimization scheduling method considering green certificate-carbon trading in order to analyze the problem of collaborative management of economic and low-carbon benefits among multiple VPPs. Paper [12], in order to solve the problems faced by multi-VPP alliances, such as the lack of monopoly prevention mechanism for electricity sales and the difficulty of multi-dimensional assessment and portrayal of individual subjective preferences, proposed a multi-VPP bidding model for participating in the electricity market a few days ago based on alliance game. Article [13] proposes a two-phase cooperative operation strategy for multiple microgrids based on Nash equilibrium considering uncertainty, which achieves the economic operation of microgrids and the rational distribution of benefits. However, the above studies only focus on improving the economic and low-carbon benefits in the multi-VPP electricity trading scenario, but do not fully consider the core requirements in the trading process: efficiency, credibility, security, and cooperativeness.

Transactions between VPPs are self-organized and autonomous. Ensuring the openness, transparency, and reliability of the transaction process is the key factor that drives VPPs to actively engage in distributed transactions. Blockchain technology is a decentralized data storage and transmission technology based on distributed ledgers. Its core philosophy is to achieve tamper-proof data, transparent traceability, and decentralized management through cryptography, consensus mechanisms, and distributed networks [14]. It can precisely meet the trust requirements of scenarios such as energy system operation and management, energy metering and certification, and power data circulation [15]. Article [16] proposes a blockchain-based optimal point-to-point energy transaction framework for the efficient management of distributed energy. Paper [17] proposes a framework for interactive home energy management using cloud energy storage under blockchain-enabled uncertainty conditions to achieve economic efficiency. Article [18] provides an insight into the application of digital twins, blockchain, and artificial intelligence in building management systems. The above research provides feasible ideas for the innovative application of blockchain technology in virtual power plants, and significant progress has been made in the relevant research on the deep integration of blockchain technology and VPP application scenarios. Paper [19] proposes a distributed scheduling strategy for VPP based on energy blockchain, using blockchain technology to achieve economic optimization and secure scheduling of distributed resources in virtual power plants. Based on the functional characteristics of VPP, Paper [20] establishes an optimized operation model for multi-virtual power plants under blockchain composed of a business chain, technology chain, and asset chain, achieving the maximization of individual VPP benefits and the improvement

of transaction efficiency. In a blockchain distributed system, consensus algorithm is the core mechanism that enables mutually distrustful network nodes to reach distributed consistency on key information such as data validity and block generation order through mathematical rules and incentives. Paper [21] proposes a practical Byzantine fault-tolerant algorithm consensus mechanism applicable to VPP. Paper [22] focuses on the problem of maximizing the benefits of multi-aggregator formation within VPP and the efficiency of trusted transaction matching and proposes a VPP master–slave multi-chain transaction matching mechanism based on an improved consensus algorithm. Paper [23] proposes a blockchain-based distributed particle swarm optimization algorithm and an optimal computational workload proof consensus algorithm. However, although the consensus algorithms used in the above studies have improved credibility to a certain extent, they still have a series of problems such as inefficiency, high latency, and security issues.

To address the aforementioned issues, this paper proposes a multi-VPP electric energy sharing trusted transaction strategy based on dual-chain blockchain. Firstly, a dual-chain blockchain electric energy transaction architecture is designed, followed by the establishment of a VPP independent operation model, on the basis of which, a decision-making model based on Nash negotiation electric energy sharing transaction is established to realize the optimal allocation of electric energy resources. Furthermore, to ensure the security, efficiency, and trustworthiness of distributed transactions, a consensus authentication scheme integrating the Schnorr protocol and Diffie–Hellman key exchange algorithm is designed, along with a smart contract for multi-VPP electricity trading. Finally, simulation results validate the practicality and application value of the proposed strategy.

2. Electricity Energy Trading Architecture and Optimization Model

2.1. Dual-Chain Blockchain-Based Architecture for Electricity Trading

Considering that the traditional single-chain blockchain often has high transaction costs and low execution efficiency in electricity transactions, this paper designs a dual-chain blockchain electricity transaction architecture that integrates economy and flexibility, which can significantly improve the economy and efficiency of the transaction, and the architecture schematic is shown in Figure 1.

Compared with the traditional single-chain distributed electricity trading architecture, the dual-chain blockchain-based electricity trading architecture designed in this paper has the following two advantages:

(1) By storing transaction information and contract information separately, it significantly reduces the capacity of each block and accelerates the transaction speed. Expanding the blockchain structure from a single chain to a dual chain enhances the credibility of the data. The dual-chain blockchain architecture includes a transaction chain and a contract chain, both of which use weakly centralized alliance chain technology, which ensures efficient and safe transactions while reducing transaction costs. Among them, the blocks of the transaction chain only save the point-to-point transaction decisions of VPPs, which are carried out based on the distributed electricity transaction mechanism; the blocks of the contract chain record the VPP transaction contracts and verify the validity of the contract information.

(2) Using the decentralized nature of the dual-chain blockchain, each distributed power trading participant VPP is committed to maximizing its own interests, thus achieving active trading decisions. This is because the data in the dual-chain blockchain is untamperable and traceable. Under the improved utility-based Byzantine fault-tolerant consensus algorithm, the trusted transactions of VPPs can be managed in a distributed manner, thus enhancing the transaction efficiency and the interests of VPPs.

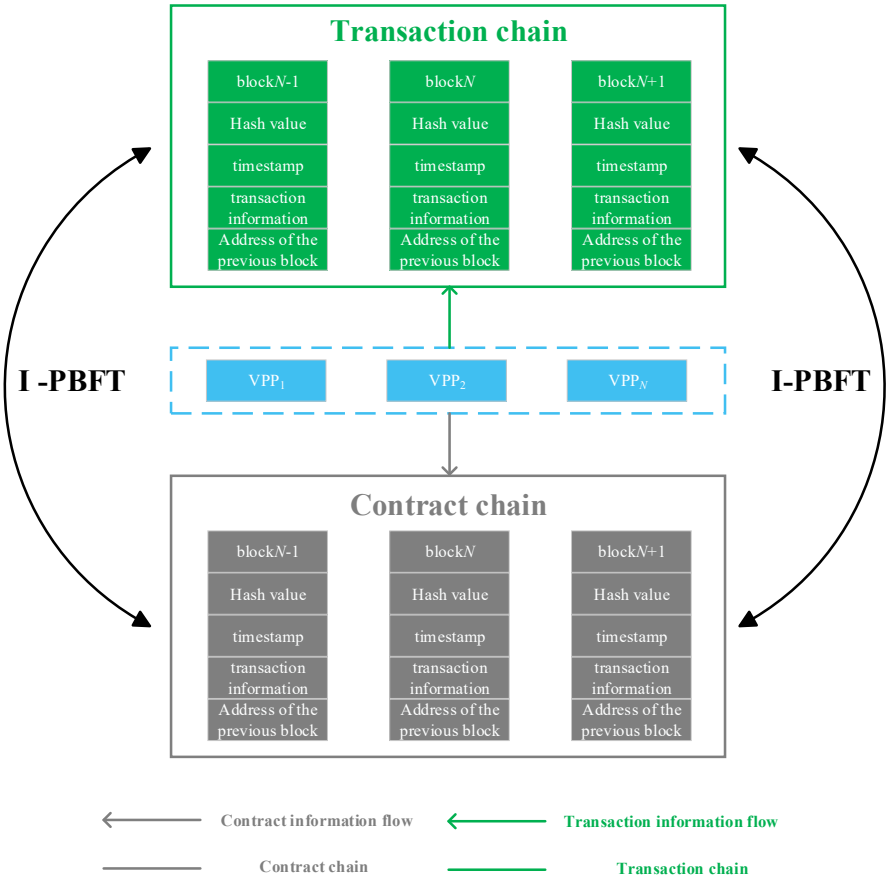


Figure 1. Dual-chain blockchain-based electricity transaction architecture.

2.2. Multi-VPP Trading Decision Model

Under the trading environment of distributed electricity market, VPPs change the selling or purchasing tariffs according to their own power selling capacity or power consumption demand. In order to realize the optimization of resource allocation in point-to-point trading in distributed electricity market, a single VPP operation model is firstly constructed, and then a multi-VPP power sharing trading decision model based on Nash negotiation is constructed.

