

Article

A Distributed Energy Trading Authentication Mechanism Based on a Consortium Blockchain

Zheng Che ¹, Yu Wang ², Juanjuan Zhao ^{1,*}, Yan Qiang ¹, Yue Ma ¹ and Jihua Liu ³¹ School of Information and Computer, Taiyuan University of Technology, Taiyuan 030024, China² School of Foreign Languages, Taiyuan University of Technology, Taiyuan 030024, China³ College of Computer Science and Technology, Lvliang University, Lvliang 033000, China

* Correspondence: zhaojuajuan@tyut.edu.cn; Tel.: +86-186-3666-7123

Received: 23 June 2019; Accepted: 24 July 2019; Published: 26 July 2019



Abstract: With the rapid development of the energy internet, the transaction of distributed renewable energy (DRE) is playing an increasingly important role in the energy market. However, in the transaction model of distributed renewable energy combined with public blockchain technology, nodes in the trading network can join or leave the network at any time without any permission, which hinders the regulation of electricity institutions. Corresponding to the transaction principle, a distributed renewable energy transaction authentication mechanism based on consortium blockchain is proposed in this paper. First, certificate authority nodes were set in the transaction network to provide nodes with access authority by controlling the public keys and private keys of trading participants so that they can complete their identity authentication. Next, essential chaincodes in the transaction authentication were designed and deployed on a Hyperledger Fabric blockchain site, and a simulation experiment of a simple DRE transaction was used to elaborate the details on the transaction process. Finally, the proposed model was evaluated according to its performance and proved to be practical and effective.

Keywords: energy internet; distributed; renewable energy; blockchain; transaction authentication; Hyperledger Fabric

1. Introduction

With the world paying close attention to environmental pollution and the energy crisis, it has become an inevitable trend to develop distributed renewable energy (DRE) vigorously, such as solar, wind, and biomass, in order to promote social transformation and sustainable development [1]. However, there is a clear demarcation line between supply and demand for multiple energy types in the scheme of a traditional energy infrastructure, which with its inefficiency in regulating and utilizing distributed energy, could not achieve distributed energy generation at a large scale (wind, solar energy, etc.). Under such conditions, the exploration of flexible access technology for distributed power generation and energy storage begins

American academic J. Rifkin puts forward the concept and expresses the prospect of energy internet in his work, titled *The Third Industrial Revolution* [2], showing that an energy internet is a complex multi-network flow system, which when taking the power system as its kernel, being based on internet and other advanced information technologies, and using DRE as its primary energy, is closely coupled with other systems, including the natural gas network and transportation network [3]. In Reference [4], the cluster load of electric vehicles is installed in the energy center of residential quarters where the cogeneration of heat and power and heat pumps are used as energy conversion devices, and it acts as a controllable electric load to promote the operation so that the energy internet is applied in residential quarters. In Reference [5], the micro-cogeneration of cooling, heating, and power is employed as an

energy conversion device, and is applied in the household energy center to maintain a comfortable temperature for average family, and at the same time, reduce total energy consumption costs. Also, integrated energy solutions for household users are proposed. However, with the rapid development of devices (for instance, distributed generators, energy storage, electric vehicles, and electric converter) in the energy internet, the boundaries between energy consumers and producers is becoming blurred and the participants are becoming gradually diversified; as such, the drawbacks of the energy internet have increasingly emerged. On the one hand, the energy internet has contributed to the complex flow directions of energy, information, and capital because of its characteristics, like numerous participants, a highly complex system, ambiguous identity, various and distributed resources, etc., which has increased the costs of transaction and management greatly in the process of energy flow and value flow for the existing centralized decision-making energy trading system, and has put the system at the risk of inefficient decision-making [6,7]. On the other hand, the energy system is gradually evolving from the traditional centralized decision-making form to the distributed decision-making form, and this will lead to issues regarding a lack of trust among the traders [8,9]. Therefore, it is urgent to introduce a new technology to support the construction of the energy internet.

The most important characteristic of blockchain technology is decentralization, which can achieve peer-to-peer (P2P) transactions on the premise that nodes do not trust each other [10,11]. In addition, it is expected to be a key technology to promote the development of the energy internet in the future in that its characteristics (such as cooperative autonomy, security and credibility, and smart contracts, etc.) have an affinity with the concept of energy interconnection to some extent [12–15]. Correspondingly, people has begun to actively explore the application of this technology in the field of multi-energy trading [16,17]. In Reference [18], a blockchain-based renewable energy trading framework is proposed, in which each household can act as either a producer or a consumer for energy, and neighbors can trade energy independently without the participation of third parties. LO3 Energy has successfully established a solar energy trading platform for residents who live in the Brooklyn Community, New York, where residents could act as energy producers and consumers when they have installed photovoltaic panels. On that platform, energy trading can be carried out freely without relying on third parties. After analyzing the project, Esther Mengelkamp et al. point out seven essential market components for creating an efficient distributed energy market [19,20]. In Reference [21], in terms of consensus bookkeeping, smart contracts, and business interaction, the ways that blockchain technology can improve the efficiency of system scheduling in the energy internet are discussed with the aim to provide an alternative form of decentralized decision-making and collaborative autonomy for the energy internet. Plaza et al. provide an energy sharing scheme for the solar energy sharing community via blockchain technology [22]. In the scheme, the solar energy producers and consumers can make use of blockchain technology and put surplus solar energy into the energy trading network of the community for transaction. Zhao et al. propose a blockchain-based integrated energy transaction mechanism, which is in accordance with the transaction principle and divides the transaction process into two stages: the call auction stage and the continue auction stage [23]. In Reference [24], a game theory approach to distributed energy management is introduced and a practical energy transaction platform is constructed via blockchain. Wang et al. propose a parallel bidding framework based on a three-layer distribution network architecture and the decentralization characteristics of blockchain to support energy trading among microgrids [25]. In this framework, multi-directional energy trading among microgrids in a distribution network is possible. In Reference [26], blockchain technology is coupled with the microgrid group transaction, and the information flow transaction model of a microgrid group based on blockchain technology is established, which realizes the power trading within the microgrid group. Although there have been many studies on the combination of blockchain technology and the energy internet, blockchain and the energy internet are only combined in the public blockchain in current literature. Any node in the public chain can join or leave the network at any time without any permission, which hinders the supervision of power institutions [27,28]. Moreover, some undesirable consequences and limitations of such a condition in actual DRE transactions have

not been addressed in previous studies. To solve the problems, this paper proposes a DRE transaction authentication mechanism based on a blockchain.

In summary, the main contributions of the paper are as follows:

- (1) This paper proposes a blockchain-based transaction authentication model, which is, in accordance with the transaction principle, divided into two stages, namely the off-chain certification stage and on-chain certification stage, and reduces the credit costs in the process of DRE transactions.
- (2) A certificate authority (CA) is introduced in the blockchain network to achieve privilege control and supervision of transaction parties by controlling the public and private keys of the participants.
- (3) A power unit chaincode, generating unit chaincode, matching unit chaincode, and the matchmaking trading chaincode are designed and deployed in the framework (Hyperledger Fabric v1.1) of a consortium blockchain to simulate the process of transaction authentication.
- (4) Hyperledger Caliper is used to evaluate the performance of the above model and results prove that while ensuring data security and information transparency, this model can improve the efficiency of transaction, thus reduce the transacting time of distributed energy.

The organization of this paper is as follows. Section 2 provides introduction to blockchain technology, the Hyperledger Fabric project, and the applicability of blockchain technology to the transaction authentication mechanism of distributed energy transactions. Section 3 puts forward the transaction authentication model of distributed energy. Section 4 proposes both the functions and elements of the chaincode constructed and deployed on Hyperledger Fabric. Section 5 validates the proposed model through a simple case study. Section 6 draws the final conclusion and elaborates on potential future work.

2. Blockchain and Hyperledger

2.1. Blockchain Technology

Blockchain technology is a decentralized and transparent database. Its transparency is maintained due to its database being shared with all network nodes, updated by miners in the network, and supervised by all network nodes. Meanwhile, decentralization is reflected in the fact that no node truly owns and controls the database, which is maintained by all nodes in the whole network, and each node has the rights to access and update the database [29]. The basic architecture of blockchain technology consists of six layers from top to bottom: the application layer, contract layer, incentive layer, consensus layer, network layer, and data layer, which are shown in Figure 1.

- Data layer: This layer mainly solves the problems of how data in the block is combined together, and encapsulates the underlying technologies including time stamps, hash functions, asymmetric encryption technology, and the chain structure of the data block [30], which lays a solid foundation for the superstructure of the blockchain network.
- Network layer: This layer encapsulates P2P networking mechanism, data transmission mechanism and data verification mechanism. Due to the equal rights and obligations of each node in the blockchain network, and the flat topology structure of communication and interaction, the data transmission in the network and the verification of new blocks are carried out between each node. Only when the verification is accomplished by more than 51% of users in the network, new blocks can be added to the main chain [31].
- Consensus layer: This layer mainly includes the consensus algorithm and consensus mechanism, which is the basis of distributed nodes in the whole blockchain network to judge the effectiveness of the same block. Currently, there are three common consensus mechanisms: POW (proof of work), POS (proof of stake), and DPOS (delegate proof of stake).
- Incentive layer: each blockchain system has its unique economic incentive and token allocation system to encourage the nodes in the blockchain network to jointly maintain the blockchain network [32].

