Zhang et al. Journal of Cloud Computing: Advances, Systems and Applications (2022) 11:4
https://doi.org/10.1186/s13677-021-00273-3

Journal of Cloud Computing: Advances, Systems and Applications

RESEARCH Open Access

Security scheduling and transaction mechanism of virtual power plants based on dual blockchains

Xiaohong Zhang[1*], Zilong Song[1], Ata Jahangir Moshayedi[1,2] and IEEE Member

Abstract

Aiming at the data authenticity and storage problems in the current coordinated scheduling of virtual power plants, as well as the opaque information and high transaction costs, a dual blockchains security mechanism is proposed to solve above problems. In the process of security scheduling, a hybrid attribute proxy re-encryption algorithm based on ciphertext strategy is designed. The algorithm is composed of an identity encryption algorithm and an attribute proxy re-encryption algorithm with ciphertext strategy. Combining blockchain, tamper-proof smart metering equipment can effectively solve data authenticity and confidentiality in the information transmission process of distributed energy. In the research process of the trading mechanism, a continuous double auction mechanism based on reputation is proposed. In order to create a favorable trading atmosphere, reputation-based market segmentation mechanisms are integrated, and participants are divided according to reputation value. Depending on the properties of the stored information, they are divided into the private blockchain (with coordination scheduling information) and the consortium blockchain (with transaction information). The system analysis shows the reliability of the dual blockchains architecture. The communication and calculation costs of the proxy re-encryption algorithm verify the practicability of the proposed scheme. The case analysis of the auction mechanism declares that the mechanism can operate effective in the electricity trading market.

Keywords: Virtual power plant, Virtual power plant, Hybrid proxy re-encryption, Distributed energy resources, Reputation, Continuous double auction

Introduction

According to the global greenhouse gas emission data in 2010, energy production such as electricity and industry accounted for 76% of the total global emissions in that year. Considering the impact of greenhouse gas emissions on climate change [1] and the cost and supply of fossil fuels, the traditional single form of thermal power generation can no longer meet the needs of people's lives, and the academic community has begun to study new power supply modes.

A long with the development of Energy Internet (EI), the power supply model in the future may be gradually transformed into Distributed Energy Resources (DER) as the main primary energy [2]. DER is mainly composed of Distributed Generation (DG), Distributed Energy Storage (DES), Dispatchable Load (DL), Electric Vehicle (EV) and so on [3]. When the clean and efficient DG represented by Wind Energy (WE), Hydroenergy (HE) and Photovoltaic (PV) are integrated into the power grid, the above greenhouse gas emission problems can be effectively alleviated [4]. Experts pointed out that by the end of 2016, about 25% of the world's electricity originated from DER, also predicted that DER generation will account for about 30% in 2022 and even more than 60% in 2050 [5]. Although DER is widely valued, there are

* Correspondence: xiaohongzh@jxust.edu.cn
[1]School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China
Full list of author information is available at the end of the article

still certain problems remaining in its application. Firstly, features of the DG are small capacity and uneven distribution, energy generation from the DER is intermittent and random making energy less reliable [6]; Secondly, when the power generated by DER is directly connected to the grid, these powers are invisible and uncontrollable. If the amount of grid-connected is too large, it is easy to cause load fluctuations, which will cause the power system to lose safety and reliability [7]; Finally, the supply-demand relationship of the power market becomes a bottleneck hindering further advancement of DER.

In order to mitigate the problems caused by DER connected to the grid directly, two different grid-connected technologies were proposed in the industry, Micro Grid (MG) and Virtual Power Plant (VPP) [8]. MG, a small power distribution system with integration of several modules composed of DG, the controllable load, energy storage and energy conversion equipment especially including monitoring and protection equipment [9], have a certain energy management function, can enhance the reliability of power supply and provide continuous power supply for important users. Nevertheless, there are certain physical limitations, the characteristics of DER (large-scale, multi-regional) would lead to results that cannot be fully utilized in the MG. In contrast, VPP is not restricted by geographical location, can coordinate and manage the market operation of centralized and distributed energy through advanced coordinated control technology, intelligent metering technology and information and communication technology without changing the original grid-connection mode of DG [10]. Currently, the research and use of virtual power plants are mainly concentrated in developed countries such as Europe and North America. Mashhour and Moghaddas-Tafreshi [11] defined VPP as the flexible combination of a portfolio of DER that could maximize market benefits through bidding. Then, they proposed a non-equilibrium model of the deterministic price-based unit commitment which took into account the constraints of VPP itself, and used genetic algorithms to solve the bidding results. It is an inevitable trend to include more and more DER in the future distribution system, and a large number of VPPs will be established. The trading strategy between VPPs is a problem to be solved. For this consideration, Shabanzadeh et al. [12] established a medium-term self-scheduling decision-making layer for VPP to solve the interests of different trading layers, the correctness of the decision is ensured by an effective risk management method based on the first-order stochastic dominance constraint. A key problem in deciding to provide bidding strategy for VPP is the accurate modeling of uncertain variables. To solve this issue, a stochastic adaptive robust optimization model was proposed by Baringo et al. [13]. The optimization model consisted of robust optimization model and stochastic programming model, and the case study results of the model proved the applicability of the scheme. In the electricity market environment of Europe and the United States, Baringo et al. [14] discussed the self-dispatching problem of VPP energy trading and reserves set up a day-ahead. They proposed a model to solve this problem by considering the uncertainty related to the virtual power plant required by the system operator to deploy reserves. A distinctive feature of the model is the use of adaptive robust optimization to model demand uncertainty. In addition to theoretical research, EU countries had already started to implement a series of VPP projects, such as VFCPP [15], FENIX [16], EDISON [17] and GVPP [18].

The above-mentioned literatures and projects show the potential of VPP in energy market trading and scheduling, and can be used for reference for further research in the future. However, there are still some common problems in the existing VPP grid connection technology:

a) DER grid connection is highly free. With the increase of the number of DER in the grid, VPP is difficult to meet the profit-seeking demand and grid connection behavior of the massive DER in the power market driven by real-time electricity price, which increases the difficulty of the designing and implementing its coordinated control technology.
b) VPP lacks an open and transparent trading platform and information platform, transactions between VPPs and transactions with other users usually have high costs. In the meantime, due to the information asymmetry between VPP and DER, so DER's enthusiasm to participate in electricity trading is not high.
c) Lacking a set of methods or mechanism to ensure the security of data and information in the existing VPP system. The information needed by dispatching is directly transmitted through two-way communication technology. If the dispatching information is tampered with maliciously during the transmission, it will seriously affect the security and stability of the current power market.

In 2008, the outbreak of the global financial crisis prompted Satoshi Nakamoto to propose a decentralized digital currency bitcoin, and the blockchain is the core technology that supports the operation of bitcoin [19]. After passing through the frenzy period of digital currency, blockchain has become one of the research hotspots in academia due to its decentralization, trustlessness, openness and transparency. With continuous research, the application range of blockchain has

become more and more extensive, and it is no longer limited to the financial sector. The integration of blockchain into the energy industry can provide new solutions to the above problems. Different from the traditional centralized system, each node on the blockchain is given the same power. Even if a single point of failure occurs, it will not affect the entire blockchain system [20]. Unguru [21] analyzed the advantages and risks of blockchain application in the energy sector, and conclused that the advantages far outweigh the disadvantages for consumers. A survey of decision makers in the German energy industry was conducted by Burger et al. [22], which showed that most people think that blockchain technology has great potential in the energy field. Hasse et al. [23] introduced the history of blockchain technology and its potential impact in different industries, and then emphatically analyzed the feasibility of applying blockchain technology to the energy industry from the perspective of consumers. At the same time, the challenges from laws or rules faced by the application of blockchain in the energy industry were also described in detail. Starting from the concepts and characteristics of blockchain technology and virtual power plant, Starting from the concepts and characteristics of blockchain technology and virtual power plant, He and Ai [24] analyzed the feasibility of blockchain technology in VPP and the complementarity between the two fusions. With the continuous growth of DER, how to reasonably integrate new participants into the energy market has become a key problem that must be solved. Therefore, Galici et al. [25] designed a physical platform to simulate the local electricity market. The platform was mainly managed by an integrator who plays the role of VPP. The integrator needed to collect and publish the quotation information of transaction participants, and then used blockchain technology to complete the user's business transaction. The development of technology promotes the evolution of smart grid to EI. For the better development of EI, Lu et al. [26] established a blockchain-based VPP transaction model for EI driven by electricity prices in real time. In order to simplify the existing complex power transaction and settlement process, a VPP distributed energy transaction smart contract based on blockchain technology was proposed. The promotion of electric vehicles not only brings clean and environmental protection, but also makes the power transaction, especially caused by charging and discharging, face more severe security challenges. Li and Hu [27] designed a two-layer optimized dispatch architecture based on consortium blockchain, and realized safe two-way power trading between electric vehicles and smart grids under the constraints of circuit power flow and vehicle travel demand. Most of the above-mentioned documents focus on the energy dispatch and transaction process, without too much analysis of blockchain technology.

This paper focuses on the specific role of blockchain technology to realize the energy dispatch and transaction process in the operation of VPP. The main contributions are summarized as follows:

a) Considering that the amount of real-time data generated by DER is too large, a storage architecture based on dual blockchains is proposed, which consists of a private blockchain at the bottom and a consortium blockchain at the top. The private blockchain is formed by each DER supplier to store the production information required for VPP scheduling calculation. The central node of the private blockchain has the risk of tampering with data. We use a more secure alliance blockchain to ensure the security of private chain data, mainly by storing private blockchain abstracts. The alliance blockchain is composed of all nodes in the system. It not only stores the private blockchain abstracts, but also stores transaction information involving the interests of participants.
b) A large amount of data and information are needed in the VPP scheduling process. To avoid malicious tampering of key information and ensure the confidentiality and authenticity of the information, a hybrid attribute proxy re-encryption algorithm based on ciphertext strategy is proposed. Agents can convert ciphertext based on attribute encryption into ciphertext identity-enabled encryption, which reduces the decryption cost of data visitors.
c) In order to ensure that participants have good market behavior, a reputation-based continuous double auction mechanism is proposed, which combines a reputation with market segmentation mechanism and a continuous double auction mechanism. The reputation value and identity of the participants are the basis for their classification. The higher the reputation value, the more preferential treatment the participants can get. In addition, this paper proposes the concept of energy currency to facilitate transactions in the electricity market, which will be the only currency in system transactions.

The rest of this paper is arranged as follows: Section 2 introduces the preliminary knowledge. In Section 3, we discuss the basic framework diagram of virtual power plant resource scheduling and transaction mechanism based on dual blockchains. We described the specific implementation details of the scheme, such as the process of re-encryption based on the attribute proxy of the blockchain, the process of the reputation-based blockchain energy transaction mechanism, and the

process of block generation in Section 4. In Section 5, we conduct a safety analysis and performance evaluation of the proposed scheme. Finally, we summarize the whole paper.

Preliminaries

Blockchain

As a whole, blockchain, which enables data storage, circulation and processing by integrating various existing technologies, is a new distributed computing parading. It uses the distributed node consensus algorithm to generate and update the data, uses cryptography to ensure the immutability and unforgeability of the stored data, and the data transmission between nodes is completed through the point-to-point network [28]. Currently, in the light of different modes of node participation, blockchain network can be divided into three types: public blockchain, consortium blockchain and private blockchain [29].

Among them, non-public blockchains such as consortium blockchain and private blockchain can be collectively referred to as permissioned blockchain. The public blockchain is also known as the permissionless blockchain, which allows any user with a network computer in the world to freely join and read block information freely. It is a completely decentralized blockchain in the true sense. Consortium blockchain refers to a multi-centralized blockchain composed of multiple organizations or institutions with the characteristics of common maintenance and access mechanisms. Only institutions certified by the consortium can join the consortium blockchain. A private blockchain refers to a blockchain in which the write permission of each node is completely controlled by an organization, and the read permission is selectively opened to the outside world by the organization. Although the consensus and verification processes of private blockchains are strictly limited to specific scopes by belongs institutions, they still have a general structure of multi-node blockchains, and private blockchains are often regarded as public blockchains within a small-scale system. The model diagram of the three blockchains is shown in Fig. 1.

Virtual power plant

The Virtual Power Plant (VPP) originated from the definition of virtual public facilities which proposed by Awerbuch and Preston [30]. Virtual public facilities refer to a flexible cooperative relationship between independent entities driven by the market. This virtual cooperative relationship enables participating entities to provide consumers with high-quality power services without having to own corresponding physical assets.

The traditional VPP is committed to regional power integration, so as to provide better power services for internal users. Nevertheless, with the addition of emerging technologies such as Demand Response (DR), Demand-Side Management (DSM) and Local Energy Market (LEM), VPP has gradually played the role of the unified DER agent in LEM. While realizing the integrated scheduling of DER, it is also necessary to provide technical support for DER to participate in the bidding and ancillary services of the electricity market. For VPP, its nerve

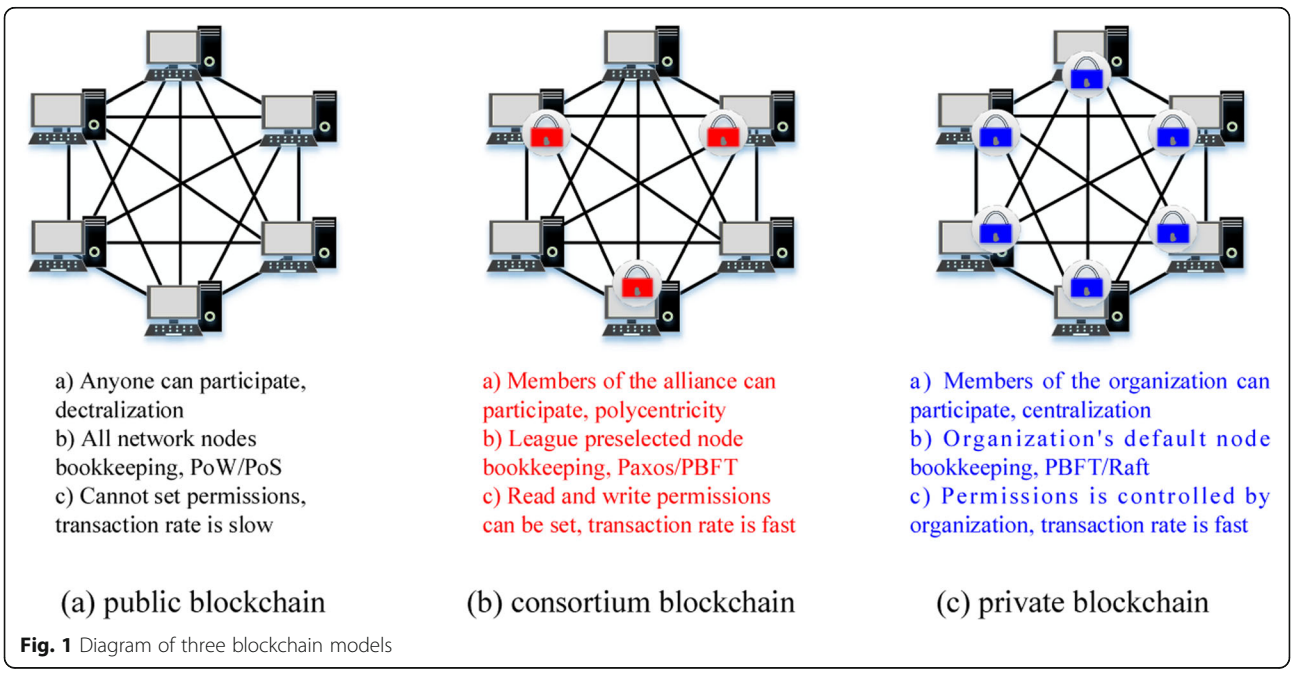


Fig. 1 Diagram of three blockchain models

center is the dispatching control center. Wei et al. [31] divides it into two modules according to their functions—Commercial VPP (CVPP) and Technical VPP (TVPP). The operation process and division of responsibilities of the two modules are shown in Fig. 2.