2.2.1. Single VPP Running Costs Models

(1) Objective function

$$\min C_{i,0} = \min C_{i,\text{grid}} + C_{i,\text{es}} + C_{i,\text{DR}} \tag{1}$$

$$C_{i,\text{grid}} = \sum_{t=1}^{T} \lambda_{t,\text{buy}} P_{i,t,\text{buy}} - \lambda_{t,\text{sell}} P_{i,t,\text{sell}} \tag{2}$$

$$C_{i,\text{es}} = \sum_{t=1}^{T} \lambda_{\text{es}} (P_{i,t,\text{cha}} + P_{i,t,\text{dis}}) \tag{3}$$

$$C_{i,\text{DR}} = \sum_{t=1}^{T} \lambda_{\text{cut}} |P_{i,t,\text{cut}}| + \lambda_{\text{tran}} |P_{i,t,\text{tran}}| \tag{4}$$

where $C_{i,0}$ is the VPP independent operation cost; T is the dispatch cycle; $C_{i,\text{grid}}$, $C_{i,\text{es}}$, $C_{i,\text{DR}}$ are the cost of purchasing and selling electricity, the cost of energy storage, and the cost of demand response, respectively; $\lambda_{t,\text{buy}}$ and $\lambda_{t,\text{sell}}$ are the price of purchasing and selling electricity, $P_{t,\text{buy}}$, $P_{t,\text{sell}}$ are the purchased and sold power, respectively; λ_{es}

is the O&M cost per unit power of energy storage; $P_{i,t,\text{cha}}$, $P_{i,t,\text{dis}}$ are the charging and discharging power, respectively; λ_{cut}, λ_{tran} are the adjusted price per unit of power for the curtailable and transferable loads, respectively; and $P_{i,t,\text{cut}}$, $P_{i,t,\text{tran}}$ are the corresponding adjusted quantities.

(2) Constraints

1. Interactive power constraints with the grid

$$\begin{aligned} 0 \le P_{i,t,\text{buy}} \le P_{i,\text{buy,max}} \\ 0 \le P_{i,t,\text{sell}} \le P_{i,\text{sell,max}} \end{aligned} \tag{5}$$

where $P_{i,\text{buy,max}}$, $P_{i,\text{sell,max}}$ are the maximum value of power purchased and sold by VPP$_i$, respectively.

2. Energy storage operational constraints

$$\begin{aligned} & S_{t+1} = S_t + \eta_{\text{cha}} P_{t,\text{cha}} - \frac{P_{t,\text{dis}}}{\eta_{\text{dis}}} \\ & S_{\min} \le S_t \le S_{\max} \\ & 0 \le P_{t,\text{cha}} \le \mu_{t,\text{cha}} P_{\text{cha,max}} \\ & 0 \le P_{t,\text{dis}} \le \mu_{t,\text{dis}} P_{\text{dis,max}} \\ & \mu_{t,\text{ch}} + \mu_{t,\text{dis}} \le 1 \end{aligned} \tag{6}$$

where S_t is the energy stored by the energy storage system in time period t; $P_{t,\text{ch}}$ and $P_{t,\text{dis}}$ are the charging and discharging powers of the energy storage system in time period t, respectively; η_{ch} and η_{dis} are the charging and discharging efficiencies of the energy storage system in time period t, respectively; $S_{\max}$ and $S_{\min}$ are the upper and lower limits of the energy stored by the energy storage system, respectively; $P_{\text{ch,max}}$ and $P_{\text{ch,min}}$ are the upper and lower limits of the charging and discharging powers of the energy storage system, respectively; $\mu_{t,\text{ch}}$ and $\mu_{t,\text{dis}}$ are the 0/1 state parameters representing the charging and discharging of the energy storage system in time period t. When their values are 1, it indicates charging/discharging.

3. Demand response constraints

Demand response is a mechanism whereby electricity consumers actively adjust their electricity consumption behavior in response to price signals or incentives to interact with the grid. Among them, curtailable load refers to the type of load that allows users to temporarily interrupt or reduce electricity consumption according to the demand of the grid during a specific period of time, while transferable load allows users to shift electricity demand from peak hours to low hours. By precisely regulating the curtailable loads and transferable loads in the flexible loads, users not only ensure the stable operation of the power system but also improve the flexibility and economy of power consumption on the user side.

$$\begin{aligned} & P_{i,t,\text{load}} = P_{i,t,\text{load}\,0} + P_{i,t,\text{cut}} + P_{i,t,\text{tran}} \\ & P_{i,t,\text{cut}} \leqslant 0 \\ & |P_{i,t,\text{cut}}| \leqslant \nu_{i,\text{cut}} \mu_{i,\text{cut}} P_{i,t,\text{load}\,0} \\ & |P_{i,t,\text{tran}}| \leqslant \nu_{i,\text{tran}} \mu_{i,\text{tran}} P_{i,t,\text{load}\,0} \\ & \sum_{t=1}^{24} P_{i,t,\text{tran}} = 0 \end{aligned} \tag{7}$$

where $P_{i,t,\text{load0}}$, $P_{i,t,\text{load}}$ are the electrical loads of VPP$_i$ at time t before and after the demand response, respectively; $P_{\text{i,t,cut}}$, $P_{i,t,\text{tran}}$ are the curtailable electrical loads and transferable electrical loads of VPP$_i$ at time t, respectively; $\mu_{i,\text{cut}}$, $\mu_{i,\text{tran}}$ are the state flag bits of the two flexible loads, whose value is 1, indicating participation in the demand response; $\nu_{\text{i,cut}}$ and $\nu_{\text{i,tran}}$ are the proportion of the total load accounted for by the two flexible loads when responding, respectively.

4. Power balance constraints

$$P_{i,t,\mathrm{wt}} + P_{i,t,\mathrm{pv}} + P_{i,t,\mathrm{buy}} + P_{i,t,\mathrm{dis}} = P_{i,t,\mathrm{load}} + P_{t,\mathrm{cha}} + P_{i,t,\mathrm{sell}} \tag{8}$$

where $P_{i,t,\mathrm{wt}}$, $P_{i,t,\mathrm{pv}}$ are the electrical loads of VPP_i at moment t before and after the demand response, respectively.

2.2.2. Nash Negotiation-Based Multi-VPP Electricity Sharing Transaction Decision Modeling

It is assumed that all VPPs can realize the goal of further reducing operating costs through bargaining transactions. Then, the decision model for multi-VPP power sharing transaction is constructed as follows:

$$\max \prod_{i=1}^{N} (C_{i,0} - C_i) \tag{9}$$

$$C_i = C_{i,\mathrm{grid}} + C_{i,\mathrm{es}} + C_{i,\mathrm{DR}} - C_{i,p2p} = C_{i,\mathrm{nan}} - C_{i,p2p} \tag{10}$$

$$C_{i,\mathrm{nan}} = C_{i,\mathrm{grid}} + C_{i,\mathrm{es}} + C_{i,\mathrm{DR}} \tag{11}$$

$$C_{i,p2p} = \sum_{t=1}^{T} \sum_{\substack{j=1 \\ i \neq j}}^{N} \lambda_{t,p2p} P_{t,p2p} \tag{12}$$

$$\text{s.t.} \quad C_i \leqslant C_{i,0} \tag{13}$$

where N is the number of VPPs participating in distributed trading; C_i is the operating cost of VPPs after participating in distributed electricity trading; $\mathrm{C}_{i,\mathrm{p2p}}$ is the cost of electricity sharing; $\mathrm{C}_{i,\mathrm{nan}}$ is the cost of operating VPP_i after participation in the sharing of electricity, net of the benefits of participation in sharing; $\lambda_{t,\mathrm{p2p}}$ is the interaction tariff between VPPs; and $P_{t,\mathrm{p2p}}$ is the amount of electricity interacted.

Equation (9) needs to be satisfied when it achieves its maximum value:

$$\prod_{i=1}^{N} (C_{i,0} - C_i) = \left[\frac{1}{N} \sum_{i=1}^{N} (C_{i,0} - C_i) \right]^N \tag{14}$$

When VPP_i and VPP_j agree on the volume and price of distributed electricity transactions, the transaction prices are equal and the transaction volumes are opposite to each other, i.e.,

$$\sum_{i=1}^{N} C_{i,p2p} = 0 \tag{15}$$

Then, the objective function Equation (9) can be transformed into

$$\max N \ln \frac{\sum_{i=1}^{N} (C_{i,0} - C_{i,\mathrm{nan}})}{N} \tag{16}$$

Since $C_{i,0}$ is the Nash negotiation rupture point and is constant, then, Equation (16) can be transformed into

$$\min \sum_{i=1}^{N} (C_{i,\mathrm{nan}}) \tag{17}$$

Since the optimal shared power $P_{t,\mathrm{p2p}}$ is obtained by solving Equation (17), it is obtained by substituting in Equation (9)

$$\min -\sum_{i=1}^{N} \ln(C_{i,0} - C_{i,\mathrm{nan}} + C_{i,P2P}) \tag{18}$$

Referring to the solution process of the Paper [24], solving the above model can determine the optimal trading power and price between the distributed trading subjects.

