applied sciences

MDPI

Article

When Energy Trading Meets Blockchain in Electrical Power System: The State of the Art

Naiyu Wang [1], Xiao Zhou [1], Xin Lu [1], Zhitao Guan [1,*], Longfei Wu [2] and Xiaojiang Du [3] and Mohsen Guizani [4]

[1] School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China; shininess_y@163.com (N.W.); 18811525086@163.com (X.Z.); 13051320793@163.com (X.L.)
[2] Department of Mathematics and Computer Science, Fayetteville State University, Fayetteville, NC 28301, USA; lwu@uncfsu.edu
[3] Department of Computer and Information Science, Temple University, Philadelphia, PA 19122, USA; dxj@ieee.org
[4] Department of Computer Science and Engineering, Qatar University, Doha 2713, Qatar; mguizani@ieee.org
* Correspondence: guan@ncepu.edu.cn

Received: 19 February 2019; Accepted: 9 April 2019; Published: 15 April 2019

Abstract: With the rapid growth of renewable energy resources, energy trading has been shifting from the centralized manner to distributed manner. Blockchain, as a distributed public ledger technology, has been widely adopted in the design of new energy trading schemes. However, there are many challenging issues in blockchain-based energy trading, e.g., low efficiency, high transaction cost, and security and privacy issues. To tackle these challenges, many solutions have been proposed. In this survey, the blockchain-based energy trading in the electrical power system is thoroughly investigated. Firstly, the challenges in blockchain-based energy trading are identified and summarized. Then, the existing energy trading schemes are studied and classified into three categories based on their main focuses: energy transaction, consensus mechanism, and system optimization. Blockchain-based energy trading has been a popular research topic, new blockchain architectures, models and products are continually emerging to overcome the limitations of existing solutions, forming a virtuous circle. The internal combination of different blockchain types and the combination of blockchain with other technologies improve the blockchain-based energy trading system to better satisfy the practical requirements of modern power systems. However, there are still some problems to be solved, for example, the lack of regulatory system, environmental challenges and so on. In the future, we will strive for a better optimized structure and establish a comprehensive security assessment model for blockchain-based energy trading system.

Keywords: energy trading; blockchain; electrical power system

---

1. Introduction

Energy crisis and environmental pollution have become two critical concerns in the last decade [1]. The smart grid with renewable energy resources is a promising approach to alleviate these problems, and its implementation can be facilitated by microgrids. In smart grids, new models, technologies, and flexible solutions are to be developed for intelligent energy management, to facilitate the optimal energy and power flow strategies. Specifically, energy trading, as an essential component in energy management, is undergoing an evolution from centralized to distributed manner. In the traditional energy market, the energy users can only buy electricity from the power utilities. In a smart grid, the energy users play a role as both power consumer and supplier. The excessive renewable energy generations can be traded with the utility and other users in the deficit of power supplies for mutual benefits.

The development of the traditional centralized energy market model has encountered bottlenecks and faced many problems [2]:

(i) Centralized management: In traditional energy market model, energy trading highly relies on the centralized third party servers, thus it is apt to cause single point of failures [3,4]. In addition, the centralized management leads to high operating costs, low transparency, and the potential risk of transaction data tampering [5].
(ii) Privacy protection and security issues. Third parties may disclose the user's energy generation pattern and predict a user's daily activities based on historical data [6,7]. Meanwhile, communication security is also a challenging issue [8].
(iii) The lack of competition between renewable energy pricing and traditional market pricing will discourage the investment in renewable energy [9].
(iv) The power grid lacks the resilience to cyber-attacks [10].
(v) Electricity comes mainly from large energy plants, which needs to pass through long-distance power transmission line before reaching the end customers. Due to the complexity of the power management, it is difficult to meet the dynamic energy demands timely and flexibly [11].
(vi) Long-distance one-way energy transmission makes the power supply be vulnerable to disruptions. In modern electrical power systems, the distributed bidirectional energy management is desirable to improve the system efficiency and stability [11,12].

Additionally, in the transition from traditional power grid to smart power grid, the efficiency, demand, cost and emission issues also need to be fully considered [13].

Meanwhile, as an emerging technology, blockchain has been widely adopted in many fields for its well-known advantages [14,15]. Blockchain was indeed flawed when it first emerged. Nevertheless, studies have found these problems and made corresponding improvements, such as the measurement research and exploration of the re-parameterization of blockchain to improve its scalability [16]; the Bitcoin-NG [17], which can tolerate Byzantine fault tolerance and achieve very good scalability; and the Protocol “Ouroboros Praos”, which can defend against complete adaptive corruption [18].

The application fields of the blockchain technology include finance, Internet of Things [19], public social services, reputation system, security and privacy, and so on [20]. For example, in [21], blockchain is used to enhance privacy through a decentralized personal information management system. It can ensure that users have control over data, proving that blockchain may serve as an important tool for trusted computing. The Hawk model proposed in [22] also addresses the issue of transaction privacy, by using an intelligent contract system that enables the compiler to automatically generate an efficient encryption protocol. As for the Internet of Things, blockchain can enable the sharing of services and resources, and automate several existing time-consuming workflows in the form of cryptographic authentication [23]. Beekeeper, a secure blockchain-based threshold IoT service system is proposed in [24]. Blockchain can also be employed for secure decentralized energy management [25]. Another study [26] has used blockchain to design privacy-protected search scheme for malicious servers. Moreover, it can also be applied to data sharing schemes to ensure the fairness of incentives [27].

The integration of blockchain technology into energy trading is a novel and promising area of research, and many studies have made efforts in this regard [28]. Before formally attempting to combine blockchain with the energy trading model, some researchers first studied the application of distributed systems to the energy market. Proof by facts, Peer-to-Peer (P2P) network model enables the energy market to operate in a consumer-centered manner and support the participation of the so-called “prosumers”, which has greatly improved the flexibility of the traditional mode of energy market [29,30]. As shown in [31], P2P network can create a competitive energy market and increase the overall efficiency of the power market. Additionally, the distributed system can also provide high-precision demand response signals [32], reduce cost and improve speed [33]. Moreover, it solves the problem of system scalability and mobility, and creates a competitive market that benefits small-scale prosumers [34]. There are also some studies on the optimization of the interaction between the main grid and the microgrid. For instance, the authors of [35] addressed the case in which two microgrids isolated from the main grid exchange energy in a P2P manner; both a centralized solution and a distributed solution are proposed to minimize the cost of power generation and transportation. In [36], a hierarchical power scheduling approach is proposed to optimize the power management in a smart grid with a microgrid and cooperative microgrids. Additionally, to improve the utilization of renewable energy, an adaptive distributed energy scheduling scheme is proposed in [37] to coordinate the microgrids and renewable energy generation.

Many studies have shown the advantages of introducing blockchain technology into the energy trading systems [38,39]. For example, high computing capacity can be realized with blockchain at a low cost, and the consensus mechanism can ensure the optimal solution. In addition, it can prevent fake transactions and establish an open and transparent credit system [40]. All nodes can work independently towards system equilibrium without central supervision [32]. The application of cryptography in blockchain can solve a number of system security problems [34,41] and significantly reduce costs [42]. More generally, blockchain enhances the role of consumers in the system and their choices [42]. In [43], the authors evaluated the local electricity market based on blockchain, and the model shows that the system has already been in the early maturity stage.

Currently, blockchain-based energy trading is not just a theoretical topic, but there are already many practical applications. For instance, Exergy team developed Brooklyn microgrid in April 2016, which is the world's first practical blockchain-based energy trading platform [44]. In France, there is a project named Sunchain [45], which uses the Hyperledger Fabric platform to create a blockchain virtual network for solar energy prosumers and can efficiently deal with the energy transactions at low cost. Although only a limited number of users are involved in Sunchain project, the development of solar power in social housing has been realized and the share of electricity generated per unit of housing can be traced. Power Ledger in Australia is a trustless, transparent, and interoperable energy exchange platform with transaction tokens that enable retailers to perform simple power transactions with each other and receive payments in real time from automated settlement systems [46]. In blockchain-based energy trading scheme, the consumers can choose the suppliers by their own preferences, i.e., trading with neighboring suppliers, or choosing clean energy, so that the electricity bill could be reduced and the return on investment in distributed renewable energy could be increased. Power-ID [47] is a small local peer-to-peer energy market in Switzerland that aims to reduce local energy costs. I-NUK [48] has created a blockchain carbon credit system that allows individuals to easily offset their daily carbon emissions. In I-NUK, everyone can produce electricity energy using their own solar power equipments, and sell the energy on the market after being certified by the blockchain and recorded as the carbon credit. Tal.Markt [49] uses private blockchain to connect citizens with the local renewable energy suppliers. The citizens can use the platform to monitor the status of renewable energy production, while the producers need to meet the capacity standard of 30 kWh if they want to join the platform to sell energy. Based on the survey of existing research work, this paper firstly expounds the problems faced by energy transaction before and after the adoption of blockchain. Then, we analyze the relevant research on combining energy transaction with blockchain. Next, existing research are summarized and classified based on different aspects in the blockchain model. Finally, we summarize and highlight the problems and challenges that still need to be addressed in this field.

The main contributions of this paper can be summarized as follows:

- A comprehensive review of blockchain-based energy trading schemes is provided, and the existing results are classified according to the various challenges in the energy trading system in this paper.
- Not only the theoretical research results, but also the practical blockchain-based energy trading applications are introduced and analyzed.

- The existing blockchain-based energy trading schemes and applications are evaluated, and the discussion of the potential future research directions are also given in this paper.

The rest of this paper is organized as follows. Section 2 gives the preliminaries. In Section 3, the challenges of blockchain-based energy trading are stated. In Section 4, an overview of blockchain-based energy trading is given. In Section 5, the methodologies for energy transactions are investigated. The consensus mechanisms are studied in Section 6. In Section 7, the methodologies for system optimization are presented in detail. In Section 8, the discussion and future directions are stated. In Section 9, the paper is concluded.

2. Preliminaries

This section introduces some basic concepts, methods and technologies involved in the blockchain-based energy trading system. Firstly, the concept of blockchain is elaborated, including the basic principles, basic models and relevant algorithms. Zero knowledge proof, ring signature, onion routing and garlic routing are to the common approaches for information hiding in communication process. Cloud computing and fog computing are mainly used to relieve the computing pressure in the system model, such as the computations for Proof-Of-Work. Game theory is mainly used to optimize the system model.

2.1. Blockchain

In the 1.0 stage of blockchain, it is actually a distributed ledger used as the underlying framework for Bitcoin [14]. As shown in Figure 1, the blockchain is a chain structure composed of different blocks connected in series. Among them, each block is composed of a block header and a block body. In block body, the transaction data of a period of time are recorded. In block header, the main three parts are Prehash, Nonce, and Root hash. Root hash is the hash result of the transaction data and the digital signature of the miner, and the hash value of the previous block. Prehash, the hash value of the previous block, is used to build the links between the blocks. When a new block is generated, it is connected to the block chain by recording the Prehash. Meanwhile, all nodes will update synchronously to get a complete backup of the entire blockchain. The consensus mechanism used in blockchain 1.0 is Proof-Of-Work (POW). When new transactions are generated and broadcasted, each node (miner) collects the new transactions into a block. All nodes (miners) try to find Nonce, the answer of one specific cryptographic puzzle. The miner who finds Nonce first will get billing right to broadcast the block to all other nodes. Other nodes check if Nonce found by the winner satisfies the cryptographic puzzle. Although the process of obtaining the answer is very difficult and requires a lot of computational effort, proving its correctness is very simple. If the new block is adopted, it will be added into the block chain.