- **Contract layer:** The blockchain has a programmable feature that allows scripts, algorithms, and smart contracts to be included in each block. The smart contract allows the blockchain system to automatically trigger the execution of contract content under constraints without additional manual intervention. This layer greatly expands the application scenario of the blockchain, making blockchain one of the technologies to reduce the cost of credit [33].
- **Application layer:** This layer is a specific application scenario of blockchain. With the development of blockchain 1.0 (peer-to-peer digital encrypted monetary system) and blockchain 2.0 (programmable finance) [34], the application of blockchain technology has gradually extended from currency and finance to other domains, including energy, Internet of things, network security, medical treatment, legal notarization, and copyright authentication, to where the technology will step into the era of blockchain 3.0, namely, the programmable society [35].

In the six-layer structure of the blockchain, the data layer, the network layer, and the consensus layer are the basic parts, which must be available to all the blockchain network. As the topological part of the blockchain, the incentive layer, contract layer, and application layer greatly improves the function and application of the blockchain, such that the blockchain can exert great potential in more application scenarios.

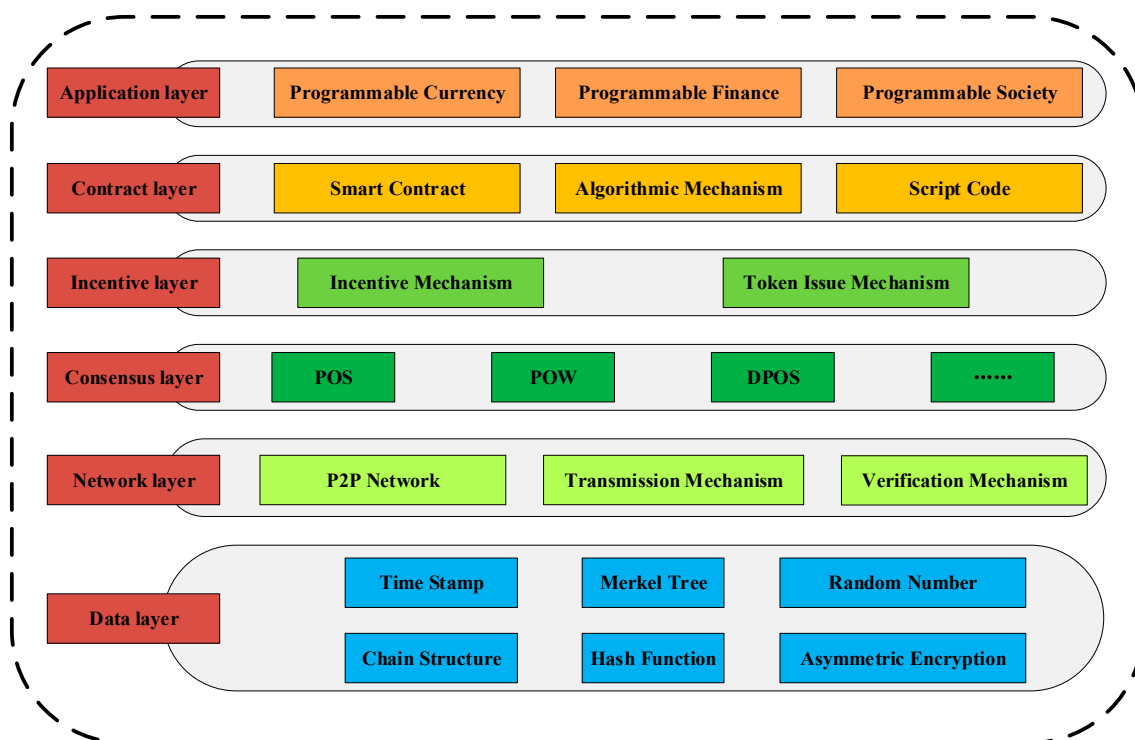


Figure 1. Six-layer structure of blockchain.

2.2. Hyperledger Fabric

Hyperledger Fabric is a consortium blockchain project led by IBM (Armonk, NY, USA). It was handed over to the Linux Foundation at the end of 2015 and then became an open source project. The project aims to establish a basic blockchain service platform that can make consensus mechanism and membership services plug-and-play through the cooperation of members and different user cases in different industries. At present, more than 250 companies and organizations are involved, including IBM, ABN AMRO (Amsterdam, The Netherlands), Intel (Santa Clara, CA, USA), Cisco (San Francisco, CA, USA), J. P. Morgan (New York, NY, USA), Accenture (Dublin, Ireland), Huawei (Shenzhen, China), Baidu (Beijing, China), and Hitachi (Tokyo, Japan).

Currently, Hyperledger Fabric has released versions better than version 1.0. Since version 1.0 was released, Fabric has split the peer's functionality and separated the blockchain's data maintenance and consensus services. The consensus service is completely separated from the peer, and the orderer node is introduced to provide a consensus service. A data maintenance service is achieved through the establishment of a channel structure, which greatly improves the performance of business isolation and data security [36].

Figure 2 shows the logical structure of Hyperledger Fabric. As can be seen from the figure below, Fabric can be logically divided into four parts: the underlying network, the blockchain service, the permission management, and the user interface. Different from the public blockchain structure, Fabric introduces a permission management module, which is responsible for providing identity registration, identity management, and rights auditing services for each member of the network. In addition, the user interface provides a command-line interface (CLI) component and a Software Development Kit (SDK) component for the developers of Fabric and the upper application. Both components are encapsulated with an application programming interface (API) that can interact with Fabric. By interacting with API, the developer or upper application can normally access the ledger and transactions, and the logic of application transaction is executed by the chaincode.

- Peer: A network entity that is used to maintain a ledger and can read and write operations on the ledger, which according to functions, can be divided into an anchor peer, endorsing peer, committing peer, and leading peer.
 - (1) Endorsing peer: Mainly responsible for the verification of transactions. When the node receives a transaction request sent by a client, the validity of the transaction will be verified and the result will be fed back to the client after a successful verification.
 - (2) Commitment peer: Mainly responsible for maintaining the ledger structure of the blockchain. This node will periodically acquire the blocks containing transactions from the orderer node and add the verified blocks to the blockchain after legal issuance and verification of these blocks.
 - (3) Anchor peer: Responsible for communication between members. Each member possesses at least one anchor peer.
 - (4) Leading Peer: Responsible for communicating with the ordering service on behalf of Member to obtain block information. There is only one leading peer for the entire member.
- Orderer: Responsible for the sorting and packaging of legitimate transactions received in the network.
- Chaincode: The application code in Hyperledger Fabric is derived from the concept of "smart contracts", which runs in isolated containers and provides different invocation commands to implement logic in the business.
- Channel: The private blockchain used in the Fabric network for data privacy and isolation. Each channel maintains its own ledger, and the state of the ledger in the channel is maintained by all members who join the channel.
- Ledger: Store all verifiable transaction information in a chain structure, jointly maintained by nodes in the same channel.
- Member: A legally separate entity that owns a unique root certificate for the network. Network components, such as peer nodes and application clients, will be linked to a member.
- CA: Mainly provides authority management service in Fabric and responsible for providing registration services and issuing certificates to computer nodes or users who join Fabric.

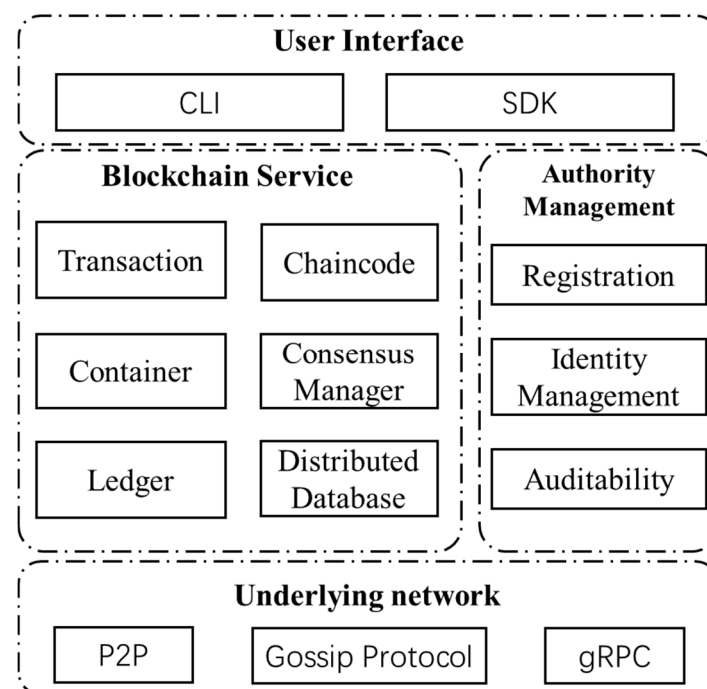


Figure 2. Logical structure diagram of Hyperledger Fabric.

2.3. Blockchain Technology in Multi-Energy Trading Work

As a decentralized distributed database, blockchain technology has many similarities with the concept of energy internet trading. First of all, both blockchain technology and the energy internet emphasize decentralization. The emerging distributed energy transactions and the links between energy producer and energy consumer reflect the requirements for decentralization in energy internet transactions [37]. Second, both the energy internet and blockchain technology advocate the idea of cooperative autonomy. The energy internet emphasizes that the system, equipment, and transaction parties constitute an energy trading ecosystem together, and blockchain technology also jointly maintains a database with all nodes in the network. In this respect, the two have a high degree of similarity [38]. Finally, it has become a common trend for both of them to pursue intelligence and contract. The emergence of intelligent power systems, such as self-discipline control and intelligent energy [39,40], marks that the development direction of energy trading is increasing the transaction automation level. The smart contract in blockchain enables the trading system to automatically execute the preset operations on the assets according to the content of the contract, which can satisfy the new requirements of the intelligent development of energy transactions.