CVPP is a VPP considered from the perspective of commercial revenue, aiming to improve the overall benefits of VPP. CVPP, regardless of the impact of VPP on the distribution network, adds DER to the electricity market in the same way as traditional power plants. CVPP receives economic parameters from DER, and then combines these parameters with market intelligence to develop a profit-driven bidding plan. Once the market authorization is obtained, CVPP will sign a medium and long-term contract with LEM, and submit DER generation schedule and operation cost information to TVPP [32]. CVPP can represent any number of DER, and DER can also arbitrarily select a CVPP to join in order to enter the electricity market for energy trading. Such as energy suppliers, trusted third parties or new market entrants can assume the responsibilities of CVPP. The purpose of CVPP is to maximize the benefits.

Different from CVPP, TVPP, from the perspective of system scheduling, mainly responsible for parameter collection and operation monitoring. After TVPP integrates the data parameters provided by CVPP and DER, it calculates the contribution that the DER belongs to, and then declares the operating characteristics of the VPP to the power dispatch operation center. When the dispatching center finds the risk of power flow overrun or power imbalance in the operation plan of VPP, the dispatching center will send dispatching instructions to TVPP, so that TVPP can ensure the stability and security of power system by responding to the dispatching instructions in a timely manner. It should be noted that the operation plan of VPP is evaluated together with that of traditional power plants. If the evaluation is approved, DER shall strictly follow the plan issued by TVPP.

Economy and safety are important cornerstones to ensure the lasting and stable operation of VPP, whereas

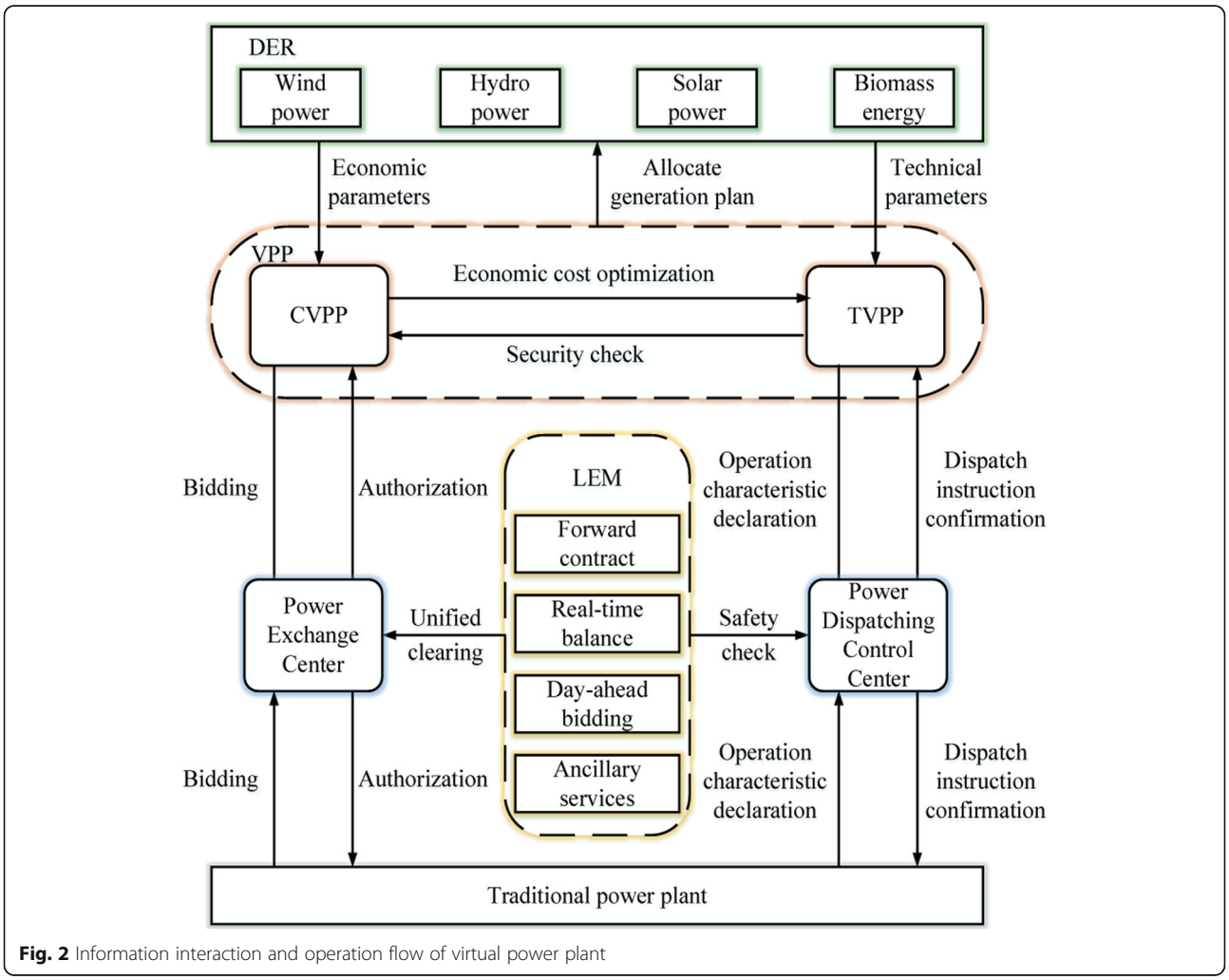


Fig. 2 Information interaction and operation flow of virtual power plant

CVPP and TVPP correspond to these two characteristics respectively. Namely, to ensure the economy and security of VPP is to ensure the stable operation of CVPP and TVPP.

Bilinear pairing

Supposing the three cyclic groups G_x, G_y and $G_z$of order p and the generator g, based on bilinear pairing, there is a mapping relationship $e: G_x \times G_y \rightarrow G_z$, and the following properties are satisfied [33]:

a) Bilinear: For $g_x \in G_x, g_y \in G_y, q, h \in Z_p^*$, there is always $\exists\ e(g_x^q, g_y^h) = e(g_x, g_y)^{qh}$.
b) Non-degeneracy: Always exists $g_x \in G_x, g_y \in G_y$, such that $e(g_x, g_y) \neq 1$.
c) Computability: There is an effective algorithm that makes $e(g_x, g_y)$ computable under the condition of $g_x \in G_x, g_y \in G_y$.

When G_x=G_y, the pairing can be called symmetric bilinear pairing, otherwise it is asymmetric. It should be noted that the bilinear pairing mentioned here is based on the prime order, that is, p is a prime number.

It should be noted that the bilinear pairing mentioned here is based on the prime order, that is, p is a prime number. Boneh et al. [34] introduced a new bilinear pairing based on composite order to the field of cryptography. The composite order bilinear pairing can prove its safety under the premise of realizing high-complexity functions through the orthogonality of sub-groups.

Access structure

Assume there is a set of parties $P = \{P_1, P_2, \ldots, P_n\}$, then we define a collection $A \subseteq 2^P$. The collection is monotonic if for any B and C, we can conclude that $C \in A$ when $B \in A$ and $B \subseteq C$. An access structure is a collection A of nonempty subsets of P (access structure and collection A are monotonic), such as $A \subseteq 2^P \backslash \varnothing$. The set in A are called authorized sets, on the contrary, they are called unauthorized sets.

Smart contract

The concept of smart contract first proposed by Szabo [35] in the late 1990s. Its basic idea is to embed part of contract into hardware or software in the form of code, so as to achieve a certain degree of decoupling with people when executing the contract, and to reduce the possibility of breach and increase the cost of breach. The essence of a smart contract is a treaty signed and recognized by both parties or even multiple parties. To ensure the effective execution of the contract, a trusted third party or arbitration institution will be needed. The smart contract incorporates the concept of machines into the execution of the contract, virtualizing part of the functions of the arbitration institution. If one party breaches the contract, the software or hardware of the machine needs to be modified, which increase the difficulty of breaching the contract.

Since 2016, the smart contract technology represented by Ethereum [36] has attracted increasing attention. The European Conference held in February 2017 pointed out that smart contract technology is the most promising one among the various applications of blockchain. Smart contracts are typically stored in blockchain as scripts, whose stored procedures can be referenced from operations in relational database management systems. Blockchain technology is the basis of smart contract, which solves the problem of contract execution in the absence of a trusted third party. Smart contract reflects its value through blockchain, and the value of blockchain is also released due to smart contract.

System model

VPP data storage and sharing model

System global model

In view of the lack of transparent VPP platform and the difficulty of data analysis, this paper proposes an information storage system based on blockchain technology. Different from most storage systems based on blockchain technology, this system will adopt two sets of blockchain systems: consortium blockchain and private blockchain. As shown in Fig. 3, VPP is divided into CVPP transaction information storage layer based on consortium blockchain and TVPP scheduling information storage layer based on private blockchain, which are referred to as Commercial Transaction Consortium Blockchain (CTCB) and Technology Scheduling Private Blockchain (TSPB).

Through the design of VPP information storage and sharing architecture of dual blockchains, the advantages of the consortium blockchain and private blockchain can be fully combined, so that they can play advantages at the level of their respective managements. Energy trading is an important part of national management. In the CVPP transaction layer, the consortium blockchain can be used to set the threshold for the entry of nodes, and the data access right of nodes can also be set and controlled. Meanwhile, the consortium chain inherits the advantages of partial decentralization of the public blockchain, and avoids the monopoly pressure similar to the high concentration of the private blockchain. Since the number of nodes in the consortium blockchain is known, a more efficient consensus algorithm can be used to improve the system performance and transaction efficiency without consuming huge computing power to maintain the system. In addition, when VPP performs energy dispatch, it needs a large amount of production

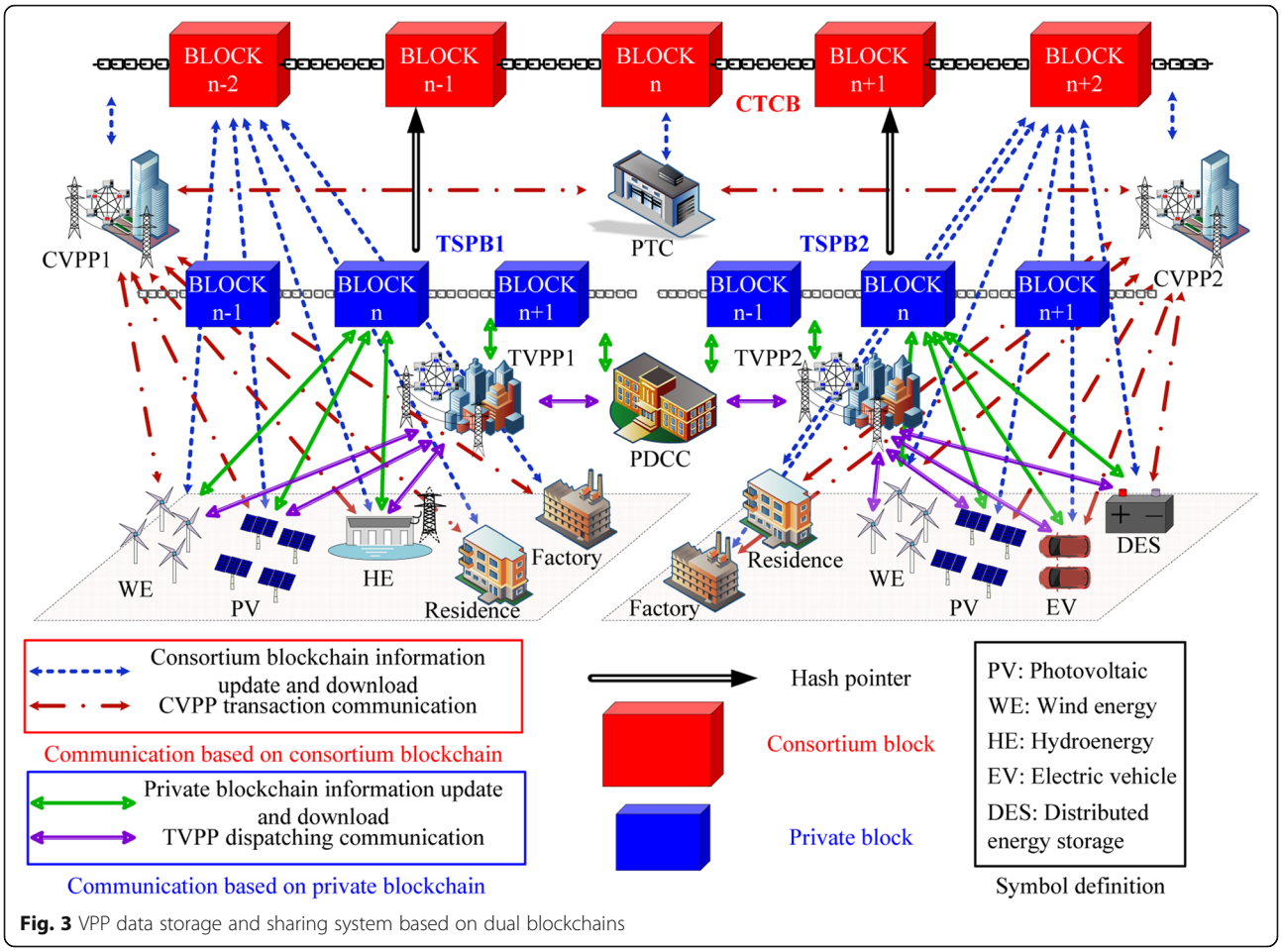


Fig. 3 VPP data storage and sharing system based on dual blockchains

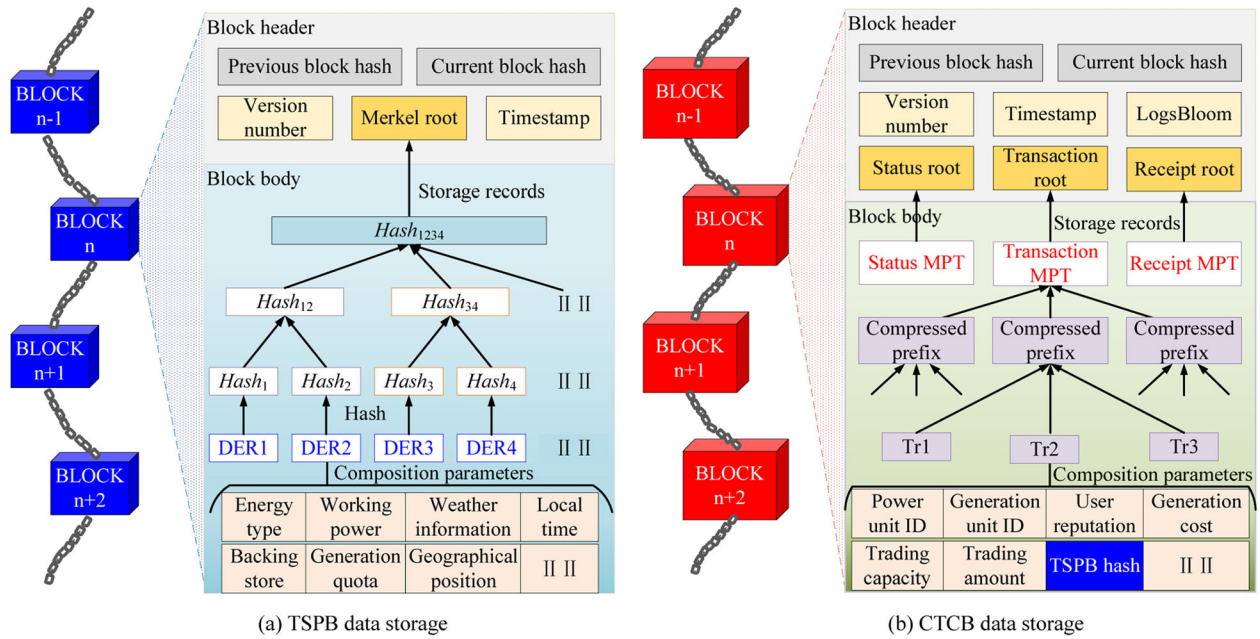
information form DER, such as energy type, working power, generation quota and other external information as for local time, geographical location, weather and so on. Using private blockchain in TVPP scheduling layer can achieve efficient, large capacity and low-cost information storage. Therefore, the purpose of this paper is to realize the complementarity of the two blockchains to form a practical information storage scheme.