Blockchain 2.0 adds smart contracts to the previous version and enables the migration from the currency market to other markets, allowing people to see the possibility of applying the advantages of blockchain to other fields [50]. Generally, the concept of blockchain 2.0 includes the smart contract, digital assets, and financial applications. Different from blockchain 1.0, blockchain 2.0 is a decentralized market that provides a wider range of application scenarios for the financial section. The key idea is to use the distributed ledger of blockchain to record, confirm and transfer various forms of contracts and properties.

A smart contract is a computer protocol designed to disseminate, verify, or execute a contract in an informational manner. Smart contracts allow for trusted transactions without a third party, which are traceable and irreversible. In blockchain 2.0, a smart contract is an application that is defined and implemented as code, which is automatically executed according to the pre-defined rules. The key characteristics of a smart contract are Autonomy, Self-sufficiency, and Decentralization: Autonomy means that, when the smart contract is launched and running, it no longer needs to make further contact with the initiating agent. Self-sufficiency means it can raise money by providing services and use that money to buy the resources it needs. Decentralization means that it is structurally distributed across network nodes.

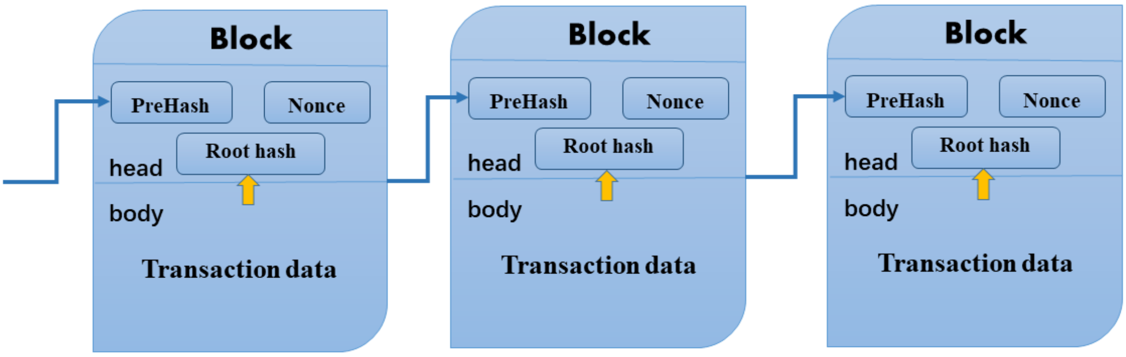

Figure 1. Illustration of Blockchain 1.0.

According to the different needs of practical applications, the blockchain technology has gradually evolved into three application modes: the public blockchain, the consortium blockchain and the private blockchain. Public blockchain is a completely decentralized blockchain, private blockchain is a completely centralized blockchain, and the degree of decentralization of consortium blockchain is between the two. Consortium blockchain is applicable to an alliance of multiple entities, and the consensus process is only completed by some specific nodes. Private blockchain, on the other hand, is more suitable to be for data management within an organization. Hence, it may not require incentives mechanism.

The idea of blockchain 3.0 is that you can think of every system in your life as somehow economic [50]. Then, blockchain technology can be applied to any other field, supporting the possibility of reconfiguration in almost all fields involved by human beings. Due to the decentralized nature of blockchain, it can more fairly realize issues related to freedom, jurisdiction and review. It will help achieve global management across international boundaries, such as Namecoin, which can break Internet censorship.

Currently, blockchain 3.0 has been developed from a theoretical model to concrete applications. Enterprise Operation System (EOS) [51], which introduces a new blockchain architecture to support vertical and horizontal extensions of distributed applications, is similar to the architecture of operating systems. It can provide multiple application scheduling. It supports millions of transactions per second, with no cost to the user.

2.2. Zero-Knowledge Proof

A zero-knowledge proof is a convincing proof to someone that "I do own something without revealing the solution or the exact content of what I own" [52,53].

- Interactive zero-knowledge proof. In the presence of both the prover and the verifier, the prover claims to possess the knowledge and the verifier keeps challenging the prover until the responses from the prover can convince the verifier that the prover does possess the claimed knowledge. However, if the two parties collude, they could spoof others into believing that they possess the knowledge without actually knowing it.
- Non-interactive proof of zero knowledge. The interactions between prover and verifier is not necessary. Instead, an additional machine program that no one knows about will be used. The proof calculated by the machine automatically prevents either party from cheating.

2.3. Ring Signature

Ring signature scheme makes use of algorithms to construct signatures with unconditional anonymity. It is mainly composed of the following algorithms [54–56]:

- Generate. A probabilistic polynomial time (PPT) algorithm, with security parameter k as input, uses different public key systems to generate public and private keys for each user and output the result.
- Sign. When signing the message m, the public key of n ring members and the private key of one of them will be used to generate a signature R with ring parameters.
- Verify. A deterministic algorithm that takes a message and a signature as inputs. If the message matches the signature, it returns "true"; otherwise, it returns "false".

2.4. Onion Routing and Garlic Routing

Onion routing is a technique for anonymous communication. In an onion network, messages are encapsulated in multiple layers of encryption like an onion. The encrypted message will pass through a series of onion routers, each of which decrypts one single layer, uncovering the next node [52]. Only the original sender knows where the destination is, and only the original sender and the destination node know the plaintext message. All intermediate nodes know only the immediately preceding and following nodes, hence achieving the anonymity of the original sender and the message.

Garlic routing is a variant of onion routing. Different to onion routing, it groups messages and disperses them through multiple tunnels, which further increases the difficulty of attack.

2.5. Cloud Computing, Edge Computing and Fog Computing

Cloud computing is a computing paradigm in which the service providers can remotely distribute computing and storage resources to users through the networks in an on-demand manner. The resources are available to users without their direct active management [57].

Edge computing does not require uploading data, but provides resources and services close to the demand (data source). Its applications are initiated at the edge, resulting in faster network service responses. Edge computing is between a physical entity and an industrial connection, or at the top of a physical entity [58].

Fog computing takes advantages of weaker and decentralized edge devices in place of the powerful servers in cloud computing. Fog computing has a closer proximity to users and larger geographical distribution [59].

2.6. Game Theory

Game theory is a mathematical theory that studies the phenomenon of competitive nature [60,61]. Optimization strategies are studied by considering the actual and predicted behaviors of individuals in games. It can be classified based on the number of players (two or more). Participants will rationally maximize their own interests, and get a game result under the premise that each player has a practical and feasible action plan. In the energy trading system, it is mainly used to realize the system model optimization such as the maximization of social welfare.

3. Challenges of Blockchain-Based Energy Trading

Currently, the research on blockchain-based energy trading has made great progress and solved many limitations of the traditional energy markets mentioned above. Meanwhile, there still exist many challenges:

(i) Low efficiency [62] and high transaction costs [63,64]. Due to the shortcomings of blockchain itself, the transaction speed cannot meet the system requirements. At the same time, the transaction costs of blockchain can raise the overall cost of the system.

(ii) Privacy protection and security issues [62,64,65]. How to avoid big data statistical prediction and behavior model analysis when the transaction is completed, as well as how can the rights and interests of both parties in the transaction be guaranteed are both severe challenges. There are also potential risks such as private key leak [15].

(iii) Real-time communication [63]. The challenge of the real-time communication of a large amount of sensor data.

(iv) Price model. How should a deal properly be priced to help buyers and sellers reach an agreement quickly.

(v) Lack of a complete incentive mechanism[15,62]. It is similar to the incentive mechanism for miners in Bitcoin. Under the premise that the system may face privacy and security problems, how to motivate more nodes to join the system is a problem that needs to be solved.

(vi) Cost minimization, multi-scene welfare maximization. In the case of multiple variables, how to ensure the minimization of the overall energy cost of the system, as well as the assurance of trust, rationality of independent individuals, and computational efficiency must be considered [60].

(vii) Lack of a regulatory framework with flexibility [38,43,63,66].

(viii) There is also the issue of environmental energy consumption, because the system requires a large carbon footprint [63].

(ix) Because of the tight network structure, there may be a cascade of physical faults [15]. In addition, there are many physical hardware limitations to consider [67].

4. Overview of Blockchain-Based Energy Trading

Currently, the application of blockchain in the field of energy trading has achieved significant success. One of the most common forms is based on P2P transactions, using the blockchain as the system framework. P2P networks can be roughly divided into two organizational modes, structured and unstructured. Each structured peer is built from a distributed hash table, and message routing is efficient but requires maintenance.The unstructured peer location is random, without the need for a centralized node search, but the query may not have a result. Jogunola et al. [12] evaluated both the structured and unstructured P2P protocols to help planners better organize their networks. The conclusion is that both are highly scalable while the structured P2P protocols are more reliable by comparison.

As shown in Figure 2, this paper classifies the existing research results according to the various challenges in the energy trading system. First, the challenges mentioned in Section 3 can be divided into three parts: those encountered in the whole energy trading process, those encountered in the process of node consensus, and those encountered in the process of system optimization.

For the first part, energy transaction, we divide it into three sub-parts: pre-transaction communication, buyer–seller matching, and transaction settlement. For example, "pre-trade communication" mainly focuses on how to achieve privacy protection in interactions under the condition of blockchain ledger disclosure. Pylon network [68], a successful practical project in Spain, is implemented with full data privacy protection.

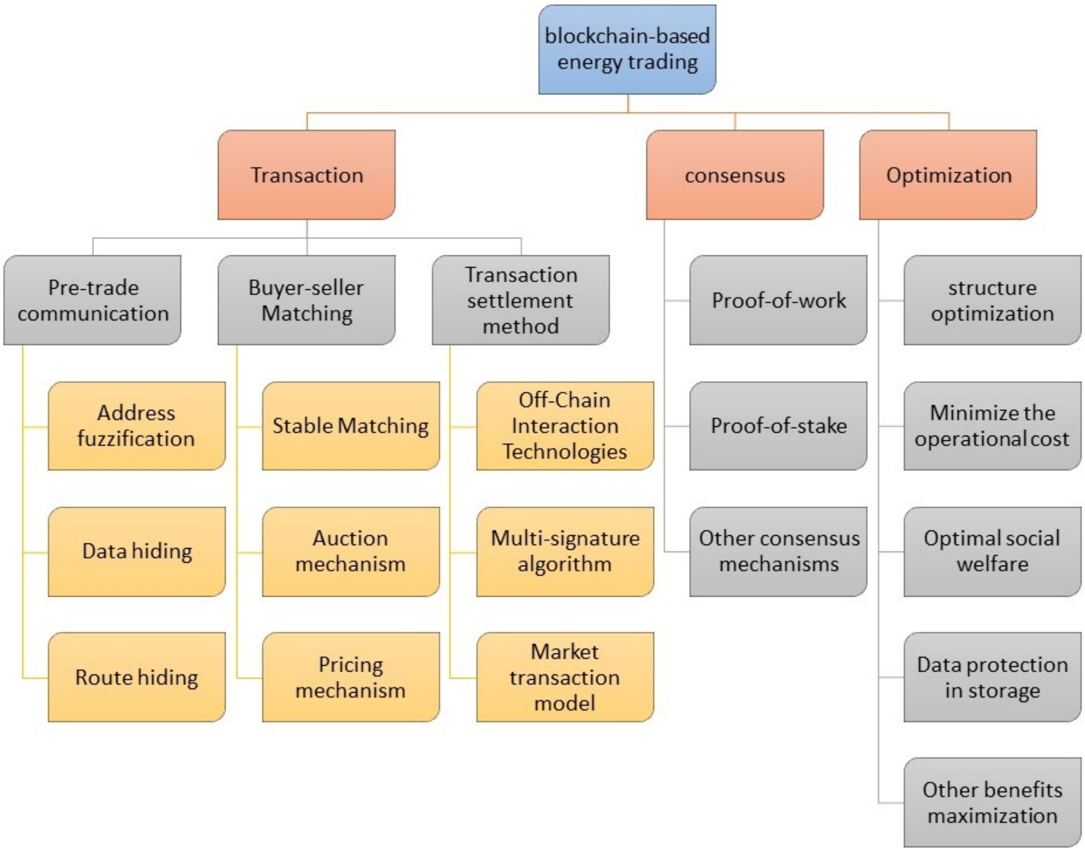

Figure 2. Classification of Blockchain-based Energy Trading.