3. Framework of DRE Transaction Authentication

In the transaction authentication model proposed in this paper, participants of transaction authentication can be classified into three types according to user requirements: power unit (PU), generating unit (GU), and matching unit (MU). Among them, the power unit is an energy demander in a DRE transaction. It needs to buy electricity from the network to meet its own needs. It can be a small power company or an average household. The generating unit is an energy supplier in the DRE transaction that generates economic benefits by selling excess electricity. It may be a small wind plant or an ordinary family with photovoltaic panels. The matching unit is a transaction medium in the DRE transaction. It is also an ordinary member of the trading network. It uses its own CA to provide identity authentication and authorization services to members in the network.

Each transaction must be authenticated by all participants before it takes effect. Each user unit that joins the trading network is abstracted into a member organization, and each organization has at least

two nodes in the blockchain network. Furthermore, each participant, whether it belongs to a power unit or a generating unit, has at least one smart meter that uploads power data to the blockchain network. Inspired by the authentication mechanism of devices in the Internet of things [41–43], transaction authentication of DRE is divided into two stages: the off-chain authentication stage and the on-chain authentication stage. In the off-chain authentication stage, the transaction participants are required to apply for access rights and transaction certificates to MU members in the network. After obtaining the identity, the trading parties can publish their own demand information by using their private keys, and MU will match the trading requirements of the trading parties and generate traceable trading orders. In the on-chain authentication stage, a PU and GU will verify the validity of the transaction in their respective member nodes and then submit the validation transaction to the ordering service for a transaction order, which will be recorded to the ledger and complete the transaction authentication.

In terms of the overall trading process of distributed energy, when a new energy request presents itself, it will be passed into the blockchain transaction API and be judged whether it accords with the requirement or not. If so, it will be submitted to the transaction system. Then, the transaction system will send the requested content to the blockchain container to complete the transaction authentication process in the container. Finally, when the authentication is completed, the transaction system will call the energy dispatch system to complete the energy scheduling according to the specific content of the request. The framework diagram of the DRE transaction authentication model combined with blockchain is shown in Figure 3.

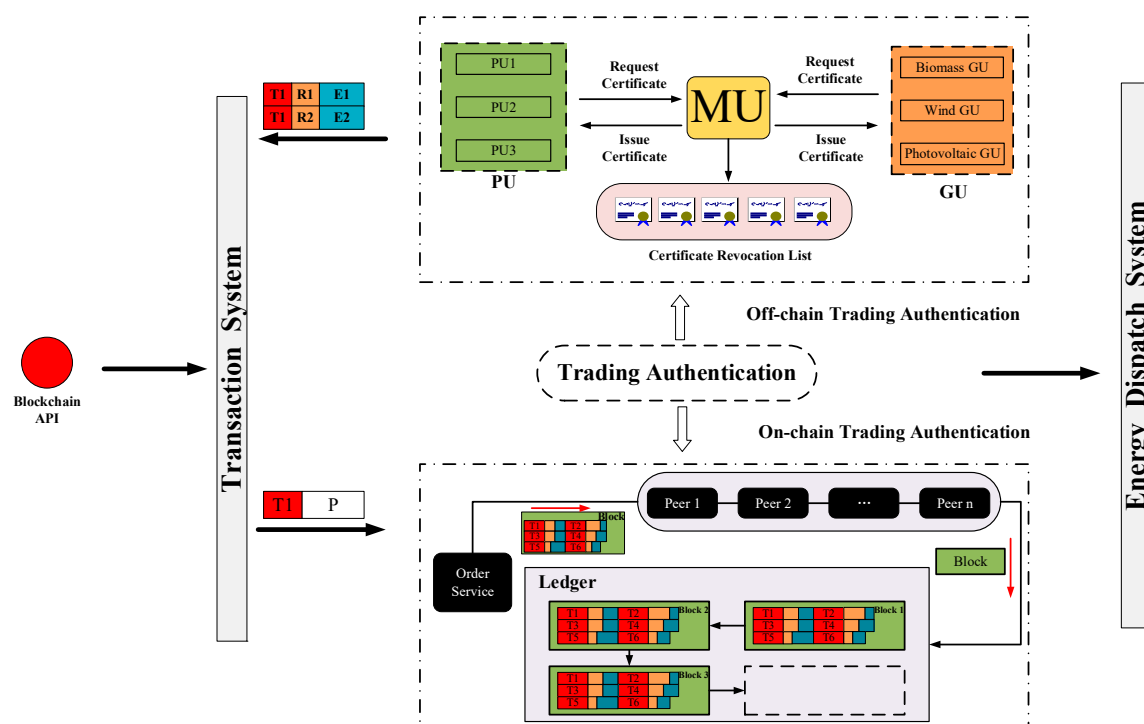


Figure 3. Blockchain framework in DRE trading authentication.

The parameters used in this section are given in abbreviations Table 1.

Table 1. Parameter list.

Item	Meaning
S^A	Encryption rules to be followed when the CA generates its own private key
MU	Matching Unit, which is responsible for issuing certificates for user units and providing member services
MPK	MU's own major private key

Table 1. Cont.

Item	Meaning
PK _r	Private key set of user units
GU	Generating unit, which is a collection of generation users
PU	Power unit, which is a collection of power units
Sig ₁	User signature generated by the PU using its own private key
Sig ₂	User signature generated by GU using its own private key
Attr	Attribute collection for each user unit
ID	ID number of each user unit
Q	Planned generation capacity of PU
P	Electricity price per kWh
Ts	Timestamp indicating the time when the transaction was reached
Dt	Delivery time
Rand	Accompanied by the selection of the corresponding power unit, generating unit, and matching unit, which is generated by a hash function
Dem	Energy demand information published by the power unit
Sup	Energy supply information published by the generating unit
Ord	Order generated after matching supply and demand information
Rec	Transaction record

3.1. Off-Chain Authentication Stage

In the off-chain authentication stage, the generating unit, and the power unit ask the matching unit for permission to access to network. The specific off-chain authentication procedure is as follows:

(1) According to the security parameter S^λ , MU generates its master private key MPK.

(2) GU and the PU apply to MU for network access to obtain the corresponding identity ID and its related attribute set Attr in the trading network, including user type, user authority, and user wallet address.

(3) MU issues a private key PK_r to each unit by using its primary private key MPK according to the attribute set Attr of each unit and transmits it to each subscriber unit through a secure channel.

$$\text{KeyGen}(\text{MPK}, \text{Attr}) \rightarrow \text{PK}_r \quad (1)$$

(4) Each PU submits demand information to MU, including its ID (own network), Addr (wallet address), Dt (expected delivery time), and identifies the final demand information with its own private key, generates Sig₁ (signature), broadcasts through MU, and continuously monitors the broadcast information of GU.

$$\text{Int}_1(\text{Dt}, \text{ID}, \text{Addr}, \text{Sig}_1) \rightarrow \text{Dem} \quad (2)$$

(5) When the demand information is collected, MU feeds back the planned power generation quantity Q to GU. Then, after receiving the feedback, GU submits its own ID, expected power generation quantity Q, and electricity price P to MU, and uses its own private key to identify the final energy supply information, generating the signature Sig₂, broadcasted by MU, and continuously monitors the requests of PU.

$$\text{Int}_2(\text{Q}, \text{P}, \text{ID}, \text{Sig}_2) \rightarrow \text{Sup} \quad (3)$$

(6) PU (GU) monitors the broadcast information to select appropriate energy supply (demand) information. When appropriate information is captured, GU (PU) will negotiate with GU (PU) through a communication protocol. Once they reach an agreement, MU will match Dem with Sup. If the match succeeds, a Ts (time-stamp) will be stamped and an Ord (transaction order) will be concluded. Once the order is concluded, the GU and PU participating in the transaction will select an appropriate MU to form an energy dispatching channel. With the formation of the trading channel, MU will generate a random number Rand.

$$\text{Match}(\text{Dem}, \text{Sup}, \text{Ts}) \rightarrow \text{Ord} \quad (4)$$

$$\text{Hash}(\text{GU}_{\text{id}}, \text{PU}_{\text{id}}, \text{DC}_{\text{id}}) \rightarrow \text{Rand} \quad (5)$$

3.2. On-Chain Authentication Stage

After the off-chain authentication stage, the completed trade orders will be submitted to the blockchain network via the blockchain API, and the nodes in each organization will perform their respective functions to complete the transaction certification on the chain:

(1) The transaction system integrates the random number Rand with the completed Ord into a transaction record, which is sent to peer 1 in each organization via the blockchain API according to the endorsement strategy in the chaincode.

$$\text{Int}_3(\text{Ord}, \text{Rand}) \rightarrow \text{Rec} \quad (6)$$

(2) Peer 1 checks the legality of the transaction. Then, it will use its own private key PK_r to sign the execution result and return it to the transaction system.

(3) When the transaction system collects sufficient results, it will send the transaction to the order service.

(4) The order service packages all transactions into a block sequentially until the block size reaches the system default threshold.