3. Blockchain Implementation of Multi-VPP Power Sharing Transactions

This section proposes a dual-chain blockchain-based implementation method of trustworthy transaction of electric energy between VPPs to ensure fair and trustworthy transaction. In the consensus layer, the I-PBFT consensus algorithm is proposed to guarantee the trustworthiness of the transaction results; in the contract layer, the smart contract for electric energy transaction is designed to realize the automatic and contract-based transaction clearing.

3.1. I-PBFT Consensus Algorithm Execution Process

3.1.1. Secret Key Negotiation Algorithm for Zero Knowledge Based Authentication

Traditional PBFT algorithms face the challenges of node identity forgery and inefficient key negotiation in large-scale distributed environments, which may lead to malicious nodes interfering with the consensus process or leaking sensitive information. Deploying the authentication protocol in the distributed consensus mechanism can effectively improve the security, reliability, and operational efficiency of the system, and safeguard the credibility of the consensus process and the consistency of the system state by verifying the legitimate identity of the participating nodes. In this paper, the traditional PBFT algorithm is designed to enhance the authentication mechanism, and the design scheme is as follows:

(1) Each network node is assigned a unique digital identity, which is permanently recorded in the blockchain distributed ledger in the form of cryptographic credentials. The automated verification of identity credentials can be realized between nodes through the smart contract function, which significantly reduces the trust cost associated with traditional centralized authentication.

(2) The authentication system adopts a zero-knowledge proof scheme based on the Schnorr protocol, which has advantages in that the proof process requires only a small number of rounds of communication interactions, has low computational complexity, and maintains complete zero-knowledge characteristics.

The Diffie–Hellman algorithm is used in the key negotiation session, which supports (1) secure key derivation in a non-pre-shared key environment, (2) forward security guarantees, and (3) collaborative computation applicable to distributed nodes.

In particular, it should be noted that all of the above schemes are built on top of discrete logarithmic mathematical puzzles, whose computational complexity provides theoretical-level security for the system.

The Schnorr proof and the Diffie–Hellman algorithm are implemented as follows:

(1) Initialization phase

The regulator selects a large prime p satisfying $q \mid (p-1)$ and a generator $g \in \mathbb{Z}p^*$, and distributes the (p, q, g) ternary to all authenticated nodes.

(2) Key parameter generation

Node i selects private key $a \in \mathbb{Z}q$ and computes the public key parameter $Y_i \equiv g^a \bmod p$. Node j selects private key $b \in \mathbb{Z}q$ and the public key parameter $Y_j \equiv g^b \bmod p$

(3) Zero-knowledge proof construction

Node i picks a random number $r_1 \in \mathbb{Z}q$, computes $R_1 \equiv gr_1 \bmod p$, $c_1 = H(R_1 \| Y_i)$, and $z_1 = r_1 + ac_1$. node j picks a random number $r_2 \in \mathbb{Z}q$, computes $R_2 \equiv gr_2 \bmod p$, $c_2 = H(R_2 \| Y_j)$, and $z_2 = r_2 + ac_2$.

(4) Authentication information exchange

The nodes exchange (Y_i, R_1, z_1) and the (Y_i, R_2, z_2) parameter sets between them via P2P network.

(5) Authentication and key negotiation

After checking that $g^{z2} \equiv R_2 - Y_i^{c2} \bmod p$ holds, the verifier computes the session key $K \equiv Y_j^b \bmod p$. This process satisfies interactional symmetry and ensures key consistency.

By organically integrating Schnorr proofs with Diffie–Hellman exchanges, this scheme realizes the security unification of two-way authentication and key negotiation while maintaining protocol simplicity.

3.1.2. I-PBFT Consensus Algorithm Execution Process

The blockchain network nodes based on DBSCAN (Density-Based Spatial Clustering of Applications with Noise) [25] algorithm are divided into k lower consensus groups. Before each round of consensus is initiated, the nodes in each group first complete mutual identification through the zero-knowledge proof mechanism and then elect a trusted leader node according to the preset rules. The elected leader broadcasts its identity information to the whole network, and other leader nodes receive the broadcast and also verify their identities using the zero-knowledge proof technique. These leaders together constitute the upper layer consensus group. In the I-PBFT consensus mechanism, a two-tier consensus architecture is formed by combining the local consensus of the lower layer consensus group with the global consensus of the upper layer consensus group. As shown in Figure 2, the leader of the lower consensus group first organizes the members of this group to complete the first round of local consensus and submits this result to the upper consensus group after success, and this leader acts as the coordinator of the global consensus of this round and dominates the second round of consensus process.

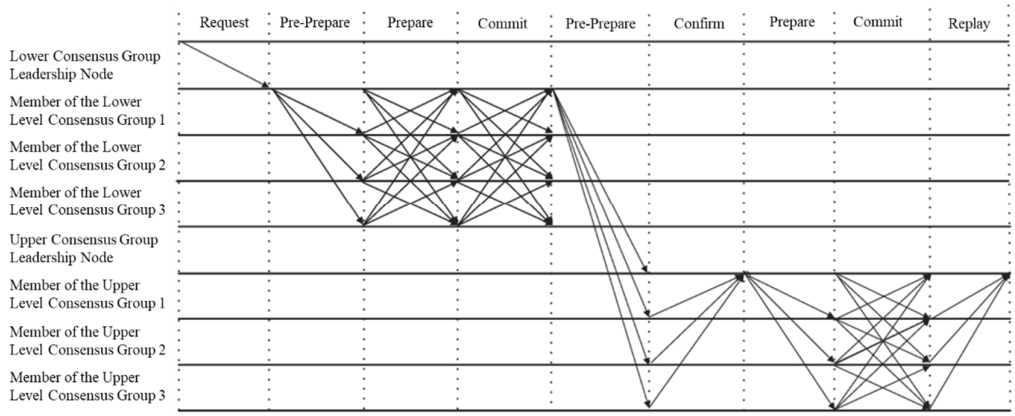


Figure 2. I-PBFT consensus algorithm execution process.

It should be emphasized that before initiating a transaction, the transaction nodes in the blockchain network must complete a two-way identity verification via a zero-knowledge proof key exchange protocol and establish a shared key to securely transmit the transaction data. All records of this authentication process will be stored on the chain. When processing encrypted transaction information, the consensus node needs to verify the on-chain identity credentials of both parties to the transaction and confirm that there is no error before entering the consensus phase.

(1) Local Consensus

The outgoing node s is responsible for packing all the transactions of the current transaction cycle and randomly selects the leader node Lc of the lower consensus group Z_c to send a message in the following format:

$$<< improved - PBFT - Request, h, d(b), t, d(m) > \delta_s, b > \quad (19)$$

where improved-PBFT-Request is the message type identification; b is the block to be confirmed; h denotes the current block height; $d(b)$ is the digital digest of the block; t is the timestamp; $d(m)$ is the digital digest of the message and δ_s is the digital signature of node s.

Upon receiving the request, L_c first verifies the identity of s through the authentication protocol. If the authentication passes, a Pre-Prepare message is constructed with the following format:

$$<< improved - PBFT - PrePrepare, v, h, d(b), t, d(m) > \delta_c, b > \quad (20)$$

where v is the current view number.

The consensus group then enters a localized consensus process, consisting of three phases: Pre-Prepare, Prepare, and Commit.

1. Pre-Prepare stage

L_c broadcasts a Pre-Prepare message to all normal nodes in the group.

2. Prepare stage

After the ordinary node receives the Pre-Prepare message and verifies that there is no error, it saves the block and generates a Prepare message based on it in the following format:

$$<< improved - PBFT - Prepare, v, h, d(b), t, d(m) > \delta_i > \quad (21)$$

The node broadcasts the message to all other nodes in the group and collects Prepare messages from other nodes. If a node receives at least $2f + 1$ valid Prepare messages (where f is the maximum number of fault-tolerant Byzantine nodes), it enters the Commit phase.