For the second part, consensus mechanism, we mainly summarize the consensus algorithms used by the nodes to reach a consensus to accept the block, such as Proof-of-Work (PoW) that is used by Bitcoin [14], Proof-of-Stake (PoS) that is applied in Ethereum, Practical Byzantine Fault Tolerant (PBFT) that is adopted by Sunchain [45] and other consensus mechanisms.

For the last part, system optimization, we mainly summarize the optimization based on the whole system model, for example, from the perspective of the structure, how to optimize the original system model; from the perspective of the operators, how to minimize the cost and how to protect the data in storage; from the perspective of consumers, how to maximize the personal interests; and so on. There are many practical projects realizing innovation in this part, such as Grünstromjeton in Germany [69]. By considering the actual interests of users, the system can be optimized to increase the capacity of renewable energy generation and the user profit at the same time.

In Table 1, we analyze some existing energy projects[44–46,68,70–74], and map the models or protocols they used with the categories listed in Figure 2. The three main categories are introduced in detail in Sections 5–7. The following notations are used in Table 1: a "✓" means mentioned, but no specific algorithm is provided and "-" means no is information available.

Table 1. Energy project overview.

	Privacy Protection for Pre-Transaction Communications	**Stable Matching**	**Auction Mechanism**	**Pricing Mechanism**	**Transaction Settlement**	**Consensus Mechanism**	**Struction Optimization**	**Operational Cost Minimization**	**Data Protection in Storage**
SolarCoin [70]	-	-	-	-	Off-chain	POS	-	✓	-
Pylon network [68]	✓	-	-	-	-	POW	-	✓	-
Exergy [44]	✓	-	-	locational marginal pricing	-	-	-	✓	-
GridSingularity [71]	-	-	-	-	on-and off-chain	POA	-	-	secret store
Power Ledger [46]	-	Fairly match	-	Double-token mechanism	Off-chain	POW(Is shifting to POS)	Consortium blockchain and public blockchain	-	-
Sunchain [45]	✓	-	-	-	-	-	Blockchain+IOT	No mining	-
Dajie [72]	-	-	-	-	-	POW	Blockchain+IOT	-	-
NRGcoin [73]	-	-	continuous double auction	-	-	various	Consortium blockchain and public blockchain	-	-
Energo Labs [74]	-	-	-	Securities market pricing mechanism	-	POW	Consortium blockchain and public blockchain	-	-

5. Category I: Energy Transaction

5.1. Pre-Trade Communication

Users often need to publish their own supply and demand before identifying the trading partners. In this process, we need to ensure security and protect users' privacy.

5.1.1. Address Fuzzification

First, there is a simple way to hide the actual address of the user, anonymous addresses, in which a new pseudonym address is generated for each transaction. Most digital currencies using blockchain technology employ anonymous addresses to provide anonymous services [3]. The system forces users to randomly generate new message addresses for each new transaction to remain anonymous [75,76]. Similarly, in [77], each user is allowed to submit their power consumption data under different pseudonyms, and bloom filters are used to determine the validity of pseudonyms and zero knowledge is used to verify the existence of pseudonyms. However, this is not "anonymous" in the strict sense: because this approach does not provide "unlinkability", there is still a chance of finding a link between the pseudonym and the user by matching the power consumption data to the user's behavior characteristics. For example, Sarah et al. [78] tried to develop a clustering heuristic algorithm for Bitcoin based on changing addresses, clustering addresses belonging to the same user. A re-identification attack is then used to find the operators behind the cluster and their interactions.

Additionally, there is another method using zero knowledge proof to achieve address fuzzification. In [53], non-interactive zero-knowledge proof is used to realize address fuzzification by hiding a coin to the coin list, which can successfully sever the link between the user and the coin. Moreover, the ring signature algorithm mixing through zero-knowledge proofs in [52] is used to generate many new wallets addresses to realize the intractability and unlinkability of transactions.

5.1.2. Data Hiding

In pre-trade communications, the data need to be protected from disclosure and damage. The basic idea of data hiding is to hide the data that need to be hidden into a large dataset.

In [79], a data confusion scheme is proposed. In the bidding mechanism of power trade, only the information regarding the overall customer transactions is released to suppliers, so that they are able to calculate monthly bills but have no access to fine-grained data. Producers need to transfer production assets to an intermediate mixing service, as proposed in [75]. Since the service simultaneously moves assets from multiple producers to multiple anonymous addresses, and the anonymous addresses are randomly generated by the prosumers, the blended assets cannot be traced back to the original prosumer. Similarly, the group signature algorithm adopted in [52] allows members of a group to send transactions in such a way that the receiver can only know that it comes from a group member but nothing more, without using a central authority.

In [80], a virtual power plant is used as the intermediator for the negotiation between prosumers and the aggregator, without sharing any private information. Additionally, to prevent the information leakage caused the side-channel attacks during data exchange, a bilinear ECDSA (Elliptic Curve Digital Signature Algorithm) signature mechanism is proposed in [81] against adaptively chosen messages attacks under the continual leakage setting.

5.1.3. Route Hiding

Besides data hiding, it is also necessary to hide the route. The garlic routing scheme proposed in [52] takes intelligent electricity meters, manufacturers and distribution system operators as the server nodes for garlic routing, and applies netDB to realize the routing allocation, thus preventing attackers from obtaining some private information of both parties in a transaction based on the routing messages.

To reduce overhead during negotiations, in [64], a routing method using the public keys as identifiers is proposed. That is, nodes with high resource availability are responsible for forming the backbone network. Backbone nodes route groups based on the destination's public key. Normal nodes can be associated with multiple backbone nodes for protection of anonymity with multiple public keys.

5.2. Buyer–Seller Matching

After the energy demand is released, the trading nodes need to get a preference list according to their needs and the current market status. Then, they would choose the most suitable trading object to match.

5.2.1. Stable Matching

The stable matching problem, also known as the stable marriage problem, was first introduced in the economic background. It is a problem of matching users in different aspects of the bipartite graph. In this case, a group of equal numbers of men and women were matched according to their preferences. The goal is that eventually everyone has a partner, and everyone is happy with their partners. This problem was later applied to other fields, and the new matching pattern allows the two groups to be in different size. In energy trading, the process of matching trading objects can also be regarded as a stable matching problem [82].

To protect the privacy of fixed residential charging piles, mobile electric cars and other charging equipment, a homomorphic encryption-based position hiding method is proposed in [82] so that the exact locations of the supplier and demanders can be known only if the stable matching is successful. Homomorphic encryption is a kind of cryptography technology which can process data under the premise of ensuring data privacy and security. When matched, the mobile suppliers need to send their updated location to the demander. After receiving the updated location information, the demander uses the homomorphic encryption algorithm to calculate the distance and get an ascending list in location preferences. Finally, based on the preference lists, the distributed stable matching algorithm obtains a matching such that every demander and supplier is satisfied.

Based on the stable matching problem, there are also other studies using different methods to achieve the optimal solution. In [83], the symmetrical allocation problem based on native auction algorithm is used to match the buyers and sellers in the energy market. The naive auction algorithm is carried out in rounds, and only one buyer bids for the desired object in each round. An automatic matching mechanism is designed in [84] to ensure the prosumer privacy and system safety. Both the buyer and seller provide a vector and some matching criteria as the premise of matching. The objective is to find an optimal set of solutions that satisfy these criteria. With further consideration of time constraints, physical constraints, and more flexible pricing updates, the system can provide the most appropriate matching strategy.

Power Ledger [46] is a blockchain based energy trading platform, which has its own trade matching algorithms to fairly deal with power trade between prosumers. In Power Ledger, the orders from producers and the orders from consumers are filled in equal increments in the energy market. When a new consumer joins the system, he will receive the equal allocation from the renewable energy pool in his area immediately, to reduce the transmission distance and carbon emissions.

5.2.2. Auction Mechanism

Many works focus on the design of auction mechanisms. When blockchain technology has not been adopted, Majumder et al. [85] proposed an efficient double auction mechanism to maximize the participants' utilities and the social welfare in a distributed system structure, which is completed by the controller in an iterative way, avoiding the need of private information. It is also widely used in distributed grid transactions [67,86,87]. After the blockchain is widely adopted, this auction mechanism's main claim is to match the parties at auction, not the goods to be traded [88,89]. The charging and discharging parties send bidding vectors to the auctioneer respectively, and auctioneer carries out multiple iterative auctions on the price matrix of both parties. The buyer and seller solve their optimal price and the best matching object from multiple iterations. The same mechanism is used in the system and an adaptive aggressive strategy is adopted to adjust the quotation according to the market changes. To prevent unexpected situations, the interests of users can also be guaranteed through multi-signed digital certificates [5]. Furthermore, there are other auction mechanisms that build on top of this. The Double Auction in [90] adopts the average mechanism, in which the reserve price is calculated on an average basis and the seller with a lower reserve price will be allocated to the buyer with a higher bid in a greedy way. The method in [91] considers the double auction as the second stage of the auction mechanism. The first stage is the call auction stage, in which buyers and sellers conduct one-time matching transactions and provide guiding prices of various types of energy for each period.

In addition to this classic double auction mechanism, there are many classic strategies and methods used in the design of auction mechanisms, such as the game theory method. On account of the contradiction and interactivity of energy transaction, the game theory method will be an effective tool to improve the system. The application of game theory in blockchain-based energy trading has been comprehensively studied in [61]. In [92], the non-cooperative game theory—Nash equilibrium—is used to adjust the matching process to achieve the optimal matching. Each player assumes to know the equilibrium strategy of the other player, and users in the system cannot increase their revenue by only modifying their own orders. In another major study, contract theory is also used in the auction mechanism. Contract theory is a typical branch of economics, which studies the economic behaviors and results of different contractors in a specific trading environment. In the scenario of EV charging [93], a dynamic optimal contract assignment and energy allocation algorithm is designed. Based on the contract theory, the optimal contracts are designed to satisfy consumers' distinct energy consumption preferences and maximize the operator's utility.

For the problem of edge resource allocation on mobile devices, it can also be realized by auction mechanism. For example, the method in [94] considers the configuration externality and authenticity, which can maximize the personal welfare. A similar auction method is proposed in [58], and a multi-layer neural network structure for the optimal auction analysis is constructed. This model also verifies the effectiveness of using deep learning for deriving the optimal auction mobile blockchain with high revenue.