TSPB local storage model

TSPB is mainly used to record the relevant information required by energy dispatching in the region under the jurisdiction of VPP, and relies on the nature of blockchain technology to ensure the authenticity, integrity and privacy of relevant information. TSPB is composed of TVPP, Power Dispatching Control Center (PDCC) and DER which TVPP belongs, each VPP can build its own TSPB. Data storage in TSPB is similar to Bitcoin, when a new block is allowed to be added to the blockchain, distributed nodes link it to the longest legal blockchain. The information recorded by the blockchain exists in these blocks, which are divided into block header and block body [37]. The block header is mainly used to store version number, previous block hash, timestamp, Merkel root and current block hash. Merkel root represents the total hash value of all transaction combinations contained in the block. The concrete information of the transaction is stored in the block body. The transaction data is hashed by pairwise pairing through the Merkel tree [38], and finally points to the Merkel root in the block header. The specific data storage model is shown in Fig. 4 (a).

CTCB local storage model

CTCB is mainly used as LEM's energy transaction record. It also relies on the nature of blockchain technology to ensure the authenticity, integrity, openness and traceability of the transaction process. CTCB is composed of Power Exchange Center (PEC), CVPP, residences, factories and DER which CVPP belongs. Unlike TSPB, there is only one CTCB in EI, and its operation is jointly maintained by all nodes in the network. CTCB adopts the data storage mode of Ethereum. Ethereum has improved the storage mode of bitcoin and proposed an account-based data storage mode. Based on the storage mode of Ethereum, there is an additional LogsBloom filter in the



(a) TSPB data storage

(b) CTCB data storage

Fig. 4 Regional model for data storage

block header. This filter is mainly used to judge whether the transaction of a block has generated a log, thereby avoiding the storage of log information in the block and saving space. What's more, it stores Merkel Patricia tree (MPT) roots instead of Merkel roots. MPT is composed of Merkel tree and Patricia tree (PT). The difference between MPT and PT is that the pointer of connection node is hash pointer, and a Merkel root will be saved in the end. PT is a variant of the prefix tree. Its working principle is similar to that of the prefix tree, but the characters of the prefix tree are compressed to save storage space. There are three types of MPT root in Ethereum: status root, transaction root and receipt root. There is only one status tree in the whole system, which records the account status of the whole blockchain network, such as account balance. In each block, there will be a transaction tree and a receipt tree. The former records the transaction information of the block, and the latter records the transaction receipt of the block. In order to ensure the security of data in TSPB, the transaction tree of CTCB should store not only transaction information, but also TSPB block hash value. The CTCB data storage model is shown in Fig. 4 (b).

VPP security scheduling model

Key technologies of VPP scheduling

As mentioned above, the key technologies of VPP scheduling include coordinated control technology, intelligent metering technology and information communication technology.

Coordinated control technology The objects controlled by the coordinated control technology are mainly DER such as DG, energy storage system, controllable load and EV etc., and the purpose is to realize the electric energy output of diversified DERs to users with high demand [31]. Considering the randomness or intermittence of renewable energy (light and wind) power stations, the DG classified into VPP should include at least one fully controllable power station (conventional power station) [39]. VPP can be divided into centralized control, decentralized control and hybrid control according to its internal DG composition and operation mode [40]. In centralized control mode, the energy coordination in the region under the jurisdiction of VPP is performed by the Control Coordination Center (CCC) located in the VPP center. CCC processes and analyzes the data from DER through appropriate algorithms (mathematical algorithm or heuristic algorithm, the former is used to solve linear programming problems, and the latter is used to solve nonlinear programming problems), so as to obtain the scheduling of each DER, then DER works according to the CCC scheduling scheme to achieve global coordination. However, this structure is only used when CCC has very strong computing power and communication bandwidth, and a single point of failure of CCC will cause the system to crash. In decentralized control mode, VPP no longer owns CCC, and each DER is in an independent alliance relationship. VPP here only provides key parameters and information exchange channels for DER, and does not participate in DER energy scheduling process. The DER belonging to it

realizes self-scheduling according to the information from VPP. Under this mode, the composition of VPP is loose, and the competition between DER is fierce, which is not conducive to long-term development. The hybrid mode integrates the characteristics of the above two patterns, which not only has CCC to coordinate the global scheduling, but also gives DER part of the autonomous control. In this mode, DERs with the same ownership are integrated and managed by the same agent, and VPP directly interacts with each agent for information. Agents share part of the integration tasks of virtual power plants, which, compared with the centralized control mode, reduces the computing burden of CCC and alleviates the communication pressure. Compared with decentralized control mode, DER ensures the internal coordination of VPP system while guaranteeing a certain degree of autonomy.

Intelligent metering technology Intelligent metering technology is an important part of VPP. Intelligent devices such as smart meters using intelligent metering technology are embedded into the power supply side or the terminal of equipment on the power side to realize real-time data recording and uploading. Finally, the data is aggregated to the VPP, and VPP will perform the aforementioned coordination scheduling based on the data. To ensure the authenticity of recorded data, smart devices should have tamper-proof features.

Information communication technology The technology guarantees the normal communication between VPP and DER. VPP mainly adopts two-way communication technology. On the one hand, VPP can receive the status information transmitted by the intelligent devices embedded in each unit. On the other hand, it can send scheduling control information to each unit.

Security scheduling model

Since VPP is data-driven, damaging the data authenticity will seriously affect the stability of the system. Different from traditional VPP information interaction, this paper adopts blockchain technology to share information. Blockchain technology can only guarantee the invariability of recorded data, while the credibility of input data cannot be guaranteed, it is necessary to use tamper-proof intelligent metering devices to input data [41]. The data of smart metering devices are updated and uploaded in real time. If it is directly transmitted to the VPP through the blockchain technology, it will cause a huge communication burden. VPP usually aggregates data every 5 or 15 minutes. To ensure the authenticity and confidentiality of data during this period, smart metering devices encrypt the data and store it in the blockchain. When data is encrypted, it is difficult to share it with other users who want to access it. Proxy re-encryption [42] can convert the encrypted file into ciphertext that the data requester can decrypt with his/her private key through a semi-trusted agent without disclosing the private key of the delegator. In the hybrid control model, each DER agent can just act as the identity of the re-encryption proxy. The specific security scheduling model is shown in Fig. 5.

The various process steps occurring in the system model are described as follows:

Step 1. The verification organization verifies the nodes that apply to join, and the verified nodes use identity-based encryption algorithms to generate exclusive public-private key pairs (PK_{ID}, SK_{ID}). In the scheduling process, it is mainly to analyze and process the information uploaded by DER. In order to ensure the confidentiality and sharing of the uploaded information, this paper adopts the ciphertext-based hybrid proxy re-encryption technology. Therefore, verification organization needs to additionally generate an encryption key SK_S for DER, which is generated by an attribute-based encryption algorithm and can encrypt uploaded information according to attributes.
Step 2. DER with built-in tamper-proof intelligent metering device uses encryption keys SK_S to encrypt the real-time production data according to attributes, and then stores the encrypted data in the private chain TSPB. At the same time, DER continuously conducts energy transactions through CVPP, and its transaction information is stored in the consortium blockchain CTCB. To ensure the security of private blockchain data, the private blockchain hash will also be stored in the consortium blockchain.
Step 3. Under the hybrid control model, DER agents share the operating pressure of TVPP, and DER agents are responsible for the same ownership of DER. When TVPP in the private chain needs a new round of scheduling, it needs to send a data access application to the DER agent.
Step 4. After receiving the data access application from TVPP, the DER agent aggregates from the private blockchain TSPB the data CT_A that has been encrypted and uploaded by DER during the period since the last scheduling.
Step 5. Since the DER agent has the ownership of the DER under its jurisdiction, the proxy re-encryption key $RK_{S\rightarrow ID_{VPP}}$ is directly generated by the DER agent, without the need for DER generation and forwarding to the DER agent. The SK_S required in the re-encryption key generation algorithm is issued and obtained by the verification organization in the Step 1. After generating

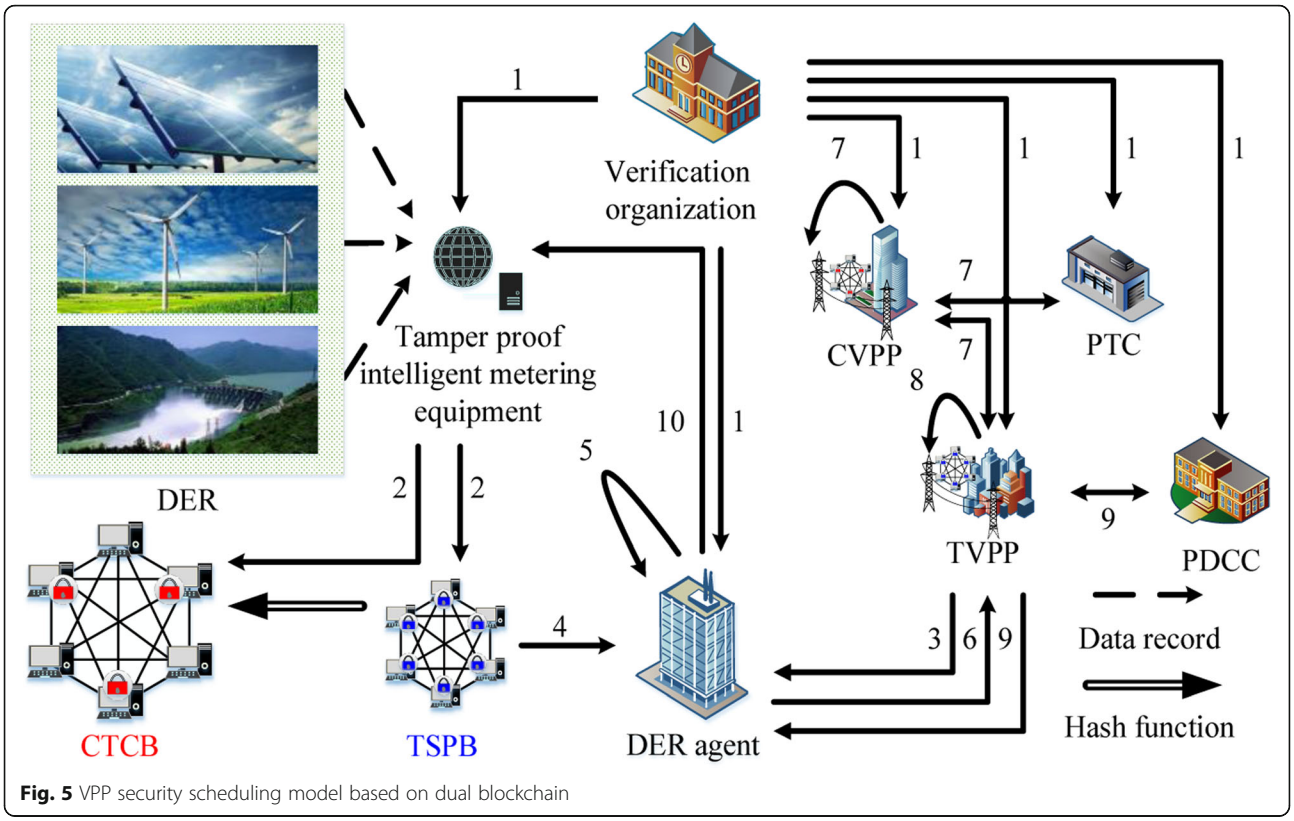


Fig. 5 VPP security scheduling model based on dual blockchain

$RK_{S \to ID_{VPP}}$, DER agents use it to re-encrypt the ciphertext CT_A to obtain the re-encrypted ciphertext $CT_{ID_{VPP}}$.

Step 6. After $CT_{ID_{VPP}}$ is generated, the DER agent immediately sends it to TVPP. TVPP obtains $CT_{ID_{VPP}}$ and decrypts it with its own private key $SK_{ID_{VPP}}$ to obtain the data required for scheduling.

Step 7. The CVPP based on the alliance blockchain collects the quotation information within its jurisdiction, and then promotes the electric energy transaction through the continuous double auction mechanism based on reputation. Participants who have not successfully traded will be handled by PTC. During the transaction, DER's reputation value and transaction volume and other relevant economic information will be transmitted in VPP's internal communications. It should be noted that the internal communication of VPP is two-way, which means that CVPP can also obtain messages from TVPP at this stage.

Step 8. Collecting production information from DER and economic parameter information from CVPP, TVPP calculates the optimal global scheduling plan by using mathematical algorithms or intelligent heuristic algorithms. During the calculation process, DER agents can share the calculation pressure for TVPP. In addition, the reputation value of DER can affect the final result to a certain extent, and those with high reputation value will appropriately consider allocating more production quotas.

Step 9. TVPP first sends the calculated scheduling plan to PDCC for security verification. If the verification passes, TVPP sends the plan to all DER agents in the same private blockchain. If the verification fails, TVPP needs to recalculate the new optimal scheduling plan.

Step 10. The DER agent sends the received scheduling plan to the DER under its jurisdiction, and then supervises the DER to respond to the scheduling optimization plan. The response rate and the degree of completion of the plan will affect the evaluation of the reputation value.

VPP market trading model

At present, DER transactions are mainly divided into two ways: P2P transactions and centralized clearing [43]. The former is a direct transaction between individuals, in which both parties have only Power Units (PU) and Generation Units (GU), and the transaction is automatically executed through a pre-made contract. The latter

is a unified transaction under the optimal scheduling of the intermediary, that is, in addition to the two parties of the transaction, there should also be a third-party platform to match the transaction. For DER transactions based on blockchain, centralized clearing may be a good choice.

According to the way of quotation, the centralized clearing can be further subdivided into call auction and Continuous Double Auction (CDA) [43]. Under the call auction mode, once the two parties of a transaction give a quotation, it is impossible to modify it. The third-party platform summarizes all the quotations and matches them according to the quotation and demand of both parties. Instead, CDA allows both parties to modify their quotations during each auction. Compared with the two parties, CDA is more conducive to realizing the goal of maximizing benefits, which is also the specific transaction mode adopted by the transaction model proposed in this paper.

To ensure that both parties have good market behavior, we have introduced the concept of reputation in the CDA auction mechanism, each user has its own reputation. The reputation of both parties to the transaction will be re-evaluated after a certain period of time, the level of the value is directly linked to the economic interests of the users, the higher reputation points of users, the more able to maximize their own interests. In addition, we will introduce a new digital cryptocurrency, named energy coin, in the transaction process. All the power transaction clearing processes in this paper are based on energy coin, and the specific transaction model is shown in Fig. 6.

The basic flow of the trading model is as follows:

Initializing variables Same as Step 1 in the scheduling process, the function of initialization is to verify the identity of the trader and provide a public-private key pair (PK_{ID}, SK_{ID}) for the passer. Only users with accounts can conduct communication transactions on the consortium chain CTCB, and (PK_{ID}, SK_{ID}) are the prerequisite for generating accounts.

