energies

MDPI

Review

Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application

Zilong Zeng [1], Yong Li [1,*], Yijia Cao [1,*], Yirui Zhao [1], Junjie Zhong [1], Denis Sidorov [2] and Xiangcheng Zeng [3]

[1] College of Electrical and Information Engineering, Hunan University, Changsha 410082, China; zengzilong@hnu.edu.cn (Z.Z.); zhaoyirui_sy@hnu.edu.cn (Y.Z.); zhongjj@hnu.edu.cn (J.Z.)
[2] Energy Systems Institute, Russian Academy of Sciences, 664033 Irkutsk, Russia; dsidorov@isem.irk.ru
[3] Xinning Electric Power Supply Company of State Grid Hunan Electric Power Company, Xinning 422700, China; zengxc_sy@163.com
* Correspondence: yongli@hnu.edu.cn (Y.L.); yjcao@hnu.edu.cn (Y.C.)

Received: 9 January 2020; Accepted: 13 February 2020; Published: 17 February 2020

Abstract: In order to ensure the information security, most of the important information including the data of advanced metering infrastructure (AMI) in the energy internet is currently transmitted and exchanged through the intranet or the carrier communication. The former increases the cost of network construction, and the latter is susceptible to interference and attacks in the process of information dissemination. The blockchain is an emerging decentralized architecture and distributed computing paradigm. Under the premise that these nodes do not need mutual trust, the blockchain can implement trusted peer-to-peer communication for protecting the important information by adopting distributed consensus mechanisms, encryption algorithms, point-to-point transmission and smart contracts. In response to the above issues, this paper firstly analyzes the information security problems existing in the energy internet from the four perspectives of system control layer, device access, market transaction and user privacy. Then blockchain technology is introduced, and its working principles and technical characteristics are analyzed. Based on the technical characteristics, we propose the multilevel and multichain information transmission model for the weak centralization of scheduling and the decentralization of transaction. Furthermore, we discuss that the information transmission model helps solve some of the information security issues from the four perspectives of system control, device access, market transaction and user privacy. Application examples are used to illustrate the technical features that benefited from the blockchain for the information security of the energy internet.

Keywords: blockchain; energy internet; information security

1. Introduction

The energy internet is used mainly to realize the optimal allocation of resources across regions, the integrated utilization of multienergy and the optimized operation of multienergy systems [1–3]. It not only includes electricity, gas, heat, cold and other multienergy physical systems, but also includes a new type of information communication system represented by the secondary system of the smart grid. The information security crisis is hidden behind the rapid development of the energy internet [4]. In 2010, the first computer virus Stuxnet for industrial control systems was discovered [5,6]. Stuxnet first penetrated the computer network through an infected USB and other devices. Therefore, even an intranet that is isolated from the external network can be attacked by Stuxnet [7]. It has been reported that more than one-fifth of Iran's nuclear power plant centrifuges were damaged by Stuxnet.

In addition to Stuxnet, the United States and other countries have repeatedly found examples of hacking in industrial systems, including the power system [8–10]. These have highlighted the vulnerability of information security. With equipment informatization and the wide application of information and communication technology, security considerations and protection of the energy system should be expanded from the physical level to the informational level.

The emerging blockchain technology originated in the financial sector and has shown remarkable development in the financial field, which enables participator to trade with others and maintain a consistent and temper-proof ledger without a centralized bank [11,12]. The core advantage of the blockchain is the non-tampering, point-to-point transitivity, distributed storage and privacy protection. These characteristics ensure that different subjects can trust each other, which greatly reduces the cost of reshaping or maintaining trust, so that the blockchain technology can be further developed in other fields besides content delivery [13], key management [14], and decentralized storage [15,16]. Regarding the application of blockchain in energy internet, some domestic and foreign scholars have carried out some researches. In [17], the application scenarios and business models of the blockchain technology are introduced for energy generation, transmission, distribution and storage. In [18], a new hybrid blockchain storage mode is proposed to improve the overall efficiency of internet running, achieve a decentralized supervision, and provide a credible, safe and efficient performance of the energy internet in the storage of massive data. In [19], blockchain technology is utilized to realize a security check and congestion management for transactions verified by the central institution. In [20], the role of blockchain technology in different parts of the energy internet is expounded, such as in energy metrology certification, energy market transaction and energy finance. In [21], the decentralized energy trading system using blockchain technology was implemented. The result demonstrates this energy trading system using blockchain technology can be resistant to significant known attacks and keep financial profiles secure and private. In [22], a blockchain-based energy trading platform is proposed for electric vehicles in smart campus parking lots. Therefore, it is feasible to introduce blockchain technology into the energy internet.

Although blockchain technology has been applied in energy internet from the above articles, it has not been explored in information security. The blockchain can be a promising technique to help cope with the information security problems in energy internet because of characteristics such as non-tampering, point-to-point transitivity, distributed storage and privacy protection. In [23], the smart grid data storage alliance chain system is constructed through the alliance blockchain technology for collectively maintaining a secure and reliable data storage database in a decentralized way to prevent single point failure caused by malicious attacks and deliberate data tampering. In [24], the blockchain-based supply-demand interaction system architecture is designed for realizing the non-tamperable modification of the information generated by supply-demand interaction to prevent single point failure.

In this article, the application of blockchain in the energy internet is investigated from the perspective of multidimensional information security. The information security requirements existing in the energy internet is analyzed from the four perspectives of system control layer, device access, market transaction and user privacy. Then blockchain technology is introduced, and its working principles and technical characteristics are analyzed. Considering the large number of demand response resources, wide distribution and difficulty in direct control, we propose the multilevel and multichain information transmission model based on the blockchain for the weak centralization of scheduling and the decentralization of transaction. According to the functional requirements, the importance of the data, the computational power and the control area, the nodes based on the blockchain in the energy internet are divided into several types. Then the operational process of the proposed model is analyzed. Furthermore, we discuss how the proposed model can play the role of information protection in system control, device access, market transaction and user privacy. The superiority of the blockchain is discussed by comparing with other information defense technologies. Finally, the feasibility of using the blockchain for improving information security is analyzed by combining existing practical projects.

2. Demand Analysis of Information Security in Energy Internet

Energy internet is mainly composed of the physical system and information system shown in Figure 1, according to the difference in function [25]. The information system realizes the currency of the information among energy subnets, the energy interface, energy switches and energy routers. All running operations require accurate and timely information for technical support, including state estimation, fault handling, fault detection, operation optimization, optimal scheduling, load transfer, etc. The information systems require far more security than physical systems. Once a fault of the information system occurs, it would affect the operation of the entire multienergy system instead of the single one. This section analyzed the information security requirements of the energy system from four aspects: system operation layer, equipment access layer, market transactions layer and user privacy layer.

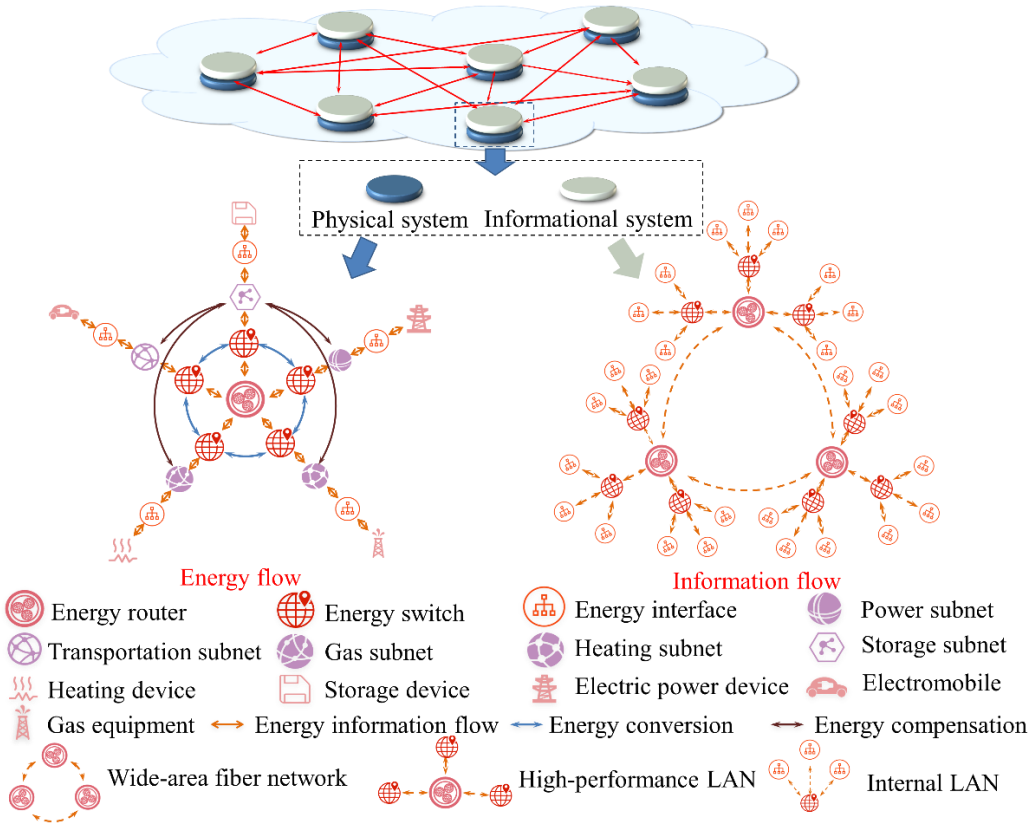

Figure 1. The partitioning-hierarchical architecture of the energy internet.

2.1. Information Security Requirements of the System Operation Layer

With the massive access of distributed devices, the energy-optimized scheduling must be developed toward being distributed. Figure 1 shows an energy internet with partitioning-distributed architecture including physical systems and information systems. The distributed control in this structure decomposes the set global optimization goals into several independent local optimization goals, which are computed in parallel on several nodes that can communicate with each other, such as the energy router in this architecture. These nodes are actually the regional control centers or the dispatching centers for each subsystem. Each node is only responsible for optimizing the local device and making adjustments based on the interaction information of adjacent nodes. This information does not necessarily come from its own system, but may also come from other energy systems. This control mode, such as the Alternating Direction Method of Multipliers (ADMM), is largely dependent on the information system, and only through continuous information interaction with neighboring

nodes can it achieve the same convergence as the centralized optimization algorithm [26]. Most distributed protection and distributed optimization are inseparable from information sharing. In [27], the integrated protection is proposed to realize more reliable and sensitive fault detection by sharing information and cooperation among different protection functions.