(5) Once a block reaches the specified threshold, the order service will submit the block to peer 1 and peer 2. Then peer 2 will verify the result and write the information into the ledger. At the same time, the transaction system will receive a transaction completion notification, which notifies the energy dispatch system to complete the energy dispatch based on the transaction requests. The sequence diagram in the energy trading process is shown in Figure 4:

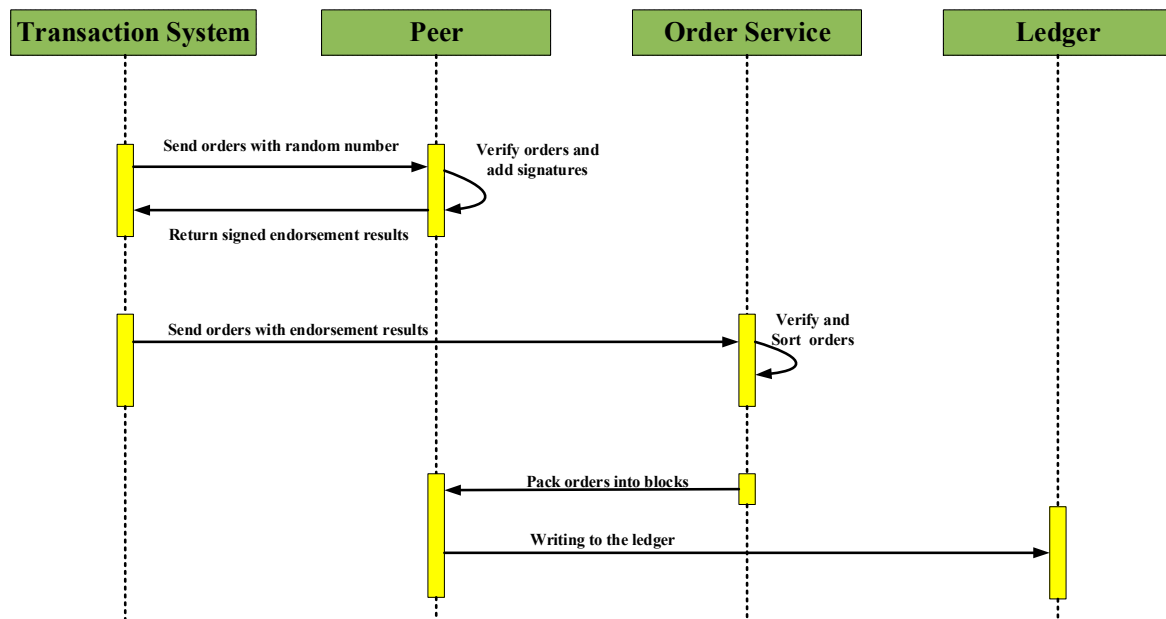


Figure 4. Energy transaction sequence diagram.

4. Formulation of the Chaincode

This section discusses the functional construction of the chaincode in Hyperledger Fabric by taking the transaction between the generating unit and power unit as an example. The functions of the chaincode are described in terms of three aspects: issuing the demand information of the power unit, issuing the sales information of the generating unit, and finally matching the transaction information, as well as publishing trading orders. The trading process involves four chaincodes in

chronological order, including the power unit chaincode, generating unit chaincode, matching unit chaincode, and the matchmaking trading chaincode.

4.1. Power Unit Chaincode

This chaincode collects and integrates energy demand information for the power unit. The inputs of this chaincode are the expected delivery time, account address, and user ID. When inputs are entered, they will be captured by the chaincode and integrated into the demand information in specific formats. The chaincode integrates the inputs mentioned above and provides a signature of the information by using the private key of the power unit. The output is the energy demand information attached to a signature of the user. The chaincode allows the power unit to revise or retreat its demand information within a certain period after being issued. The basic elements of the chaincode are presented in Table 2.

Table 2. Basic elements of Power Unit Chaincode.

Parameter	Type	Meaning
Power unit address	Byte	Account address of the power unit
Power unit ID	Byte	ID of the power unit
Energy demand information	Byte	Generated by the power unit chaincode
Signature	Byte	Generated by the private key of power unit
Delivery time	Int64	Determined by power unit

4.2. Generating Unit Chaincode

This chaincode collects and integrates the sales information of the generating unit, and then posts it online. The inputs of this chaincode are the total amount of required energy for the power unit in a certain period, and electricity sales, electricity price, account address, and user ID of the generating unit. The chaincode integrates the inputs mentioned above and provides a signature of the information by using the private key of the generating unit. The output is the energy sales information attached to a signature from the user or users. The basic elements of the chaincode are shown in Table 3.

Table 3. Basic elements of Generating Unit Chaincode.

Parameter	Type	Meaning
Generating unit address	Byte	Account address of the generating unit
Generating unit ID	Byte	ID of the generating unit
Energy sale information	Byte	Generated by the generating unit chaincode
Signature	Byte	Generated by the private key of generating unit
Delivery time	Int64	Determined by generating unit
Electricity supply	Float64	Planned sales of generating unit
Price of energy	Float64	Energy price per kWh

4.3. Matching Unit Chaincode

This chaincode has two functions: one is to apply for the user ID and wallet address for new users of the trading network in order to identify them, and the other is to award new users private keys to achieve privilege management for them.

The inputs of this chaincode include the user types and user information of the power units and generating units, which apply for network access. Wherein, if the user is a self-employed household, the information would be the name and ID number of the user; if the user is a company or an enterprise, then the information would be name of the company, and the name and ID number of the corporate juridical person. The outputs consist of the user number and account address in the network. The basic elements of the chaincode are provided in Table 4.

Table 4. Basic elements of the matching unit chaincode.

Parameter	Type	Meaning
User name	Byte	Name of the user or juridical person of the company
Corporate name	Byte	Part of user information
User type	Byte	Part of user information
User address	Byte	Wallet account address
User private key	Byte	User private key
ID number	Int32	Part of the user information
Unit ID	Int32	User number in the trading network

4.4. The Matchmaking Trading Chaincode

The inputs of the chaincode comprise the energy demand information issued by the power unit and the energy sale information issued by the generating unit. The chaincode will match a power unit with a generating unit after they reach an agreement and complete the transaction authentication according to the principles described in Section 3.1. In this way, a specific energy trading channel will be created for each pair of energy buyer and seller to present trading records, generate a random number via the private key of all the information in the channel, and then submit the number to Fabric. The basic elements of the chaincode are provided in Table 5.

Table 5. Basic elements of the matchmaking trading chaincode.

Parameter	Type	Meaning
Generating unit address	Byte	Account address of the generating Unit
Generating unit ID	Byte	ID of the generating unit
Power unit address	Byte	Account address of the power unit
Power unit ID	Byte	ID of the power unit
Transaction record	Byte	Transaction records in the blockchain
Hash	Byte	Encrypt order information
Electricity supply	Float64	Planned sales of generating unit
Price of energy	Float64	Energy price per kWh

5. Case Study

In this section, the trading authentication model proposed in this paper is simulated, and the feasibility of trading structure is verified by taking a distributed energy trading authentication case as an example to deploy chaincodes. Then, Hyperledger Caliper is used to evaluate the performance of the Fabric network. The experiment of the case study is completed using three computers, all of which were equipped with an Intel Core i5-4590s CPU 3.00 GHz, 16 GB of memory, and Ubuntu18.04 system. Among them, the deployed chaincodes were written by the Go language. Go language is a lightweight programming language with a high efficiency and high concurrency, whose features can satisfy the requirements of a blockchain network to realize a distributed system, data encryption, big data transmission, and storage. It is the preferred development language designated by Hyperledger [44].

A simplified Fabric network environment was adopted to simulate a simple DRE transaction scenario as it makes no sense to study transaction authentication without involving actual transaction. Based on the Fabric v1.1 architecture, a consortium blockchain was set up to test the network and three generating units, three power units, and three matching units were installed. When the transaction authentication succeeds, the logical relationship among participants is shown in Figure 5.

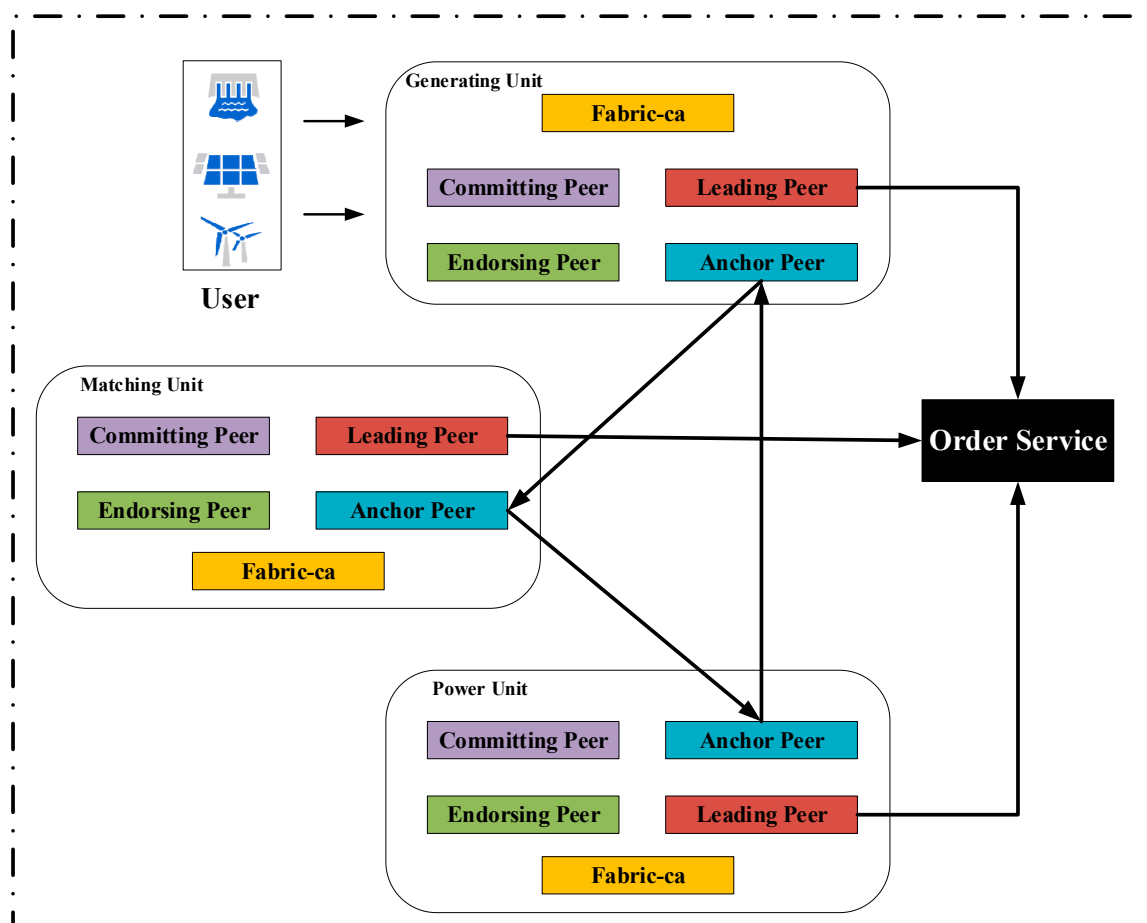


Figure 5. Logical structure diagram of the participants.