Reputation-based CDA auction stage PU and GU send their own quotations, demand and reputation to CVPP. CVPP matches transactions according to the reputation-based CDA auction mechanism, and continuously feeds back matching information to each participant entities, so as to make timely quotation revisions. Once the transaction is matched successfully, CVPP will broadcast the transaction information in the CTCB of the alliance blockchain. At this time, it is not recorded in the block.

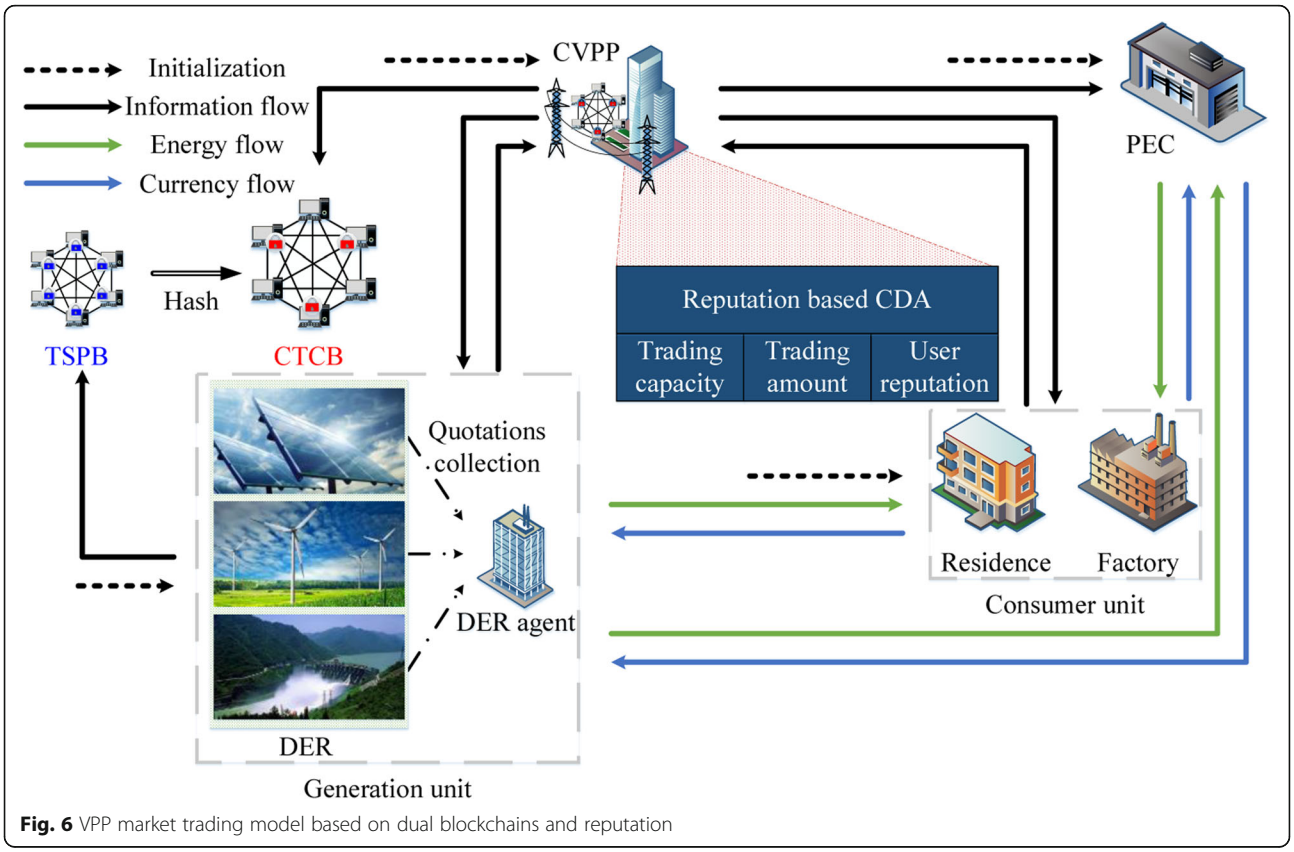


Fig. 6 VPP market trading model based on dual blockchains and reputation

Only when all stages are completed will the transaction information be stored in the block.

After the auction ends, the unmatched information will be sent to PTC, and PTC will be responsible for related transactions. More details about the reputation-based CDA auction mechanism will be introduced in subsequent sections. It should be noted that when DER agents aggregate all local DER quotations and submit them to CVPP, their DERs have been continuously uploading production information to their private blockchain TSPB.

Transaction and settlement stage The successfully matched GU checks the transaction information, and after confirmation is correct, it supplies power to the corresponding PU according to the determined transaction power. After the PU receives the determined amount of electricity, it pays energy coins at the price negotiated in advance. In this process, any party who fails to complete the transaction as required will be punished economically by the system, and a certain amount of reputation value will be deducted. PU that has not successfully matched can choose to sell the excess electricity to PTC, thereby obtaining a certain amount of energy currency as a reward. At the same time, the PU can also choose to store electrical energy in its own energy storage equipment and wait for the next round of auctions. The unmatched power users directly purchase electricity from PTC.

Energy currency is the only transaction currency of this system. When the user registers for the first time, the system will give a certain amount of energy currency to the user. When users have insufficient energy coins, they can purchase energy coins from PTC or DER agents. In addition, users with good reputation have the opportunity to participate in the consensus process of the system, thereby obtaining energy coins rewarded by the system.

System implementation

Hybrid attribute proxy re-encryption scheme based on ciphertext policy

Attribute-based proxy re-encryption (ABPRE) [44] is an encryption mode. Proxy can convert ciphertext encrypted based on ciphertext policy (CP) or key policy (KP) into new re-encrypted ciphertext under the authorization of the data owner. The process does not change the plaintext information. However, most ABPRE schemes have efficiency problems when applied to incentive scenarios, because these schemes need to calculate the key components of all internal attributes in the re-encryption key generation stage, even if the data applicant has only one attribute. This working mechanism is likely to cause waste of computing power and time. To solve this problem, we combine the cost-effective identity-based encryption algorithm (IBE) [45] with ABPRE, and propose a hybrid attribute proxy re-encryption algorithm based on ciphertext strategy (CP-HAPRE).

CP-HAPRE consists of a tuple (*Setup*, *KGen*, *Enc*, *RKGen*, *ReEnc*, *Sig*, *Dec*, *ReDec*). In the actual VPP security scheduling information sharing model, DER uses the ciphertext strategy attribute to encrypt the information recorded by the tamper-proof meter in real-time and upload it to the blockchain. When VPP requires DER to provide information for related scheduling operations, the DER agent uses the *CP* secret key SK_S and the ID of the VPP to generate a re-encryption secret key $RK_{S\to ID_{VPP}}$, and then uses $RK_{S\to ID_{VPP}}$ to generate a re-encrypted ciphertext $CT_{ID_{VPP}}$, which VPP can decrypt with the private key generated by its own ID. The combination of this algorithm and the blockchain ensures that VPP can obtain real and safe DER information. VPP performs a series of calculations and predictions based on this information, and finally obtains a reliable scheduling scheme. The variable notations involved in the CP-HAPRE scheme are shown in Table 1. The following is a specific program description:

Step1: System initialization

$Setup(1^{\ell}, U) \to (GP, MSK)$: The verification organization executes the algorithm. Input the system safety parameters ℓ and the system attribute set U, and then construct two multiplicative cyclic groups G and G_T of order p, with p being a prime number. The g, g_1, g_2 and g_3 are all generators of G, G and G_T satisfy the bilinear mapping relationship $e: G \times G \to G_T$. Randomly select an element $\alpha \in Z_p^*$ and define three hash functions $H_1: (0,1)^* \to G$, $H_2: G_T \to G$, $H_3: G_T \to Z_p^*$. Finally, output the system public parameters GP and the master key MSK.

Table 1 Symbol definition of our system implementation

Symbol	Definition
ℓ, M	System security parameters, Plaintext
U, S	System/ User attribute set
GP, GP_{IBE}	System/IBE public parameters
MSK, MSK_{IBE}	System/IBE master secret key
SK_S	CP key
PK_{ID}, SK_{ID}	IBE public/ private key
(A, ρ)	Shared structure
$RK_{S\to ID_{VPP}}$	Re-encryption key
CT_A, $CT_{ID_{VPP}}$	Initial/ Re-encrypted ciphertext

$$GP = \left(p, g, g_1, g_2, g_3, e(g,g)^{\alpha}, H_1, H_2, H_3\right), MSK = \alpha \tag{1}$$

It should be noted that the system public parameters and master key of *IBE* have been included in Eq. 1. The specific *IBE* system public parameters GP_{IBE} and master key MSK_{IBE} are as follows.

$$GP_{IBE} = (p, g_1, e(g,g)^{\alpha}, H_1, H_3), MSK_{IBE} = MSK = \alpha \tag{2}$$

From the master key MSK_{IBE}, the system public key is $PK_{IBE} = g_1^{\alpha}$.

Step2: Key generation

$KGen_{IBE}(GP_{IBE}, MSK_{IBE}, ID) \rightarrow SK_{ID}$: Input the *IBE* system public parameters, master key MSK_{IBE} and user $ID \in (0,1)^*$, and output the public-private key pair corresponding to the *ID*.

$$\begin{cases} PK_{ID} = H_1(ID) \\ SK_{ID} = g_1 H_1(ID)^{\alpha} \end{cases} \tag{3}$$

$KGen_{CP}(GP, MSK, S) \rightarrow SK_S$: Input the system public parameters *GP*, master key *MSK* and DER attribute set $S = \{a_1, \ldots, a_{|S|}\} \subseteq U$, $|S|$ means the base of *S*. Randomly choose $t \in Z_p^*$, then calculate

$$K_0 = g^{\alpha} g_1^t, K_1 = g^t, K_{i,2} = H_1(a_i) g_2^{-t} \tag{4}$$

The verification organization outputs the key of the attribute set *S* as

$$SK_S = \left(K_0, K_1, \left\{K_{i,2}\right\}_{i=1}^{|S|}\right) \tag{5}$$

Step3: Data encryption

$Enc_{CP}(GP, (A,\rho), M) \rightarrow CT_A$: Input system public parameters *GP*, access structure (A,ρ) (A is a $l \times n$ matrix, and the function $\rho : [l]$ maps each row of the matrix A to an attribute) and plaintext information $M \in G_T$. Choose a random element $s \in Z_p^*$ and form a vector $\vec{v} = (s, y_2, \ldots y_n)$. $y_2, \ldots y_n$ is also randomly selected from Z_p^*. For the *i-th* row A_i of A, we have $\lambda_i = \vec{v} A_i (i = 1, 2, \ldots, l)$. Randomly select l parameters $t_1, t_2, \ldots, t_l \in Z_p^*$, and calculate the following formula.

$$\begin{cases} W = Me(g,g)^{\alpha s}, W_0 = g^s, \\ W_{i,1} = g_1^{\lambda_i} g_2^{t_i}, W_{i,2} = H_1(\rho(i))^{-t_i}, W_{i,3} = g^{t_i} \end{cases} \tag{6}$$

CP-HAPRE provides two encryption options for DER: When DER only wants to share data with DER agents and does not want to re-encrypt the data, then the output ciphertext is

$$CT_A = \left(W, W_0, \left\{W_{i,1}, W_{i,2}, W_{i,3}\right\}_{i=1}^{l}\right) \tag{7}$$

When DER needs to re-encrypt the data, it must calculate $W_4 = g_3^s$, and the final output ciphertext is

$$CT_A = \left(W, W_0, \left\{W_{i,1}, W_{i,2}, W_{i,3}\right\}_{i=1}^{l}, W_4\right) \tag{8}$$

Since only the ciphertext referred to in Eq. 8 supports re-encryption, we will focus on the ciphertext.

Step4: Re-encryption key generation

$RKGen(GP, SK_S, PK_{ID_{VPP}}) \rightarrow RK_{S \rightarrow ID_{VPP}}$: The algorithm inputs the system public parameters *GP*, the *CP* key SK_S of DER and the public key $PK_{ID_{VPP}}$ of VPP. DER agent randomly selects elements $t', s' \in Z_p^*$ and calculates

$$\begin{cases} RK_0 = K_0 g_3^{t'}, RK_1 = K_1, \left\{RK_{i,2} = K_{i,2}\right\}_{i=1}^{l} \\ RK_3 = H_2\left(e(g,g)^{\alpha s'}\right) g^{t'}, RK_4 = PK_{ID_{VPP}}^{s'}, RK_5 = g^{s'} \end{cases} \tag{9}$$

Finally, the complete re-encryption key is shown in Eq. 10

$$RK_{S \rightarrow ID_{VPP}} = \left(RK_0, RK_1, \left\{RK_{i,2}\right\}, RK_3, RK_4, RK_5\right) \tag{10}$$

Step5: Re-encryption

$ReEnc(GP, RK_{S \rightarrow ID_{VPP}}, CT_A) \rightarrow CT_{ID_{VPP}}$: Input the system public parameters *GP*, re-encryption key $RK_{S \rightarrow ID_{VPP}}$ and ciphertext CT_A. If the attribute set *S* satisfies the access structure (A,ρ), let $I = \{i : \rho(i) \in S\}$, then there is a coefficient $\{\omega_i \in Z_p^*\}_{i \in I}$, so that $\Sigma_{i \in I} \omega_i A_i = (1, 0, \ldots, 0)$. Then, the DER agent calculates

$$V = \frac{e(W_0, RK_0)}{\prod_{i \in I} \left(e\left(W_{i,1}, RK_1\right) e\left(W_{i,2}, g\right) e\left(W_{i,3}, RK_{j,2}\right)\right)^{\omega_i}} \tag{11}$$

where j is the index of attribute $\rho(i)$ in *S*. After finding *V*, the DER agent re-encrypts the ciphertext

$$W' = W/V, W_0' = RK_3, W_1' = RK_4, W_2' = RK_5, W_3' = W_4 \tag{12}$$

The final re-encrypted ciphertext output by the DER agent is

$$CT_{ID_{VPP}} = \left(W', W_0', W_1', W_2', W_3'\right) \tag{13}$$

Step6: Digital signature

$Sig(GP, W', SK_{ID_{proxy}}) \rightarrow \sigma$: Input the system public parameters *GP*, part of the re-encrypted ciphertext W' and

the private key $SK_{ID_{proxy}}$ of the DER agent. DER agent randomly selects two random numbers $k_1, k_2 \in Z_p^*$, and then calculates

$$\begin{cases} P_1 = g_1^{k_1}, P_2 = g_1^{k_2} \\ q = e(P_1, P_2), H = H_3\left(W^{'}, q\right) \\ U = SK_{ID_{proxy}}^{H} P_1^{k_2} \end{cases} \tag{14}$$

The final digital signature output by the DER agent is $\sigma = (U, q)$.

Step7: Ciphertext decryption

$Dec(GP, CT_A, SK_S) \rightarrow M$: Input the system public parameters GP, ciphertext CT_A and DER CP key SK_S. If the attribute set S satisfies the access structure (A, ρ), for $I = \{i : \rho(i) \in S\}$, there is a coefficient $\{\omega_i \in Z_p^*\}_{i \in I}$, such that $\sum_{i \in I} \omega_i A_i = (1, 0, \ldots, 0)$. Decryption algorithm calculation

$$M^{'} = \frac{e(W_0, K_0)}{\prod_{i \in I} \left(e\left(W_{i,1}, K_1\right) e\left(W_{i,2}, g\right) e\left(W_{i,3}, K_{j,3}\right)\right)^{\omega_i}} \tag{15}$$

where j is the index of attribute $\rho(i)$ in S. The plaintext information is $M = W/M^{'}$.