The information attacks vary in their type, form and impact, such as (1) GPS spoofing attacks [28], (2) time synchronization attacks [29], (3) Denial-of-Service (DOS) attacks [30] and False Data Injection (FDI) attacks [31]. The FDI attack is the more common information attack. If the attacker successfully launches an attack by manipulating or injecting false data either in the measurements or the control signals to the energy internet, it may lead to the wrong decision of the control center and eventually cause the chain failure. Countermeasures against FDI attacks are classified in the literature into protection-based methods [32] and detection-based methods [33]. However, when FDI attacks closely imitating the normal distribution of the measurements, these methods have the incapability of detecting the attacks [34]. Meanwhile the data mining technology is used to identify and correct data that may contain bad data or attack information [35]. However, the data mining technology is not a strict information protection technology. The defense measures applied to the smart grid are to establish a more targeted defense model for specific attacks, which has poor generalization ability. As soon as a new information attack technology emerges, it needs to be upgraded [20].

2.2. Information Security Requirements of the Equipment Access Layer

The distributed equipment connected to the system is rich and diverse, including electric vehicles, air conditioners and other smart home, as well as energy storage, power-to-gas, distributed energy and other large equipment [36,37]. At the same time, access methods are also various, which can be either through the industrial communication network or through open network access systems such as the internet [38–40]. It is difficult to manage and control the information interface of access equipment uniformly. The attacker can use the security vulnerability to obtain the identity information of the access device, interact with other devices through forgery or counterfeit identity, and initiate a Distributed Denial of Service (DDOS) attack [41,42], spreading illegal content [43], trace users identity and other information attacks by listening to the information and issuing false messages to interfere with the normal operation of the device.

2.3. Information Security Requirements of the Market Transactions Layer

With the development of energy internet, the distributed energy sources will be connected to the power grid [44,45]. Meanwhile, information data and the information scale will increase dramatically, the centralized decision-making method will increase the operating cost of the trading center and the time-consuming [46,47]. If the trading center operates is attacked by an external hacker, the security of the transaction and the privacy of the participants cannot be guaranteed [48]. Under this background, the distributed trading model with many participants and small trading volume has gradually become a trading trend [49]. Due to opaque information, unpublished rules and untimely subsidies during the distributed energy transaction process, the security of the transaction cannot be guaranteed [50]. For example, users cheat high subsidies by faking their own transactions and electricity usage data [51]. Furthermore, the distributed energy sources have small capacity and random output, so it is difficult to be directly connected with power grid [52]. Many scholars have proposed the control concept of virtual power plants to reduce the impact of these problems by aggregating distributed energy sources and centrally managing them [53,54]. This process requires accurate and reliable measurement and multilateral trust between virtual power plants and distributed energy sources. At present, due to the lack of a credible trading platform and an open transparent information platform, it is impossible to trade between virtual power plants or between virtual power plant and other users in a symmetrical environment. That increases transaction costs and transaction risks. The blockchain can help cope with the trust problem because of characteristics such as non-tampering, point-to-point transitivity, distributed storage and privacy protection [55].

2.4. Information Security Requirements of the User Privacy Layer

The energy consumption monitoring is an important component of energy internet [56,57]. For users, it helps to understand their own energy consumption situation, so that users can reduce excessive energy consumption and make more efficient use of energy by making reasonable energy use plans without affecting normal life. For the energy management department, it helps to optimize the allocation of energy and further provides them with real and effective data to reasonably schedule energy and reducing the energy rescheduling costs [58]. In the process of interaction, a large amount of information such as time, location, behavior, participants and purpose will inevitably be generated, which may contain personal sensitive information. If it cannot be effectively protected, it is easy to be intercepted by attackers in the process of information interaction or sharing [59–61]. If personal information is leaked, it may bring risks to personal property, life and even personal safety. If the equipment information is abused, it may affect the normal production order and constitute a serious security threat. Therefore, while providing users with better services, it is necessary to protect the private data of the user.

3. Principle and Technical Characteristics of Blockchain Technology

The build process of the blockchain is simplified as shown in Figure 2 and includes three main steps. The first block begins from the "Genesis Block" [62]. The newly generated blocks are connected from the previous block in chronological order. The block link is accomplished via the hash value metadata index of the father block. The blockchain users search the numerical solution that corresponds to the specific hash value, which is called "digging mine". When a user in the blockchain finds the solution, the user will broadcast the value solution over the entire network, and other users in the network will stop looking for the solution and turn to verifying the numerical solution. Once the numerical solution is verified, the newly built blocks are added to the existing blockchain. Then, the complete blockchain is generated.

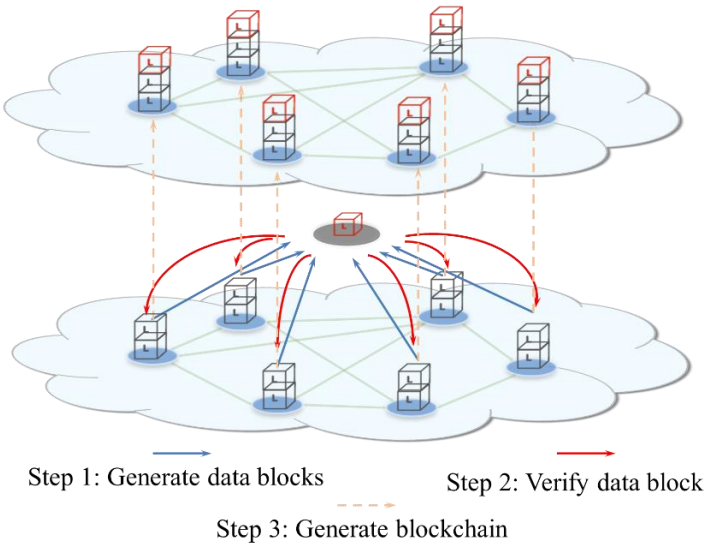

Figure 2. Workflow of blockchain technology.

The blockchain generally utilizes an intelligent contract to automate contract terms, a hashing algorithm to safeguard information confidentiality, a consensus mechanism to safeguard data integrity and an asymmetric key to safeguard data flow security. Figure 3 illustrates the security features of the blockchain technology.

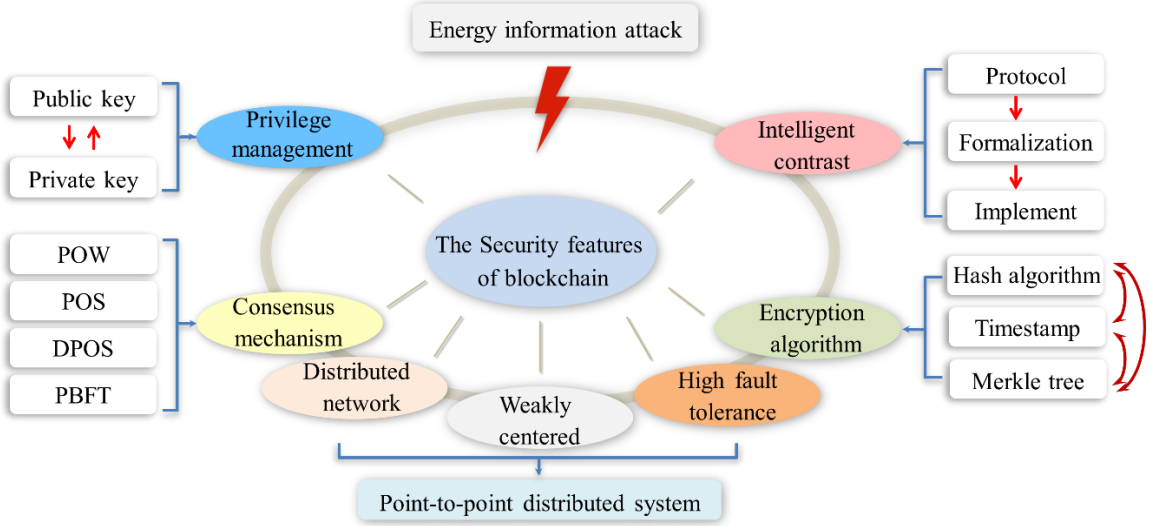

Figure 3. Security features of the blockchain technology.

3.1. Distributed Network, Weakly Centered and High Fault Tolerance

The major drawback of a traditional centralized architecture is that third-party owners can change data in a non-public way. The distributed architecture of the blockchain can solve the problem of tampering with data. In the blockchain network, there is no absolute central device and management organization, so that each device can serve as a node. Each node in the blockchain network has the same rights and obligations. Furthermore, each node has a full backup of data, tampering with information on any node cannot pass the consistency check of the global network. The only way to tamper with the information is to change more than 51% of the backup data [63]. Only in this way can the previous consistency condition be broken and a forged consistency check condition be established. It is not possible in the energy internet due to the number of nodes. Of course, not all nodes need to have a full backup. In addition, these nodes can also be set to nodes with different functional attributes according to different functional requirements.

3.2. Encryption Algorithm

The encryption algorithm mainly contains three parts, including the hash algorithm, the timestamp and the Merkle tree structure. The SHA-256 (Secure Hash Algorithm-256) hash algorithm is a one-way cipher system that ensures that transaction information cannot be tampered. The hash algorithm is used to encrypt the information block into an output hash that consists of a string in a one-way irreversible manner. In addition to the SHA-256, the typical hash algorithm includes the MD5, SHA1 and SM3. Table 1 is the performance comparison of the four algorithms [64]. The advantage of SHA-256 is still relatively obvious from Table 1. At present, the hash algorithm of Bitcoin is mainly SHA-256. The timestamp is part of the block metadata, which naturally causes the block to include a time attribute and proves the time validity of the data. Furthermore, each subsequent timestamp will enhance the pre-order timestamp, so the time security of the final blockchain is further promoted. The Merkle tree structure is used to store hash values for all transaction data and ultimately obtain a uniform hash value. The Merkle tree is similar to a tree structure in which the branches are the hash values of the transaction data [65]. The trunk is the hash value generated by the hash algorithm after combining the hash values on all branches. The Merkle tree greatly reduces the amount of data transmission and the difficulty of calculation in terms of data consistency. Once the information block is tampered with, including arbitrary information and the timestamp, the hash value will be different from the original and then cannot be verified by other nodes [66]. In other words, the best way to validate the data is checking the hash value.

Table 1. The performance comparison of the typical hash algorithms.

Hash Algorithm	Security Level	Calculating Speed	Output Byte
MD-5	Lowest	Fastest	128
SHA-1	Middle	Middle	160
SHA-256	Higher	Slightly slower than SHA-1	256
SM-3	Highest	Slightly slower than SHA-1	256

3.3. Consensus Mechanism

The consensus mechanism of the blockchain can ensure the consistency of data in the blocks of each node at a system with highly dispersed decision-making power. Every node in the system has read and write permissions for the block. However, only the node that first solves this complex but is easy to verify the mathematical problem can exercise the write permission. The mathematical problem is to find a random number such that the double hash value of the block header is less than or equal to a target hash value. As long as one node finds the random number, other nodes will start to verify the random number. Once more than half of the nodes pass the verification, they will stop searching for the random number and broadcast the random number directly. All nodes have reached consensus on the information in this block. According to different functional requirements, the current consensus mechanism is mainly divided into the following five categories: Proof of Work (POW) [67], Proof of Stake (POS) [68], Delegated Proof of Stake (DPOS) and Practical Byzantine Fault Tolerance (PBFT) [69]. Energy internet has the dispatch center, so it cannot be completely decentralized. From the Table 2, the PBFT not only have the highest efficiency and requires the lowest computational power, but also can realize the weakly centralized. It can be seen that PBFT is more suitable for the energy internet comparing other consensus mechanisms.