3. Commit phase

The node sends a Commit message to all other nodes in the group in the following format:

$$<< improved - PBFT - Commit, v, h, d(b), t, d(m) > \delta_i > \quad (22)$$

Meanwhile, nodes continuously receive Commit messages from other nodes. If a node receives at least $f + 1$ valid Commit messages, the local consensus is complete.

(2) Global Consensus

When the local consensus is completed, the leader node L_c of the lower consensus group will act as the representative of the global consensus in this round and organize other nodes within the upper consensus group to complete the global consensus. Compared with local consensus, global consensus additionally introduces the Confirm phase, so the complete process contains five phases: Pre-Prepare, Confirm, Prepare, Commit, and Reply.

1. Pre-Prepare stage

L_c broadcasts a Pre-Prepare message within the upper consensus group in the following format:

$$<< improved - PBFT - PrePrepare, v, h, d(b), t, d(m) > \delta c, b > \quad (23)$$

2. Confirmation stage

After the ordinary node of the upper consensus group receives the Pre-Prepare message and verifies that it passes, it saves the block and generates a Confirm message to send to the leader node in the format:

$$<< improved - PBFT - Confirm, v, h, d(b), t, d(m) > \delta c > \quad (24)$$

L_c collects Confirm messages from common nodes, if more than $2f$ are received and all of them are verified, it enters the Prepare phase.

3. Prepare stage

Lc sends Prepare messages to all common nodes in the format:

$$<< improved - PBFT - Prepare, v, h, d(b), t, d(m) > \delta c > \quad (25)$$

4. Commit phase

After the ordinary node receives the Prepare message and verifies that it is correct, it broadcasts a Commit message to the other nodes in the group in the format:

$$<< improved - PBFT - Commit, v, h, d(b), t, d(m) > \delta c > \quad (26)$$

Meanwhile, the node continuously receives Commit messages from other nodes. If each node receives more than $2f + 1$ valid Commit messages, it enters the Reply phase.

5. Reply stage

Global consensus is completed when nodes within the upper consensus group have collected at least $f + 1$ Reply messages. Each node updates the local blockchain according to the new block and broadcasts the final confirmation message within the lower consensus group to which it belongs, in the following format:

$$<< improved - PBFT - Result, v, h, d(b), t, d(m) > \delta c > \quad (27)$$

At the end of the consensus, the blockchain network updates the node status based on the transactions within the new block and elects the leader for the next round of consensus according to the leader node point election strategy to prepare for a new round of consensus.

3.1.3. I-PBFT Consensus Algorithm Attack Resistance Mechanism and Security Analysis

(1) Defense against sybil attacks

Sybil attack, as a typical security threat in the field of distributed systems, the attacker often implements damage to P2P networks and systems by creating a large number of false identities or nodes. To address this security risk, the I-PBFT algorithm constructs an identity authentication system that combines the schnorr protocol with the Diffie–Hellman key exchange algorithm. Under this mechanism, each node participating in the transaction is endowed with a unique digital identity and corresponds one-to-one with the entity that has the qualification of electricity transaction in reality. Based on the asymmetric encryption principle, each node uses its private key to digitally sign the transaction information and contract information, while other nodes verify the authenticity of the signatures through the corresponding public key. Since the attacker cannot obtain the private key of the node, it is impossible to forge the identity of the node and the signature of the information, which eliminates the possibility of a single node creating multiple identities from the root and effectively guarantees the security of the system.

(2) Defense against eclipse attacks

In an eclipse attack, the attacker attempts to construct malicious nodes around the target node, making the target node establish connections only with the malicious nodes while isolating or blocking the connections with honest nodes. The I-PBFT algorithm can

effectively resist such an attack. The reasons are as follows: Firstly, the I-PBFT adopts an identity authentication mechanism, and only legitimate nodes can join the blockchain network. Secondly, the I-PBFT uses the DBSCAN algorithm to shard the blockchain network. Before the sharding is completed, the nodes will not know the situation of the remaining nodes in the sharded network. Therefore, it is difficult for the attacker to gather malicious nodes in the same shard to launch an eclipse attack.

The I-PBFT consensus authentication scheme shows significant advantages in resisting the above attacks. However, in order to present its competitiveness in security more intuitively, the comparison with other schemes is unfolded from the dimension of attack resilience, as shown in Table 1.

Table 1. Comparative analysis of attack resistance.

Program	Attack	Security
Traditional PBFT	sybil attacks + eclipse attacks	vulnerable
Schnorr + PBFT	sybil attacks + eclipse attacks	Dependent on complex interactions
I-PBFT	sybil attacks + eclipse attacks	defend against attack

(Results of the simulation of the models in this paper).

3.2. Smart Contract Design

Smart contract is an automated execution program deployed in the blockchain system, which is capable of constructing diversified transaction rules, collaboration modes and market mechanisms in electric energy transaction scenarios. The program can standardize the complex transaction behavior, covering the core links of information interaction, value transfer, asset control, and so on. In essence, the smart contract clarifies the rights and responsibilities of both parties to the transaction in digital form. Once the transaction process triggers the pre-set conditions, the built-in smart contract will be automatically activated, realizing the functions of matching and settlement of transaction subjects, credit rating management, and priority scheduling. Smart contract establishes a reliable contract system through technical means, effectively avoiding the uncertainty brought by human intervention, thus providing a more secure and accurate execution guarantee for trading activities.

In this paper, the following principles are followed to design a smart contract for multi-VPP electricity trading based on a two-chain blockchain.

(1) Only verified market participants are eligible to trade.

(2) The contract will ensure that the transaction data are open, transparent, and traceable, and the data cannot be tampered with once they are uploaded to the chain.

(3) The general-purpose smart contract is open to all network nodes for calling privileges, while the special contract involving regulatory functions is only open to regulatory nodes with corresponding privileges so as to maintain the security and stability of the order of electric energy transactions.

The multi-VPP power sharing trusted transaction mechanism based on dual-chain blockchain proposed in this paper will operate based on smart contracts, as shown in Figure 3, and the participating subject VPPs can invoke smart contracts on the blockchain platform to conduct transactions.

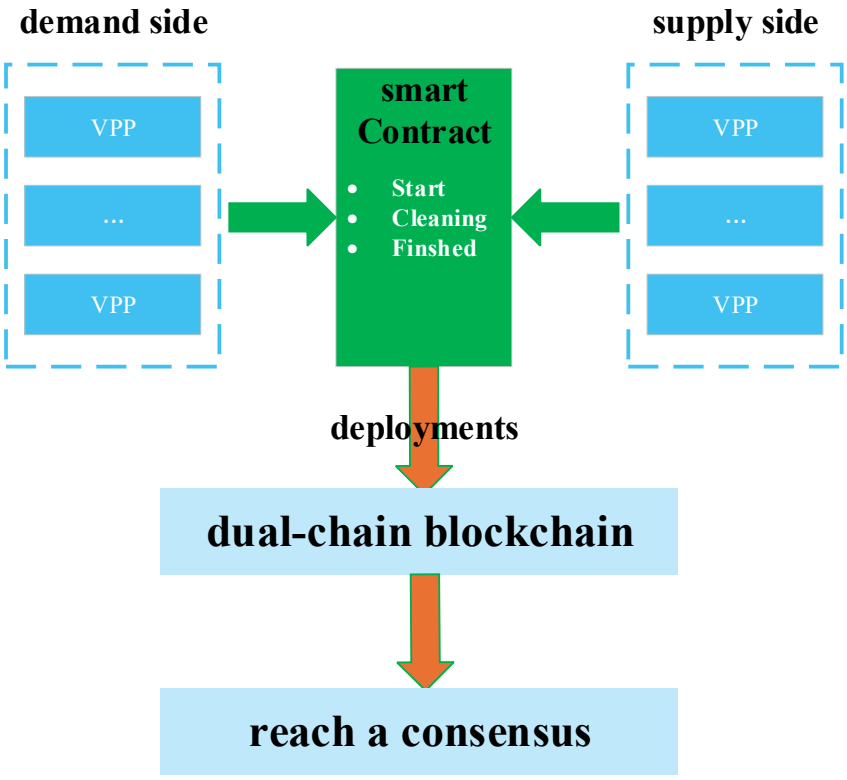


Figure 3. Smart contract-based trusted transaction mechanism for multi-VPP power sharing.