Step8: Re-encrypted ciphertext decryption

$ReDec(GP, CT_{ID_{VPP}}, SK_{ID_{VPP}}, PK_{IBE}, PK_{ID_{proxy}}, \sigma) \rightarrow M$: Input system public parameters GP, re-encrypted ciphertext $CT_{ID_{VPP}}$, VPP IBE private key $SK_{ID_{VPP}}$, system IBE public key PK_{IBE}, DER agent's IBE public key $PK_{ID_{proxy}}$ and re-encrypted ciphertext signature σ. First, VPP needs to calculate $H = H_3(W^{'}, q)$, then verify if $e(U, g_1) = qe(PK_{IBE} PK_{ID_{proxy}}^{H}, g_1)$ is established. if it is not established, resend the data access request to the DER agent, if it is established, calculate

$$\frac{e\left(gSK_{ID_{VPP}}, W_2^{'}\right)}{e\left(g, W_1^{'}\right) e\left(g_1, W^{'}\right)} = e(g, g)^{\alpha s^{'}} \tag{16}$$

and

$$W_0^{'} / H_2\left(e(g, g)^{\alpha s^{'}}\right) = g^{t^{'}} \tag{17}$$

Finally, VPP recovers the plaintext information $M = W^{'} e(g^{t^{'}}, W_3^{'})$.

Correctness verification

We first prove the correctness of the initial ciphertext decryption. When the ciphertext is CT_A and the key is SK_S, if the attribute set S satisfies the access structure (A, ρ), $\sum_{i \in I} \omega_i \lambda_i = s$ can be obtained, therefore

$$\begin{aligned} M^{'} &= \frac{e(W_0, K_0)}{\prod_{i \in I} \left(e\left(W_{i,1}, K_1\right) e\left(W_{i,2}, g\right) e\left(W_{i,3}, K_{j,2}\right)\right)^{\omega_i}} \\ &= \frac{e\left(g^s, g^{\alpha} g_1^{t}\right)}{\prod_{i \in I} \left(e\left(g_1^{\lambda_i} g_2^{t_i}, g^t\right) e\left(H_1(\rho(i))^{-t_i}, g\right) e\left(g^{t_i}, H_1(\rho(i)) g_2^{-t}\right)\right)^{\omega_i}} \\ &= \frac{e(g^s, g^{\alpha}) e(g^s, g_1^t)}{\prod_{i \in I} \left(e\left(g_1^{\lambda_i}, g^t\right) e(g^{t_i}, g_2^t) e\left(H_1(\rho(i))^{-t_i}, g\right)\right)^{\omega_i}} \cdot \\ &\quad \frac{1}{\prod_{i \in I} \left(e\left(g_2^{t_i}, g^{-t}\right) e\left(g^{t_i}, H_1(\rho(i))\right)\right)^{\omega_i}} \\ &= \frac{e(g^s, g^{\alpha}) e(g^s, g_1^t)}{e(g_1, g)^{t \sum_{i \in I} \omega_i \lambda_i}} \\ &= \frac{e(g^s, g^{\alpha}) e(g^s, g_1^t)}{e(g_1, g)^{ts}} \\ &= e(g^s, g^{\alpha}) \end{aligned} \tag{18}$$

Then, DER can get the plaintext message by calculating $M = W/M^{'} = Me(g^s, g^{\alpha})/e(g^s, g^{\alpha}) = M$.

Next, we prove the correctness of the decryption of the re-encrypted ciphertext. If the attribute set satisfies the access structure, the DER agent can calculate

$$\begin{aligned} V &= \frac{e(W_0, RK_0)}{\prod_{i \in I} \left(e\left(W_{i,1}, RK_1\right) e\left(W_{i,2}, g\right) e\left(W_{i,3}, RK_{j,2}\right)\right)^{\omega_i}} \\ &= \frac{e\left(g^s, g^{\alpha} g_1^t g_3^{t^{'}}\right)}{\prod_{i \in I} \left(e\left(g_1^{\lambda_i} g_2^{t_i}, g^t\right) e\left(H_1(\rho(i))^{-t_i}, g\right) e\left(g^{t_i}, H_1(\rho(i)) g_2^{-t}\right)\right)^{\omega_i}} \\ &= \frac{e(g^s, g^{\alpha}) e\left(g^s, g_1^t\right) e\left(g^s, g_3^{t^{'}}\right)}{\prod_{i \in I} \left(e\left(g_1^{\lambda_i}, g^t\right) e\left(g_2^{t_i}, g^t\right) e\left(H_1(\rho(i))^{-t_i}, g\right)\right)^{\omega_i}} \cdot \\ &\quad \frac{1}{\prod_{i \in I} \left(e\left(g^{t_i}, g_2^{-t}\right) e\left(g^{t_i}, H_1(\rho(i))\right)\right)^{\omega_i}} \\ &= \frac{e(g^s, g^{\alpha}) e\left(g^s, g_1^t\right) e\left(g^s, g_3^{t^{'}}\right)}{e(g_1, g)^{t \sum_{i \in I} \omega_i \lambda_i}} \\ &= \frac{e(g^s, g^{\alpha}) e\left(g^s, g_1^t\right) e\left(g^s, g_3^{t^{'}}\right)}{e(g_1, g)^{ts}} \\ &= e(g^s, g^{\alpha}) e\left(g^s, g_3^{t^{'}}\right) \end{aligned} \tag{19}$$

Then, the DER agent continues to calculate

$$\begin{aligned} W^{'} &= W/V = Me(g^s, g^{\alpha})/e(g^s, g^{\alpha}) e\left(g^s, g_3^{t^{'}}\right) \\ &= M/e\left(g^s, g_3^{t^{'}}\right) \end{aligned} \tag{20}$$

In the re-decryption algorithm, VPP first needs to be verified

$$\begin{aligned} e(U,g_1) &= e\left(SK_{ID_{proxy}}^{H}P_1^{k_2},g_1\right) \\ &= e\left(SK_{ID_{proxy}}^{H},g_1\right)e\left(P_1^{k_2},g_1\right) \\ &= e\left(g_1H_1\left(ID_{proxy}\right)^{\alpha H},g_1\right)e\left(P_1,g_1^{k_2}\right) \\ &= e\left(g_1^{\alpha}H_1\left(ID_{proxy}\right)^{H},g_1\right)e(P_1,P_2) \\ &= qe\left(PK_{IBE}PK_{ID_{proxy}}^{H},g_1\right) \end{aligned} \tag{21}$$

Then, calculate

$$\begin{aligned} \frac{e\left(gSK_{ID_{VPP}},W_2^{'}\right)}{e\left(g,W_1^{'}\right)e\left(g_1,W_2^{'}\right)} &= \frac{e\left(gg_1H_1(ID_{VPP})^{\alpha},g^{s^{'}}\right)}{e\left(g,H_1(ID_{VPP})^{s^{'}}\right)} \\ &= e(g,g)^{\alpha s^{'}} \end{aligned} \tag{22}$$

and

$$\begin{aligned} W_0^{'}/H_2\left(e(g,g)^{\alpha s^{'}}\right) &= H_2\left(e(g,g)^{\alpha s^{'}}\right)g^{t^{'}}/H_2\left(e(g,g)^{\alpha s^{'}}\right) \\ &= g^{t^{'}} \end{aligned} \tag{23}$$

Finally, VPP can get the plaintext information that it wants to access by calculating $M = W^{'}e(g^{t^{'}}, W_3^{'})$.

Reputation-based continuous double auction mechanism

CDA is an effective market mechanism to solve the problem of distributed resource allocation. Distributed resource allocation usually involves multiple participants, and each participant wants to maximize his own revenue. CDA improves the overall efficiency by constantly matching the quotations of transaction participants. According to the identity of the participant who submitted the quotation, CDA stores the received quotations in the Bid List (BL) of the buyer and the Offer List (OL) of the seller, respectively. In BL, the sorting rule is price from high to low (descending order); on the contrary, the sorting rule in OL is sorting from low to high price (ascending order). The buyer's highest quotation is called the optimal buying price, and the seller's lowest quotation is called the optimal selling price. Only when the optimal buying price is greater than or equal to the optimal selling price, the buyer and seller can match successfully. To maximize the interests of each participant, the transaction price is the average of the optimal buying price and the optimal selling price. It should be noted that CDA is matched according to the matching rule of "price first, time first". When the price is the same, it will be matched with the participant who submitted the quotation earlier.

Table 2 Market segmentation machine based on reputation

Buyer/Seller reputation values	Level	Matchable level range
[0,2]	1	3
(2,4]	2	3, 2
(4,6]	3	3, 2, 1

Reputation-based trading system can ensure that participants have good market behavior, which is composed of market segmentation mechanism and priority-value-order mechanism [41]. The market segmentation mechanism divides the corresponding list according to the reputation level. Its purpose is to enable the buyer or seller with high reputation values to obtain more and better quotations. The detailed market segmentation mechanism is shown in Table 2. Priority-value-order mechanism is a sort method based on user reputation and quotation. The reputation-based CDA mechanism proposed in this paper mainly integrates the reputation-based market segmentation machine into the CDA mechanism. The sorting mechanism still uses the original CDA sorting mechanism instead of the reputation-based priority-value-order mechanism.

The reputation-based CDA mechanism includes three entities: buyers, sellers and auctioneers. In this paper, *PU* such as houses and factories represent buyers, *GU* such as photovoltaic power plants and hydroelectric power plants represent sellers, and CVPP assumes the responsibility of auctioneer. At the beginning of the trading cycle, *PU* and *GU* submit the initial $B_{i,k}^1$ and $S_{j,k}^1$ to CVPP, respectively. $B_{i,k}^1$ represents the transaction information submitted by PU_i for the first time in the *k-th* transaction cycle. Similarly, $S_{j,k}^1$ means that the transaction information submitted by GU_j for the first time in the *k-th* transaction cycle. The concrete content of the two is as follows:

$$\begin{cases} B_{i,k}^1 = \left(E_{i,d}^1, P_{i,b}^1, RS_i^k, Sig_i^1\right) \\ S_{j,k}^1 = \left(E_{j,s}^1, P_{j,o}^1, RS_j^k, Sig_j^1\right) \end{cases} \quad i,j,k = 1,2,\cdots,n \tag{24}$$

In the formula, $E_{i,d}^1$, $P_{i,b}^1$ represent the power demand and bid price of PU_i in the first round of trading, RS_i^k and Sig_i^1 represent the reputation value of PU_i in the *k-th* trading cycle and the signature of the submitted information. $E_{j,s}^1$ and $P_{j,o}^1$ represent the power supply and the quoted price of GU_j in the first round of trading. The definitions of RS_j^k and Sig_j^1 are similar to the above.

After receiving $B_{i,k}^1$ and $S_{j,k}^1$ submitted by PU_i andGU_j, the CVPP matches the buyer and the seller according to the reputation-based CDA mechanism. First, CVPP constructs a matching list by checking

the identity and reputation value of the information submitter. Different from the traditional CDA mechanism, a reputation-based market segmentation mechanism is introduced here. According to this mechanism, we further divide BL and OL. The specific division is shown in Eq. 25

$$\begin{cases} BL_1^t = \{RL_i = 1\} \\ BL_2^t = \{RL_i = 2\} \\ BL_3^t = \{RL_i = 3\} \\ OL_1^t = \{RL_j = 3\} \\ OL_2^t = \{RL_j = 3, RL_j = 2\} \\ OL_3^t = \{RL_j = 3, RL_j = 2, RL_j = 1\} \end{cases} \quad t, i, j = 1, 2, \cdots, n \tag{25}$$

It can be seen that both BL and OL are divided into three lists, where t represents the number of rounds of the transaction, RL_i represents the reputation level of PU_i, and the relationship between RL and RS is shown in Table 2. Only part of the symbol definitions are explained here, other symbol definitions are similar to the explained symbols. $BL_1^t = \{RL_i = 1\}$ means that BL_1^t only contains PU with $RL = 1$. $OL_1^t = \{RL_j = 3\}$ means that OL_1^t only contains GU with $RL = 3$. After the construction of the matching list, the CVPP performs matching between lists according to Table 2, that is, BL_l^t matches for OL_l^t transaction matching ($l = 1, 2, 3$).

At the beginning of the trading cycle, both PU and GU want to obtain more benefits, so the initial purchase price of PU will be the lowest, and the initial sale price of will be the GU highest. In this case, the number of successful trade matches in the first round will be relatively small. For more matches in subsequent transactions, after each round of transactions, CVPP needs to do two things. The first thing is to match the successfully matched PU_i and GU_j for transaction, and upload the transaction information Tx_{ij} to the blockchain, Tx_{ij} is as follow

$$Tx_{ij} = \left(ID_i, ID_j, RS_i^k, RS_j^k, E_{ij}, P_{ij}, Sig_i, Sig_j\right) \tag{26}$$

ID_i represents the identity of PU_i, E_{ij} represents the capacity of electricity traded between PU_i and the GU_j, and P_{ij} represents the trading amount between the two.

The second thing is to calculate the competitive equilibrium price E_p and announce it to the unmatched transaction parties. The calculation method of E_p is as follows

$$E_p = \sum_{s=A,A+1,\ldots,B}^{B-A} (\omega_s p_s) \tag{27}$$

A represents the estimated starting transaction number, B represents the ending transaction number, s represents an increasing integer from A to B, p_s represents the transaction price of the s-th transaction, and ω_s represents the weight of the transaction price. The sum of ω_s in the estimation range $[A, B]$ is 1, and $\omega_{s+1} = \beta\omega_s$, β represents the weight coefficient.

Before the start of the next round of trading, PU and GU which have not yet been matched will recalculate their quotations $P_{i,b}^t$ and $P_{j,o}^t$ according to E_p, respective. The calculation formula is as follows

$$\begin{cases} P_{i,b}^t = \begin{cases} P_{i,b}^1, t = 1 \\ P_{i,b}^{t-1} + \eta\left|E_p - P_{i,b}^{t-1}\right|, t \geq 2 \end{cases} \\ P_{j,o}^t = \begin{cases} P_{j,o}^1, t = 1 \\ P_{j,o}^{t-1} - \eta\left|E_p - P_{j,o}^{t-1}\right|, t \geq 2 \end{cases} \end{cases} \tag{28}$$

The value range of η is $[0, 1]$. From the above formula, it is not difficult to see that the constraint condition of $P_{i,b}^t$ is $P_{i,b}^1 \leq P_{i,b}^2 \leq \cdots \leq P_{i,b}^t$, and the constraint condition of $P_{j,o}^t$ is $P_{j,o}^1 \geq P_{j,o}^2 \geq \cdots \geq P_{j,o}^t$. In addition, $P_{j,o}^t$ should be greater than the power generation cost of GU_j.

After calculating the bid price of the next round of transaction, both parties submit the transaction information of the new round as follows

$$\begin{cases} B_{i,k}^t = \left(E_{i,d}^t, P_{i,b}^t, RS_i^k, Sig_i^t\right) \\ S_{j,k}^t = \left(E_{j,s}^t, P_{j,o}^t, RS_j^k, Sig_j^t\right) \end{cases} \quad t \geq 2; i, j, k = 1, 2, \ldots, n \tag{29}$$

CVPP receives the transaction information and looks at the current total matching time T_M of each round of transactions. If $T_M < T$, T represents the total duration of each transaction cycle, a new round of matching will be performed. If $T_M \geq T$, the period of the transaction ends, and the transaction information is submitted to the power trading center. So far, the power required by PU is directly provided by the power grid controlled by PTC. GU can choose to sell the remaining power to PTC at a low price, or store it in its own storage device, and then trade in the next trading cycle.