Table 2. The comparison of the typical consensus mechanisms.

Assessment Criteria	Degree of Centralization	Efficiency of Consensus	Computational Power	Fault Tolerance
POW	Lowest	Lowest	Highest	50%
POS	Lower	Lower	Middle	50%
DPOS	Middle	Middle	Lower	50%
PBFT	Highest	Highest	Lowest	33%

3.4. Intelligent Contrast

Intelligent contract refers to the program code stored in the distributed ledger, which realizes the functions of receiving, storing and transferring information [70]. Essentially, it is the computer program that can automatically execute the pre-set contract terms. By writing and storing the contents of the contract in the form of code, the system will be automatically executed without the outside parties once the conditions of the contract terms are met. Due to the decentralized nature and the cryptographic algorithms of the blockchain, the participating parties do not have the authority to change the clauses individually, which makes them trustful [71]. An intelligent contract greatly improves the degree of automation and idle resources integration ability.

3.5. Privilege Management

Privilege management is implemented primarily through asymmetric keys (public key and private key). The public key is full-net publicly visible; the private key has information owner control. In the permission control, information is encrypted by one of the keys and must then be decrypted with another key that matches it, which makes the information more manageable. The private key is signed to the information. The public key validates the signature. The information is encrypted by the public key and decrypted by the private key. These two processes achieve the effective transmission of

information. The blockchain stores data content in the form of code and creates an algorithmic trust between codes. In an open platform without third-party endorsement, these special characters can guarantee information security.

4. Information Transmission Model of Energy Internet Based on Blockchain

With the wide access of distributed energy, flexible and controllable multienergy devices such as distributed power generation, energy storage, controllable load, heat pump and power-to-gas equipment will become important regulating equipment in the energy internet. The energy internet is no longer a traditional single energy system. The number of distributed physical devices that need to be coordinated is uncountable at the energy internet. Therefore, traditional top-down centralized decision scheduling is no longer applicable, and decentralized distributed scheduling will become the development direction of energy internet. Based on whether there is subjective initiative in the defense strategy, the information defense strategy is classified into the proactive defense, the proactive defense and other defense strategies. So, we mapped the distributed architecture of blockchain and segmentation principle of the node permission to the hierarchical architecture and key nodes at energy internet to construct a multilevel and multichain information transmission model for realizing the weak centralization of scheduling and the decentralization of transaction. Figure 4 shows the multilevel and multichain information transmission model of energy internet based on the blockchain.

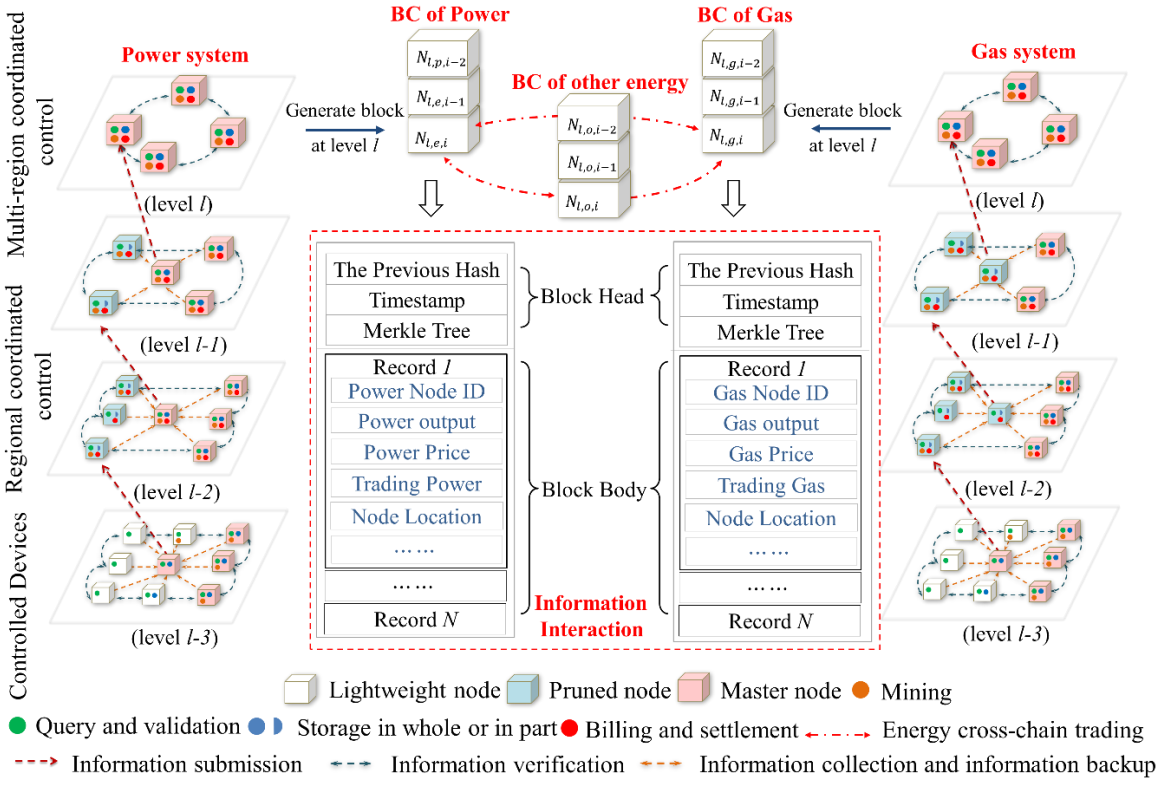

Figure 4. The multilevel and multichain information transmission model of energy internet based on blockchain.

4.1. The MultiLevel and MultiChain Information Transmission Model

Blockchain technology is to achieve decentralization by saving the complete blockchain on most nodes. Considering the different computational power of the node in the blockchain, it is not required that all nodes can provide the same amount of computational resources. Similarly, according to the functional requirements, the importance of the data, the computational power and the control area, the nodes in the energy internet are divided into the following types:

1. The master node: It stores the entire blockchain, verifies the new blocks that are broadcasted onto the network and ensures that information contained in blocks follow protocol rules. In addition to including the original functionality of the blockchain node, it can be considered as an energy trading node with the billing and settlement capabilities. Meanwhile it also can be considered as a control center for energy dispatch in the region.
2. The lightweight node: It only downloads block headers rather than the entire blockchain. The size of block headers is smaller than the block body. So, the lightweight node does not require very large storage space. It also needs to validate information authenticity by the simplified payment verification. The information authenticity is validated by solving a mathematical problem that is hard to solve but easy to verify. So, it does need the strong of the computational power. The lightweight node is easy to maintain and run than the master one. Most devices in the energy system can be considered as the lightweight node. Since they do not have the super computational power and the large storage space and just need to follow the instructions that can be validated by the decryption algorithm.
3. The pruned node: It only stores the latest fixed-length blockchain. In the energy internet, the scheduler does not directly control the distributed device, but only issues scheduling instructions to the agent. So, these agents can be a pruned node. It only needs to adjust the controlled equipment according to the latest superior scheduling instructions and the latest energy information of the controlled area.

The traditional centralized management will greatly increase the communication of the system pressure considering the number of the access devices. It cannot achieve real-time transmission of information and influence the execution of the scheduling plan. In case of communication network failure or a malicious attack, the stable operation of the whole system will be affected. Therefore, we divided the energy internet information system into multiple levels. The principle of hierarchical division in the different energy system is similar. So, we only described the principle in the power system. Firstly, the power system was divided into several levels according to the voltage level, and then each level was further divided into several areas according to the regional and network structure. In each area, we chose an agent that is responsible for coordinating the distributed devices within the region. These agents can be divided according to the control scope or the control functions [72,73]. The scheduler does not directly control the distributed device, but only issues scheduling instructions to the agent. The control center at each level is responsible for only one level of scheduling. It is natural that the communication pressure is reduced by the hierarchical approach. Meanwhile, the upper control center does not directly control the lower control center, but only makes a backup correction for the instructions of the lower control center. It keeps the autonomy of subordinate control centers.

Considering the differences, like the time inertia, between the different energy systems, it is impossible to build a unified blockchain for storing the entire information of the whole system. An exclusive blockchain, like the blockchain of power and the blockchain of gas, is built to store its own information of its own system. By cross-chain technology, energy trading and information fusion are achieved among the different blockchains [74]. In the hierarchical structure of the information transmission model, energy trading is not just initiated by the highest-level agents, and all agents can initiate energy transactions with other agents at the same level. So, the blockchain of different layers will be established. The different energy systems at each level will have their own blockchain. At last, the multilevel and multichain information transmission model of energy internet is built. It is beneficial to make the communication and negotiation between the source and the seller more convenient and improve the transaction timeliness and demand matching.

4.2. The Operational Process of the Proposed Information Transmission Model

Based on the multilevel and multichain information transmission model proposed in this paper, the system's operating process is shown in Figure 5. The process can be divided into three parts shown as follows:

1. Collect information: All nodes with scheduling and trading functions will collect information related to their functions. This information comes from the homologous system and heterologous system. The information collected in the homologous system includes the lower-level energy production plan, the higher-level energy scheduling plan, energy price, operation constrain, the location of energy-rich supply node and so on. The information collected in the heterologous system mainly includes the energy demand and the energy supply. When the load fluctuates greatly, it is likely that the shortage or surplus of the energy supply at the original system will occur, resulting in an imbalance in energy supply and demand. At this moment, on the premise of obtaining the information of energy supply and demand of other energy systems, energy trading can be used to alleviate the problem of the energy imbalances.
2. Energy trading: Each node firstly formulates its own energy dispatching strategy including energy trading with other system based on the collected relevant information and broadcast these dispatching strategies at the same level of blockchain network. The node with the "mining" capabilities collects all reasonable response strategies and packages them into a block. If this scheduling strategy in the block is executed directly without verifying, it is likely to cause the system to crash. So, the miner verifies whether these response strategies of each at this stage meet the convergence conditions before the response strategies are executed [75]. If not, the correction variables are added to these response strategies and recompose the new response strategy. No correction variable is added until these scheduling strategies of all nodes meet the convergence conditions. Once these scheduling strategies meet the convergence conditions, the miner adds this block to the local blockchain and broadcasts the latest blockchain to the whole network.
3. Execute scheduling instruction: Each device queries the latest blockchain and obtains the encrypted files stored in the new block. The scheduling instruction in the encrypted files is encrypted by the recipient's public key. The device only uses the private key to decrypt the files for obtaining the scheduling instruction. At last, the scheduling instruction is executed by the corresponding device.