5.1. Deploying the Matching Unit Chaincode

The matching unit chaincode was deployed in the endorsing peer which exists in the matching unit and consisted of an initialization function, a calling function, a receiving function, an authentication function, and an encryption function. The receiving function was responsible for collecting personal information of the users who applied for the network access. After receiving the information, it issued a request to the CA institution. Then, the CA institution granted the private key to the users who applied for network access. The authentication function gave the user ID of the applicant users in the trading network and employed the encryption function, which generated wallet addresses for the users based on their private keys. The wallet address was a series of random numbers and letters. In the simulation experiment, some key information of users applying for network access is shown in Table 6. It was assumed that all users were companies or enterprises.

Table 6. User attributes in the trading network.

Corporate Name	User Type	Net ID	Address
Company A	Generating Unit	G0001	e3cff020d7ebf0ddd162d386644c8d84cf7304fc686f1c984773d56680bf0e3
Company B	Generating Unit	G0002	fb2ff65e1a1e79a4fae0b3ded3968b3894e352f58d3c69c9d7c8bc0bda9fd53f
Company C	Generating Unit	G0003	f4355c55b16a2b0a56cd9e66ebbb46fc9e4b02fe56f79c75cde2626fca4838d5
Company D	Power Unit	P0001	88db1aaf0b1aee4962e628852213c75094c21530353957d2858b6f73427fb2b
Company E	Power Unit	P0002	2c9a47f798a0c31973d6bd7a89be7fa53357a34f64a3b14f32a7754023161a5a
Company F	Power Unit	P0003	23c08d6e79f9d52d84c259bc2f3dd6c013f8d7095aab4ded2e8d2eb884f02616

5.2. Deploying the Power Unit Chaincode

The power unit chaincode was deployed in the endorsing peer which exists in the power unit and consisted of an initialization function, a calling function, an accumulation function, an information splicing function, and a signature function. The accumulation function allowed the users to submit their own demand for electricity in a certain period, and then submitted the total electricity consumption of the power unit after accumulating. The information splicing function collected user information of the power unit and output that information according to a specific format, as shown in Table 7. It should be noted that only the demand information within the same delivery time was sent to the same chaincode.

Table 7. Information splicing function parameters.

Net ID	Address	Delivery Time
P0001	88db1aaf0b1aee4962e628852213c75094c21530353957d2858b6f73427fb2b	08:00–09:00
P0002	2c9a47f798a0c31973d6bd7a89be7fa53357a34f64a3b14f32a7754023161a5a	08:00–09:00
P0003	23c08d6e79f9d52d84c259bc2f3dd6c013f8d7095aab4ded2e8d2eb884f02616	08:00–09:00

5.3. Deploying the Generating Unit Chaincode

The generating unit chaincode was deployed in the endorsing peer which exists in the generating unit. The generating unit used the chaincode to publish its own sales information. The contract consisted of an initialization function, a calling function, a quotation function, the other kind of information splicing function, and a signature function. The information of the generating unit is shown in Table 8. It should be noted that only sales information within the same delivery time was sent to the same chaincode.

The energy selling price in the table refers to the average price of new energy units, according to State Energy Administration's Regulatory Bulletin on the State Power Price in 2017, issued by the National Energy Bureau [45].

Table 8. The generating unit's information.

Net ID	Generate Type	Delivery Time	Supply Quality (kWh)	Price (CNY/kWh)
G0001	Wind	08:00–09:00	610	0.56
G0002	Solar	08:00–09:00	270	0.99
G0003	Biomass	08:00–09:00	300	0.76

5.4. Deploying the Matchmaking Trading Chaincode

This chaincode collected the demand information of the power unit and sales information of the generating unit, and then matched the information of buyers and sellers. The matchmaking trading chaincode was deployed in the endorsing peer of the matching unit, which mainly included initialization functions, calling functions, two information capture functions, transaction matching functions, signature functions, judgment functions, and commit functions. The two information capture functions captured data from the energy seller and the energy buyer, respectively, and assigned them to different order sets according to the delivery time. For demonstration purposes, it was assumed that all demand information was in the same delivery time and all electricity information had the same delivery time. All transaction orders reached are shown in Table 9.

Table 9. Transaction order.

Parameter	Order Information			
Order Number	01	02	03	04
Power unit	P0001	P0002	P0002	P0003
Generating unit	G0001	G0001	G0003	G0002
Matching unit	M0002	M0003	M0001	M0003
Transaction price (CNY/kWh)	0.56	0.56	0.76	0.99
Trading electric quantity(kWh)	310	300	290	270
Energy type	Wind	Wind	Biomass	Solar

For the trade orders that have been completed, the matching unit used its private key to encrypt, generate a hash value, and package the transaction information of the energy buyer and the energy seller to submit them to the block. When the block met the restrictions, it was submitted to the Fabric ledger. The encrypted hash value is shown in Table 10.

Table 10. The hash of orders.

Order Number	Hash
01	ffb0e4fd0a24d28ded0d3140aa2a15862ae24b8958a83cdf9df90492db472519
02	4c13835ca9e2dc5603e060bc6808fc6d4a2134ea5a4f0f9d25285ac80abcd93
03	f7eaa7fb45f327308a503e0c1d86fdb175a37da50a55a6086e667ff8ee6db57c
04	bad1f5c53b343867069277c6d1f0ccdc4bf8cf79fcf610f248fce95328640447

5.5. Performance Evaluation

This section evaluates and analyzes the results of this case in terms of three aspects: transaction processing capability, block generating policy, and information transparency of the platform, with the aim of pointing out the superiority of this model in actual transactions.

5.5.1. Transaction Processing Capability

Based on Hyperledger Caliper (source code access of Caliper: <https://github.com/hyperledger/caliper>), the transaction processing capability was evaluated in this case. Caliper is a blockchain performance benchmark framework that allows users to test different blockchain solutions with predefined use cases and get a set of performance test results.

Throughput and latency were mainly analyzed in this case. Throughput was used to describe the quantity of transaction requests per second of the blockchain platform, which is a major metric to evaluate the performance of the blockchain platform and has an important impact on the time spent on completing a DRE transaction. Latency is the period from transaction requests being issued by transaction system to the requests being responded to by the blockchain platform. Caliper tests the platform under pressure, constantly sending transaction requests to the trading system and observing the changes of throughput and latency in accordance with a change in the send rate. Hyperledger Caliper tested the proposed blockchain model under pressure and the results are provided in Appendix A.

Figure 6 presents the performance of throughput and latency in the proposed model. The results show that throughput increased linearly as send rate increased at the beginning, but when it reached the threshold at about 250 tps (transaction per second), it stops increasing and remained in a stable state. Latency had a similar performance to throughput. When the send rate was less than 250 tps, latency was generally on the rise but with a low growth rate, which stayed below 1000 ms, and was basically at a lower level. When the send rate was higher than 250 tps, the latency increased rapidly. After the saturation point, a higher send rate caused the lower throughput due to the server bottleneck.

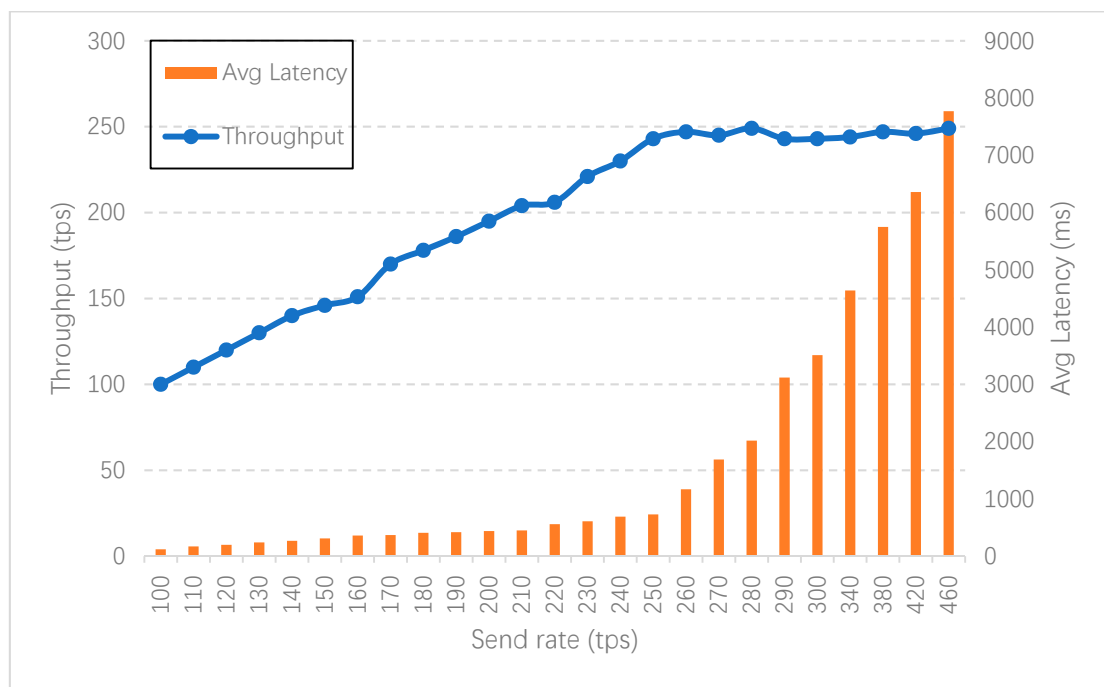


Figure 6. The performance of the throughput and latency.