(1) Participating subject information registration update contract (_Start). Before the start of each transaction cycle, the platform performs information synchronization operations by calling this contract to verify the reputation scores of all participating subjects. After a newly registered subject passes the authentication, its blockchain address will be entered into the smart contract, and the system will automatically assign an initial reputation value based on the subject's attribute category. When the subject's credibility score hits the lower threshold, the system will instantly freeze all of its trading privileges; after the subject completes the payment of fines in accordance with the regulations, it will be able to reactivate its trading qualifications only after the system audit.

(2) Trading out contract (_Clearing). After the start of a cycle of trading, the VPPs participating in the trading can call the _Clearing contract to construct the VPP independent operation cost model according to Equations (1)–(8) and solve for the amount of electricity traded and the traded tariffs among the VPPs according to Equations (9)–(18).

(3) Trade settlement contract (_Finshed). After the completion of each cycle of trading, this contract will automatically transfer funds based on the quoted price and trading volume.

(4) Auxiliary functions. Realize the query of order information, marking and reputation value management and other functions.

4. Example Analysis

In order to verify the advantages of the dual-chain blockchain transaction decision-making proposed in this paper, the transaction chain and the contract chain are constructed separately in the Ethernet client. Using Solidity language, we write three main functional contracts to categorize and store transaction and contract information as well as implement the transaction process. These contracts are deployed on the dual-chain blockchain, and the simulation test of multi-VPP electricity transactions is conducted on the Ethernet test network.

4.1. Clearance of Transactions

The optimization results of each VPP carrying out P2P electric energy interaction are shown in Figure 4. From the figure, it can be seen that in the time periods of 00:00–09:00 and 16:00–24:00, VPP1 has a surplus of electric energy and plays the role of a seller to supply electric energy to other VPPs. In the 06:00–10:00 time period, VPP2 buys electric energy from VPP3; in the 09:00–16:00 time period, VPP2 shares electric energy to VPP1. In the 09:00–16:00 time slot, VPP3 sells electric energy to VPP1. As a result, this multi-VPP power sharing credible trading mechanism promotes the production motivation of the seller and stimulates the consumption potential of the buyer, effectively improving the level of resource sharing.

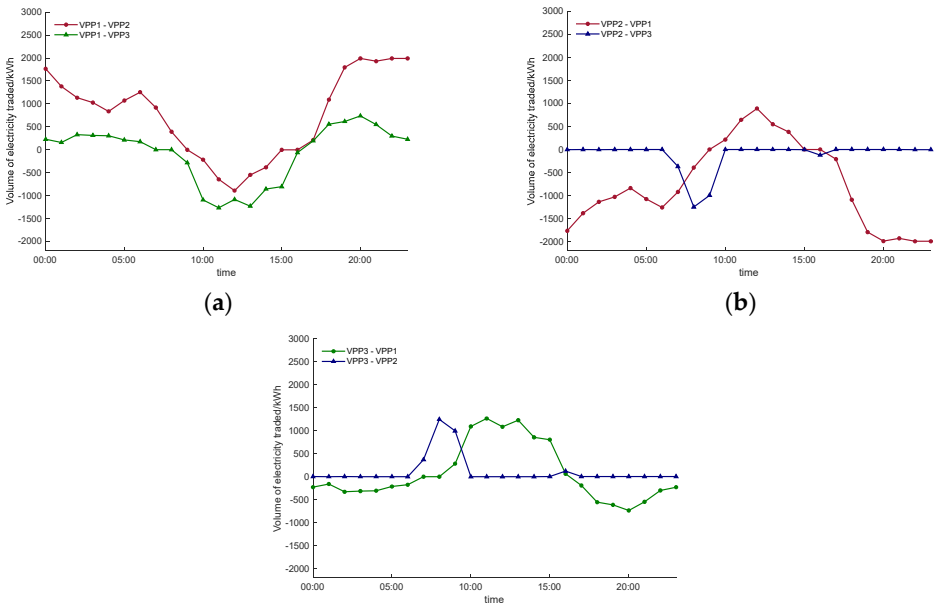


Figure 4. Results of power sharing between VPPs: (**a**) VPP1; (**b**) VPP2; (**c**) VPP3 (results of the simulation of the models in this paper).

The electricity trading price of each VPP subject is shown in Figure 5. The transaction price determined based on Nash negotiation remains within the regional electricity price limit throughout the dispatch cycle. Especially during the off-peak service hours, the price is obviously at a low level, effectively avoiding the risk of over-dependence on the superior grid. It can be seen that the Nash negotiation between VPPs in the region can not only purchase energy at a more economical price but also dispose of excess power in a timely manner and achieve optimal control of operating costs.

A graph comparing the independent operating cost of each VPP after the clearing of electricity trading among VPPs with the operating cost after conducting p2p trading is shown in Figure 6. As can be seen from the figure, the running cost of each VPP is reduced to different degrees after power sharing. The details are shown in Table 2. Among them, VPP1 saves cost 2129.704$, VPP2 saves cost 8549.638$, and VPP3 saves cost 1188.54$. The results show that the transaction clearing method proposed in this paper improves the participation motivation of each market member and maximizes social welfare.

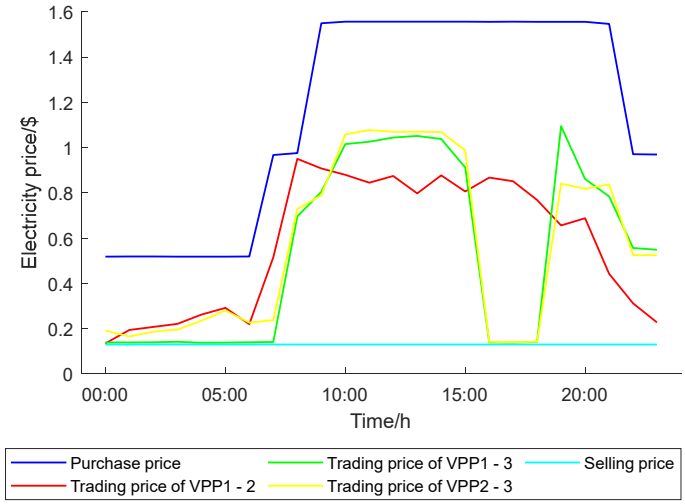


Figure 5. Prices of electricity traded between VPPs (results of the simulation of the models in this paper).

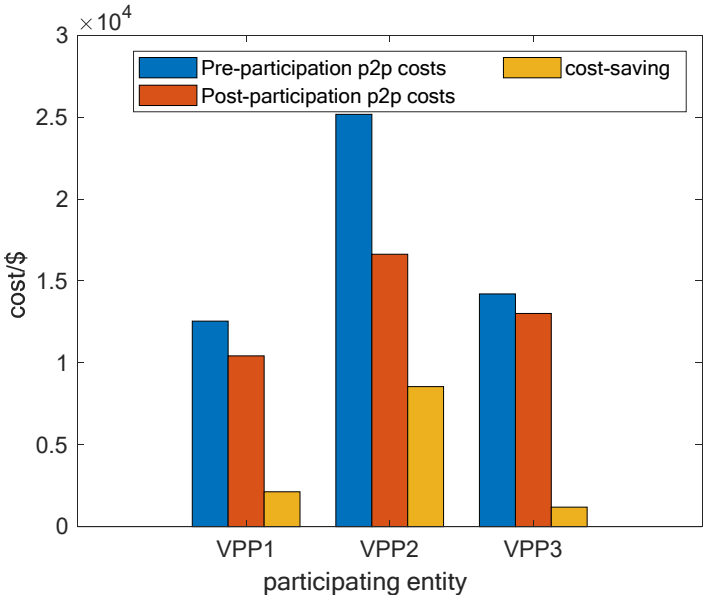


Figure 6. VPP cost change chart (results of the simulation of the models in this paper).

Table 2. VPP cost improvement.

VPP Number	Stand-Alone Operating Costs/$	P2P Transaction Running Costs/$
VPP_1	12,553.2	10,423.5
VPP_2	25,183.14	16,633.6
VPP_3	14,208.61	13,020.07

(Results of the simulation of the models in this paper).

4.2. I-PBFT Consensus Process

In the consensus process of VPP electrical energy sharing transaction, it is set that the lower consensus group A includes three nodes, where VPP1 is the leader node 1, VPP2 and VPP3 are the ordinary nodes 2 and 3. Meanwhile, the leader nodes of these lower consensus groups together constitute the upper consensus group.