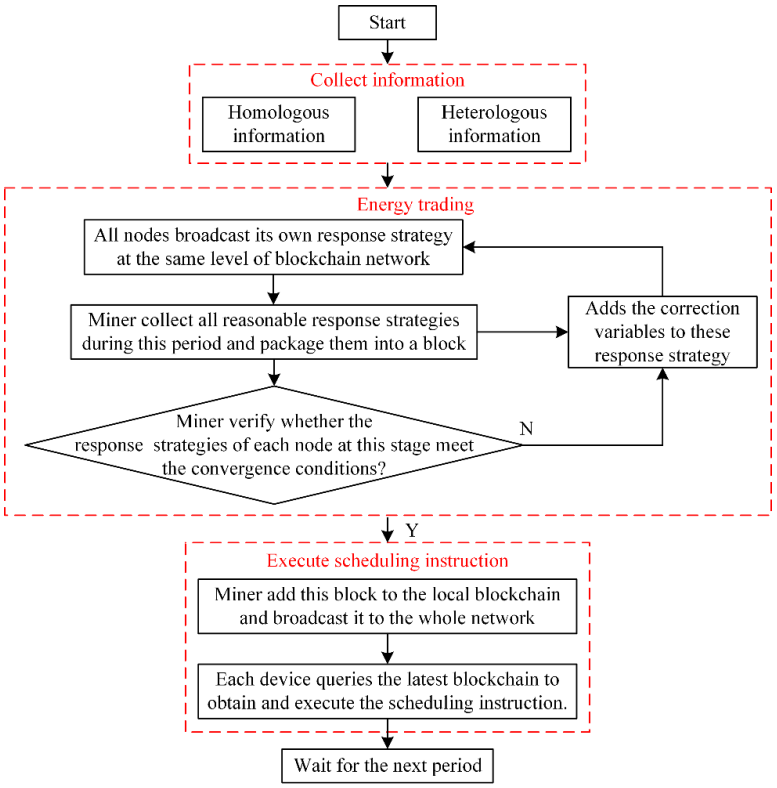

Figure 5. The flowchart of the multilevel and multichain information transmission model.

5. Application of the Information Transmission Model in the Information Security of Energy Internet

In this section, the solutions of the blockchain technology for the information security problems in the energy internet were discussed from the structural layer, the data layer, the value layer and the privilege layer, as shown in Figure 6. At last, we compared the advantages and disadvantages of the proactive defense, passive defense and blockchain in information security.

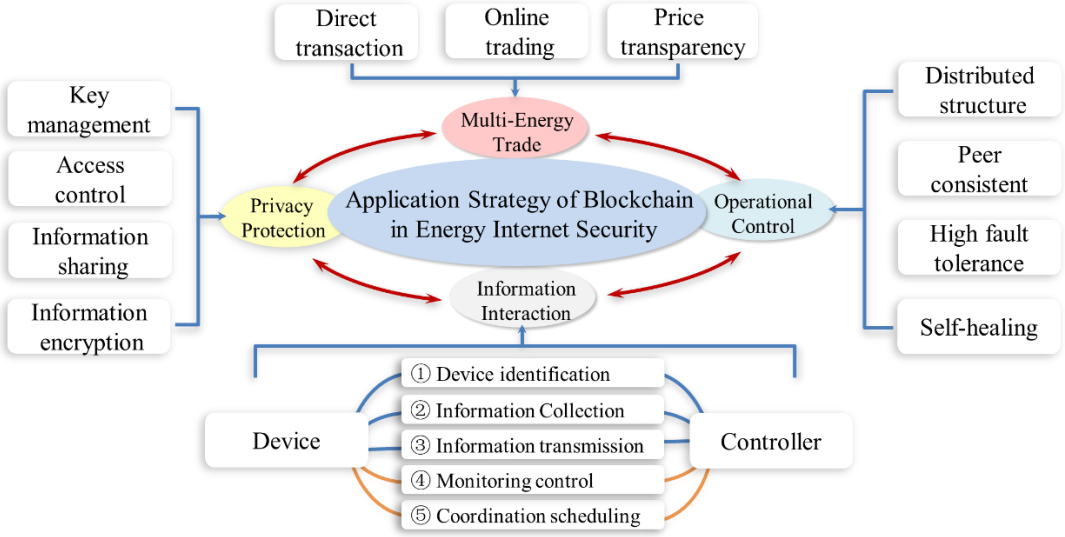

Figure 6. Illustration on the application of blockchain technology in the energy internet.

5.1. Security from the Operational Control Layer of the Energy Internet

Figure 7 compares the information flow of the traditional centralized and blockchain architectures. The traditional centralized architecture exists in the central server, the information gathering center and the control center. Once the central server is abnormal, the secure operation of the information system will weaken, even causing cascading failures of non-homogeneous energy systems. The blockchain adopts a decentralized architecture that can solve the inherent problems.

The multilayer block network, which can be weakly centered or completely decentralized, should be constructed considering the number of controlled devices or area control centers. Each device and control center can act as a node in the multilayer block network. All nodes are divided into different layers according to control area and function attribute. Peer nodes in the same layer of the block-chain have the same rights and obligations, while these nodes can retain their own matching properties. Each device or control center has its own private key. When these nodes broadcast their own data, they will add a digital signature encrypted with the private key at the end of the data package. Only the authorized node can decrypt the encrypted packet with the public key matching the private key. Since the attacker does not have the public key, it is impossible to decrypt the data even if the packet is intercepted. The communication between nodes adopts a mesh structure, and the transmission link is not unique. Even if an attacker blocks some communication links between nodes, information can still be transmitted through other paths. Furthermore, the control center of the same layer has written a complete backup of the blockchain data. Even if some control centers of this layer are paralyzed by an attack, they can be repaired through the database of other nodes in the same layer or other special nodes in the upper and lower layers.

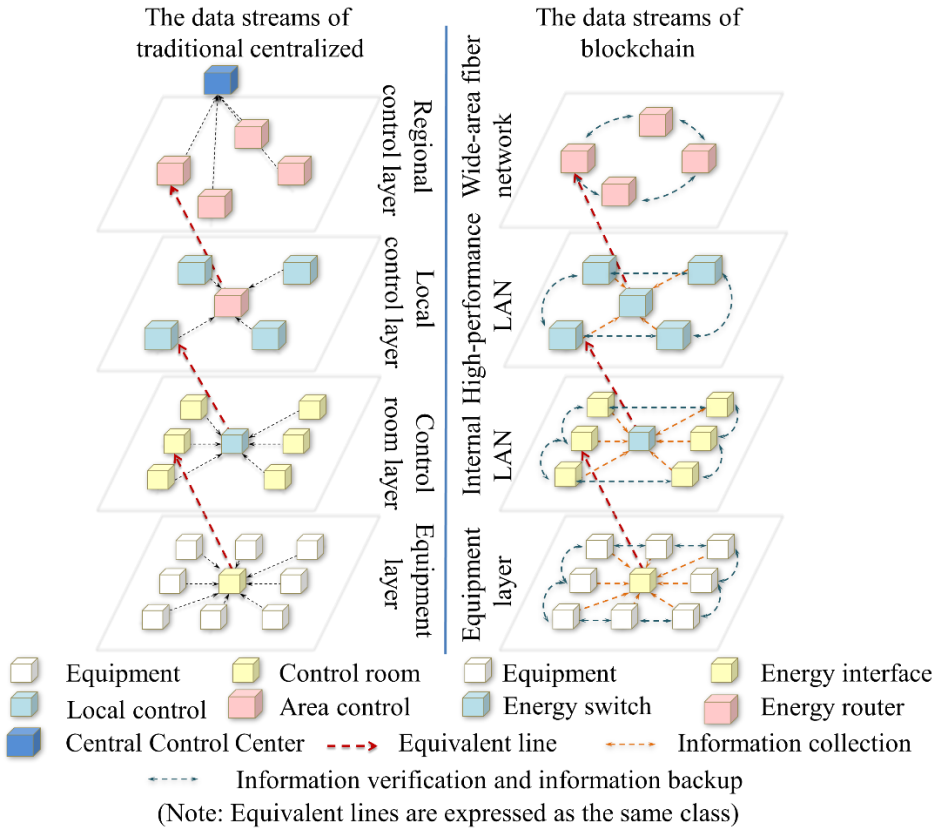

Figure 7. Comparison on information flow and structures between the traditional centralized and blockchain technologies.

With the help of the ADMM, it is explained how the proposed model can be applied in distributed optimization. The ADMM is one of the methods to solve distributed optimization problems. It combines the decomposability of dual rising method and the good convergence of multiplier method. The ADMM has the advantages of simple form, good convergence and strong robustness. The standard form of the ADMM is shown as follow [76]:

$$\begin{cases} \min f(x) + g(z) \\ Ax + Bz = c \end{cases} \tag{1}$$

where f(x) and g(z) are both convex functions; x and z are the variables. A, B and c are the known parameters.

The augmented Lagrange function is shown as follows:

$$L_\rho(x, z, \lambda) = f(x) + g(z) + \lambda^T(Ax + Bz - c) + \frac{\rho}{2}\|Ax + Bz - c\|_2^2 \tag{2}$$

where λ is the dual variable and $\rho \geq 0$ is the penalty coefficient.

The standard format for variable substitution in the $k + 1$ -th iteration is shown as follows:

$$\begin{cases} x^{k+1} = argmin_x L_\rho\left(x, z^k, \lambda^k\right) \\ z^{k+1} = argmin_z L_\rho\left(x^{k+1}, z, \lambda^k\right) \\ \lambda^{k+1} = \lambda^k + \rho\left(Ax^{k+1} + Bz^{k+1} - c\right) \end{cases} \tag{3}$$

The convergence conditions are shown as follows:

$$\begin{cases} \|Ax^{k+1} + Bz^{k+1} - C\|_2 \leq \varepsilon_1 \\ \|\rho A^T B\left(Z^{k+1} - Z^k\right)\|_2 \leq \varepsilon_2 \end{cases} \tag{4}$$

where ε_1 and ε_2 are the preset thresholds.

System S1 and system S2 represent the different systems of the energy system to describe this process. In the proposed information transmission model, f (x) and g (z) can be considered as the different objective function of system S1 and system S2. A, B and c represent the collected information described in the above subsection. x and z represent the different response strategy of the different system. It is obvious that in this problem exists two objective functions. However, it is easy to convert the multiple targets model into the single target model by introducing the weight coefficient. At first, S1 and S2 make the response strategy based on the collected information, respectively. Then the miner verifies whether these response strategies meet the convergence conditions (4). If not, S1 and S2 revise the strategy shown in (3), which is based on the previous response strategy. Until these response strategies meet the convergence condition meet the convergence conditions, the final scheduling policy is determined.