In order to further evaluate the effectiveness of the proposed model, a throughput curve of the proposed model and another two common public blockchain models, Bitcoin blockchain and Ethereum blockchain, were compared. The data required in the comparison experiment were derived from two different public data sets [46,47], which collect some of the data generated by two public blockchains in actual transactions. As shown in Figure 7, the results show that compared with the transaction model combined with the public chain, the throughput of the proposed model had obvious advantages.

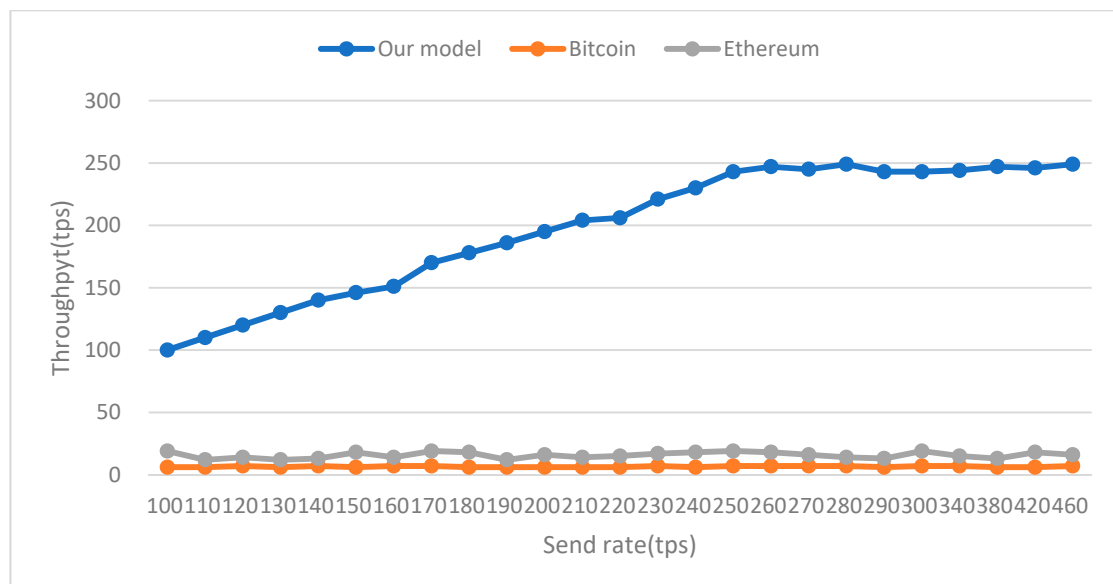


Figure 7. Throughput Comparison.

5.5.2. Block Generating Policy

Whether the blockchain network can deal with transactions efficiently is decisively affected by the block generating policy. When the system generates new blocks is mainly determined by the

message count and block size. Message count specifies the maximum number of transactions in a block. If the value of message count is set too low, there will be too many uploaded blocks in the network such that the network load would be increased, resulting in network congestion; if the value is set too high, there will be too many messages to be processed in blocks, resulting in inefficient network processing. Block size specifies the size of memory. The value being set too low will lead to insufficient space for messages and too fast a speed of generating blocks, increasing the burden of accounting nodes; the value being set too high will lead to faster broadband transmission than a P2P network, thus reducing the throughput of blockchain network [48]. Therefore, it is necessary to discuss how the message count and block size have an effect on throughput. Extensive experiments have been conducted to analyze the impact of different parameters on throughput.

This section employs variable-controlling approaches to find the optimal value of message count and block size. When looking for the optimal value of message count, the experiment set a larger block size so it would not affect the experiment, and vice versa.

Figure 8 shows how count size affected the throughput of the blockchain system. Looking at the curves separately, throughput value increased with the increase of send rate at the beginning, but when the rate reached a certain value, the throughput tended to saturate. On the whole, with the increase of message count, the saturation rate of throughput kept increasing until message count increased to 80. Then, the saturation rate of throughput did not change with the increase of message count any more, and levelled out at 150 tps. Therefore, it can be concluded that the optimal value of message count was 80. Figure 9 plots the throughput curves over different block sizes, in which similar outcomes as Figure 8 could be found. When block the size exceeded 8 MB, the transaction performance could not be improved any more via increasing the block size. In addition, due to the influence of a consensus mechanism, it will be more difficult and take more time to generate new blocks [49]. Consequently, the overall throughput value was about 150 tps, lower than that in query operations.

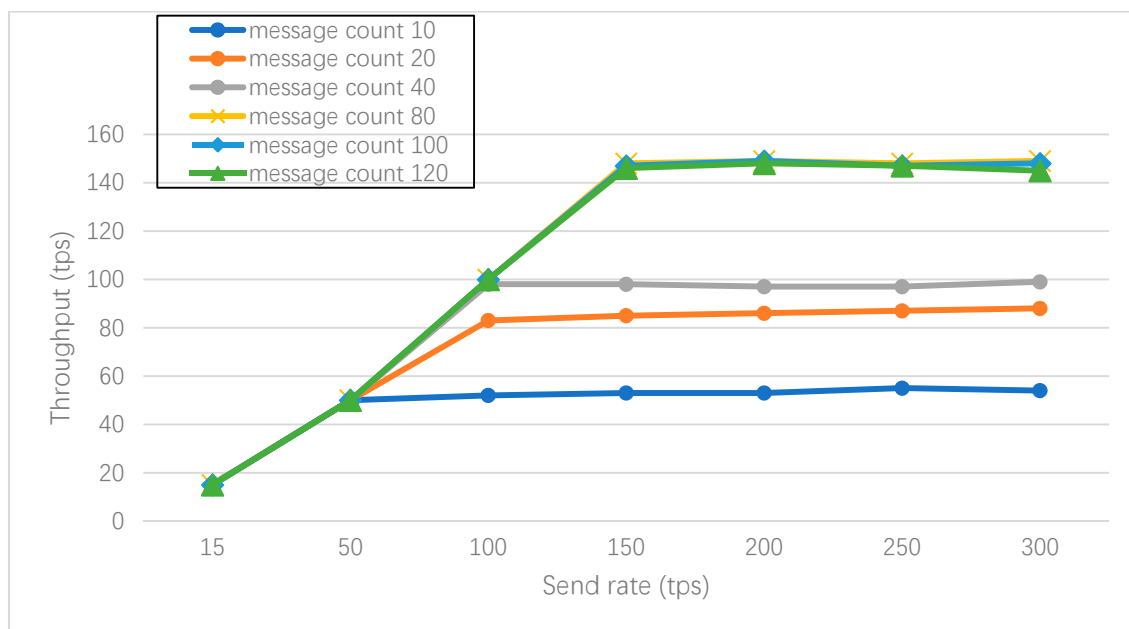


Figure 8. Impact of message count on throughput.

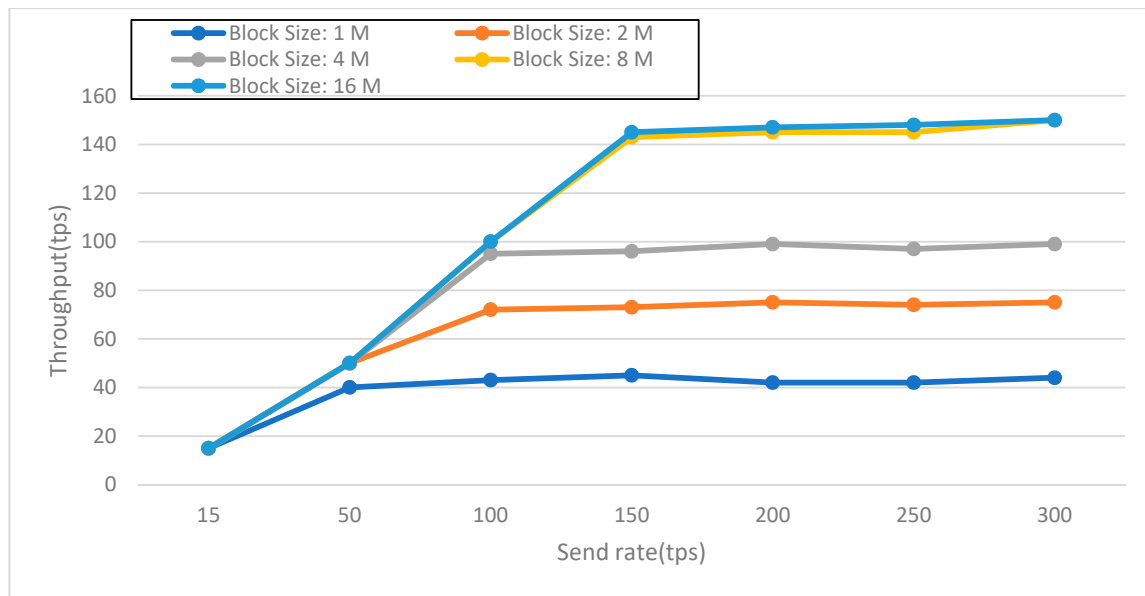


Figure 9. Impact of block size on throughput.