Additionally, some researchers have studied the auction mechanism in the energy trading market. For example, a battery state model for electric vehicles is proposed in [95], which is responsible for clarifying the factors that buyers and sellers need to consider when determining the transaction price and volume during the auction process. The auctioneer determines the optimal allocation by controlling the bidding increment. Similarly, a parallel multidimensional willingness bidding strategy is proposed in [96]; specifically, it is to update the bidding price and give a list of up to three willing trading objects by using historical transaction records, bidding antagonism and other factors between buyers and sellers in the discussion of bidding.

Some studies attempt to establish a general market auction model. In [97], a local auction market is suggested, in which a generic, low-cost solution is implemented using blockchain technology, Specifically, blockchain-based aggregators can perform market clearing, battery energy storage system (BESS) execution and other obligations to ensure that they are applicable to BESS of any size. In [98], an incentive auction mechanism is adopted to transfer the auction calculations to users to reduce the burden on the hubs, in which the auction mechanism is compatible with incentives.

5.2.3. Pricing Mechanism

The pricing scheme in energy system is very important, it is also related to the system performance. The first thing we need to address is the privacy issue in the pricing process. The secure Multi-Party Computation (MPC) is a way to solve the problem of privacy protection in pricing-related interactions. It can solve the collaborative computing problem of protecting privacy among a group of participants who do not trust each other, and ensure the independence of input and the correctness of calculation without disclosing their input values. For this reason, a bidding protocol based on secure MPC is proposed in [79], allowing mutually distrustful parties to compute without disclosing fine-grained electricity consumption data. The trade price and bids selection are performed in a distributed, oblivious manner.The billing protocol is based on a simple privacy-friendly aggregation technique that can prevent the detailed consumption data from leaking to suppliers when they calculate customers' monthly bills.

In the actual pricing process, some economic concepts are used to help build the model. In 1993, Gode and Sunder [99] proposed a concept of "zero-intelligence" (ZI) trader in their research and suggested that the convergence to the theoretical equilibrium price is largely determined by the market structure rather than the intelligence of traders. Since then, the concept of "zero-intelligence plus" (ZIP) traders has been introduced based on ZI traders [100]. Similar to ZI traders, these simple agents do random bidding, but ZIP traders use a basic form of machine learning that is closer to human traders in terms of performance. This concept of trader is also being used as an agent to join distributed energy trading systems. In [89], ZIP traders participate as agents in an auction mechanism that automatically adjusts profit margins within specific budget constraints.

After the wide application of the distributed generation system integration technology of renewable energy, we also need to consider the issue of direct transaction pricing between small-scale electricity suppliers and end-users. In [101], the authors considered this issue, making use of the coalitional game theory to realize the pricing scheme with fair distribution of benefits among small power suppliers and end users. In practical projects, many effective pricing mechanisms have been implemented to encourage renewable energy production. In Germany's Grünstromjeton project [69], for example, smart meters calculate the share of electricity generated by renewable energy in a user's total electricity consumption. Users with higher share of renewable energy will be rewarded with a currency called Gruenstromjeton, which has real value. Similarly, France's I-NUK project [48] will also give small solar energy producers higher prices to promote the development of the clean energy.

In addition to the basic transaction pricing, there are many other aspects to be considered in a pricing mechanism, such as the maximization of system performance. For example, there are some pricing algorithms based on game theory. Through comparison and evaluation of multiple pricing mechanisms, it is concluded that the pricing mechanisms based on game theory can achieve the best local energy scheduling [102]. In [103], an optimal loan pricing strategy in a credit-based payment scheme is proposed, which makes it possible for buyers who do not have enough coins to buy energy. It also computes the best count of loan for each borrower and the penalty rate through a noncooperative Stackelberg game. Stackelberg game theory is also used in [104,105], in which the service demand pricing of miners is considered from the perspectives of unified pricing and discriminatory pricing respectively, both of which are calculated to determine the best price for profit maximization.

While most pricing mechanisms take into account the optimization of system benefits, Long et al. [106] compensated prosumers by introducing compensation prices, realizing a pricing mechanism that can ensure that every participant can obtain economic benefits. Similarly, a consumer-centric pricing mechanism using the mid-market rate is proposed to ensure the stability of the prosumer coalition and the interests of prosumers in [107]. In other words, this is a mechanism to decide whether the electricity needs to be purchased from or sold to the grid according to the relationship between the total power generation and the demand, so as to coordinate the price.

5.3. Transaction Settlement Method

The next step is the process of settling accounts between the two parties of a transaction.

5.3.1. Off-Chain Interaction Technologies

Off-chain is a payment method to solve the problem of Bitcoin scalability, which is similar to creating a third-party escrow account between the two parties. By using Bitcoin scripts for secure offline transactions, Bitcoin can be scaled up to billions of users without hosting risk or blockchain centralization. Moreover, both parties can conduct multiple transactions without writing to the blockchain. As long as the off-chain channel is open, no transaction fee will be charged. The only fee required is to open and close the channel [108]. Off-chain technologies can also help to increase the speed of transaction confirmation with minor sacrifice of the decentralization [91]. Through offline communication, the transmission of clearing price, matching result and other market signals are realized within certain timing constraint [76], and the distribution system operators can also request asset transfer [52].

Up to now, several studies have applied off-chain technology to their system models. In [109], the off-chain payment is applied to the network optimization model of electric vehicle charging station, which not only solves the problem of privacy exposure in conventional charging system, but also addresses the drawbacks of low efficiency and high transaction cost in Bitcoin network. The matching method in [84], as mentioned in Section 5.2.1, is performed using an off-blockchain solver. The solving of the matching problem is divided into two parts, the off-blockchain solver is running to find a solution on powerful computers based on the latest offers, and the smart contract on the chain only needs to verify the feasibility of the solution and to select from the multiple candidate solutions.

The idea put forward in [110] is very similar. The contract and ledger are stored separately to enhance the width of the chain from the traditional single chain to double chain, which increases reliability of the blockchain. In addition, each pair of contract block and ledger block is equipped with a high-frequency verifier, to inspect any inconsistencies and malicious manipulations. If any inconsistency is found between the recalculated ledger and the existing one, an alert will be sent to the prosumer to prevent possible data manipulations.

5.3.2. Multi-Signature Algorithm

Multi-signature algorithm is used to ensure transaction validity. It is basically about finding someone else to prove that neither side has cheated. If the third party fails to satisfy both parties, it may be replaced. The conditions under which a transaction can be redeemed are defined using a multi-key script, the minimum M public keys can be signed to prevent theft [3,64]. If they only want to trade partial ownership, they could also adopt time locked multi-signature to refund the transaction.

Similarly, Zhao et al. [91] proposed the concept of multi-signature wallet, which acts as a token broker with the buyer's and exchange's signatures. Firstly, participants in energy trading must authorize the exchange to transfer a set of tokens from their blockchain accounts to a multi-signature wallet. Then, an order contract containing information about the buyer and the seller is signed with the private keys of both parties and sent to the exchange. The exchange classifies the orders according to the kind of energy and the delivery time, so that the orders could be settled in the same period. Settlement contracts are created and deployed to the main chain to secure the trader's assets. After the agreement is reached, the smart meter automatically uploads the data to the smart contract and then the token is transferred to the seller. This also guarantees the validity of the transaction and prevents either party from cheating.

5.3.3. Market Transaction Model

Three market transaction models are studied in [111,112]. First, the market is cleared the day before it operates [113]. The products considered in the proposed day ahead market are energy and flexibility. The next day's hourly clear of demand and supply generates 24 market prices and quantities. The supply and demand participants are matched before the payment is executed. If the supply and demand do not match, a distributed flexible load is allocated to cover an inflexible supply. The load owners need to set a price and the cheapest loads will be to cover the inflexible supply. If there is still a mismatch between supply and demand after the allocation, the rest will be traded in the wholesale market. Similar ideas are applied in [9]; the gap between the market and renewable energy pricing is explored firstly, and then an hourly alternative energy pricing scheme is proposed that would help expand renewable energy production while reducing the carbon footprint. One of the projects that has been done so far is an international project called SolarCoin, which advocates that all solar manufacturers, for every kilowatt-hour of energy they produce and put into the grid, get a SolarCoin to drive renewable energy generation [70]. In another project in Belgium, the idea behind NRGcoin is to compensate for inadequate subsidies for renewable energy and encourage citizens to use local renewable energy by paying them in a cryptocurrency called NRGcoin [73]. It is a virtual currency that can be redeemed with a legal tender (the euro).

Real time trading is performed to conduct market clearing at the same time, or close to, as operation [111,113,114]. It generally has a certain frequency. periodically, the node sends the predicted deviation to the market and eliminates it by trading energy. In contrast to the previous settlement model, it uses a flexible payload to correct bid bias. If the flexible load in the system can successfully eliminate deviations, then the market price will be the price of the last accepted flexible load.

The final model is a system based on grid operators sending quotes and node responses. When the operator anticipates congestion, the node provides flexibility to reduce power at its own time stage, then the node sends the quantity and price it can offer, and the operator selects the tender that meets the requirements.

6. Category II: Consensus Mechanism

For traditional blockchain, there are several mature consensus mechanisms. When combined with energy trading, it is also likely to adopt a more traditional model or slightly modified model to meet the requirements of the system. Several common consensus mechanisms, e.g., Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), are summarized in [75,115]. In this paper, we only cover the most commonly used consensus mechanisms.

6.1. Proof-of-Work

Since the proof-of-work mechanism was initially used in Bitcoin, the most common early-stage consensus mechanism in blockchain-based energy trading was POW. The consensus proof is achieved by solving a difficult problem, that is, finding a nonce to form a hash value satisfying the condition. Double-spending can be avoided to some extent because finding an answer requires a lot of computing resources, but it is easy for other nodes to verify the answer. However, its weaknesses are obvious, such as the long delay to confirm a trade [111]. Additionally, POW in Bitcoin cannot be directly used for energy transactions, because it can only provide integrity check for things, which is far from enough for energy transactions [84].

Later, many improved methods have been proposed on this basis.The first emerging solution is to reduce the burden by outsourcing the computations. For example, the auction-based market model is designed precisely because of the characteristics of POW mechanism in [60]. Limitations on computing resources have led miners to outsource computing to cloud computing servers. The overhead of proof-of-work is too high for mobile devices, so edge computing [104,116] and cloud/fog computing [105] are used as a network support device. In [58], the interests of edge computing service providers are also taken into account. To maximize their interests, the marginal resource allocation mechanism that ensures incentive compatibility and individual rationality is still open. Two pricing models for uniform and discriminatory pricing schemes are further proposed to assist [105]. That is, regarding the rewards given to the miners, there are fixed rewards and variable rewards, so that the competitive factors of the miners are not only related to the calculation force, but also related to the size of the block for certification.