5.2. Security from the information Interaction Layer of the Energy Internet

As shown in Figure 7, the data in the traditional system are aggregated into the centralized control center and are then transmitted. While the blockchain system integrates all information into the information block and then broadcasts and stores the information block after verification, different nodes in the same layer save full backup files. In the traditional system, if any node or any control center is at fault, the control area of the abnormal center will collapse. However, the blockchain system utilizes the backup of adjacent nodes from the same layer to maintain control of the fault area, which makes information systems more reliable and robust.

The self-description of the intelligent device is stored in the blockchain in the form of code, and the distributed database of device attributes is built. The intelligent device is identified by the distributed database and is connected to the energy network. The intelligent device and the control center allocate asymmetric key pairs separately. The packets generated on the intellectual device are encrypted by the hash algorithm and are attached with the private key signature. The control center uses the matching public key to decrypt the packet. The decision system will automatically generate commands that pass to the related device by similar encryption and decryption methods. In summary, the distributed database allows efficient identification of the equipment, the hash algorithm guarantees the authenticity of information security and the asymmetric key of the encryption and decryption methods facilitates the precise transmission of information.

5.3. Security from the Privacy Protection Layer of the Energy Internet

Information right management of the energy internet can be classified as information sharing, privacy protection (information non-sharing) and access controls [77]. As shown in Figure 8, multidomain information sharing achieves high precision of energy optimization configurations. The lack of comprehensive information will cause decision deviation. For the user, it is necessary to manage the access rights of the information, which contains privacy content such as the user's customary information, head of household information, etc.

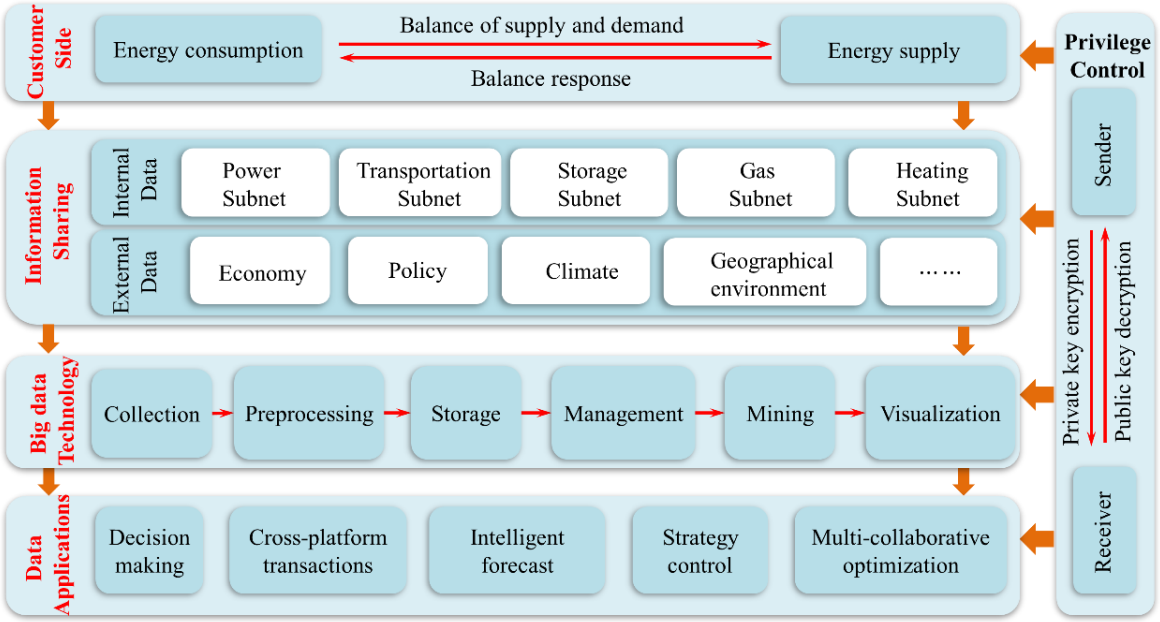

Figure 8. Achieving multioptimization configuration through information sharing based on the blockchain.

The blockchain records the internal information of the multienergy system (the operating state of the equipment, the load demand of each node, the real-time energy price, etc.) and the external information except for the multienergy system (weather conditions, wind speed, wind direction, illumination, etc.). The real-time sharing of information can be processed by big data technology for mining the potential of the multienergy systems and can optimize the operating state of the system.

Figure 9 shows the process of information protection in the blockchain. An attacker acquires the characteristics of the user's behavior, energy dissipation characteristics, etc. by stealing information and then performs an accurate attack on the system or the users. The "asymmetric key" in the blockchain realizes the privilege control of information. The sender uses the private key to sign the information and the recipient's public key to encrypt the information. The recipient uses the sender's public key to verify his/her identity and decrypts the encrypted information with his/her own private key. As long as the public key and private keys are controlled, the user can control the permissions of the information to protect the security of the information. In addition to managing the original single private key, the secret sharing scheme of private key can be used to protect the private keys [78,79]. Firstly, the private key is divided into n pieces, which are jointly stored by the n participants. Only when more than t participants cooperate together, the private key can be reconstructed. It greatly improves the security of the private key.

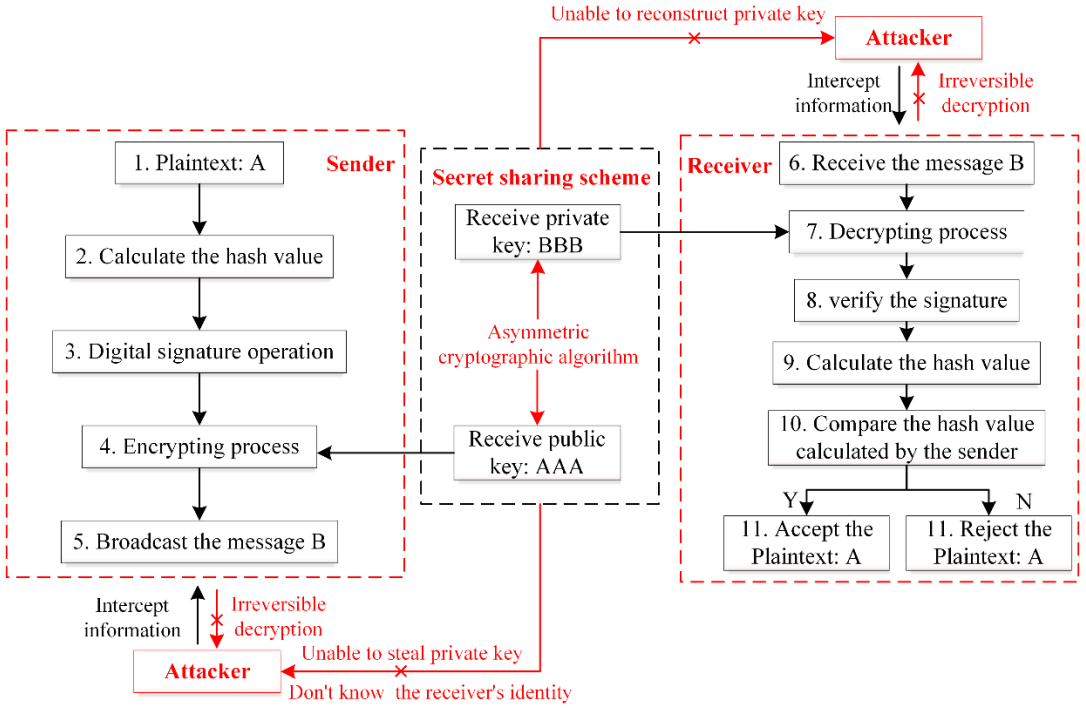

Figure 9. Flow chart of information protection in the blockchain.

5.4. Security from the Energy Trade Layer of the Energy Internet

The integration of distributed energy and the innovation of energy technology make the energy flow change from unidirectional flow to bidirectional flow. In the new type of energy system, traditional energy consumers are considered not only as energy producers but also as energy makers. As shown in Figure 8, the boundary energy prices are generated by utilizing the shared information stored in the block chain and indirectly promote the transformation from the traditional single-energy commercial transaction model to the cross-platform multienergy commercial transaction mode.

Traditional trading is from sellers to clients, but now, users in some small areas can directly trade with other users or energy sellers. The innovation in the energy market allows users to have multiple options for energy suppliers. Users not only can choose the energy sellers but also can independently sell energy produced by themselves at a real-time price. In this process, the blockchain not only verifies the credit of energy sellers but also provides trading platforms. The distributed "book keeping" principle and the authentication mechanism guarantee the authority of metrology and certification. Any assets can be stored in the form of code and can then be transformed into intelligent assets in the blockchain. Blockchain record, track and monitor the properties and changes of assets to prevent tampering. Furthermore, Smart contracts can be formulated in the blockchain. Once the contract is reached, the contract terms will be automatically enforced. This not only guarantees the implementation and reliability of the contract but also is conducive to the fairness of the energy market.

5.5. Comparison of the Blockchain and Other Security Technologies

Important information in the energy internet is mainly transmitted and exchanged through the intranet, mostly by carrier communication, which is easily disturbed and attacked. For data that may contain bad data or attack information, data mining techniques are used to identify and correct such issues. It is not universal that a specific model must be established for a specific attack problem. Based on whether there is subjective initiative in the defense strategy, the information defense strategy is classified into the proactive defense, the proactive defense and other defense strategies. Table 3

compares the advantages and disadvantages of the proactive defense, passive defense and blockchain in information security.

Table 3. Advantages and disadvantages of proactive defense, passive defense and the blockchain.

Categories	Advantages	Disadvantages
Firewall technology	1. Monitor network access to Strengthen the security strategy 2. Check the information to reject suspicious access.	1. Once the attack is successful, the original defense system is no longer defensive. 2. Illegal operation of legitimate users cannot provide better defense.
Intrusion monitoring	1. Track the attacker's attack line. 2. Detect flood attacks committed by hackers as legitimate users.	1. Cannot make up for the system vulnerabilities without user involvement. 2. Cannot prevent an attack without user involvement.
Honeypot technology	1. Analyze the captured behavior to obtain the hacker's feature. 2. Regulate the behavior of the intruder to reduce the damage.	1. Only track and capture activities that interact directly with it. 2. Exposed the real operating system to attackers.
Trusted computing	1. Build an absolutely trust root stored outside the trust platform. 2. Build the trust chain among the connected devices.	1. The trust root is stored outside the trusted platform module. 2. Once a component is changed, the value of the PCR needs to be recalculated.
Blockchain	1. Establish a trust mechanism. 2. Remove the harmful parts. 3. Ensure the data's integrity. 4. Control the access rights of the information network.	1. Difficult to balance between the degree of decentralization and the efficiency of the consensus. 2. Difficult to balance between storage capacity and processing performance.

(1) Passive Defense: This is a pre-set defense against known attacks, but the lack of subjective considerations makes passive defense lose the ability to fully protect real-time information systems. A firewall is the most common passive defense technology and establishes a barrier (security gateway) between the internal trusted network and external non-trusted network to prevent external users from intruding into the internal network by illegal means [80]. Although a firewall can defend against known attacks by designing defensive rules in advance, it is helpless in defending against the threat of internal attacks and backdoor attacks. At the same time, this is the most serious flaw of the passive defense system. In addition, passive defense includes identity authentication technology [81], access control [82], intrusion detection [83] and other technologies.