5.5.3. Information Transparency

This paper adopts a qualitative evaluation method to evaluate information transparency in the proposed transaction model. Blockchain technology was first applied to Bitcoin, aiming to solve the trust problem in the process of peer-to-peer transaction without the participation of a third-party authority. Accordingly, this paper combines the traditional energy transaction authentication method with blockchain technology and uses cryptography to ensure that transaction data of the users will never be leaked. Moreover, by introducing the management of public and private keys in a consortium blockchain, the access and management authority of public and private keys are given to MU nodes in a blockchain network, which, to some extent, improves the condition that nodes in a public chain cannot be supervised. Besides, the traditional transaction model, the public chain transaction model, and the transaction model proposed in this paper are compared qualitatively, and the specific comparison results are shown in Table 11.

Table 11. Information transparency comparison table.

Comparison item	Traditional	Public Blockchain	Proposal
Transaction Record Tracer	Third-party agencies only	All Network nodes	All Network nodes
Transaction Amount Tracer	Third-party agencies only	All Network nodes	All Network nodes
User Anonymity	Non-anonymous	Anonymous	Anonymous
Regulatory Level	High	Low	High

5.6. Results

This section is divided into two parts. The first part takes a distributed energy transaction authentication process as an example to simulate the transaction authentication model proposed in this paper and verifies the feasibility of the transaction structure by deploying chaincodes in Fabric v1.1. The second part evaluates and further analyses the simulation results of this case based on several indicators.

In the first part of the simulation experiment, whether it was a power company or a household user who had additional demand for electricity, they could apply to participate in the blockchain trading network according to the transaction authentication mechanism in Section 3 and publish their

demand information according to the rules. MU issued user certificates and public and private keys to applicants, and conducted DRE transaction authentication in an orderly manner under supervision.

In the second part, the simulation results were further discussed in terms of three aspects: transaction processing capability, block generation policy, and information transparency. Regarding transaction processing capability, throughput and latency was analyzed and the results show that there existed a threshold, which was 250 tps, for both of them. After this threshold, throughput changed from a continuous linear growth to a stable state, levelling out at about 250 tps; meanwhile, latency changed from a slow growth to a dramatic growth. Therefore, a conclusion can be drawn that the upper limit of transaction processing in the proposed model was 250 tps, which is obviously superior to the traditional public chain structure. In terms of block generating policy, this paper discussed and analyzed the settings of message count and block size by employing variable-controlling approaches. The analysis shows that when 80 was set as the value of message count and 8 M as the value of block size, throughput reached its optimal performance (150 tps) during the process of generating blocks. In terms of information transparency, which was qualitatively analyzed, it can be concluded that the proposed model can deal with DRE transactions openly, transparently, and efficiently on the premise of guaranteeing transaction supervision in comparison with the existing public chain transaction model.

6. Conclusions

In order to reduce the credit cost of distributed decision-making mode in an energy system, a DRE energy transaction authentication mechanism based on blockchain technology was established. Meanwhile, CA was introduced into the blockchain network to manage public and private keys and certificates of the users, which enhanced the supervision of power institutions by participants in the transaction. For a specific case of DRE transaction, the proposed transaction authentication model was simulated in a Fabric v1.1 blockchain network, and the transaction authentication of DRE was completed through four chaincodes. Finally, in order to further study the performance of the proposed model, the performance of its throughput and latency was analyzed and compared. Relevant results show that the throughput reached 250 tps, which is superior to the transaction model of a traditional public chain. Additionally, the optimal values of message count and block size were explored and the results show that when 80 was set as the value of message count and 8 M as the value of block size, the throughput reached its optimal performance (150 tps) during the process of generating blocks. The DRE transaction authentication mechanism proposed in this paper can be applied to various platforms of consortium blockchains and a broader energy trading market in the future, and is not just limited to distributed energy trading.

Although good results have been obtained in the study, there are still some limitations and deficiencies to be further addressed. This paper adopts a consensus mechanism (solo) to do instances research, which with low-cost and low-complexity transaction simulation process in a laboratory, is able to meet the requirements of researchers. However, this mechanism cannot work in practical production because of the huge volume of transactions that the system needs to deal with per second. Apart from that, the next step of this study is to fuse the CA mechanism, which is more authoritative and has a more complete certification system, with the distributed energy transaction.

Author Contributions: Conceptualization, Z.C.; Data curation, J.Z.; Formal analysis, Z.C.; Funding acquisition, Y.Q.; Investigation, Z.C. and J.L.; Methodology, Z.C.; Project administration, J.Z.; Resources, Y.Q.; Software, Y.M.; Supervision, Y.Q.; Validation, Y.W.; Writing—original draft, Y.W.; Writing—review and editing, Y.W., Y.M. and J.L.

Funding: This study was funded by the National Natural Science Foundation of China (grant number 61872261), State Key Laboratory of Virtual Reality Technology and Systems (grant number VRLAB2018B07), and State Key Laboratory of Virtual Reality Technology and Systems (grant number VRLAB2018A08).

Acknowledgments: Special thanks must be given to Yu Wang, from school of foreign languages in TYUT, for her generous help. It is she who spends much time on the translating and revising work. Without her enlightening impressive kindness and patience, I could not give birth to my current thesis. I have also benefited a lot from Wenting Zhao. As a distinguished scholar, she has encouraged me and given me inspiration of doing such a research. Besides, I am grateful to my families who have selflessly supported my education and academic research. Last but not least, I would like to thank all my friends, especially my lovely postgraduate classmates for their encouragement and support.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Hyperledger Caliper Pressure Test Results

In order to evaluate the performance of the proposed model, the fifth part of the paper used Hyperledger Caliper to test the proposed model under pressure, namely, through a certain http port, continuously sending transaction requests to the blockchain model at a specific rate, and monitoring the related performance of the blockchain. The test results are shown in Table A1.

Table A1. Hyperledger Caliper pressure test results.

Test	Name	Succ	Fail	Send Rate	Max Latency	Min Latency	Avg Latency	Throughput
1	query	1000	0	100 tps	0.19 s	0.04 s	0.12 s	100 tps
2	query	1000	0	110 tps	0.23 s	0.06 s	0.17 s	110 tps
3	query	1000	0	120 tps	0.38 s	0.03 s	0.20 s	120 tps
4	query	1000	0	130 tps	0.47 s	0.06 s	0.24 s	130 tps
5	query	1000	0	140 tps	0.49 s	0.12 s	0.27 s	140 tps
6	query	1000	0	150 tps	0.52 s	0.17 s	0.31 s	146 tps
7	query	1000	0	160 tps	0.61 s	0.26 s	0.36 s	151 tps
8	query	1000	0	170 tps	0.69 s	0.29 s	0.37 s	170 tps
9	query	1000	0	180 tps	0.59 s	0.28 s	0.41 s	178 tps
10	query	1000	0	190 tps	0.63 s	0.20 s	0.42 s	186 tps
11	query	1000	0	200 tps	0.77 s	0.27 s	0.44 s	195 tps
12	query	1000	0	210 tps	0.89 s	0.25 s	0.45 s	204 tps
13	query	1000	0	220 tps	0.96 s	0.32 s	0.56 s	206 tps
14	query	1000	0	230 tps	0.89 s	0.49 s	0.61 s	221 tps
15	query	1000	0	240 tps	1.02 s	0.50 s	0.69 s	230 tps
16	query	1000	0	250 tps	1.38 s	0.43 s	0.73 s	243 tps
17	query	1000	0	260 tps	1.59 s	0.91 s	1.17 s	247 tps
18	query	1000	0	270 tps	2.12 s	0.94 s	1.69 s	245 tps
19	query	1000	0	280 tps	3.95 s	0.99 s	2.02 s	249 tps
20	query	1000	0	290 tps	4.87 s	1.01 s	3.12 s	243 tps
21	query	1000	0	300 tps	5.34 s	1.23 s	3.51 s	243 tps
22	query	1000	0	340 tps	7.25 s	1.93 s	4.64 s	244 tps
23	query	1000	0	380 tps	8.58 s	2.32 s	5.75 s	247 tps
24	query	1000	0	420 tps	9.10 s	2.49 s	6.36 s	246 tps
25	query	1000	0	460 tps	10.36 s	2.87 s	7.77 s	249 tps

References

1. China National Renewable Energy Center. Prospects for Renewable Energy in China. 2018. Available online: <http://www.cnrec.org.cn/cbw/zh/2018-10-22-541.html> (accessed on 17 March 2019).
2. Rifkin, J. The third industrial revolution: How lateral power is transforming energy, The economy, and the world. *Survival* **2011**, *2*, 67–68.
3. Ma, Z.; Zhou, X.; Shang, Y.; Sheng, W. Exploring the concept, key technologies and development model of energy internet. *Power Syst. Technol.* **2015**, *39*, 3014–3022.
4. Zhang, H.; Wen, F.; Zhang, C.; Wang, F.; Meng, J.; Lin, G. Operation Strategy for Residential Quarter Energy Hub Considering Energy Demands Uncertainties. *Electr. Power Constr.* **2016**, *37*, 14–21.
5. Yan, Y.; Zhao, J.; Wen, F.; Chen, X. Blockchain in Energy Systems: Concept, Application and Prospect. *Electr. Power Constr.* **2017**, *38*, 12–20.
6. Zhang, H.; Wen, F.; Zhang, C.; Meng, J.; Lin, G.; Dang, S. Operation optimization model of home energy hubs considering comfort level of customers. *Autom. Electr. Power Syst.* **2016**, *40*, 32–39.