The second is the proof-of-work based on energy contribution. For example, in [88], the traditional proof-of-work and proof of energy contribution are combined to achieve consensus. The former is for local aggregators (LAGs) about data audit; it is similar to the traditional pow in Bitcoin, which generate a unique hash value of difficulty for each block. The latter is for Plug-in Hybrid Electric Vehicles

(PHEVs) about energy contributions, the discharge PHEV that contributes the most to the power supply is awarded with energy currency as an additional incentive. The total energy emitted is measured and recorded by smart meters, which is PHEV 's specific working proof of energy contribution. Similarly, in [117], the authors first defined two concepts, the data coin and the energy coin, as cryptocurrencies for Electric Vehicles (EV) applications. During the interaction, vehicle records are stored in the consortium blockchain, and the proof of work is done with the Proof of Data Contribution Frequency and the Proof of Energy Contribution Amount. In the process of information interaction, the data coin is defined according to the proof of frequency contribution of electric vehicle data, and in the process of energy interaction, the energy coin is defined according to the proof of its energy contribution. On the basis of these two proofs, the representativeness of majority decision is determined. That is, if the EV contributes to the collaborative intelligence more frequently, it will receive more data coins, will be given higher priority to access the resource pool, and its data will be given greater credibility. If it gives more energy back to the grid or other entities, it will have more energy coins and get higher priority or a lower energy price.

A final improvement is to authorize only a portion of the nodes for the consensus process. This method is used in [103], and an additional leader node is added to issue the audit content to the authorized node for verification. Then, the authentication results are compared. If the authentication results are consistent, the transaction will be made, and the leader node will receive additional rewards. In addition, a credit-based payment mechanism is designed to reduce the transaction confirmation time.

6.2. Proof-of-Stake

This is an alternative that requires little CPU power. It was first proposed in PPcoin and applied in the operation of the coins [118]. In the proof-of-stake system, instead of competing, miners maintain a set of validators that participate in the block creation process. Each verifies that it has a stake in the grid, and the equity is used to determine the likelihood that the node adds the next block of transactions to the blockchain. The system requires participants to prove the ownership of the currency. People with more money are less likely to attack networks. However, this mechanism tends to make the rich richer and the poor poorer.Compared with POW, POS mechanism does not need to find a suitable Nonce from unlimited space, so it saves energy and improves efficiency. After the PPCoin, to solve the security problems, such as malicious nodes being able to use the age of the coin to obtain a larger network weight, a new currency protocol based on POS, blackcoin, was developed [119]. Later, Vericoin [120] was proposed to improve POS, by reducing the risk of collusion and increasing the difficulty and cost of manipulating consensus. On this basis, POS based security protocols came into being, including the Snow White and Ouroboros [121,122]. Snow White was the first to formalize a set of consensual candidate requirements for POS and Ouroboros successfully implemented strict security guarantee.

POS has not been widely applied in the actual energy system model design. However, in [32], the demand response program is verified based on the POS consensus mechanism. Each distributed energy prosumer in the grid can act as an energy transaction verifier and can be the next effective block miner, and each verifier holds a certain stake. In addition, SolarCoin uses a low energy proof of stake algorithm, and on a similar scale uses less than 0.001% of the energy required for Bitcoin [70].

If the POS mechanism is a direct democracy, then Delegated proof of stake (DPOS) can be said to be a representative democracy. The nodes select specialized nodes and delegate them to generate and verify the blocks. If these selected nodes fail to perform their duties, they will lose this right. A typical application of DPOS is Bitshares [123], a smart contract platform.

6.3. Other Consensus Mechanisms

In addition to the two common consensus algorithms POW and POS, some other consensus algorithms are adopted. We briefly introduce some of them below.

6.3.1. PBFT

It is necessary to know the Byzantine Generals problem before we can understand this consensus algorithm [124]. In short, it is an abstract model of how a computer system handles faults. When certain parts of the system fail, they may send conflicting messages to different parts of the system. Generally speaking, this kind of fault that falsifies the response are called Byzantine fault, while those that do not falsify the response are called non-byzantine fault. The problem of dealing with Byzantine fault is abstracted as a Byzantine general problem, in which a group of general lead the Byzantine army camped outside an enemy city, and each general would observe the enemy and communicates with each other only by a messenger. They need to work out a common plan of actions. However, there may be traitors among the generals, who are trying to confuse the loyal generals. Hence, we need an algorithm to make sure that, no matter what the traitors do, the loyal generals will have a unified plan of action.

The practical Byzantine fault-tolerant algorithm is a replication algorithm that can tolerate Byzantine failures. It is practical and works in asynchronous environments [20,125]. PBFT is suitable for small networks, consortium blockchain or private blockchain.Because the consensus process requires three rounds of voting and each of which is broadcast, each node needs to know the identity of every other node in the network. Because it does not have the same mining process as POW, it saves a lot of energy. The right consensus can be reached when the number of malicious nodes is less than one-third of the total number of nodes. Hyperledger Fabric uses PBFT to reach consensus [126].

In the BeeKeeper system [24], the consensus mechanism of PBFT is also adopted. To ensure that the blockchain does not fork, the system assumes that at least two-thirds of the nodes are honest.

6.3.2. DBFT

Based on PBFT, some professional nodes, but not all of them, are used to record transactions, and that is delegated Byzantine fault tolerance (DBFT). This consensus algorithm was first proposed in NEO blockchain [127]. The consensus node is voted on by NEO holders and takes turns as speaker and delegates. The speaker is responsible for sending a proposal for a new block to the system, and the delegates are responsible for voting on the speaker's proposal. The proposal is approved when more than two-thirds of the votes are passed. This algorithm uses some characteristics of the POS mechanisms for reference, it can protect the network from Byzantine fault with the minimum resources, and also solves the scalability problem of the current blockchain. In [93], a reputation based delegated Byzantine fault tolerance (DBFT) consensus algorithm is proposed, which reach a consensus through the cooperation of the ordinary nodes and the consensus nodes. After all non-leader consensus nodes complete this process, the appointed leader will broadcast the proposal message and send its candidate blocks to other consensus nodes. The non-leading consensus nodes compare state sets, and, when different consensus nodes receive at least the same M-f consensus, which means there are at least f consensus same results out of M consensus nodes, new blocks can be generated.

6.3.3. Tendermint

Tendermint is also a consensual mechanism based on the Byzantine general problem mentioned above [20,128]. In this mechanism, a new concept of a validator is proposed. After each round of broadcasting a block, the validator selects whether to broadcast the pre-vote on the proposed block. If more than two-thirds of the nodes agree, then the submission of the block is broadcast by the validator. Thus, similar to PBFT, all nodes must be known, but it can provide more stringent guarantees. A node must lock its coin to become a verifier. If it is dishonest, it will be punished.

6.3.4. Ripple

Ripple is a low-latency, consistent algorithm that can handle secure, reliable transactions in seconds [129]. By using a unique node list (UNL) to handle the "collective trusted subnetworks", each node only needs to query its own UNL, rather than the entire network. It can tolerate less than a fifth of the node error. Ripple, a payments network with the same name, implements this consensus. It has successfully implemented a currency Ripple that could be traded with the real money [130].

6.3.5. Proof-of-Authority

Proof-of-Authority (POA) [131] is a consensus mechanism used primarily in consortium blockchain or private blockchain. Nodes with particular keys hold the state of the validator, and only the validators are allowed to add blocks on the chain, acting as a set of authorities to create and protect the chain. In comparison, it has lower latency, less computation, and is more secure.

7. Category III: System Optimization

7.1. Structure Optimization

Firstly, there are many structural optimization models to improve the performance from the system design level.

7.1.1. IOTA

IOTA is a new cryptocurrency that retains the core principles of blockchain but has a lightweight blockchain structure [132]. It mainly solves the problem that Bitcoin does not support micro-payment and that the scalability is limited. It is based on the structure of the Internet of Things (but not limited to this), and can be applied to any other micro-payment application. The underlying technology of IOTA is the "Tangle" ledger, a new type of blockless distributed ledger where each transaction is individually identified. The system incentivizes each user to maintain their own consensus mechanism, and whenever a transaction occurs, the sender must verify the previous two transactions. Since the verification is done by active participants on all chains, the transaction time is reduced and the zero-fee settlement transaction is achieved. In a sense, it is a combination of a blockchain and a physical object, fully enabling machine-to-machine communication. In the long run, IOTA has a lot of flexibility for quantum computing.

7.1.2. Blockchain+

This structural optimization is a combination of blockchain with other technologies, such as the Internet of Things and cloud computing models. In [133], an e-commerce model is developed based on the Internet of Things and blockchain. Distributed autonomous companies are used as cross-departmental entities to process data and property. In [134], cloud computing and blockchain are still used as partners, while a new model, BCPay, is built to solve security problems in outsourcing services, achieving stability and the so-called robust equity. Analogously, in [135], a demand response model based on fog computing is proposed. The nodes in fog computing are reconstructed as a sanitizer to utilize homomorphic operations to randomly transmit encrypted energy states and demand response strategies. The attacks can be resisted by consensus-based optimization and access control encryption. Demand response participants are divided into groups to reach consensus, and Nash equilibrium based on game theory is used to realize the random global optimization; all demand response participants are satisfied with the utility obtained.

Other works only use blockchain as part of the system to perform partial functions. For example, the system in [136] consists of three subsystems: the consumer system, the blockchain system and the transaction system. The users participate specifically in the consumer system and has a smart meter associated with it. Blockchain systems provide storage and are responsible for running smart contracts. The trading system provides robot advisors to advise users on the most suitable preference schemes to maximize the profits. It constitutes a private, decentralized and free energy market.

7.1.3. The Combination of Multiple Blockchain Models

For the storage problem, Wu et al. [137] designed a hybrid Blockchain architecture and a new storage mode which combines the public chain with private chain to improve the efficiency. Specifically, the public chain is used to identify data integrity, while the private chain is used to verify transaction accuracy. All blocks can be divided into management blocks and storage blocks, which are independent to each other. Users can query the data record in the management block, but they can only see the encrypted hash value instead of the original data. At the same time, the system also has the incentive mechanism driven by interests to attract more users to join the system.

7.1.4. Other Structure Optimization

In addition to the above methods, there are many other structural optimization models based on various functional improvements. In [87], a new interactive energy control model, including framework, mathematical model and pricing rules, is proposed, which can accurately match the solutions of centralized mechanisms while maintaining the privacy of the microgrid. It can be processed in parallel to reduce the time spent. For P2P energy sharing, intensive sensing and communication infrastructure is needed to build a central control system. Therefore, the control framework that requires the fewest measurements and communications is required. In [106], the authors proposed a two-stage aggregation control approach that requires only measurements at common coupling points and one-way communication points. In the first stage, the layer constrained non-linear programming method with a rolling horizon is adopted to minimize the energy cost of the community. In the second stage, the control set-points are updated according to the real-time measurement results.

Considering to the impact of factors such as intermittent power generation and the grid load consumption level, it may be unable to meet the requirements from smart grid components, hence storage units are deployed in [138]. A new framework is proposed, which combines the double auction market model and non-cooperative game theory to generate a dynamic pricing mechanism that enables geographically distributed storage units to interact and trade energy. In contrast, Ilic et al. [139] focused on market energy transactions at the regional level, in which the price of energy transactions includes the necessary transmission costs but is hidden from end users. At the same time, intelligent agents are adopted to act on behalf of the end user, considering the massive interaction between the end user and the market. There are also multi-agent systems to meet different needs [83]. The role of an agent is also studied in [140], which addresses the issue of proportionately fair and two-sided energy auctions.