(2) Proactive Defense: This defense is based on the independent analysis and judgement of procedural behavior, which can be more proactive in searching and dealing with hazards. It can counter the attackers to safeguard the security of the information system. Honeypot technology is the most common active defense technology, which designs deliberate system vulnerabilities to guide hackers to attack [84]. It can detect eavesdropping hackers and collects all kinds of hacker attack tools for later defense. Proactive defense makes up for the lack of passive defense through the consideration of subjective factors and can take active defense measures against an attack. In addition, proactive defense technology includes trap technology, vulnerability scanning [85], trusted computing technology [86] and other technologies.

(3) Blockchain: A blockchain is not a type of information defense technology, but its unique properties can provide higher anti-interference and confidentiality to the information data. Block technology can be used as the bottom of the energy internet information system technology. Each perceptual device assigns a fixed private key and adds a digital signature encrypted with multiple private keys at the end of the resulting packet. The information node chain of the whole system forms

a mesh structure, which makes the data path have high redundancy. The digital signature not only makes it difficult for attackers to forge sensor data but also makes it impossible for attackers to decrypt the data content. Even if the attacker blocks part of the data path in the network, the highly redundant mesh structure allows the information to be transmitted across other data paths.

6. Typical Application Scenario of The Blockchain in energy internet

The concept and construction mode of blockchain have been relatively mature, and some research results have been obtained in the application analysis of energy utilization. Meanwhile, the application of blockchain in information security at the energy internet also has begun to emerge. This section analyzes the feasibility of using the blockchain for improving information security from several projects.

6.1. Case 1: Info-Interconnection Among Devices

ADEPT (autonomous decentralized peer-to-peer telemetry) was jointly created by the International Business Machines Corporation and the Samsung Group to build an internet of things based on the blockchain, aiming to solve the problem of informational interconnection among devices [87]. The system consists of three elements: BitTorrent (file sharing), Ethereum (intelligent contract) and TeleHash (a point-to-point information transmitting system). BitTorrent is used to transmit data. It can ensure the dispersion characteristics of data and can avoid the impact of network instability. TeleHash is a terminal-to-terminal cryptographic library designed for application connections between devices and management devices. These elements can be used for achieving device registration and certification, formulating interaction rules based on the consensus mechanism, automatizing contract executions and other functions.

When the information interacts between the devices, the Adept system will execute the function of the distributed storage and track the relationships between the participants. The Adept system can build a bridging information link between devices via various types of protocols. The self-describing file of the device stored in the blockchain can help the device understand the functions of other devices. In other words, it allows devices to track relationships with other devices or the user. As shown in Figure 10, intelligent washing machines achieve information interconnection with other devices using the Adept system. By obtaining the amount of the user's exercise and the frequency of laundry from the smartphone or the smart watch, the intelligent washing machine can automatically calculate the residual amount of detergent and complete the online purchase behavior. The opening time of the washing machine can be automatically regulated based on the power market time-sharing price.

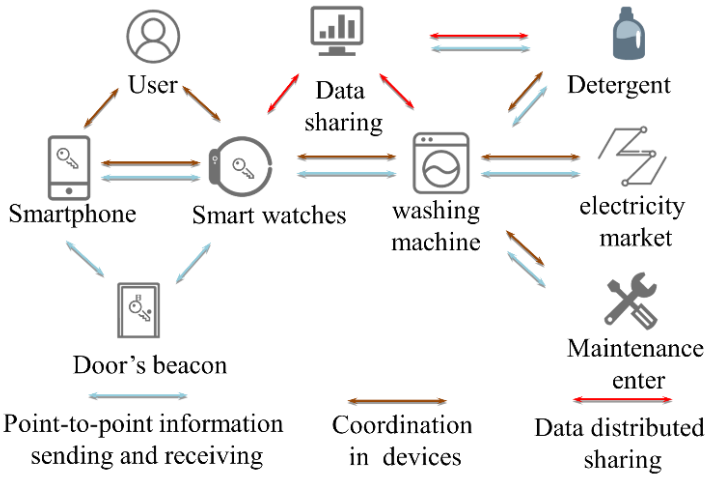

Figure 10. Application scenarios of the autonomous decentralized peer-to-peer telemetry (ADEPT) system.

6.2. Case 2: Operation Monitoring of Devices

Filament is the application of IoT (Internet of Things) software stack based on the blockchain shown in Figure 11, which makes a unique identity for each device [88]. Filament has two main hardware units: Filament Tap and Filament Patch. The Filament platform includes five protocols: Blockname, TeleHash, Smart contract, Pennybank and BitTorrent. The operation of Filament Tap depends on the first three protocols, and the user can choose the next two protocols as a technology extension. Blockname generates a unique identifier in the embedded chip of the device and stores it in the blockchain. TeleHash provides peer-to-peer encryption channels. BitTorrent supports file sharing. Pennybank creates a hosted service between two devices that allows them to settle transactions when they are online. It achieves perfect communication between the internet and other devices by creating an intelligent device directory.

Filament uses block-chain technology to upgrade the transmission equipment in the traditional Australian grid. By arranging a set of "taps" for sensor monitoring on the poles and establishing a corresponding communication mechanism, the poles are built into a digital node. It can monitor the operation of the equipment based on the data published and shared in the blockchain system. If the smart digital pole caught fire or began to tip, it would generate an incident report in real time into the blockchain and notify the maintenance crews to deal with the fault. Meanwhile, the nearest working pole would take over responsibility for the faulty pole. In addition to monitoring its own status, smart digital poles can perform fault diagnosis and fault location through information sharing. Once the digital node senses any exception, the monitoring platform will issue a status alert.

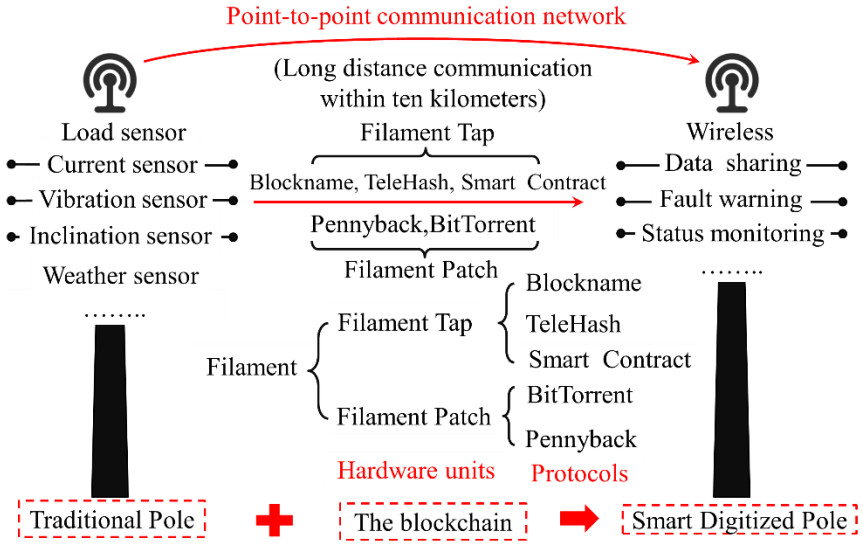

Figure 11. Application of the blockchain in the communication poles of the Filament project.

6.3. Case 3: Free and Direct Trade Among Users in the Micro-grid

The transactive grid is a trading platform developed by the Lo3 energy and consensus systems, shown in Figure 12 [89]. The residents that participate in the project use solar energy to generate electricity, and each household has a smart meter connected to the blockchain. The smart meter can monitor the energy flow from the sides of the energy supplier and consumers in order to achieve a dynamic balance of supply and demand. Energy trading can be automatically executed by using an intelligent contract. Participants can perform autonomous transactions without relying on third parties. On the one hand, the excess energy can be fed back to the grid; on the other hand, it can be directly sold to other users.

Smart meters based on the blockchain can record the flow of energy and enable autonomous management and transactions of energy. Secure and credible transactions require trusted metering

and authoritative certification. The technical characteristics of the blockchain can guarantee the authority. More importantly, the blockchain can expand the scope of the transaction. Once the trading conditions are met, it can build the trading channels by the authentication mechanism without trust between participants.

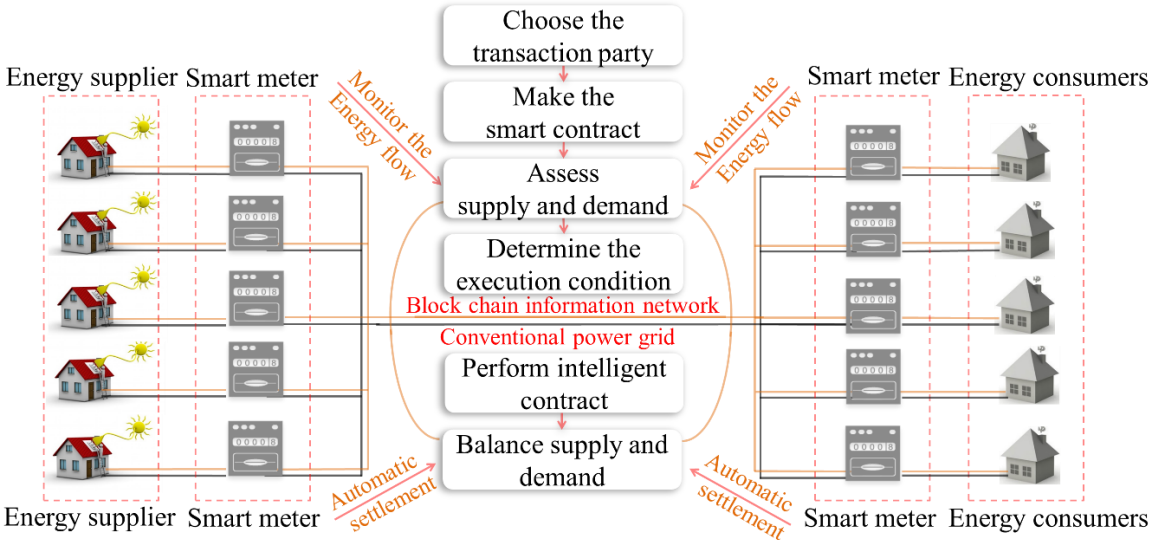

Figure 12. Demonstration of the blockchain technology in the energy market of a smart community.

7. Conclusions

Blockchain technology provides a series of innovation concepts to energy systems. The research goal in this paper was to improve information security of the energy internet. On the basis of summarizing the information security, the principle and technical characteristics of the blockchain were expounded. Furthermore, by comparing the blockchain to other information defense technologies, this paper discussed the superiority of the blockchain in information security. Based on the superiority of blockchain in information security, the multilevel and multichain information transmission model was proposed for the weak centralization of scheduling and the decentralization of transaction. Then we systemically analyzed a way to use this model for improving the information security of the energy internet. Finally, by combining existing practical projects, the final section analyzed the feasibility of using the blockchain for improving information security.