7. Li, Q.; Tang, X.; Zhao, Q.; Deng, P.; Chen, J.; Mi, Y.; Gao, H. Analysis of applying weak-centralized blockchain technology in energy trading system of energy internet. *Power Systems and Big Data*. **2019**, *22*, 22–27.
8. Ding, W.; Wang, G.; Xu, A.; Chen, H.; Hong, C. Research on Key Technologies and Information Security Issues of Energy Blockchain. *Proc. CSEE* **2018**, *38*, 1026–1034.
9. Liu, L.; Chen, X.; Lu, Z.; Wang, L.; Wen, X. Mobile-Edge Computing Framework with Data Compression for Wireless Network in Energy Internet. *Tsinghua Sci. Technol.* **2019**, *24*, 271–280. [[CrossRef](#)]
10. Satoshi Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted 2009. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 17 June 2017).
11. Tencent Fit, Tencent Research Institute. Tencent Block Chain Scheme White Paper. 2017. Available online: <https://wenku.baidu.com/view/f9b8b5183868011ca300a6c30c2259010202f3e5.html> (accessed on 10 February 2019).
12. Baidu Search Company, Baidu Block Chain Laboratory. Baidu Block Chain White Paperv1.0. 2018. Available online: <http://www.xker.com/a/2935.html> (accessed on 21 October 2018).
13. Jingdong Digital Technology Co., Ltd. Jingdong Blockchain Technology Practice White Paper (2018). 2018. Available online: https://www.sohu.com/a/226393423_99912465 (accessed on 3 September 2018).
14. Ministry of Industry and Information Technology of China. China Block Chain Industry White Paper 2018. 2018. Available online: <http://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf> (accessed on 20 March 2019).
15. Technical Report by UK Government Chief Scientific Adviser: Distributed Ledger Technology: Beyond Blockchain. 2016. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.2016 (accessed on 20 March 2019).
16. Zhumabekuly Aitzhan, N.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secure Comput.* **2018**, *15*, 840–852. [[CrossRef](#)]
17. Liu, N.; Yu, X.; Wang, C.; Li, C.; Ma, L.; Lei, J. An Energy Sharing Model with Price-based Demand Response for Microgrids of Peer-to-Peer Prosumers. *IEEE Trans. Power Syst.* **2017**, *32*, 3569–3583. [[CrossRef](#)]
18. Xie, P.; Yan, W.; Xuan, P.; Zhu, J.; Wu, Y.; Li, X.; Zou, J. Conceptual Framework of Blockchain-based Electricity Trading for Neighborhood Renewable Energy. In Proceedings of the 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 20–22 October 2018.
19. Nguyen, C. An indie, off-the-Grid, Blockchain-Traded Solar Power Market Comes to Brooklyn. 2016. Available online: <http://motherboard.vice.com/read/the-plan-to-power-brooklyn-with-a-blockchain-based-microgrid-transactive-solar> (accessed on 20 May 2018).
20. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [[CrossRef](#)]
21. Zeng, M.; Cheng, J.; Wang, Y.; Li, Y.; Yang, Y.; Dou, J. Primarily Research for Multi Module Cooperative Autonomous Mode of Energy Internet Under Blockchain Framework. *Proc. CSEE* **2017**, *37*, 3672–3681.
22. Plaza, C.; Gil, J.; de Chezelles, F.; Strang, K.A. Distributed solar self-consumption and blockchain Solar energy exchanges on the public grid within an energy community. In Proceedings of the Environment and Electrical Engineering and Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Palermo, Italy, 12–15 June 2018.
23. Zhao, S.; Wang, B.; Li, Y.; Li, Y. Integrated Energy Transaction Mechanisms Based on Blockchain Technology. *Energies* **2018**, *11*, 2412. [[CrossRef](#)]
24. Noor, S.; Yang, W.; Guo, M.; van Dam, K.H.; Wang, X. Energy Demand Side Management within micro-grid networks enhanced by blockchain. *Appl. Energy* **2018**, *228*, 1385–1398. [[CrossRef](#)]
25. Wang, N.; Xu, W.; Xu, Z.; Shao, W. Peer-to-Peer Energy Trading among Microgrids with Multidimensional Willingness. *Energies* **2018**, *11*, 3312. [[CrossRef](#)]
26. Xu, Z.; Yang, D.; Li, W. Microgrid Group Trading Model and Solving Algorithm Based on Blockchain. *Energies* **2019**, *12*, 1292. [[CrossRef](#)]
27. She, W.; Yang, X.; Hu, Y.; Liu, Q.; Liu, W. Transaction certification model of distributed energy based on consortium blockchain. *J. Univ. Sci. Technol. China* **2018**, *48*, 307–313.
28. Chang, W. The Design of Online Drug Retailing Model based on Consortium Blockchain Platform. *China Business and Market*. **2019**, *33*, 14–23.
29. Melanie Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly: Springfield, MO, USA, 2015; pp. 55–58.

30. Mattila, J.; Seppälä, T. *Industrial Blockchain Platforms: An Exercise in Use Case Development in the Energy Industry*; Etna Working Papers; Institute for Research on Labor and Employment: Berkeley, CA, USA, 2016.
31. Wang, D.; Zhou, J.; Wang, A. Loopring: A Decentralized Token Exchange Protocol. 2018. Available online: https://github.com/Loopring/whitepaper/raw/master/en_whitepaper.pdf (accessed on 2 July 2018).
32. He, Y.; Li, H.; Cheng, X.; Liu, Y.; Yang, C.; Sun, L. A blockchain based truthful incentive mechanism for distributed p2p applications. *IEEE Access* **2018**, *6*, 27324–27335. [CrossRef]
33. Yuan, Y.; Wang, F.Y. Blockchain: The state of the art and future trends. *Acta Autom. Sin.* **2016**, *42*, 481–494.
34. Buterin, V. A Next Generation Smart Contract and Decentralized Application Platform. 2014. Available online: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 6 May 2019).
35. Ping, Z.; Xu, S. Hyperledger White Paper. 2016. Available online: <https://www.8btc.com/article/97034> (accessed on 6 September 2018).
36. Cachin, C. Architecture of the hyperledger blockchain fabric. In Proceedings of the Workshop on Distributed Crypto currencies and Consensus ledgers (DCCL 2016), Chicago, IL, USA, 25 July 2016.
37. Wang, B.; Li, Y.; Zhao, S.; Chen, H.; Jin, Y.; Ding, Y. Thoughts on Key Technologies of Distributed Energy Transaction Based on Blockchain. *Autom. Electr. Power Syst.* **2019**, *43*, 1–12.
38. Zhang, N.; Wang, Y.; Kang, C.; Cheng, J.; He, D. Blockchain Technology in Energy Internet: A Study of Research Framework and Typical Applications. *Chin. Soc. Electr. Eng.* **2016**, *36*, 4011–4023.
39. Zhang, J.; Chen, L.; Zhang, M.; Wang, P.; Fang, M.; Sun, H. The concept and application of power distribution intelligent terminal. *High Volt. Eng.* **2019**, *45*, 1729–1736.
40. Zhang, D.; Zhang, Z.; Chen, L.; Li, S.; Huang, Q.; Liu, Y. Blockchain Technology Hyperledger Framework in the Internet of Energy. In Proceedings of the 2018 4th International Conference on Renewable Energy Technologies (ICRET 2018), Kuala Lumpur, Malaysia, 16–18 January 2018.
41. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, Kona, HI, USA, 13–17 March 2017; pp. 618–623.
42. Liu, H.; Zhang, Y.; Yang, T. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Netw.* **2018**, *32*, 78–83. [CrossRef]
43. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
44. The Linux Foundation. A Blockchain Platform for the Enterprise—Hyperledger Fabric. 2019. Available online: <https://hyperledger-fabric.readthedocs.io/en/latest/index.html> (accessed on 10 August 2019).
45. China National Energy Administration. National Energy Administration’s Notice on the Supervision of National Electricity Prices in 2017(2018). 2018. Available online: http://www.nea.gov.cn/2018-10/09/c_137519800.htm (accessed on 6 March 2019).
46. Bitcoin Historical Data. Available online: <https://www.kaggle.com/mczielinski/bitcoin-historical-data> (accessed on 17 March 2019).
47. Ethereum Historical Data. Available online: <https://www.kaggle.com/kingburrito666/ethereum-historical-data> (accessed on 17 March 2019).
48. Wang, X.; Gan, G.; Wu, L. Quantitative Analysis of Blockchain Performance. *Comput. Eng. Appl.* **2019**, 1–9. Available online: [http://kns.cnki.net/KCMS/detail/11.2127.tp.20190605.1639.003.html?uid=WEEvREcwSIJHSLdRa1FhdXNXaEd2OS9TbE1QNTISazAxSEZmbGhESjcwRT0=\\$9A4hF_YAuvQ5obgVAqNKPCYcEjKenS4lQMovwHtwkF4VYPoHbKxJw!!&v=MjgzNDhJMW9THo3TWFiRzRIOWpNcVk5QVpPc05ZdzlNem1SbjZqNTdUM2ZscVdNMENMTDdSN3FIYnVab0Z5emtXNzNL](http://kns.cnki.net/KCMS/detail/11.2127.tp.20190605.1639.003.html?uid=WEEvREcwSIJHSLdRa1FhdXNXaEd2OS9TbE1QNTISazAxSEZmbGhESjcwRT0=$9A4hF_YAuvQ5obgVAqNKPCYcEjKenS4lQMovwHtwkF4VYPoHbKxJw!!&v=MjgzNDhJMW9THo3TWFiRzRIOWpNcVk5QVpPc05ZdzlNem1SbjZqNTdUM2ZscVdNMENMTDdSN3FIYnVab0Z5emtXNzNL) (accessed on 13 July 2019).
49. Pu, Y.; Xiong, X.; Lei, L.; Kan, Z. Design and Implementation on Hyperledger-Based Emission Trading System. *IEEE Access.* **2019**, *7*, 6109–6116.