Algorithm 1: Reputation Based CDA Algorithm

// T_M is the sum of matching time of previous rounds.
1: **Input:** T
2: **Initialization:** $B_{i,k}^t \to \left(BL_1^t, BL_2^t, BL_3^t\right)$, $S_{j,k}^t \to \left(OL_1^t, OL_1^t, OL_1^t\right)$, $1 \to t$, $1 \to flag$, $0 \to trigger$;
3: **while** $flag$ and $\sim trigger$ **do**
4: **if** some unexpected events happen in electricity trading **then**
5: $1 \to trigger$, and CVPP terminates the procedure and prepares to restart Algorithm 1.
6: **else**
7: Based on CDA matching rules, CVPP generates Tx_{ij} and E_p , and then broadcasts them;
8: Based on E_p , PU_i recalculate $P_{i,b}^{t+1}$ to renew $B_{i,k}^{t+1}$,and submit $B_{i,k}^{t+1}$ to CVPP;
9: Based on E_p , GU_j recalculate $P_{j,o}^{t+1}$ to renew, $S_{j,k}^{t+1}$ and submit $S_{j,k}^{t+1}$ to CVPP;
10: $t+1 \to t$;
11: **if** $T_M \geq T$, **then**
12: CVPP sends $B_{i,k}^t$ and $S_{j,k}^t$ to PTC;
13: The system calculates the RS^{k+1} for all trading participants;
14: $0 \to flag$, $t-1 \to t$.
16: **end if**
17: **end if**
18: **end while**
19: **Output:** Tx_{ij} , E_p , $B_{i,k}^{t+1}$, $S_{j,k}^{t+1}$, RS^{k+1}

After each round of the trading cycle, the system will conduct a new round of reputation value evaluation based on the trading performance of each participant in this cycle. If some unexpected event occurs during the energy transaction, this will activate the trigger. Then, CVPP restarts Algorithm 1 and re-initializes the parameters.

Bitcoin has opened the 1.0 era of blockchain, and Ethereum integrated with smart contract has opened the 2.0 era of blockchain. Smart contract gives the blockchain more possibilities, so that the blockchain is no longer restricted to the financial field. Algorithm 1 is the pseudo code of reputation-based CDA algorithm. The actual code needs to be deployed to the blockchain network in the form of smart contract.

Generation of data blocks

The system mentioned in this article is mainly composed of a globally maintained transaction consortium blockchain and multiple scheduling private blockchains constructed by VPP itself. On the private chain constructed by VPP, we uniformly adopt the strong-leader Raft consensus mechanism [46] to generate new data blocks. There are three identities of leader, candidate and follower in the Raft consensus mechanism. Under normal working conditions, there is only one leader, and all other nodes are followers. The difference between a candidate and a follower is that when the leader cannot function normally, a new leader will be selected from the candidates. Here, we will briefly explain the workflow of using the Raft consensus mechanism to generate new blocks in the scheduling of private blockchains. First, the leader node reviews the data from DER and sends it to the DER agent for re-inspection. Secondly, the DER agent rechecks the data sent by the leader node and returns the result of the recheck to the leader node. Finally, the leader node packs the data that has passed the verification and re-inspection into blocks and uploads it to the private blockchain, and sends its block hash value to the transaction consortium blockchain.

As mentioned above, PoW is usually a consensus algorithm adopted by public blockchain and has the highest security. However, its work efficiency is low and resource consumption is large, and it cannot meet the

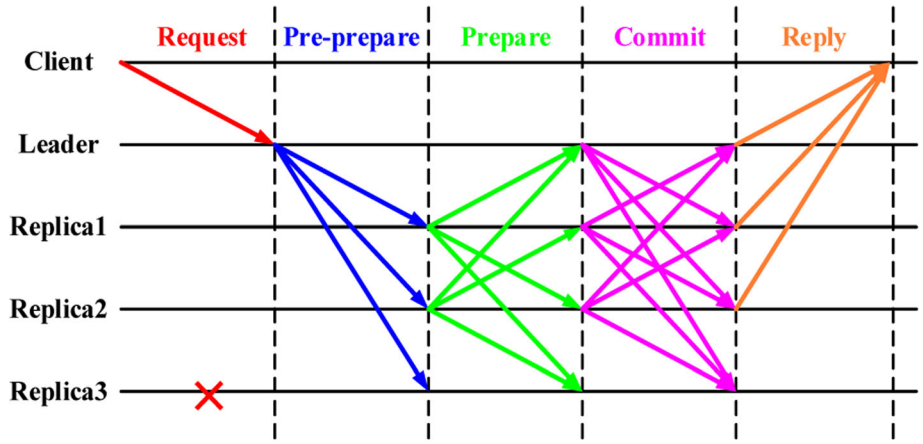


Fig. 7 Simplified PBFT algorithm consensus flow chart

real-time needs of users. Although PoS reduces the resource consumption problem of PoW to a certain extent, it has the problem of excessive concentration. Therefore, the consortium blockchain usually uses the PBFT consensus algorithm to complete the generation of new blocks. The transaction consortium blockchain proposed in this paper uses the PBFT consensus algorithm to generate new blocks. The difference is that the consensus node in this article is constantly changing. According to the reputation value of participating nodes, the system randomly selects a certain number of nodes to form a consensus committee. Before each transaction cycle in the system starts, a new consensus committee will be generated, and the working time of the consensus committee is the transaction cycle time. After the transaction cycle ends, the system will reconfigure a new consensus committee based on the current node reputation value. It should be noted that the total number of nodes in the consensus committee remains unchanged, except for the first configuration of the committee consensus nodes are all new nodes, and subsequent reconfigurations only randomly replace a certain number of old nodes. After the consensus committee is generated, it starts to run the PBFT consensus algorithm. There are two types of consensus nodes in the PBFT algorithm, leader nodes and replica nodes. There is only one leader node in the consensus process, and the others are replica nodes. The specific PBFT distributed consensus process is divided into five stages: request, pre-prepare, prepare, commit and reply. The three stages of pre-prepare, prepare and commit determine the correctness of the final consensus result. The simplified PBFT algorithm consensus process has 5 stages, which are shown in Fig. 7.

Request stage when a client sends a request to any node, the consensus node that first activates the node service operation is called the leader.

Pre-prepare stage after receiving the information request from the client, the leader node broadcasts the execution sequence of the transaction to each replica node.

Table 3 Security comparison between our scheme and some references

Security Features	Ref. [24]	Ref. [25]	Ref. [26]	Our scheme
Authenticity	×	√	×	√
Confidentiality	×	×	√	√
Transparency	√	√	√	√
Traceability	√	√	√	√
Immutability	√	√	√	√
Non-repudiation	×	×	√	√

Prepare stage when each replica node receives a message from the leader node, there are two different options, the first is to accept and spread the message again, the second is to not accept and refuse to make any response. In Fig. 7, replica1 and replica2 choose the first option, and replica3 chooses the second option. At this time, the replica3 may be down or maliciously hijacked.

Commit stage if each consensus node receives $(n - f)$ identical requests in the "prepare stage", it will enter the "commit stage" and broadcast the commitment information throughout the network. n is the total number of consensus nodes, f is the maximum number of Byzantine nodes that can be accommodated in the consensus node.

Reply stage if the consensus node collects enough same commitment information, the node will feed it back to the client. If and only if $f \leq (n - 1)/3$ [28], the consensus result is trustworthy.

The verified information will be constructed into a new block, and then linked to the end of the current transaction consortium blockchain, the block height adds 1. In order to encourage nodes to participate more actively in the consensus process, all selected consensus nodes can receive energy coins issued by the system as rewards during the block generation process.

Analysis and evaluation

System security analysis

In the scheduling and transaction process of VPP, the security of data sharing and storage process is very important for the entire system. In this section, we compare with the existing schemes in terms of system security, and the comparison results are shown in Table 3. The comparison results show that the security of this scheme is better than other schemes, and it is more suitable for data sharing and storage in VPP. In the meantime, we theoretically explained how to uses blockchain technology to realize the security features in the process of data sharing and storage.

Authenticity This paper repeatedly mentions that VPP is a data-driven technology. If VPP cannot get real data, then all subsequent operations are meaningless. Most of the existing literatures default that the data on the blockchain is real. In nature, blockchain technology can only guarantee the authenticity of the data on the chain, but cannot guarantee the authenticity of the input data. To ensure the authenticity of the input data, this paper proposes to use tamper-proof smart metering equipment for data collection at the data end, and upload the collected data to the local blockchain in real time. So far,

the data on the chain and off-chain are authentic, and VPP can process the data with confidence.

Confidentiality Tamper proof intelligent metering equipment will upload users' various data and information in real time. If this information are not encrypted before uploading, it is easy to cause user privacy disclosure. When the DER want to share encrypted data with VPP, it needs to download the ciphertext CT_A and decrypt it, and then encrypt it with the public key $PK_{ID_{VPP}}$ of the VPP. In this case, encrypting data brings a lot of extra cost to the DER, which is not worth it. In order to solve this problem, this paper uses proxy re-encryption technology to re-encrypt CT_A, so that CT_A can be accessed by VPP without decrypting through the DER. This method effectively reduces the cost of the data owner and protects the confidentiality of the data.

Transparency and Traceability The data stored on the blockchain is open and transparent to all nodes that join. Although for confidentiality of the data, the stored here may be ciphertext CT_A, but it can be passed to the data owner submit an application to gain access. Furthermore, the public and private keys (PK_{ID}, SK_{ID}) in this paper are generated based on identity, and each piece of information on the blockchain will be closely linked to its own (PK_{ID}, SK_{ID}). It is also worth noting that the blockchain is linked by a hash pointer to the blocks containing the previous block hash. The characteristics of the hash function make the information stored in the blockchain not lost and falsify. Under the combined effect of these conditions, the information stored on the blockchain is traceable.

Immutability and Non-repudiation Immutability on the blockchain is related to the adopted consensus mechanism. In the dual blockchains architecture used in this paper, the private blockchain uses the strong leader Raft consensus algorithm, and the consortium blockchain uses the PBFT consensus algorithm. In the private blockchain, the leader may tamper with the data. To avoid this situation, we store the hash of the private chain in the consortium blockchain, and rely on the unforgeability of the consortium blockchain to ensure the non-tamperable modification of the private blockchain. Since the consensus nodes of the consortium blockchain are selected based on reputation, and nodes with higher reputation can reap more benefits, more than one-third of high-reputation consensus nodes attacking the alliance blockchain at the same time violate their own interests and are unlikely to happen. Therefore, it can guarantee the unforgeability of consortium blockchain and private blockchain. Non-repudiation is achieved by digital signatures. The generation of each transaction requires the user to sign the transaction. Once the user denies, we can use his public key PK_{ID} to verify the correctness of the signature σ to achieve the purpose of accountability.

CP-HAPRE algorithm performance evaluation

Computational overhead evaluation

The computational cost of the algorithm is mainly composed of four operations: encryption, re-encryption, decryption and re-decryption. In the literature we consulted, we did not find similar literature with the same ideas as ours in terms of energy. In order to better evaluate the algorithm performance, we found papers using similar ideas to solve information security problems in cloud, Internet of things and Internet of vehicles for performance comparison. These papers are represented in references [47, 48] and [49], the computational cost of the CP-HAPRE algorithm is compared and analyzed. The comparison results of computational overhead are shown in Table 4 with these references. In this table, T_P represents the time required for the bilinear pairing operation, and T_E represents the exponential operation time. Since other operations time is very small compared with these two operations, we ignore the operation time of other operations here. In addition, $|l|$ represents the number of attributes in the access structure, and $|I|$ represents the number of attributes that satisfy the access structure.

T_p: bilinear pairing operation time; T_E: exponential operation time; $|l|$: the number of attributes in the access structure; $|I|$: the number of attributes that satisfy the access structure

A test run was performed on a computer with an Intel i5 processor CPU with a running memory of 8G and a frequency of 3.0GHz. Finally, it was concluded that the above two operations took 1.57ms and 0.31ms respectively. Based on this data, we can get a comparison

Table 4 Comparison of computational overhead

Scheme	Encryption	Re-encryption	Decryption	Re-decryption
Ref. [47]	$T_p+(3\|l\|+6)T_E$	$(2\|l\|+3)T_P$	$(2\|l\|+3)T_P+T_E$	$(2\|l\|+4)T_P+T_E$
Ref. [48]	$(6\|l\|+3)T_E$	$(8\|l\|+3)T_P+2T_E$	$(4\|l\|+2)T_P$	$2T_P+(4\|l\|+1)T_E$
Ref. [49]	$T_p+(3\|l\|+2)T_E$	$(4\|l\|+9)T_P$	$(2\|l\|+5)T_P+(\|l\|+1)T_E$	$3T_P+2(\|l\|+1)T_E$
Our scheme	$T_p+(3\|l\|+1)T_E$	$(3\|l\|+1)T_P$	$(3\|l\|+1)T_P$	$6T_P$

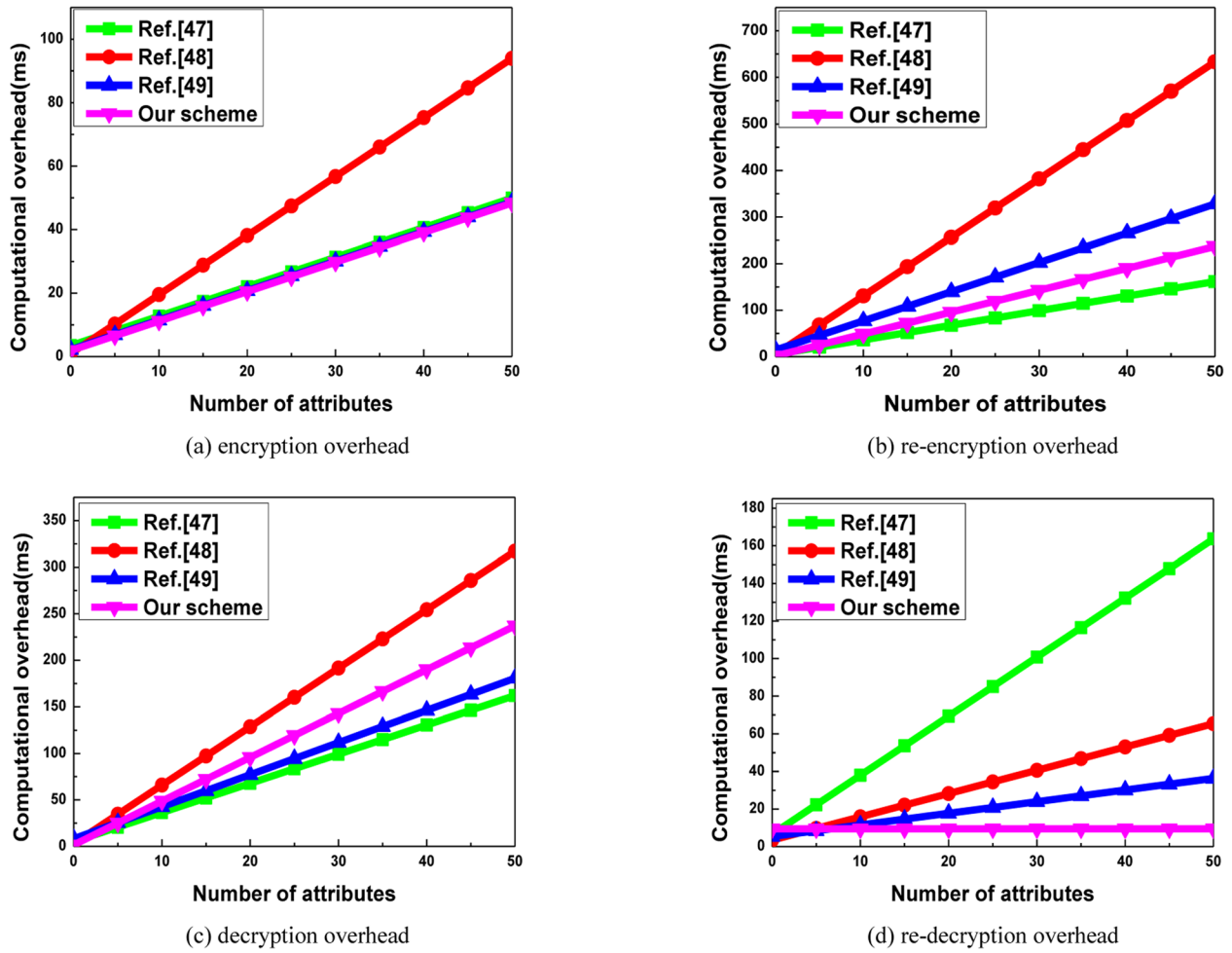


Fig. 8 Computational overhead comparison diagram

diagram of each part of the computational overhead as shown in Fig. 8 with references [47, 48] and [49].