At present, most research regarding the blockchain pays more attention to virtual currency, finance and computers and less attention to the fields of energy. The only research regarding the combination of blockchain and the energy internet focuses on the research directions of energy trading, market mechanisms and demand response. These research directions can explain the characteristics of the blockchain to some extent, but they do not expound on their unique characteristics in information security. The biggest advantage of the blockchain in information security is its ability to prevent tampering. When tampering with notarized information, attackers must tamper with more than 51% of the node's backup information for establishing a new consistency test condition, which requires very large amounts of computing power. It is very difficult for an ordinary information attacker to possess such powerful computing power. The new-type chain information security defense system is the most important research method for the blockchain. In detail, a multilevel information security protection system combined with multiple security technologies must be built for protecting the security of systems from every aspect, such as the perception layer, the data transmission layer and the application control layer. This is expected to truly achieve information security and information self-healing

Author Contributions: Conceptualization, Y.L. and Y.C.; methodology, D.S. and Y.C.; writing—original draft preparation, Z.Z., J.Z., X.Z. and Y.Z.; writing—review and editing, Z.Z., J.Z., X.Z. and Y.L.; investigation, Y.L. and Y.C.; supervision, Y.C. and D.S.; funding acquisition, Y.L. and Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant U1966207, in part by the Key Research and Development Program of Hunan Province of China under Grant 2018GK2031, in part by the 111 Project of China under Grant B17016, in part by the Innovative Construction Program of Hunan Province of China under Grant 2019RS1016, in part by the Excellent Innovation Youth Program of Changsha of China under Grant KQ1802029, and in part by the program of fundamental research of SB of Russian Academy of Sciences, reg. no. AAAA-A17-117030310442-8, research project III.17.3.1.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Tsoukals, L.H.; Gao, R. From smart grids to an energy internet: Assumptions, architectures and requirements. In Proceedings of the International Conference on Electric Utility Deregulation & Restructuring & Power Technologies, Nanjing, China, 6–9 April 2008. [CrossRef]
2. Wang, K.; Yu, J.; Yu, Y.; Qian, Y.; Zeng, D.; Guo, S.; Xiang, Y.; Wu, J. A survey on energy internet: Architecture, approach, and emerging technologies. *IEEE Syst. J.* **2017**, *12*, 2403–2416. [CrossRef]
3. Ma, Y.; Wang, X.; Zhou, X.; Gao, Z.; Wu, Y.; Yin, J.; Xu, X. An overview of energy internet. In Proceedings of the Control & Decision Conference, Yin Chuan, China, 28–30 May 2016. [CrossRef]
4. Dan, G.; Sandberg, H.; Ekstedt, M.; Bjorkman, G. Challenges in power system information security. *IEEE Secur. Priv.* **2012**, *10*, 62–70. [CrossRef]
5. Tatar, U.; Bahsi, H.; Gheorghe, A. Impact assessment of cyber-attacks: A quantification study on power generation systems. In Proceedings of the 2016 11th System of Systems Engineering Conference, Kongsberg, Norway, 12–16 June 2016. [CrossRef]
6. Shakarian, P.; Shakarian, J.; Ruef, A. Attacking Iranian nuclear facilities: Stuxnet. *Introd. Cyber-Warf.* **2013**, 223–239. [CrossRef]
7. Karnouskos, S. Stuxnet worm impact on industrial cyber-physical system security. In Proceedings of the. Conference of the IEEE Industrial Electronics Society, Melbourne, Australia, 7–10 November 2011. [CrossRef]
8. Khan, R.; Maynard, P.; Mclaughlin, K.; Laverty, D.; Sezer, S. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. *Int. Symp. ICS SCADA Cyber Secur. Res.* **2016**, 53–63. [CrossRef]
9. Robert, L.; Anton, C. Blackenergy Trojan Strikes Again: Attacks Ukrainian Electric Power Industry. Available online: http://www.we-livesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-Attacks-Ukrainianan-electric-power-industry/ (accessed on 4 January 2016).
10. Titcomb, J. Ukrainian Blackout Blamed on Cyber-Attack. Available online: http://www.tele-graph.co.uk/technology/news/12082758/Ukr-ainian-blackout-blamed-on-cyber-attack-in-world-first.html (accessed on 5 January 2016).
11. Christidis, K.; Devetsikiotis, M. Blockchain and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
12. Yang, Z.; Zheng, K.; Yang, K.; Leung, V.C. A blockchain-based reputation system for data credibility assessment in vehicular networks. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 Octorber 2017. [CrossRef]
13. Herbaut, N.; Negru, M. A model for collaborative blockchain-based video delivery relying on advanced network services chain. *IEEE Commun. Mag.* **2017**, *55*, 70–76. [CrossRef]
14. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.P.A.; Sun, Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet Things J.* **2017**, *4*, 1832–1842. [CrossRef]
15. Cai, C.; Yuan, X.; Wang, C. Hardening Distributed and Encrypted Keyword Search via Blockchain. In Proceedings of the 2017 IEEE Symposium on Privacy-Aware Computing (PAC), Washington, DC, USA, 1–4 August 2017. [CrossRef]

16. Cai, C.; Yuan, X.; Wang, C. Towards trustworthy and private keyword search in encrypted decentralized storage. In Proceedings of the 2017 IEEE International Conference on Communications, Paris, France, 21–25 May 2017. [CrossRef]
17. Wang, A.; Fan, J.; Guo, Y. Application of blockchain in energy interne. *Electr. Power Inf. Commun. Technol.* **2016**, *14*, 1–6. [CrossRef]
18. Wu, L.; Meng, K.; Xu, S.; Li, S.; Ding, M.; Suo, Y. Democratic centralism: A hybrid blockchain architecture and its applications in energy internet. In Proceedings of the IEEE International Conference on Energy Internet, Beijing, China, 17–21 April 2017. [CrossRef]
19. Tai, X.; Sun, H.; Guo, Q. Electricity transactions and congestion management based on blockchain in energy internet. *Power Syst. Technol.* **2016**, *40*, 3630–3638. [CrossRef]
20. Zhang, N.; Wang, Y.; Kang, C.; Chen, J.; Dawei, H. Blockchain technique in the energy internet: Preliminary research framework and typical applications. *Proc. CSEE* **2016**, *36*, 4011–4012. [CrossRef]
21. Aitzhan, N.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
22. Suiva, F.C.; A Ahmed, M.; Martinez, J.M.; Kim, Y.C. Design and Implementation of a Blockchain-Based Energy Trading Platform for Electric Vehicles in Smart Campus Parking Lots. *Eneigies* **2019**, *12*, 4814. [CrossRef]
23. Ding, W.; Wang, G.; Xu, A.; Hong, C. Research on key technologies and information security issues of energy blockchain. *Proc. CSEE* **2018**, *38*, 1026–1034. [CrossRef]
24. Li, B.; Zhang, J.; Qi, B.; Li, D.; Shi, K.; Cui, G. Blockchain: Supporting technology of demand side resources participating in grid interaction. *Electr. Power Constr.* **2017**, *38*, 1–8.
25. Sun, Q.; Teng, F.; Zhang, H. Energy Internet and Its Key Control Issues. *Acta Autom. Sin.* **2017**, *42*, 176–194. [CrossRef]
26. Mhanna, S.; Verbic, G.; Chapman, A.C. Adaptive ADMM for Distributed AC Optimal Power Flow. *IEEE Trans. Power Syst.* **2019**, *34*, 2015–2035. [CrossRef]
27. He, J.; Liu, L.; Li, W.; Zhang, M. Development and research on integrated protection system based on redundant information analysis. *Prot. Control Mod. Power Syst.* **2016**, *1*, 108–120. [CrossRef]
28. Liu, S.; Liu, X.; Saddik, A. Denial-of-Service (dos) attacks on load frequency control in smart grids. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 Feburary 2013. [CrossRef]
29. Zhang, Z.; Gong, S.; Dimitrovski, A.; Li, H. Time Synchronization Attack in Smart Grid: Impact and Analysis. *IEEE Trans. Smart Grid* **2013**, *4*, 87–98. [CrossRef]
30. Konstantinou, C.; Sazos, M.; Musleh, A.; Keliris, A.; Al-Durra, A.; Maniatakos, M. GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 180–187. [CrossRef]
31. Liang, G.; Zhao, J.; Luo, F.; Weller, S.; Dong, Z. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [CrossRef]
32. Yang, Q.; Yang, J.; Yu, W.; An, D.; Zhang, N.; Zhao, W. On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 717–729. [CrossRef]
33. Khalid, H.; Pend, J. A Bayesian Algorithm to Enhance the Resilience of WAMS Applications Against Cyber Attacks. *IEEE Trans. Smart Grid* **2016**, *7*, 2026–2037. [CrossRef]
34. Gu, C.; Panida, J.; Mehul, M. Detecting False Data Injection Attacks in AC State Estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [CrossRef]
35. Xu, L.; Jiang, C.; Wang, J.; Yuan, J.; Ren, Y. Information Security in Big Data: Privacy and Data Mining. *IEEE Access* **2014**, *2*, 1149–1176. [CrossRef]
36. Chen, H.; Wang, X.; Li, Z.; Chen, W.; Cai, Y. Distributed sensing and cooperative estimation/detection of ubiquitous power internet of things. *Prot. Control Mod. Power Syst.* **2019**, *4*, 151–158. [CrossRef]
37. Hannan, M.; Faisal, M.; Ker, P.J.; Mun, L.H.; Parvin, K.; Mahlia, T.M.I.; Blaabjerg, F. A Review of Internet of Energy Based Building Energy Management Systems: Issues and Recommendations. *IEEE Access* **2018**, *6*, 38997–39024. [CrossRef]