7.2. Operational Cost Minimization

The cost minimization involves both the individual users and the overall energy cost. For example, Lin et al. [114] mainly considered the perspective of individual end users. The mixed integer linear programming is used to reduce energy waste and minimize energy cost. In [64], a proof-of-concept architecture based on secure private blockchain is proposed. The concept of atomic meta-transactions is introduced. The energy consumer will commit to pay, and, after receiving the energy, an energy receipt confirmation will be generated for confirmation and connected with the smart contract. The system has proven to be able to reduce the cost, processing time, and block size of energy transactions. In [141], similarly, the operation cost of electric vehicle charging stations is prioritized, while the energy supply is not affected. It is proposed that renewable energy can be used for the operation of charging stations during the day, while the central battery pack stores the excess energy at night. In this way, the charging cost of EV owners can be minimized.

In terms of the total cost, in [11], the energy transaction between isolated island microgrids are studied, and a distributed convex optimization framework is developed for it. A cost minimization algorithm based on sub-gradient is proposed, which can expand the number of microgrids and maintain the privacy of local consumption. Hajiesmaili et al. [142] focused on solving the heterogeneity between microgrid devices. A crowd-sourcing storage system to design a centralized online algorithm is adopted, which can minimize the cost while achieving supply and demand balance. The hybrid approach combines the smart contracts of blockchain with the use of traditional computing platforms in [84].

Power-ID [47], a Swiss pilot project, uses blockchain to create a small peer-to-peer energy market of 20 consumers and 20 prosumers. The cost of the network is flexible by concentrating the distributed network on solar energy and batteries. If a large amount of local energy is self-sufficient (such as a sunny day), then participants only have to pay their own network costs, which helps reduce the overall cost of the system.

7.3. Social Welfare Optimization

The concept of social welfare is originated from the Kelly mechanism. The Kelly mechanism is a type of auction algorithm that allows an agent to bid separately, with bidders receiving bids allocating shares in proportion to the value of the bid. This bidding mechanism can maximize the overall benefits of all agents, the so-called social welfare, which is realized through effective auction [140]. This paper also proves that double auction is easier to minimize the efficiency loss caused by price expectation than single auction, and has proposed a distributed iterative auction algorithm, which allows the selfish agent to estimate the expected price behavior through the information of previous iterations.

To achieve this, there have been many studies using different strategies. In [143], it is proposed to maximize social welfare through smart contract of blockchain and automatic initiation of fine-tuned rules. Jiao et al. [60] designed two different cloud-based auction mechanisms for different scenes. For the constant-demand scheme, each miner bids for a fixed and limited price. For the multi-demand scenario, the miners ask for their own needs and then issue corresponding demands freely. Both models can maximize social welfare.

In [88], considering the social welfare objective function, the optimization is calculated according to different constraints. However, detailed information is required for calculation. A reasonable mechanism is needed to extract information for calculation while ensuring user privacy. To the same end, edge computing and deep learning are used in [58] to achieve an optimal auction, which transforms based on the miner’s bid and calculates payment rules, considering the authenticity and computational efficiency [94].

7.4. Data Protection in Storage

In addition to data protection in the communication process, Gai et al. [65] focused on the data stored in blocks; these data may be subject to link attacks or malicious data mining, hence threatening the privacy of users. In this paper, a noise-based privacy-preserving blockchain-support transaction model is proposed to generate noise to hide the transaction distribution trend. The energy sales of sellers are screened by mining the energy transaction volume. In [77], a method of grouping users is proposed. One user is randomly set to be the aggregator in each time interval. Even if the aggregators are malicious, the tampered data will be discovered by others.

In [144], existing household energy storage units have been used to blur household consumption and reduce the cost of load hiding. The opportunistic joint use of electric vehicles, heating, ventilation and air-conditioning systems can reduce or eliminate the reliance on locally dedicated rechargeable batteries. The mutual information between the original household load and the mask load is used as the privacy protection measure. For the mask load time series and the original load time series, the combination of existing thermal appliances and energy storage units is used to hide the household load.

7.5. Other Benefits Maximization

In addition to the cost and social welfare, there are many other performance indicators that need optimization.

In [145], an optimal charging scheduling scheme is proposed for electric vehicles by using Nondominated Sorting Genetic Algorithm (NSGA), which can maximize user satisfaction and minimize cost based on a double-objective optimization model. A novel process and an incentive mechanism are proposed to coordinate, allocate and settle energy transactions in [102], which allow producers to choose their preferred pricing strategy to maximize profits while keeping consumer costs to a minimum. There are many published studies achieving these two goals. For example, the market premium or discount based on the market price one day in advance [9], an extensible framework consisting of two independent nonlinear programming models for the coordination of residential load [80], and the pricing mechanism of the intermediate market interest rate proposed in [107].

There are also performance optimizations using game theory methods, for example, to solve the problem of energy management, Tushar et al. [146] for the first time used the shared facility controller to play an uncooperative Stackelberg game between the residential and the shared facility controller. The cost minimization and benefit maximization can be achieved. On this basis, Lee et al. [147] proposed a completely distributed energy trading mechanism, in which the seller needs to weigh the satisfaction of income and energy storage. The buyer needs to make a bid to track the seller's behavior, and the Stackelberg game is used to solve the case with multiple leaders and multiple followers, so as to realize the maximization of all micro-grid benefits. To maximize the utility of the operator, a method based on the contract theory is proposed to analyze the optimal contract, which can meet the individual energy consumption preference of electric vehicles and maximize the utility of the operator [93]. The two-stage Stackelberg game is used to maximize the benefits of cloud computing services and miners in a consensus process in [105].

There is also a common mode to maximize the benefits of system users by formulating appropriate auction mechanism. In [90], distributed controllers and centralized auctions are used to perform market clearing. The maximum welfare of market users can be ensured without the need for user's personal information.

For a progressive summary, in Table 2, we assess some existing energy projects and summarize whether they address the challenges mentioned in the three sections above.

Table 2. Energy project assessment.

	High Efficiency	Low Cost	Privacy Protection	Real-Time Communication	Incentive Mechanism	Eco-Friendly	Energy Certification	User-Benefit
Sunchain [45]	✓	✓				✓	✓	
Power ledger [46]	✓	✓		✓			✓	
I-NUK [48]				✓	✓	✓	✓	✓
Pylon Network [68]			✓			✓	✓	✓
Tal.Markt [49]						✓		
Grünstromjeton [69]		✓			✓	✓		✓
Power-ID [47]		✓				✓		✓
NRGcoin [73]		✓			✓	✓		✓
Exergy [44]		✓	✓		✓	✓		
SolarCoin [70]					✓	✓	✓	✓

8. Discussion and Future Directions

As far as we are concerned, the development of Blockchain from 1.0 through 2.0 to 3.0 is accompanied by increasing de-specialization, universalization and radicalization. From a single currency to the entire economic and financial market, and then to various fields of social life, it can solve the problem of mutual trust and data security in all walks of life.

From the perspective of energy trading, based on the study presented above, we found that there are still some issues that have not been well-addressed.

The first is the improvement of consensus mechanism. At present, most systems still use POW, or the improved POW, when applying the consensus mechanism. However, many problems exist in this mechanism, such as the long time it takes to reach an agreement, and the high computational overhead. The system discussed about above requires a large carbon footprint in part because of this consensus mechanism. Some of the proposed mechanisms, such as POS and PBFT, are proposed cope with the shortcomings of POW. However, they are not widely used in energy trading currently.

The second is the process of transmission. There are few technologies related to route hiding. This can bring troubles to the privacy and security of users.

The last problem is the application of such systems in real life, which needs a lot of experimental and simulation tests [63]. The specific challenges include:

- Lack of regulatory mechanisms. In most countries, power grid taxation is an essential part of national financial income. Although transaction fees can be used to make proper adjustments in the blockchain system, establishing applicable systems of laws and regulations is still needed. Without statutory guidance, it is hard to be widely adopted, especially by large companies.
- Implementation of the physical layer. Few systems have actually considered the implementation of hardware at the physical level, and the limitations of hardware have a significant impact on the design of the system. Moreover, although the distributed grid model has largely reduced the incidence of cascading errors, due to the adjacent decoupled network structure of the blockchain system, there are still potential cyber-physical contingency or even catastrophic cascading errors [15].
- Environmental challenges. Blockchain requires a high carbon footprint and energy consumption. Currently, as people are paying more attention to the ecological environment, there should be more structures such as IOTA that can reduce the carbon footprint. Additionally, scalability is also a challenge as more and more nodes are integrated into the grid. SolarCoin [70] mentioned above is exactly an environmentally friendly currency. It is an entirely free additional income for users, the first currency to protect natural capital, and the first global non-governmental solar energy incentive mechanism. More importantly, it is also a liquid asset that can be traded with government currencies.

Apart from the application form of blockchain described in this paper, there are more extensive application forms, such as those described in [66,148], in which blockchain can be used to register and store carbon emissions, or to promote the use of renewable energy. For example, the concept of green blockchain is proposed in [149], which has been applied to another area of the energy market, namely the industrial operating systems, to manage environmental certificates, emission permits and other projects.

In the future, we will delve into the following aspects.

- Sharding Network. Each node only manages its own (shard of) data, not all of the blocks, which solves the problem of scalability and reduces data redundancy and storage space. However, it may be difficult to achieve fragment reconstruction and node consistency. For example, Ethereum 2.0 uses sharding to solve the scalability problems. Ethernet network is divided into two layers: the upper layer is the existing Ethernet main chain, while the lower layer is the fragment chain [150]. Zilliqa sharding technology performs the division of network nodes through POW algorithm.

It selects a Boss sharding and multiple work sharding, each sharding contains no fewer than 600 nodes. Each transaction is mapped to a work sharding according to the address, and the sharding verifies the transaction through the PBFT consensus algorithm and forms a sub-block in the current work shard. Then, the work sharding sends the sub-blocks to the boss sharding. After the boss sharding's verification, the final blocks are merged and generated.

- Change the structure of the single chain. For example, the Huobi Chain [151] adopts double chain structure and dynamic collaboration. The trading chain is responsible for transaction clearing, pursuing transaction speed and reducing fees. The contract chain supports complex applications such as financial contracts. The IOTA mentioned above also uses a Tangle structure instead of a single chain.
- Privacy protection and regulatory mechanism are two contradictory problems. In the future, a system framework can be developed to balance the privacy protection and the regulation. Perhaps Idemix, zero-knowledge proof, attribute encryption and other methods can help solve this problem. At present, some studies have begun to focus on the regulatory system of blockchain. Analyzing the regulatory mechanisms of the European Union and the United States indicates that it is possible to have greater value added with the minimum regulatory limit [152].
- A unified safety evaluation system can be established for different safety defects. This is not only conducive to the development of blockchain products, but also conducive to security audit. For example, Zhang and Preneel [153] developed several evaluation metrics based on the security of work certificates.
- Energy certification and verification. Measures should be implemented to prevent cheating producers whose energy is actually generated from fossil fuels but claim it is renewable energy. Sunchain [45], for example, has added such checks to its program.

9. Conclusions

In this paper, we summarize the existing literature on blockchain-based energy trading markets. We investigated many relevant issues, from the removal of the centralized control and the transition to a distributed architecture, the security and privacy issues, transaction object matching issues, the auction pricing mechanism at the time of settlement, to the cost minimization and benefit maximization of the system. Finally, we highlighted the unsolved problems and provided insights for future directions.