4.2.1. Analysis of Common Node Evil Scenarios

It is assumed that common node 2 is the evil-doing slave node. In the Pre-Prepare phase of local consensus, node 1 broadcasts a Pre-Prepare message to other ordinary nodes including node 2. After receiving the message, node 2 intentionally tampers with the message content in an attempt to interfere with the consensus process. However, after receiving the message, node 3 strictly verifies the message based on the authentication protocol based on zero-knowledge proof with the Diffie–Hellman algorithm. Since node 2's altered message cannot pass the authentication, other nodes will reject the message and mark node 2 as an abnormal node. In the Prepare phase, node 3 generates a Prepare message based on the correct Pre-Prepare message and broadcasts it to other nodes. At this time, due to the malicious behavior of node 2, it may not send the correct Prepare message, but this does not affect the consensus among other nodes. When node 3 receives more than 2f (f = 1 in this scenario) correct Prepare messages, it enters the Commit phase. During the Commit phase, node 3 continues to send Commit messages following the consensus process. Similarly, the local consensus is completed as soon as the node receives more than f + 1 correct Commit messages. Since the malicious behavior of node 2 is identified and excluded, normal nodes can successfully complete the local consensus, ensuring the consistency and integrity of the transaction data. The flow is shown in Figure 7.

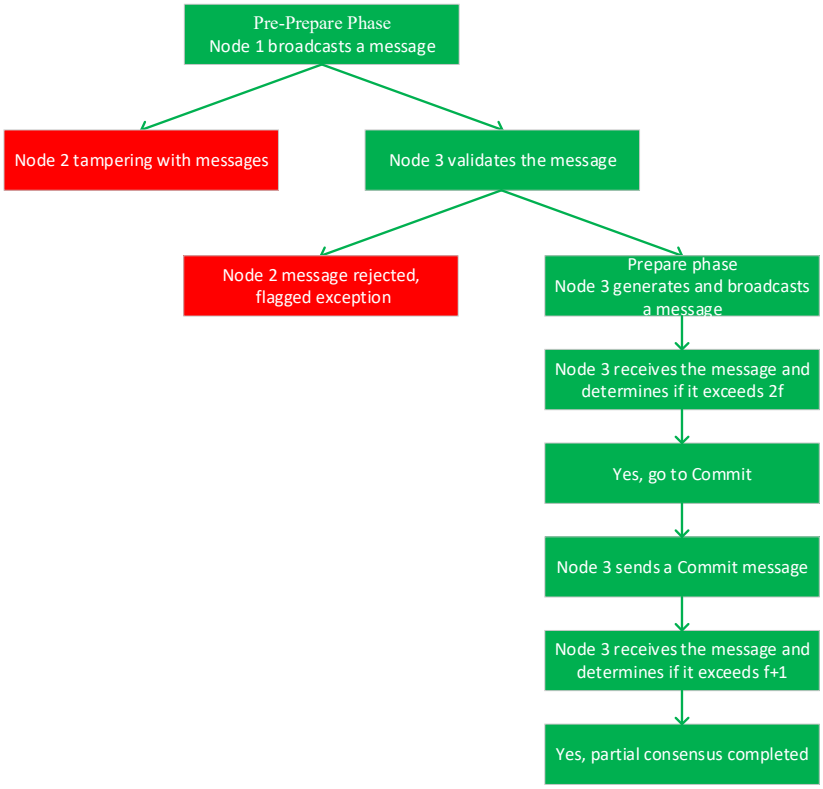


Figure 7. Common nodes do evil.

4.2.2. Leader Node Evil Scenario Analysis

Suppose node 1 (the leader node of the lower consensus group A and also a member of the upper consensus group) commits an evil act during the consensus process. During the local consensus phase, node 1 intentionally packages wrong transaction data and broadcasts a Pre-Prepare message to other nodes. After receiving the message, the other nodes discover through the authentication protocol that the transaction data in the message is faulty and does not satisfy the consistency requirement. At this time, nodes 2–3 report the situation to the upper layer consensus set, triggering the view change mechanism.

After receiving the report, the upper layer consensus set will revisit the situation of the lower layer consensus set A. According to the consensus set leader node election strategy, a reliable node from nodes 2–3 is re-elected as the new leader node, assuming that node 2 is elected as the new leader node. The new leader node will reorganize the local consensus process to generate and broadcast messages according to the correct transaction data from the Pre-Prepare phase. The other normal nodes will respond positively and redo the Prepare and Commit phases. In the re-conducted consensus process, the local consensus can be successfully completed due to the correct guidance of the new leader node and the collaboration of other normal nodes. Subsequently, the new leader node submits the local consensus result to the upper consensus set and participates in the global consensus process to ensure that the whole distributed power transaction can continue to proceed normally, avoiding transaction failures or data errors due to the master node's evil. The process is shown in Figure 8.

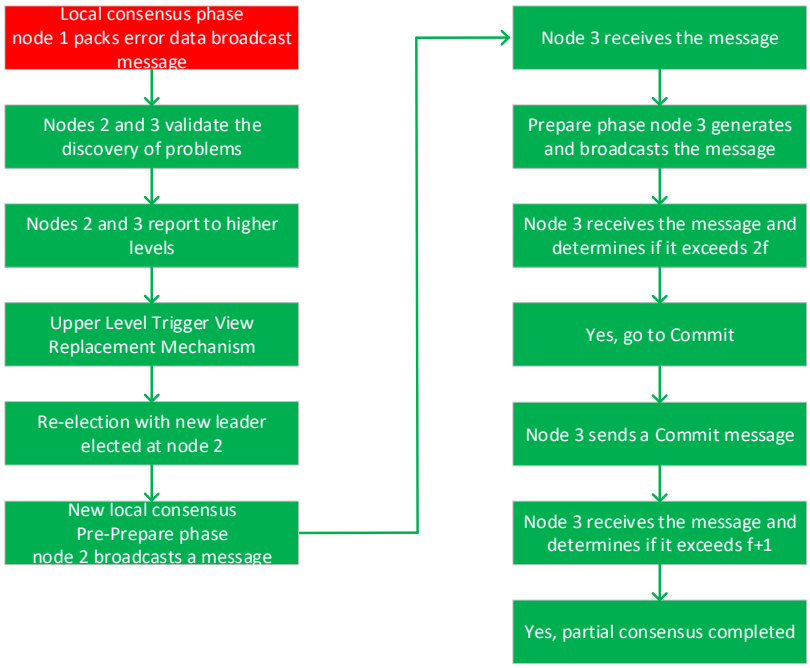


Figure 8. Leader nodes do evil.

Using the I-PBFT consensus algorithm proposed in this paper, the transaction still proceeds normally when there is a malicious behavior or failure of the master node of the slave node.

4.2.3. Time Delay Analysis

Consensus delay is a key indicator for evaluating the strengths and weaknesses of the consistency algorithm, which indicates the time spent from the client initiating the transaction request to the successful confirmation of the transaction. The lower the delay, the shorter the execution time of the consensus algorithm, the higher the consensus efficiency, the faster the network nodes reach agreement, and the system operation is more secure, stable, and efficient. In order to verify the superiority of the I-PBFT consensus algorithm proposed in this paper, the method of this paper is compared with three common consensus algorithms, namely, PBFT, P-PBFT, and C-PBFT, to conduct a delay comparison test. The results are shown in Figure 9, where it can be observed that the consensus latency of the PBFT algorithm is significantly higher than that of the C-PBFT, P-PBFT, and I-PBFT algorithms for the same number of nodes. The reason is that the latter three algorithms

utilize the group consensus mechanism, which greatly reduces the communication cost in the consensus process. With the gradual increase in the number of nodes, the latency of all four algorithms shows an upward trend. However, it is worth noting that the I-PBFT algorithm shows the most moderate growth. For example, when the number of nodes is 150, the consensus latency of the I-PBFT algorithm is reduced by about 62% compared to the P-PBFT algorithm, and by about 72% compared to the C-PBFT algorithm.