38. Cheng, L.; Yu, T.; Jiang, H.; Shi, S.; Tan, Z.; Zhang, Z. Energy Internet Access Equipment Integrating Cyber-Physical Systems: Concepts, Key Technologies, System Development, and Application Prospects. *IEEE Access* **2019**, *7*, 23127–23148. [CrossRef]
39. Strielkowski, W.; Streimikiene, D.; Formina, A.; Semenova, E. Internet of Energy (IoE) and High-Renewables Electricity System Market Design. *Energies* **2019**, *12*, 4790. [CrossRef]
40. Pan, J.; Jain, R.; Paul, S.; Vu, T.; Saifullah, A.; Sha, M. An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype, and Experiments. *IEEE Commun. Mag.* **2018**, *56*, 35–41. [CrossRef]
41. Li, X.; Li, W.; Du, D.; Sun, Q.; Fei, M. Dynamic State Estimation of Smart Grid Based on UKF UnderDenial of Service Attacks. *Acta Autom. Sin.* **2019**, *45*, 120–131. [CrossRef]
42. Behal, S.; Kumar, K. Detection of DDoS attacks and flash events using novel information theory metrics. *Comput. Netw.* **2017**, *116*, 96–110. [CrossRef]
43. Piasecki, P. Design and security analysis of bitcoin infrastructure using application deployed on Google apps engine. Master's Thesis, Politechnika Lodzka, Lodz, Poland, 2012.
44. Wu, X.; Li, Y.; Tan, Y.; Cao, Y.; Rehtanz, C. Optimal energy management for the residential MES. *IET Gener. Transm. Distrib.* **2019**, *13*, 1786–1793. [CrossRef]
45. Wang, Y.; Wu, X.; Li, Y.; Yan, R.; Tan, Y.; Qiao, X.; Cao, Y. An Autonomous Energy Community Based on Energy Contract. *IET Gener. Transm. Distrib.* **2019**. [CrossRef]
46. Dong, Z.; Luo, F.; Liang, G. Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems. *J. Mod. Power Syst. Clean Energy* **2018**, *6*, 958–967. [CrossRef]
47. Jogunola, O.; Ikpehai, A.; Anoh, K.; Adebisi, B.; Hammoudeh, M.; Son, Y.; Harris, G. State-of-the- art and prospects for peer-to-peer transaction-based energy system. *Energies* **2017**, *10*, 2106. [CrossRef]
48. Wang, B.; Li, Y.; Zhao, S.; Chen, H.; Jin, Y.; Ding, Y. Key Technologies on Blockchain Based Distributed Energy Transaction. *Autom. Electr. Power Syst.* **2019**, *43*, 53–64. [CrossRef]
49. Bahrami, S.; Amini, M.; Shafie-khah, M.; Catalao, J. A Decentralized Electricity Market Scheme Enabling Demand Response Deployment. *IEEE Trans. Power Syst.* **2018**, *33*, 4218–4227. [CrossRef]
50. Wang, Y.; Li, P.; Cui, H. Comprehensive Value Analysis for Gas Distributed Energy Station. *Autom. Electr. Power Syst.* **2018**, *40*, 136–142. [CrossRef]
51. Li, B.; Cao, W.; Qi, B.; Sun, Y.; Guo, N.; Su, Y.; Cui, G. Overview of Application of Blockchain Technology in Ancillary Service Market. *Power Syst. Technol.* **2017**, *41*, 736–744. [CrossRef]
52. Cui, S.; Wang, Y.; Xiao, J. Peer-to-Peer Energy Sharing Among Smart Energy Buildings by Distributed Transaction. *IEEE Trans. Smart Grid* **2019**, *6*, 6491–6501. [CrossRef]
53. Yang, H.; Yi, D.; Zhao, J.; Dong, Z. Distributed Optimal Dispatch of Virtual Power Plant via Limited Communication. *IEEE Trans. Power Syst.* **2013**, *28*, 3511–3512. [CrossRef]
54. Koraki, D.; Strunz, K. Wind and Solar Power Integration in Electricity Markets and Distribution Networks Through Service-Centric Virtual Power Plants. In Proceedings of the 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, USA, 5–10 August 2018. [CrossRef]
55. Li, B.; Qin, Q.; Qi, B.; Sun, Y.; Li, D.; Shi, K.; Yang, B.; Xi, P. Design of Distributed Energy Trading Scheme Based on Blockchain. *Power Syst. Technol.* **2019**, *43*, 961–972. [CrossRef]
56. Junior, W.L.R.; Borges, F.A.; Veloso, A.F.D.S.; de AL Rabêlo, R.; Rodrigues, J.J. Low voltage smart meter for monitoring of power quality disturbances applied in smart grid. *Measurement* **2019**, *147*, 106890. [CrossRef]
57. Avancini, D.B.; Rodrigues, J.J.; Martins, S.G.; Rabêlo, R.A.; Al-Muhtadi, J.; Solic, P. Energy meters evolution in smart grids: A review. *J. Clean Prod.* **2019**, *217*, 702–715. [CrossRef]
58. Lin, Y.; Tsai, M. An Advanced Home Energy Management System Facilitated by Nonintrusive Load Monitoring with Automated Multiobjective Power Scheduling. *IEEE Trans. Smart Grid* **2015**, *6*, 1839–1851. [CrossRef]
59. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy(SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858. [CrossRef]
60. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184. [CrossRef]
61. Alladi, T.; Chamola, V.; Sikdar, B.; Choo, K.K.R. Consumer IoT: Security Vulnerability Case Studies and Solutions. *IEEE Consum. Electron. Mag.* **2019**, *9*, 6–14. [CrossRef]

62. Bahga, A.K.; Madisetti, V. Blockchain Platform for Industrial Internet of Things. *J. Softw. Eng. Appl.* **2016**, *9*, 533–546. [CrossRef]
63. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Consulted* **2009**, *75*, 1042–1048.
64. Sasaki, Y.; Wang, L.; Aoki, K. Preimage attacks on 41-step SHA-256 and 46-step SHA-512. *IACR Cryptol. ePrint Arch.* **2009**, 479–494.
65. Wu, Z.; Liang, Y.; Kang, J.; Yu, R.; He, Z. Secure data storage and sharing system based on consortium blockchain in smart grid. *J. Comput. Appl.* **2017**, *37*, 2742–2747. [CrossRef]
66. Lee, B.; Lee, J. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *J. Supercomput.* **2017**, *73*, 1152–1167. [CrossRef]
67. Valdeolmillos, D.; Mezquita, Y.; González-Briones, A.; Prieto, J.; Corchado, J.M. Blockchain Technology: A Review of the Current Challenges of Cryptocurrency. In *International Congress on Blockchain and Applications*; Springer: Cham, Switzerland, 2019; Volume 1010, pp. 153–160. [CrossRef]
68. Massimo, B.; Stefano, L.; Alessandro, S.P. A Proof-of-Stake Protocol for Consensus on Bitcoin Subchains. In Proceedings of the the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 26 February 2017. [CrossRef]
69. Li, K.; Li, H.; Hou, H.; Li, K.; Chen, Y. Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In Proceedings of the IEEE 3rd International Conference on Data Science and Systems, Bangkok, Thailand, 18–20 December 2017. [CrossRef]
70. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
71. Mezquita, Y.; Valdeolmillos, D.; González-Briones, A.; Prieto, J.; Corchado, J.M. Legal Aspects and Emerging Risks in the Use of Smart Contracts Based on Blockchain. In *International Conference on Knowledge Management in Organizations*; Springer: Cham, Switzerland, 2019; Volume 1027, pp. 525–535. [CrossRef]
72. Manickavasagam, K. Intelligent Energy Control Center for Distributed Generators Using Multi-Agent System. *IEEE Trans. Power Syst.* **2015**, *30*, 2442–2449. [CrossRef]
73. Mezquita, Y.; González-Briones, A.; Casado-Vara, R.; Chamoso, P.; Prieto, J.; Corchado, J.M. Blockchain-Based Architecture: A MAS Proposal for Efficient Agri-Food Supply Chains. In *International Symposium on Ambient Intelligence*; Springer: Cham, Switzerland, 2019; pp. 89–96. [CrossRef]
74. Deng, L.; Chen, H.; Zeng, J.; Zhang, L.J. Research on Cross-Chain Technology Based on Sidechain and Hash-Locking. In *International Conference on Edge Computing*; Springer: Cham, Switzerland, 2018; pp. 144–151. [CrossRef]
75. Ping, J.; Chen, S.; Yan, Z. A Novel Energy Blockchain Technology for Convex Optimization Scenarios in Power System. *Proc. CSEE* **2019**. [CrossRef]
76. Boyd, S.; Parikh, N.; Chu, E.; Peleato, B.; Eckstein, J. Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers. *Found. Trends Mach. Learn.* **2010**, *3*, 1–122. [CrossRef]
77. Wang, J.; Meng, K.; Cao, J.; Chen, Z.; Gao, L.; Lin, C. Information technology for energy internet: A survey. *J. Comput. Res. Dev.* **2015**, *52*, 1109–1126. [CrossRef]
78. Farras, O.; Padro, C. Ideal Hierarchical Secret Sharing Schemes. *IEEE Trans. Inf. Theory* **2012**, *58*, 3273–3286. [CrossRef]
79. Lin, C.; Hu, H.; Chang, C.; Tang, S. A Publicly Verifiable Multi-Secret Sharing Scheme with Outsourcing Secret Reconstruction. *IEEE Access* **2018**, *6*, 70666–70673. [CrossRef]
80. Al-shaer, W.H.; Hamed, H.H. Modeling and management of firewall policies. *IEEE Trans. Netw. Serv. Manag.* **2004**, *1*, 2–10. [CrossRef]
81. Zhou, L.S.; Yang, J.; Tan, P.Z.; Pang, F.; Zeng, M.Q. Identity authentication technology and its development trend. *Commun. Technol.* **2009**, *1*, 183–185.
82. Jajodia, S.; Samarati, P.; Sapino, M.L.; Subrahmanian, V.S. Flexible support for multiple access control policies. *ACM Trans. Database Syst.* **2001**, *26*, 214–260. [CrossRef]
83. Denning, D.E. An intrusion-detection model. *IEEE Trans. Softw. Eng.* **1987**, *2*, 222–232. [CrossRef]
84. Egupov, A.A.; Zareshin, S.V.; Yadikin, I.M.; Silnow, D.S. Development and implementation of a Honeypot-trap. In Proceedings of the the Young Researchers in Electrical & Electronic Engineering, Saint Petersburg, Russia, 1–3 Feburary 2017. [CrossRef]
85. Holm, H.; Sommestad, T.; Almroth, J.; Persson, M. A quantitative evaluation of vulnerability scanning. *Inf. Manag. Comput. Secur.* **2011**, *19*, 231–247. [CrossRef]

86. Sandhu, R.; Zhang, X. Peer-to-peer access control architecture using trusted computing technology. *Symp. Sacmat* **2005**, 147–158. [CrossRef]
87. Pureswaran, V.; Panikkar, S.; Nair, S. The IoT Is Predicted to Scale to Hundreds of Billions of Devices. Blockchain May Be the Key to the IoT Device Decentralization and Democratization Needed for a Connected Future. IBM Corporation. Available online: https://www.ibm.com/downloads/cas/QYYYV9VK?mhsrc=ibmsearch_a&mhq=Adept (accessed on 15 April 2015).
88. Tapscott, D.; Tapscott, A. How Blockchain Technology Can Reinvent the Power Grid [EB/OL]. Available online: http://fortune.com/2016/05/15/blockchain-reinvents-power-grid/ (accessed on 15 May 2016).
89. Nguyen, C. An Indie, Off-The-Grid, Blockchain-Traded Solar Power Market Comes to Brooklyn [EB/OL]. Available online: https://motherboard.vice.com/en_us/article/the-planto-power-brooklyn-with-a-blockchain-based-microgrid-transactive-solar (accessed on 18 March 2016).