Increasingly more experiments show that the distributed system architecture employed by blockchain can bring greater flexibility and better performance to the energy trading market. The development of blockchain-based energy trading has made some progress and is gradually maturing. In general, the most common application form of blockchain technology in energy trading is the main framework of the system, which plays an important role in storing transaction data and ensuring security. Meanwhile, there are also those who use blockchain only as an implementation tool to achieve certain functions.

Furthermore, we have seen that more and more blockchain products have solved the intrinsic problems of blockchain (e.g., IOTA). Different types of blockchain can also be combined to achieve the improvement of system performance with their own advantages, for example, the combination of the consortium blockchain and the private blockchain. Besides, the blockchain products should also provide interfaces for customization. We also found a trend towards more and more system models that take into account the interests of individuals, which means that the market has shifted its focus from macro improvement to the detailed optimizations when designing new systems.

In existing practical applications, a better incentive mechanism has been adopted to stimulate users to join the system. The renewable energy power generation is encouraged by giving benefits to users. However, the regulatory mechanisms for these projects remains an urgent problem. Overall, although most of the projects are small pilot projects, they have yielded considerable results. There are also global anarchic systems such as SolarCoin [70] dedicated to environmentally friendly causes. There are reasons to believe that blockchain-based energy transactions will continue growing into a global model in the future.

Author Contributions: Conceptualization, Z.G.; investigation, N.W., Z.G.; methodology, N.W., X.Z., X.L. and Z.G.; writing—original draft, N.W., X.Z. and X.L.; writing—review & editing, L.W., Z.G., X.D. and M.G.

Funding: This research was funded by Beijing Natural Science Foundation (grant number 4182060).

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

References

1. Lan, H.; Yin, H.; Wen, S.; Hong, Y.Y.; Yu, C.D.; Zhang, L. Electrical Energy Forecasting and Optimal Allocation of ESS in a Hybrid Wind-Diesel Power System. *Appl. Sci.* **2017**, *7*, 155. [CrossRef]
2. Du, X.J.; Xiao, Y.; Guizani, M.; Chen, H.H. An Effective Key Management Scheme for Heterogeneous Sensor Networks. *Ad Hoc Netw.* **2007**, *5*, 24–34. [CrossRef]
3. Aitzhan, N.Z.; 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]
4. Wu, J.; Tran, N.K. Application of Blockchain Technology in Sustainable Energy Systems An Overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
5. Wang, J.; Wang, Q.; Zhou, N.; Chi, Y. A Novel Electricity Transaction Mode of Microgrids Based on Blockchain and Continuous Double Auction. *Energies* **2017**, *10*, 1971. [CrossRef]
6. Du, X.J.; Chen, H.H. Security in Wireless Sensor Networks. *IEEE Wirel. Commun.* **2008**, *15*, 60–66.
7. Guan, Z.T.; Zhang, Y.; Wu, L.F.; Wu, J.; Li, J.; Ma, Y.L.; Hu, J.J. APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. *J. Netw. Comput. Appl.* **2019**, *125*, 82–92. [CrossRef]
8. Guan, Z.T.; Zhang, Y.; Zhu, L.H.; Wu, L.F.; Yu, S. EFFECT: An Efficient Flexible Privacy-Preserving Data Aggregation Scheme with Authentication in Smart Grid. *Sci. Chin. Inf. Sci.* **2019**, *62*, 1–14. [CrossRef]
9. Ettlin, A. Dynamic Modeling of Peer-to-Peer Power Market Making. In Proceedings of the 2018 15th International Conference on the European Energy Market (EEM), Lodz, Poland, 27–29 June 2018.
10. Mylrea, M.; Gourisetti, S.N.G. Blockchain for smart grid resilience Exchanging distributed energy at speed, scale and security. In Proceedings of the 2017 Resilience Week (RWS), Wilmington, DE, USA, 18–22 September 2017.
11. Gregoratti, D.; Matamoros, J. Distributed Energy Trading: The Multiple-Microgrid Case. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2551–2559. [CrossRef]
12. Jogunola, O.; Ikpehai, A.; Anoh, K.; Adebisi, B.; Hammoudeh, M.; Gacanin, H.; Harris, G. Comparative Analysis of P2P Architectures for Energy Trading and Sharing. *Energies* **2017**, *11*, 62. [CrossRef]
13. Fang, X.; Misra, S.;Xue, G.L.; Yang, D.J. Smart Grid—The New and Improved Power Grid: A Survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. [CrossRef]
14. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 31 October 2008).
15. Yang, T.Y.; Guo, Q.L.; Tai, X.; Sun, H.B.; Zhang, B.M.; Zhao, W.L.; Lin, C.H. Applying blockchain technology to decentralized operation in future energy Internet. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017.
16. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Sirer, E.G.; et al. On scaling decentralized blockchains. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 106–125.
17. Eyal, I.; Gencer, A.E.; Sirer, E.G.; Renesse, R.V. Bitcoin-NG: A scalable blockchain protocol. In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16), Santa Clara, CA, USA, 16–18 March 2016; ISBN 978-1-931971-29-4.
18. David, B.; Gaži, P.; Kiayias, A.; Russell, A. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, 29 April–3 May 2018; Springer: Cham, Switzerland, 2018.

19. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras L.; Janicke, H. Blockchain Technologies for the Internet of Things Research Issues and Challenges. *IEEE Internet Things J.* **2018**, *1*. [CrossRef]
20. Zheng, Z.B.; Xie, S.A.; Dai, H.N.; Chen, X.P.; Wang, H.M. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
21. Zyskind, G.; Nathan, O.; Pentland, A.S. 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.
22. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.K.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2016.
23. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
24. Zhou, L.J.; Wang, L.C.; Sun, Y.R; Lv, P. BeeKeeper: A Blockchain-based IoT System with Secure Storage and Homomorphic Computation. *IEEE Access* **2018**, *6*, 43472–43488. [CrossRef]
25. Li, Z.; Mohammad, S.; Liu, X. Cyber-secure decentralized energy management for IoT-enabled active distribution networks. *J. Mod. Power Syst. Clean Energy* **2018**, *6*, 900–917. [CrossRef]
26. Hu, S.S.; Cai, C.J.; Wang, Q.; Wang, C.; Luo, X.; Ren, K. Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization. In Proceedings of the IEEE Conference on Computer Communications (Infocom 2018), Honolulu, HI, USA, 16–19 April 2018.
27. Huang, L.X.; Zhang, G.X.; Yu, S.; Fu, A.M.; Yearwood, J. Customized Data Sharing Scheme based on Blockchain and Weighted Attribute. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 9–13 December 2018; pp. 1–6.
28. Park, C.; Taeseok, Y. Comparative review and discussion on P2P electricity trading. *Energy Procedia* **2017**, *128*, 3–9. [CrossRef]
29. Sousa, T.; Soares, T.; Pinson, P.; Moret, F.; Baroche, T.; Sorin, E. Peer-to-peer and community-based markets: A comprehensive review. *Comput. Soc.* **2018**, *104*, 367–378. [CrossRef]
30. Murkin, J.; Chitchyan, R.; Byrne, A. Enabling peer-to-peer electricity trading. In Proceedings of the 4th International Conference on ICT for Sustainability (ICT4S 2016), Amsterdam, The Netherlands, 29 August–1 September 2016; pp. 234–235.
31. Abdella, J.; Shuaib, K. Peer to Peer Disributed Energy Trading in Smart Grids A Survey. *Energies* **2018**, *11*, 1560. [CrossRef]
32. Pop, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids. *Sensors* **2018**, *18*, 162. [CrossRef]
33. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
34. Shuaib, K.; Abdella, J.A.; Sallabi, F.; Abdel-Hafez, M. Using Blockchains to Secure Distributed Energy Exchange. In Proceedings of the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018. [CrossRef]
35. Matamoros, J.; Gregoratti, D.; Dohler, M. Microgrids Energy Trading in Islanding Mode. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012.
36. Wang, Y.; Mao, S.W.; Nelms, R.M. On Hierarchical Power Scheduling for the Macrogrid and Cooperative Microgrids. *IEEE Trans. Ind. Inf.* **2015**, *11*, 1574–1584. [CrossRef]
37. Zhu, X.Z.; Leung, K. An adaptive distributed power scheduling algorithm for renewable Microgrid cooperation. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017. [CrossRef]
38. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A blockchain-based smart grid towards sustainable local energy markets. *Comput. Sci. Res. Develop.* **2018**, *33*, 207–214. [CrossRef]
39. Kounelis, I.; Steri, G.; Giuliani, R.; Geneiatakis, D.; Neisse, R.; Nai-Fovino, I. Fostering consumers' energy market through smart contracts. In Proceedings of the 2017 International Conference in Energy and Sustainability in Small Developing Economies (ES2DE), Funchal, Portugal, 10–12 July 2017. [CrossRef]

40. Gao, C.Y.; Ji, Y.C.; Wang, J.Z.; Sai, X. Application of Blockchain Technology in Peer-to-Peer Transaction of Photovoltaic Power Generation. In Proceedings of the 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, 25–27 May 2018. [CrossRef]
41. Rahmadika, S.; Ramdania, D.R.; Harika, M. Security Analysis on the Decentralized Energy Trading System Using Blockchain Technology. *J. Online Inf.* **2018**, *3*, 44–47. [CrossRef]
42. Hwang, J.; Choi, M.; Lee, T.; Jeon, S.; Kim, S.; Park, S.; Park, S. Energy Prosumer Business Model Using Blockchain System to Ensure Transparency and Safety. *Energy Procedia* **2017**, *141*, 194–198. [CrossRef]
43. Richter, B.; Mengelkamp, E.; Weinhardt, C. Maturity of Blockchain Technology in Local Electricity Markets. In Proceedings of the 2018 15th International Conference on the European Energy Market (EEM), Lodz, Poland, 27–29 June 2018.[CrossRef]
44. Orsini, L.; Collins, B.; Webb, M.; Montgomery, C.; Conte, B.; Adamson, M.; Heitmann, P.; Kessler, S.; Brown, M. Exergy-Technical White Paper. Exergy. Available online: https://lo3energy.com/wp-content/uploads/2018/04/Exergy-BIZWhitepaper-v11.pdf (accessed on 16 March 2019).
45. Sunchain. Available online: http://www.Sunchain.fr (accessed on 16 March 2019).
46. Power Ledger. Available online: https://www.powerledger.io (accessed on 16 March 2019).
47. Blockchains and Energy Transition. Available online: http://www.im.ethz.ch/people/sschopfer.html (accessed on 25 March 2019).
48. Inuk. Available online: http://www.inuk.co (accessed on 15 March 2019).
49. Tal.Markt. Available online: http://www.wsw-talmarkt.de/#/home (accessed on 16 March 2019).
50. Swan, M.; *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
51. Eosio. Available online: https://eos.io/ (accessed on 25 December 2018).
52. Bergquist, J.; Laszka, A.; Sturm, M.; Dubey, A. On the design of communication and transaction anonymity in blockchain-based transactive microgrids. In Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers (SERIAL'17), Las Vegas, NV, USA, 11–15 December 2017.
53. Miers, I.; Garman, C.; Green, M.; Rubin, A.D. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013. [CrossRef]
54. Xiao, Y.; Rayi, V.K.; Sun, B., Du, X.J.; Hu, F.; Galloway, M. A Survey of Key Management Schemes in Wireless Sensor Networks. *J. Comput. Commun.* **2007**, *30*, 2314–2341. [CrossRef]
55. Xiao, Y. ; Du, X.J; Zhang, J.Y.; Guizani, S. Internet Protocol Television (IPTV): The Killer Application for the Next Generation Internet. *IEEE Commun. Mag.* **2007**, *45*, 126–134. [CrossRef]
56. Du, X.J.; Guizani, M.; Xiao, Y.; Chen, H.H. Transactions papers a Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1223–1229. [CrossRef]
57. Wu, J.; Dong, M.X.; Ota, K.; Li, J.H.; Guan, Z.T. Big Data Analysis-Based Secure Cluster Management for Optimized Control Plane in Software-Defined Networks. *IEEE Trans. Netw. Serv. Manag.* ***2018**, 15, 27–38.* [CrossRef]
58. Luong, N.C.; Xiong, Z.H.; Wang, P.; Niyato, D. Optimal Auction for Edge Computing Resource Management. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018. [CrossRef]
59. Wu, J.; Dong, M.X.; Ota, K.; Li, J.H.; Guan, Z.T. FCSS: Fog-Computing-based Content-Aware Filtering for Security Services in Information-Centric Social Networks. *IEEE Trans. Emerg. Topics Comput.* **2018**, *1*, 1. [CrossRef]
60. Jiao, Y.T.; Wang, P.; Niyato, D.; Suankaewmanee, K. Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks. *arXiv* **2018**, arXiv:1804.09961.
61. Tushar, W.; Yuen, C.; Mohsenian-Rad, H.; Saha T.; Poor, H.V.; Wood, K.L. Transforming Energy Networks via Peer to Peer Energy Trading: Potential of Game Theoretic Approaches. *IEEE Signal Process. Mag.* **2018**, *35*, 90–111. [CrossRef]
62. Morstyn, T.; Farrell, N.; Darby, S.J.; McCulloch M.D. Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants. *Nat. Energy* **2018**, *3*, 94–101. [CrossRef]