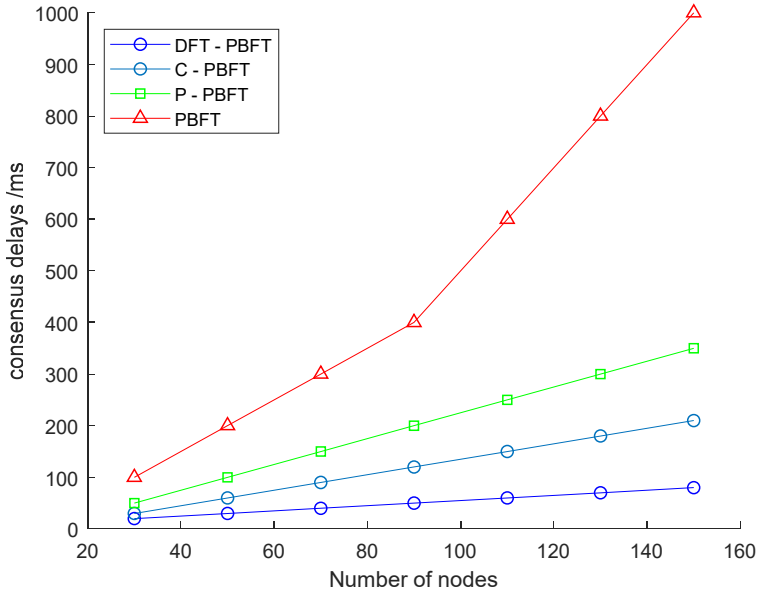


Figure 9. Comparison of consensus latency for different algorithms (Results of the simulation of the models in this paper).

4.2.4. Communications Overhead

Communication overhead refers to the amount of communication generated during the execution of consensus algorithm by nodes. The PBFT algorithm, as an algorithm relying on the information interaction between nodes to complete the consensus, has its operational efficiency and performance directly affected by the size of the communication volume; therefore, the communication volume has also become one of the key evaluation indexes to measure the strengths and weaknesses of PBFT and its derivative algorithms.

Under laboratory conditions, this paper launched a test for the single transaction communication overhead of three consensus algorithms in a distributed electricity trading scenario. In the experiment, 100 VPP nodes are first divided into 20 lower consensus groups, and then the test samples are expanded in the scale of 100 nodes per increment. By analyzing the simulation results in Figure 10, it can be found that with the increase in the number of VPP nodes, the communication overheads of all three algorithms show an increasing trend. Among them, the communication overhead of the I-PBFT algorithm is lower than that of the C-PBFT and P-PBFT algorithms in all test phases, and the larger the node size is, the more significant its advantage is. This is because I-PBFT adopts a two-layer consensus mechanism, in which only the lower consensus set needs to complete the initial consensus in each round, and then the reliable upper consensus set carries out the secondary confirmation. This mechanism not only ensures the accuracy of the consensus but also reduces the communication overhead. When the number of nodes is extended to 300, the communication overhead of I-PBFT is reduced by 36.5% compared to P-PBFT and 52.1% compared to C-PBFT; when the number of nodes reaches 500, the communication overhead of I-PBFT is reduced by 38.6% and 57.3% compared to P-PBFT and C-PBFT, respectively. This indicates that the I-PBFT algorithm has a significant advantage in communication efficiency optimization in a certain scale distributed electricity trading network.

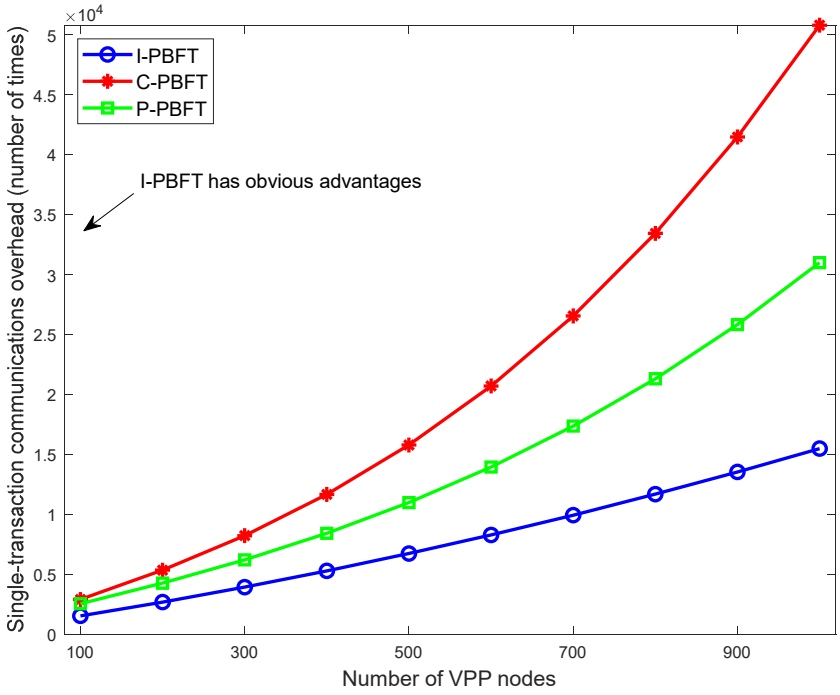
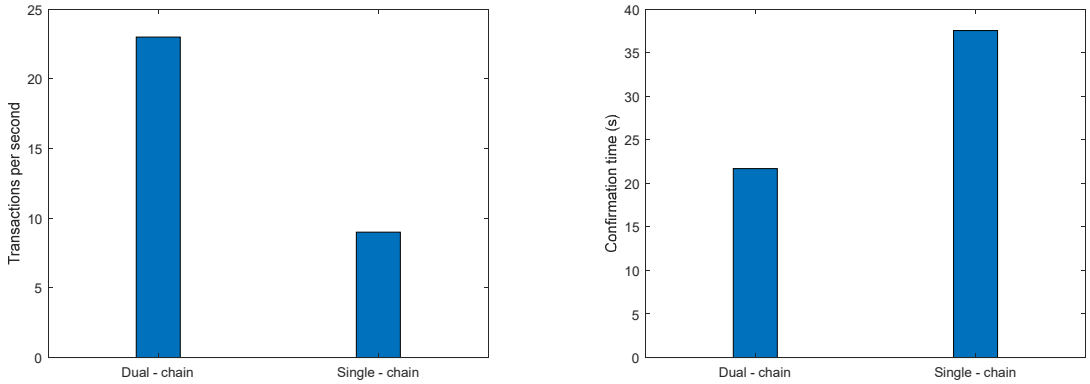


Figure 10. Comparison of communication overhead of three consensus algorithms for distributed electricity transactions (results of the simulation of the models in this paper).

4.3. Comparative Analysis of Dual-Chain Blockchain Performance

The blockchain of dual-chain and single-chain architectures are deployed on the Ethernet simulation platform to compare and analyze the performance of the two. In this simulation, the size of each block is 1 MB, the block creation time is 100 s, the bytes occupied by each transaction information is 1 KB, and the bytes occupied by the contract information is 500 B, and the performance comparison between the dual-chain and single-chain blockchain is shown in Figure 11.



(**a**) (**b**)

Figure 11. Dual-chain vs. single-chain blockchain performance comparison: (**a**) number of transactions processed per second; (**b**) average confirmation time per block (results of the simulation of the models in this paper).

As can be seen from the figure, the transaction chain of the dual-chain blockchain can process 23 transactions per second, while the single-chain blockchain can only process nine transactions per second. With the dual-chain deployment model of transaction data and contract data, the dual-chain blockchain can process more transactions than the single-chain blockchain in the same time dimension. The block confirmation time involves the

communication time between nodes and the information verification time, the block confirmation of single-chain blockchain covers the confirmation of transaction and calibration adjustment information, and the total confirmation time is 37.53 s; in dual-chain blockchain, the transaction is confirmed on the transaction chain, which consumes 12.26 s, and the calibration adjustment information is confirmed in the contract chain, which consumes 9.43 s. It can be clarified that the overall confirmation time of dual-chain blockchain is more than that of dual-chain blockchain, and it is more than that of a dual-chain blockchain. The dual-chain blockchain has a shorter overall confirmation time than the single-chain type, and for VPP, the dual-chain type blockchain is more advantageous in terms of transaction processing efficiency and performance.

5. Conclusions

In order to solve the problems of high cost, low efficiency, and lack of credibility in the process of VPP participation in distributed transactions, this paper proposes a credible transaction strategy for multi-VPP electric energy sharing based on the dual-chain blockchain. A multi-VPP power sharing transaction decision model based on dual-chain blockchain architecture applying Nash negotiation theory is established, and the I-PBFT consensus algorithm and multi-VPP power transaction smart contract is designed. The results show that the strategy proposed in this paper realizes the economy, credibility, efficiency, and security of distributed transactions among VPPs.