Fig. 8 (a) shows the encryption overhead that occurs as the number of attributes increases, and the least encryption overhead is our scheme. Fig. 8 (b) shows the re-encryption calculation overhead, which changes with the number of attributes. It can be seen from the figure that the re-encryption overhead in [47] is the smallest, followed by ours. Fig. 8 (c) shows the decryption overhead comparison chart. Our scheme ranks third, which is only slightly less expensive than literature [48]. This is the disadvantage of our scheme. Fig. 8 (d) shows the re-decryption overhead. It is not difficult to find that our scheme will not change with the number of attributes, and its re-decryption time is always maintained at 9.42ms. Compared with the other three schemes, our scheme is at a disadvantage when the number of attributes is less than 5. This is because we join the signature verification process, so that we can be held responsible when the data is wrong. However, when the number of

Table 5 Comparison of communication overhead

Scheme	System parameters	Encryption key	Ciphertext	Re-encrypted ciphertext
Ref. [47]	$8\|G\|+2\|G_T\|$	$(2\|S\|+4)\|G\|$	$(2\|I\|+5)\|G\|+\|G_T\|$	$(2\|I\|+8)\|G\|+3\|G_T\|$
Ref. [48]	$(8\|U\|+6)\|G\|+\|G_T\|$	$6\|S\|\|G\|$	$(6\|I\|+2)\|G\|+\|G_T\|$	$2\|G\|+(2\|I\|+1)\|G_T\|$
Ref. [49]	$6\|G\|+\|G_T\|$	$(\|S\|+2)\|G\|$	$(3\|I\|+3)\|G\|$	$6(\|I\|+1)\|G\|+\|G_T\|$
Our scheme	$6\|G\|+\|G_T\|$	$(\|S\|+2)\|G\|$	$(3\|I\|+2)\|G\|+\|G_T\|$	$4\|G\|+\|G_T\|$

$|G|$, $|G_T|$: the lengths of the cyclic groups G and G_T; $|U|$: the attribute complete set size; $|S|$: the user attribute set size; $|I|$: the number of attributes in the access structure; $|I|$: the number of attributes that satisfy the access structure

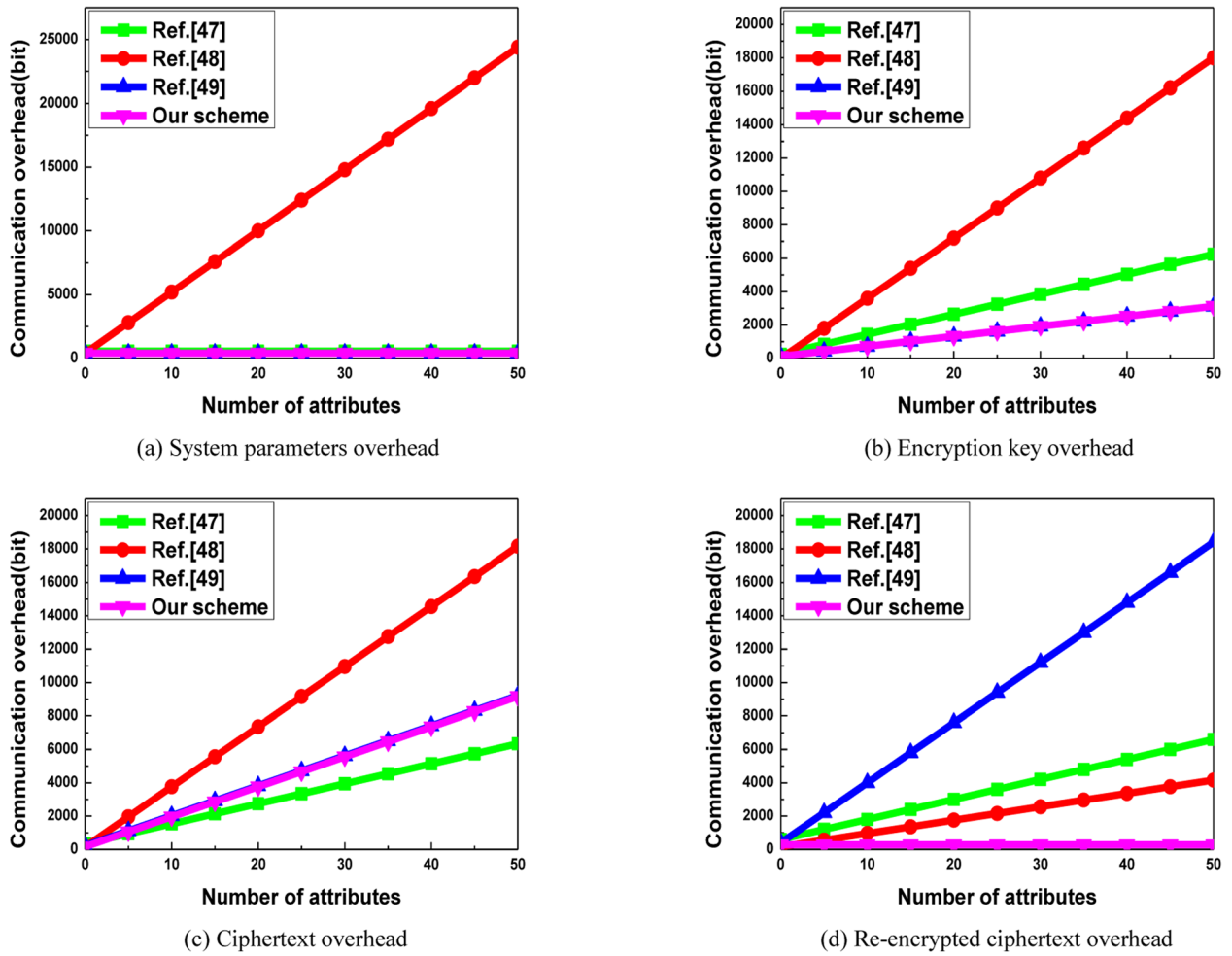


Fig. 9 Communication overhead comparison diagram

attributes exceeds 5, our scheme has obvious advantages, and the more the number of attributes, the greater the advantage.

Based on the four-part comparative performance, our scheme performed unsatisfactorily in the decryption stage, while in the re-decryption stage, our solution showed great superiority. In actual application, the encrypted data uploaded by DER is mainly shared to TVPP for viewing. Therefore, during the entire algorithm operation process, the decryption operation process will be very few, most of the time is running the re-decryption process, this concept coincides with our solution. In summary, the comparison of computational overhead shows the applicability and efficiency of our solution in the actual application scenarios of this paper.

Communication overhead evaluation

Here, we assume that $|G|$ and $|G_T|$ represent the lengths of the cyclic groups G and G_T, respectively, with values of 60 bits and 40 bits. Since the length of Z_p^* is very small, we ignore it. The communication overhead comparison is shown in Table 5, where $|U|$ represents the size of the attribute complete set, $|S|$ represents the size of the user attribute set, and $|l|$ and $|I|$ are defined as above.

Fig. 9 shows a comparison diagram of various parts of the communication overhead, including system parameters, encryption key, ciphertext and re-encrypted ciphertext. Fig. 9 (a) shows the comparison of the communication overhead of the system parameters. It can be seen from the figure that, except for the literature [48], which changes with the number of attributes, the other three schemes are kept constant. The system parameter length of our scheme and literature [49] is the smallest, both are 400 bits, while the length of literature [47] is 560 bits. Fig. 9 (b) shows the comparison of encryption key. Reference [49] and our scheme equals the encryption key length, tied for the first performance. The communication overhead comparison of ciphertext is shown in Fig. 9 (c). At this time, as the number of

Table 6 Quotation information of all participants

GU	Offer (USD/Unit)	Capacity (Unit)	Reputation value	*PU*	Bid (USD/Unit)	Capacity (Unit)	Reputation value
GU_1	1.13	11	2.82	PU_1	1.33	1	2.34
GU_2	1.20	15	0.07	PU_2	1.18	5	1.45
GU_3	1.15	12	2.02	PU_3	1.22	4	2.42
GU_4	1.17	13	0.97	PU_4	1.29	9	0.58
GU_5	1.20	10	4.77	PU_5	1.19	16	0.79
GU_6	1.27	19	1.87	PU_6	1.44	11	5.65
GU_7	1.12	20	3.17	PU_7	1.18	7	5.74
GU_8	1.46	17	0.99	PU_8	1.19	14	3.45
GU_9	1.48	6	3.61	PU_9	1.17	12	0.36
GU_{10}	1.30	3	1.58	PU_{10}	1.19	20	1.41
GU_{11}	1.30	16	3.92	PU_{11}	1.27	15	2.12
GU_{12}	1.24	18	4.14	PU_{12}	1.22	3	4.93
GU_{13}	1.46	2	4.49	PU_{13}	1.47	6	0.09
GU_{14}	1.25	14	2.70	PU_{14}	1.27	19	0.26
GU_{15}	1.14	7	0.50	PU_{15}	1.17	10	1.01
GU_{16}	1.41	9	1.37	PU_{16}	1.46	2	3.89

attributes increases, the minimum ciphertext length comes from literature [47], and our scheme still ranks second. The length of re- encrypted ciphertext shown in Fig. 9 (d) is similar to the re-decryption process in comparison of the computational cost. The length of the re-encrypted ciphertext in our scheme is always maintained at 280 bits, once again showing the great advantages of the algorithm.

Combining the evaluation of computational cost and communication cost, we can conclude that the algorithm in this paper has superior performance, whether in comparison of computational cost or communication cost. In the re-decryption calculation cost and re-encrypted ciphertext communication cost stage, we are far ahead of the other three schemes. This advantage helps us realize the rapid sharing of re-encrypted ciphertext, which is very suitable for the use scenarios of this paper.

Evaluation of effectiveness of the reputation-based CDA algorithm

Assuming that there are 16 DER generation units and 16 residential power units participating in the electricity bidding auction process organized by CVPP in this area, the quotation information they submit to CVPP is shown in Table 6. After CVPP receives the quotation information from each participant, it performs list division and list matching according to the reputation-based CDA algorithm. For details, see Tables 7, 8 and 9. The quotation information, capacity and reputation value in the table are all generated by random functions, and the

Table 7 Matching list of OL_1^t and BL_1^t

GU	Offer (USD/Unit)	Capacity (Unit)	Reputation value	*PU*	Bid (USD/Unit)	Capacity (Unit)	Reputation value
GU_5	1.20	10	4.77	PU_{13}	1.47	6	0.09
GU_{12}	1.24	18	4.14	PU_4	1.29	9	0.58
GU_{13}	1.46	2	4.49	PU_{14}	1.27	19	0.26
				PU_{10}	1.19	20	1.41
				PU_5	1.19	16	0.79
				PU_2	1.18	5	1.45
				PU_{15}	1.17	10	1.01
				PU_9	1.17	12	0.36

Table 8 Matching list of OL_2^t and BL_2^t

GU	Offer (USD/Unit)	Capacity (Unit)	Reputation value	*PU*	Bid (USD/Unit)	Capacity (Unit)	Reputation value
GU_7	1.12	20	3.17	PU_{16}	1.46	2	3.89
GU_1	1.13	11	2.82	PU_1	1.33	1	2.34
GU_3	1.15	12	2.02	PU_{11}	1.27	15	2.12
GU_5	1.20	10	4.77	PU_3	1.22	4	2.42
GU_{12}	1.24	18	4.14	PU_8	1.19	14	3.45
GU_{14}	1.25	14	2.70				
GU_{11}	1.30	16	3.92				
GU_{13}	1.46	2	4.49				

value ranges of the three parties are [1.1-1.5], [1-20] and [0-6].

Analyzing the validity of algorithm to PU

From Table 6, we can find that the quotations of PU_7 and PU_{15} are both 1.18 USD/Unit, and the quotation of PU_{10} is 1.19 USD/Unit. After this round of matching, PU_7 is matched successfully, but PU_{10} and PU_{15} failed to match. The main reason is *that* the reputation value of PU_7 is 5.74 , which is in the third level. In the case given in this paper, there are only 3 *PU* with *reputation* at third level, and 16 *GU* that can be selected. The reputation values of PU_{10} and PU_{15} are in the first level. As shown in Table 7, there are only 3 *GU* that can be matched, while 8 *PU* are waiting to be matched. Under such conditions, even though the bid of PU_7 is lower, it can still be successfully matched, which is the benefit of high reputation value to *PU*.

Analyzing the validity of algorithm to GU

For *GU*, the higher the reputation value, the more benefits can be obtained. Taking GU_2 and GU_{12} as examples, the offer of GU_{12} is 1.24 USD/Unit, and the offer of GU_2 is 1.20 USD/Unit. In the normal CDA auction mechanism, only after the number of GU_2 to be sold is purchased, the higher offer of GU_{12} may be successfully

Table 9 Matching list of OL_3^t and BL_3^t

GU	Offer (USD/Unit)	Capacity (Unit)	Reputation value	*PU*	Bid (USD/Unit)	Capacity (Unit)	Reputation value
GU_7	1.12	20	3.17	PU_6	1.44	11	5.65
GU_1	1.13	11	2.82	PU_{12}	1.22	3	4.93
GU_{15}	1.14	7	0.50	PU_7	1.18	7	5.74
GU_3	1.15	12	2.02				
GU_4	1.17	13	0.97				
GU_5	1.20	10	4.77				
GU_2	1.20	15	0.07				
GU_{12}	1.24	18	4.14				
GU_{14}	1.25	14	2.70				
GU_6	1.27	19	1.87				
GU_{11}	1.30	16	3.92				
GU_{10}	1.30	3	1.58				
GU_{16}	1.41	9	1.37				
GU_{13}	1.46	2	4.49				
GU_8	1.46	17	0.99				
GU_9	1.48	6	3.61				

matched. But in our proposed reputation-based CDA auction mechanism, GU_{12} with a higher offer was matched successfully, and GU_2 with a lower offer failed. The main reason is that GU_{12} has a reputation value of 4.14 and the reputation value of GU_2 was only 0.07. According to the market segmentation mechanism, the reputation level of GU_{12} is 3 and the reputation level of GU_2 is 1. Therefore, the quotation of GU_{12} can be seen by all PU. However, the quotation of GU_2 can only be seen by PU with a reputation level of 3. In the end, GU_{12} was successfully matched in Table 7 where the supply exceeded demand, while GU_2 failed in Table 9, where supply exceeded demand. The GU which fails to match need to continue to lower their offers and then participate in the next round of auctions. On the contrary, the PU which fails to match needs to increase their bids. Participants' specific quotations for the next auction can be obtained according to Eq. (28), where E_p is provided by CVPP from Eq. 27.

Analyzing the validity of algorithm to the whole transaction

Analyzing Tables 7, 8 and 9 according to the CDA auction mechanism, we can find that PU_4, PU_{13} and PU_{14} in Table 7 can be successfully matched to GU, and PU in Table 8 that can be successfully matched are PU_1, PU_3, PU_8, PU_{11} and PU_{16}. All 3 PU included in Table 9 can be matched successfully. After summarizing, it is found that among the 16 PU, 11 PU in this round of transactions can be successfully matched in this auction, and the unmatched ones are PU_2, PU_5, PU_9, PU_{10} and PU_{15}. In the ordinary CDA auction mechanism, there is only one matching list, and the reason why participants fail to match is only related to the price. The reputation-based CDA auction mechanism proposed in this paper divides three matching lists according to the reputation-based market segmentation mechanism. In this mechanism, the reason for the failure of the participants to match is not only related to the price, but also to the reputation value of the participants.

All in all, the reputation-based CDA auction mechanism proposed in this paper can not only operate normally in CVPP, but also encourage all participants to develop good market behavior. Because the reputation value directly affects their own interests, it can be foreseen that each participant will strive to increase the reputation value in order to maximize their own interests. Even if the reputation values of all participants are at the same level, according to the matching mechanism of "price first, reputation first, time first", our program can still operate normally.

Conclusion

Based on the virtual power plant existing storage, scheduling and trade issues, this paper proposes a VPP security scheduling and transaction mechanism with dual blockchains. In order to store huge data sets from DER in real time and quickly, we adopt a private chain structure. Since the data in the private blockchain may be tampered with by the leader node, we store the hash value of the private blockchain in the consortium blockchain, which is mainly used to store the transaction information of the electricity market participants. The transparency and traceability of the blockchain itself can provide VPP with a low-cost, transparent and open information and transaction platform. In the process of VPP scheduling, the authenticity of data is particularly important. Under the premise of ensuring the authenticity of data and the confidentiality of user information, we propose the CP-HAPRE algorithm. Performance evaluation shows that the algorithm has great advantages in the process of secure data sharing. There are many participants in the electricity market, we put forward a reputation-based CDA auction mechanism to maximize the benefits of each participant. Effectiveness analysis shows that the scheme can effectively operate and create an electricity market with good trading behavior.

Acknowledgments

We want to thank the authors of the literature cited in this paper for contributing useful ideas to this study.

Authors' contributions

Xiaohong Zhang: Validation, Writing - review & editing, Visualization. Zilong Song: Conceptualization, Methodology, Software, Writing - original draft. Ata Jahangir Moshayedi: Security analysis and essay polishing. The authors read and approved the final manuscript.

Authors' information

Xiaohong Zhang received the B.S. degree in physics from Jiangxi Normal University, Jiangxi, China, in 1984. The M.S. degree in Optical Information Processing from Chinese Academy of Sciences, Changchun, China, in 1990, and the PH. D degree in control theory, information safety, from the University of Science and Technology Beijing (USTB) and Beijing University of Posts and Telecommunications (BUPT) in 2002, 2006, respectively. She was a Visiting Scholar with the University of California, Berkeley, USA, from 2014 to 2015. She is currently a full Professor with the Department of College of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China. Her main research interests are blockchain technology, information security, nonlinear dynamics, wireless sensor network, etc.

Zilong Song received the B.S. degree in electronic and information engineering from Jiangxi University of Science and Technology, Jiangxi, China, in 2019, where he is currently pursuing the M.S. degree with the school of information and communication engineering. His current research interests focus on blockchain technology, renewable energy and information security.

Ata Jahangir Moshayedi received the B.S. degree in Power electrical Engineering from Azad University, Iran in 2004. The M.S. degree in Instrumentation Science from Pune University, India in 2009 and PhD in Electronic Science in electronic and Robotic from Savitribai Phule Pune University, India in 2015. Currently working as Associate professor at College of Information Engineering, Jiangxi University of Science and Technology, China, IEEE member. His research interest includes: Robotics and Automation/ Sensor modeling/Bio inspired robot, Mobile Robot Olfaction/ Virtual reality, Machine vision/Artificial Intelligence

Funding

This work is jointly supported by the National Natural Science Foundation of China (Nos. 61763017, 51665019), Scientific Research Plan Projects of Jiangxi

Education Department (No. GJJ150621), Natural Science Foundation of Jiangxi Province (Nos. 20161BAB202053, 20161BAB206145), and the Innovation Fund for Graduate Students in Jiangxi Province (Grant No: YC2020-S443).

Availability of data and materials

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

Declarations

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author details

[1]School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China. [2]KhomeiniShahr Branch, Islamic Azad University, Isfahan, Iran.

Received: 3 August 2021 Accepted: 23 November 2021
Published online: 28 January 2022

References

1. Ramanathan V, Feng Y (2009) Air pollution, greenhouse gases and climate change: Global and regional perspectives. Atmos Environ 43(1):37–50. https://doi.org/10.1016/j.atmosenv.2008.09.063
2. Dong Z, Zhao J, Wen F, Xue Y (2014) From smart grid to energy internet: basic concept and research framework. Autom Electr Power Syst 38(15):1–11. https://doi.org/10.7500/AEPS20140613007
3. Bai J, Xin S, Liu J, Zheng K (2015) Roadmap of realizing the high penetration renewable energy in China. Proc CSEE 35(14):3699–3705. https://doi.org/10.13334/j.0258-8013.pcsee.2015.14.026
4. Kieny C, Berseneff B, Hadjsaid N, Besanger Y, Maire J (2009) On the concept and the interest of virtual power plant: Some results from the European project Fenix. In: 2009 IEEE Power & Energy Society General Meeting. IEEE, pp 1–6. https://doi.org/10.1109/PES.2009.5275526
5. Siano P, De Marco G, Rolán A, Loia V (2019) A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. IEEE Syst J 13(3):3454–3466. https://doi.org/10.1109/JSYST.2019.2903172
6. Ahmad A, Khan JY (2019) Real-time load scheduling and storage management for solar powered network connected EVs. IEEE Trans Sustain Energy 11(3):1220–1235. https://doi.org/10.1109/TSTE.2019.2921024
7. Shao W, Xu W, Xu Z, Liu B, Zou H (2019) A Grid Connection Mechanism of Large-scale Distributed Energy Resources based on Blockchain. In: 2019 Chinese Control Conference (CCC). IEEE, pp 7500–7505. https://doi.org/10.23919/ChiCC.2019.8866604
8. Mashhour E, Moghaddas-Tafreshi SM (2009) A review on operation of micro grids and virtual power plants in the power markets. In: 2009 2nd International Conference on Adaptive Science & Technology (ICAST). IEEE, pp 273–277. https://doi.org/10.1109/ICASTECH.2009.5409714
9. Wang C, Li P (2010) Development and challenges of distributed generation, the micro-grid and smart distribution system. Autom Electr Power Syst 34(2):10–14. https://doi.org/10.13535/j.cnki.11-4406/n.2015.33.071
10. Shao W, Xu W, Xu Z, Wang N, Nong J (2018) Research on virtual power plant model based on blockchain. Comput Sci 45(2):25–31. https://doi.org/10.11896/j.issn.1002-137X.2018.02.005
11. Mashhour E, Moghaddas-Tafreshi SM (2010) Bidding strategy of virtual power plant for participating in energy and spinning reserve markets—Part I: Problem formulation. IEEE Trans Power Syst 26(2):949–956. https://doi.org/10.1109/TPWRS.2010.2070884
12. Shabanzadeh M, Sheikh-El-Eslami MK, Haghifam MR (2017) Risk-based medium-term trading strategy for a virtual power plant with first-order stochastic dominance constraints. Iet Gener Transm Distrib 11(2):520–529. https://doi.org/10.1049/iet-gtd.2016.1072
13. Baringo A, Baringo L (2016) A stochastic adaptive robust optimization approach for the offering strategy of a virtual power plant. IEEE Trans Power Syst 32(5):3492–3504. https://doi.org/10.1109/TPWRS.2016.2633546
14. Baringo A, Baringo L, Arroyo JM (2018) Day-ahead self-scheduling of a virtual power plant in energy and reserve electricity markets under uncertainty. IEEE Trans Power Syst 34(3):1881–1894. https://doi.org/10.1109/TPWRS.2018.2883753
15. Soter S, Bertling F (2004) Adjustable converter for injection of fuel cell power as a part of a virtual power plant. In: 2004 IEEE 35th Annual Power Electronics Specialists Conference (IEEE Cat. No. 04CH37551), IEEE, pp 1988-1990. https://doi.org/10.1109/PESC.2004.1355422.
16. Nikonowicz LB, Milewski J (2012) Virtual power plants-general review: structure, application and optimization. J Power Technol 92(3):135 https://papers.itc.pw.edu.pl/index.php/JPT/article/view/284
17. Binding C, Gantenbein D, Jansen B, Sundstrom O, Andersen PB, Marra F, Poulsen B, Traeholt C (2010) Electric vehicle fleet integration in the Danish EDISON project - A virtual power plant on the island of Bornholm. In: IEEE PES General Meeting. IEEE, pp 1–8. https://doi.org/10.1109/PES.2010.5589605
18. You S, Træholt C, Poulsen B (2009) Generic virtual power plants: Management of distributed energy resources under liberalized electricity market. In: 8th International Conference on Advances in Power System Control, Operation and Management (APSCOM 2009). IET, pp 1–6. https://doi.org/10.1049/cp.2009.1764
19. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. White Paper. https://doi.org/10.2139/ssrn.3440802.
20. Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami JJ (2015) Blockchain contract: A complete consensus using blockchain. In: 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE). IEEE, pp 577–578. https://doi.org/10.1109/GCCE.2015.7398721
21. Unguru M (2018) Blockchain technology: opportunities for the energy sector. Euroinfo 2(1):53–58. https://ideas.repec.org/a/iem/eurinf/v2y2018i1p53-58.html.
22. Burger C, Kuhlmann A, Richard P, Weinmanm J (2016) Blockchain in the energy transition. A survey among decisionmakers in the German energy industry, DENA German Energy Agency 60. https://www.researchgate.net/publication/341441255_Blockchain_in_the_energy_transition_A_survey_among_decisionmakers_in_the_German_energy_industry.
23. Hasse F, von Perfall A, Hillebrand T, Smole E, Lay L, Charlet M (2016) Blockchain–an opportunity for energy producers and consumers. PwC Global Power Util:1–45. https://www.pwc.com/ca/en/power-utilities/publications/pwc-blockchainopportunity-for-energy-producers-and-consumers-2016-11-en.pdf.
24. He Q, Ai Q (2017) Application Prospect of Block Chain Technology in Virtual Power Plant. Electr Energy Manag Technol 41(3):14–18. https://doi.org/10.16628/j.cnki.2095-8188.2017.03.003
25. Galici M, Ghiani E, Troncia M, Pisano G, Pilo F (2019) A cyber-physical platform for simulating energy transactions in local energy markets. In: 2019 IEEE Milan PowerTech. IEEE, pp 1–6. https://doi.org/10.1109/PTC.2019.8810656
26. Lu J, Wu S, Cheng H, Xiang Z (2020) Smart contract for distributed energy trading in virtual power plants based on blockchain. Comput Intell. https://doi.org/10.1111/coin.12388
27. Li Y, Hu B (2019) An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain. IEEE Trans Smart Grid 11(3):2627–2637. https://doi.org/10.1109/TSG.2019.2958971
28. Zeng S, Huo R, Huang D, Liu J, Wang S, W. Feng (2020) Overview of blockchain Technology: principle, progress and Application. J Commun 41(1): 134-151. https://doi.org/10.11959/j.issn.1000-436x.2020027
29. Sun G, Dai M, Zhang F, Yu H, Du X, Guizani M (2020) Blockchain-Enhanced High-Confidence Energy Sharing in Internet of Electric Vehicles. IEEE Internet Things J 7(9):7868–7882. https://doi.org/10.1109/JIOT.2020.2992994
30. Awerbuch S, Preston A (eds) (2012) The Virtual Utility: Accounting, Technology & Competitive Aspects of the Emerging Industry. Springer Sci Bus Media Berlin. https://doi.org/10.1007/978-1-4615-6167-5
31. Wei Z, Yu S, Sun G, Sun Y, Yuan Y, Wang D (2013) Concept and development of virtual power plant. Autom Electr Power Syst 37(13):1–9. https://doi.org/10.7500/AEPS201210156
32. Pudjianto D, Ramsay C, Strbac G (2017) Virtual power plant and system integration of distributed energy resources. IET Renew Power Gener 1(1):10–16. https://doi.org/10.1049/iet-rpg:20060023
33. Freeman D, Scott M, Teske E (2010) A taxonomy of pairing-friendly elliptic curves. J Cryptol 23(2): 224-280. 10.1007/ s00145-009-9048-z

34. Boneh D, Goh EJ, Nissim K (2005) Evaluating 2-DNF Formulas on Ciphertexts. In: Theory of cryptography conference. Springer, Berlin, pp 325–341. https://doi.org/10.1007/978-3-540-30576-7_18
35. Szabo N (1997) Formalizing and Securing Relationships on Public Networks. First Monday 2(9). https://doi.org/10.5210/fm.v2i9.548
36. Buterin V (2014) A next-generation smart contract and decentralized application platform. White Paper. https://translatewhitepaper.com/wp-content/uploads/2021/04/EthereumOrijinal-ETH-English.pdf.
37. Zhang X, Chen X (2019) Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network. IEEE Access 7:58241–58254. https://doi.org/10.1109/ACCESS.2018.2890736
38. Yu Y, Li Y, Tian J, Liu J (2018) Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. IEEE Wireless Communications 25(6): 12-18. https://doi.org/10.1109/MWC.2017.1800116.
39. Hropko D, Ivanecký J, Turček J (2012) Optimal dispatch of renewable energy sources included in Virtual power plant using Accelerated particle swarm optimization. In: 2012 ELEKTRO. IEEE, pp 196–200. https://doi.org/10.1109/ELEKTRO.2012.6225637
40. Liu J, Li M, Fang F, Niu Y (2014) Review of virtual power plant. Proc CSEE 34(29):5103–5111. https://doi.org/10.13334/j.0258-8013.pcsee.2014.29.012
41. Khaqqi KN, Sikorski JJ, Hadinoto K, Kraft M (2018) Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. Appl Energy 209:8–19. https://doi.org/10.1016/j.apenergy.2017.10.070
42. Blaze M, Bleumer G, Strauss M (1998) Divertible Protocols and Atomic Proxy Cryptography. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, pp 127–144. https://doi.org/10.1007/BFb0054122
43. Wang P, Li Y, Zhao S, Chen H, Jin Y, Ding Y (2019) Key technologies of distributed energy trading based on blockchain. Autom Electr Power Syst 43(14):53–64. https://doi.org/10.7500/AEPS20181203010
44. Liang X, Cao Z, Lin H, Shao J (2009) Attribute based proxy re-encryption with delegating capabilities. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, pp 276–286. https://doi.org/10.1145/1533057.1533094
45. Boneh D, Boyen X (2004) Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: International conference on the theory and applications of cryptographic techniques. Springer, Berlin, pp 223–238. https://doi.org/10.1007/978-3-540-24676-3_14
46. Ongaro D, Ousterhout J (2014) In search of an understandable consensus algorithm. In: 2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14), pp 305–319. https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro.
47. Feng Z, Luo W, Qin Z, Yuan D, Zou L (2019) Attribute-based proxy re-encryption scheme with multiple features. J Commun 40(6):177–189. https://doi.org/10.11959/j.issn.1000-436x.2019127
48. Obour Agyekum KOB, Xia Q, Sifah EB, Gao J, Xia H, Du X, Guizani M (2019) A Secured Proxy-Based Data Sharing Module in IoT Environments Using Blockchain. Sensors 19(5):1235. https://doi.org/10.3390/s19051235
49. Wang D, Zhang X (2020) Secure Data Sharing and Customized Services for Intelligent Transportation Based on a Consortium Blockchain. IEEE Access 8: 56045–56059. https://doi.org/10.1109/ACCESS.2020.2981945

Publisher's Note