(1) Nash negotiation between VPPs allows them to both purchase energy at more economical prices and sell excess power in a timely manner, resulting in optimization of operating costs and efficient allocation of resources.

(2) The I-PBFT consensus algorithm can effectively resist the risk of node mischief or downtime, maintaining the credibility and security of transaction results in the autonomous transaction environment, while the low latency ensures the high efficiency of consensus.

(3) Dual-chain blockchain has higher transaction processing efficiency and security feasibility than single-chain blockchain.

The scalability of the model will be optimized to support larger distributed power trading networks with VPP participation, with a particular focus on optimizing the performance of the model under high load scenarios. In addition, exploring more efficient and secure privacy protection means is also a key direction of this paper.

Author Contributions: Conceptualization, W.H.; methodology, C.Z. (Chao Zheng) and W.H.; formal analysis, W.H. and X.H.; investigation, W.H. and X.L.; data curation, W.H. and S.Z.; writing—original draft preparation, G.L. and S.S.; writing—review and editing, C.Z. (Chenyang Zhao) and Q.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Research and Demonstration of Key Technologies for Virtual Power Plants in Cooperative Games Involving Multiple Participants of Distributed Energy Resources (grant number: 202302AF080006) and the Research on Key Technologies for Cooperative Operation of Virtual Power Plants in Multi-Agent Collaborative Games (grant number: YNKJXM20240051).

Data Availability Statement: The data used in this article have been given in detail in the article for the reader's reference.

Acknowledgments: The authors are extremely grateful to each of the authors who have helped and contributed to this paper. It is their joint efforts that made this paper successfully published.

Conflicts of Interest: Authors Wei Huang, Chao Zheng, Xuehao He, Suwei Zhai and Shi Su were employed by the company Yunnan Power Grid Co., Ltd. Authors Xiaojie Liu and Guobiao Lin were employed by the company Dongfang Electronics Cooperation. The remaining authors declare that

the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Gao, C.; Chen, Y.; Shi, K.; Wang, J.; Xiao, T. Distributed power trading among park microgrid-type virtual power plants based on trend distribution identification. *Power Supply* **2024**, *41*, 112–119. [CrossRef]
2. Zuo, J.; Ai, Q.; Wang, W.; Zhao, J.; Yu, T.; Tao, W. Status Quo of Virtual Power Plant Standardization and Architecture Design. *Power Syst. Autom.* 1–13. Available online: https://http-kns_cnki_net.shiep.vpn358.com/kcms/detail/32.1180.TP.20250326.1417.002.html (accessed on 21 April 2025).
3. Wang, D.; Ai, Q.; Yu, T.; Zuo, J.; Lu, Y.; Li, J. Technical Difficulties and Solutions for Trusted Transactions in Virtual Power Plants. *Power Syst. Autom.* 1–18. Available online: https://http-kns_cnki_net.shiep.vpn358.com/kcms/detail/32.1180.TP.20241030.1550.006.html (accessed on 21 April 2025).
4. Liang, Y.; Zuo, J. Virtual power plant technology and outlook. *New Power Syst.* **2025**, *3*, 12–32. [CrossRef]
5. Zuo, J.; Ai, Q.; Wang, D.; Wang, W.; Xu, C. Privacy-preserving trading strategies for virtual power plants in the power peaking market. *Power Syst. Autom.* **2024**, *48*, 149–157.
6. Li, D.; Yang, K.; Guo, Q. A privacy-preserving settlement model for virtual power plant power transactions. *Power Syst. Technol.* **2024**, *48*, 3713–3723. [CrossRef]
7. Zhang, L.; Bao, F. Research on Cooperative Operation of Multi-Virtual Power Plant Containing Distributed New Energy. *Electr. Meas. Instrum.* 1–9. Available online: https://http-kns_cnki_net.shiep.vpn358.com/kcms/detail/23.1202.th.20240621.1130.002.html (accessed on 21 April 2025).
8. Zhao, Y.; Song, W.; Li, W.; Meng, Y.; Ma, G. Optimized operation method of multi-virtual power plant considering shared energy storage capacity allocation. *Grid Clean Energy* **2024**, *40*, 92–101.
9. Cheng, X.; Wang, J.; Jin, Y.; Li, R.; Bao, Y.; Deng, H. Cooperative gaming strategy for multiple virtual power plants taking into account distribution network operation constraints. *South. Power Grid Technol.* **2023**, *17*, 119–131. [CrossRef]
10. Zhu, Y.; Guo, J.; Zhou, Y.; Han, H.; We, Z. A multi-virtual power plant electricity-carbon P2P trading model considering carbon-green certificate market coupling. *Power Autom. Equip.* **2025**, *45*, 51–58. [CrossRef]
11. Xu, H.; Tian, Y.; Zhao, Y.; Chai, Y.; Fang, Q. Optimal scheduling of multi-virtual power plant hybrid game considering green certificate-carbon trading. *Intell. Power* **2024**, *52*, 1–7+16.
12. Liu, W.; Chen, Z.; Du, P.; Chen, J.; Li, B. A model of multi-virtual power plant participation in day-ahead power market bidding based on coalition game. *Power Autom. Equip.* **2024**, *44*, 135–142+150. [CrossRef]
13. Han, H.; Xu, Y.; Wu, C.; Jiang, X.; Cao, S.; Zang, H.; Chen, S.; Wei, Z. Nash Equilibrium-Based Two-Stage Cooperative Operation Strategy for Multi-Microgrids Considering Uncertainty. In *Protection and Control of Modern Power Systems*; PSPC: Xuchang, China, 2024; Volume 9, pp. 42–57. [CrossRef]
14. Bate, W.G. Blockchain and the Future of Tokenization. *Res.-Technol. Manag.* **2025**, *68*, 59–62. [CrossRef]
15. Ping, J.; Yan, Z.; Chen, S.; Yao, L.; Qian, M. Coordinating EV charging via blockchain. *J. Mod. Power Syst. Clean Energy* **2020**, *8*, 573–581. [CrossRef]
16. Alam, K.S.; Kaif, A.D.; Das, S.K. A blockchain-based optimal peer-to-peer energy trading framework for decentralized energy management with in a virtual power plant: Lab scale studies and large scale proposal. *Appl. Energy* **2024**, *365*, 123243. [CrossRef]
17. Salehi, M.K.; Rastegar, M. Blockchain-enabled framework for transactive home energy management with cloud energy storage under uncertainties. *Energy Build.* **2024**, *317*, 17. [CrossRef]
18. Sadri, H. AI-Driven Integration of Digital Twins and Blockchain for Smart Building Management Systems: A Multi-Stage Empirical Study. *J. Build. Eng.* **2025**, *105*, 112439. [CrossRef]
19. Wang, H.; Fei, F.; Chen, K. A distributed scheduling strategy for virtual power plants based on energy blockchain. *J. Syst. Manag.* **2022**, *31*, 406–411.
20. Zhou, B.; Zhang, Y.; Zang, T.; Cao, Q.; Zhang, Y.; Peng, H. Optimized operation of multi virtual power plant master-slave game based on blockchain. *Power Syst. Autom.* **2022**, *46*, 155–163.
21. Ren, J.; Zhang, Q. Two-stage robust optimal scheduling of virtual power plant based on energy blockchain. *Power Autom. Equip.* **2020**, *40*, 23–33. [CrossRef]
22. Wang, W.; Ai, Q.; Li, X.; Wang, D.; Chen, M. Master-slave multi-chain transaction matching mechanism for virtual power plant based on improved consensus algorithm. *Power Eng. Technol.* **2024**, *43*, 69–80.
23. Liu, Y.; Fan, Y.; Bai, X.; Song, Y. Virtual power plant model and scheduling strategy based on optimized computational blockchain system. *J. Electrotechnol.* **2023**, *38*, 4178–4191. [CrossRef]

24. Wu, J.; Lou, P.; Guan, M.; Huang, Y.; Zhang, W.; Cao, Y. Optimization strategy for power sharing operation of multiple microgrids based on asymmetric Nash negotiation. *Grid Technol.* **2022**, *46*, 2711–2723. [CrossRef]
25. Fu, J.; Jing, C.; Du, M. Review and progress of DBSCAN research on spatial density clustering pattern mining method. *Sci. Surv. Mapp.* **2018**, *43*, 50–57.