63. Nguyen, V.H.; Besanger, Y.; Tran, Q.T.; Le, M.T. On the Applicability of Distributed Ledger Architectures to Peer-to-Peer Energy Trading Framework. In Proceedings of the 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Palermo, Italy, 12–15 June 2018. [CrossRef]
64. Ali, D.; Ambrose, H.; Salil, S.K.; Jurdak, R.; Luo, F.J.; Dong, Z.Y. Peer-to-Peer EnergyTrade A Distributed Private Energy Trading Platform. *arXiv* **2018**, arXiv:1812.08315.
65. Gai, K.K.; Wu, Y.L.; Zhu, L.H.; Qiu, M.K.; Shen, M. Privacy-preserving Energy Trading Using Consortium Blockchain in Smart Grid. *IEEE Trans. Ind. Inf.* **2019**, 1. [CrossRef]
66. Brilliantova, V.; Thurner, T.W. Blockchain and the future of energy. *Technol. Soc.* **2018**. [CrossRef]
67. Vytelingum, P.; Ramchurn, S.D.; Voice, T.D.; Rogers, A.; Jennings, N.R. Trading agents for the smart electricity grid. In Proceedings of the AAMAS '10 Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems, Toronto, ON, Canada, 10–14 May 2010; pp. 897–904.
68. Pylon Network Team. Pylon Network WhitePaper v.2.0. Available online : https://pylon-network.org/wp-content/uploads/2019/02/WhitePaper_PYLON_v2_ENGLISH-1.pdf (accessed on 25 March 2019).
69. Grünstromjeton. Available online: https://www.energieagentur.nrw/eanrw/sev_gruenstromjetons_blockchain-anwendung_macht_gruenstromverbrauch_sichtbar (accessed on 25 March 2018)
70. Solarcoin. Available online: http://www.solarcoin.org (accessed on 15 March 2019).
71. Grid Singularity. Available online: https://energyweb.atlassian.net/wiki/spaces/EWF/ (accessed on 28 March 2019).
72. Dajie. Available online: https://www.dajie.eu (accessed on 28 March 2019).
73. NRGcoin. Available online: http://www.nrgcoin.org (accessed on 15 March 2019).
74. Energolabs. Available online: https://www.energolabs.com/#/ (accessed on 28 March 2019).
75. Laszka, A.; Dubey, A.; Walker, M.; Schmidt, S. Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers. In Proceedings of the IoT '17, Linz, Austria, 22–25 October 2017.
76. Kvaternik, K.; Laszka, A.; Walker, M.; Schmidt, D.; Sturm, M.; lehofer, M.; Dubey, A. Privacy-Preserving Platform for Transactive Energy Systems. *arXiv* **2018**, arXiv:1709.09597.
77. Guan, Z.T.; Si, G.L.; Zhang, X.S.; Wu, L.F.; Guizani, N.; Du, X.J.; Ma, Y.L. Privacy-preserving and Efficient Aggregation based on Blockchain for Power Grid Communications in Smart Communities. *IEEE Commun. Mag.* **2018**, *56*, 82–88. [CrossRef]
78. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.M.; Savage, S. A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet measurement conference, Barcelona, Spain, 23–25 October 2013; pp. 127–140.
79. Abidin, A.; Aly, A.; Cleemput, S.; Mustafa, M.A. Secure and Privacy-Friendly Local Electricity Trading and Billing in Smart Grid. *arXiv* **2018**, arXiv:1801.08354.
80. Azar, A.G.; Nazaripouya, H.; Khaki, B.; Chu, C.C.; Gadh, R.; Jacobsen, R.H. A Non-Cooperative Framework for Coordinating a Neighborhood of Distributed Prosumers. *IEEE Trans. Ind. Inf.* **2018**, 1. [CrossRef]
81. Yu, Y.; Ding, Y.J.; Zhao, Y.Q.; Li, Y.N.; Du, X.J. Guizani Mohsen LRCoin, Leakage-resilient Cryptocurrency Based on Bitcoin for Data Trading in IoT. *IEEE Internet Things J.* **2018**. [CrossRef]
82. Yucel, F.; Bulut, E.; Akkaya, K. Privacy Preserving Distributed Stable Matching of Electric Vehicles and Charge Suppliers. In Proceedings of the IEEE Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018.
83. Nunna, H.K.; Doolla, S. Multiagent-Based Distributed-Energy-Resource Management for Intelligent Microgrids. *IEEE Trans. Ind. Electron.* **2013**, *60*, 1678–1687. [CrossRef]
84. Laszka, A.; Dubey, A.; Eisele, S.; Walker, M.; Kvaternik, K. Design and Implementation of Safe and Private Forward-Trading Platform for IoT-Based Transactive Microgrids. Available online: http://www.isis.vanderbilt.edu/node/4868 (accessed on 18 October 2018).
85. Majumder, B.P.; Faqiry, M.N.; Das, S.; Pahwa, A. An efficient iterative double auction for energy trading in microgrids. In Proceedings of the 2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG), Orlando, FL, USA, 9–12 December 2014. [CrossRef]
86. Ramachandran, B.; Srivastava, S.K.; Edrington, C.S.; Cartes, D.A. An Intelligent Auction Scheme for Smart Grid Market Using a Hybrid Immune Algorithm. *IEEE Trans. Ind. Electron.* **2011**, *58*, 4603–4612. [CrossRef]
87. Liu, W.J.; Zhan, J.P.; Chung, C.Y. A Novel Transactive Energy Control Mechanism for Collaborative Networked Microgrids. *IEEE Trans. Pow. Syst.* **2018**. [CrossRef]

88. Kang, J.W.; Yu, R.; Huang, X.M.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Trans. Ind. Inf.* **2017**, *13*, 3154–3164. [CrossRef]
89. Guerrero, J.; Chapman, A.C.; Verbič, G. Decentralized P2P Energy Trading under Network Constraints in a Low-Voltage Network. *IEEE Trans. Smart Grid* **2018**, 1. [CrossRef]
90. Khorasany, M.; Mishra, Y.; Ledwich, G. Auction based energy trading in transactive energy market with active participation of prosumers and consumers. In Proceedings of the 2017 Australasian Universities Power Engineering Conference (AUPEC), Melbourne, VIC, Australia, 19–22 November 2017. [CrossRef]
91. Zhao, S.N.; Wang, B.B.; Li, Y.C.; Li, Y. Integrated Energy Transaction Mechanisms Based on Blockchain Technology. *Energies* **2018**, *11*, 2412. [CrossRef]
92. Zhang, C.H.; Wu, J.Z.; Zhou, Y.; Cheng, M.; Long, C. Peer-to-Peer energy trading in a Microgrid. *Appl. Energy* **2018**, *220*, 1–12. [CrossRef]
93. Su, Z.; Wang, Y.T.; Xu, Q.C.; Fei, M.; Tian, Y.C.; Zhang, N. A secure charging scheme for electric vehicles with smart communities in energy blockchain. *IEEE Internet Things J.* **2018**, 1. [CrossRef]
94. Jiao, Y.T.; Wang, P.; Niyato, D.; Xiong, Z.W. Social Welfare Maximization Auction in Edge Computing Resource Allocation for Mobile Blockchain. In Proceeding of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018. [CrossRef]
95. Kim, J.; Lee, J.; Park, S.; Choi, J.K. Battery Wear Model based Energy Trading in Electric Vehicles a Naive Auction Model and a Market Analysis. *IEEE Trans. Ind. Inf.* **2018**. [CrossRef]
96. Wang, N.; Xu, W.S.; Xu, Z.Y.; Shao, W.H. Peer-to-Peer Energy Trading among Microgrids with Multidimensional Willingness. *Energies* **2018**, *11*, 3312. [CrossRef]
97. Truong, C.N.; Schimpe, M.; Bürger, U.; Hesse, H.C.; Jossen, A. Multi-Use of Stationary Battery Storage Systems with Blockchain Based Markets. *Energy Procedia.* **2018**, *155*, 3–16. [CrossRef]
98. Zhong, W.F.; Yang, C.; Xie, K.; Xie, S.L.; Zhang, Y. ADMM-Based Distributed Auction Mechanism for Energy Hub Scheduling in Smart Buildings. *IEEE Access* **2018**, *6*, 45635–45645. [CrossRef]
99. Gode, D.K.; Sunder, S. Allocative Efficiency of Markets with Zero-Intelligence Traders: Market as a Partial Substitute for Individual Rationality. *J. Politic. Econ.* **1993**, *101*, 119–137. [CrossRef]
100. Cliff, D. Minimal-Intelligence Agents for Bargaining Behaviors in Market-Based Environments. Available online: https://pdfs.semanticscholar.org/9d26/6f3113262d7b029f933462d571e292ed1281.pdf (accessed on 20 December 2018).
101. Lee, W.; Xiang, L.; Schober, R.; Wong, V.W.S. Direct Electricity Trading in Smart Grid A Coalitional Game Analysis. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1398–1411. [CrossRef]
102. Meeuw, A. Design, Implementation, and Evaluation of a Blockchain-enabled Multi-Energy Transaction System for District Energy Systems. Master's Thesis, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, April 2018.
103. Li, Z.T.; Kang, J.W.; Yu, R.; Ye, D.D.; Deng, Q.Y.; Zhang, Y. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Trans. Ind. Inf.* **2018**, *14*, 3690–3700. [CrossRef]
104. Xiong, Z.H.; Feng, S.H.; Wang, W.B.; Niyato, D.; Wang, P.; Han, Z. Edge computing resource management and pricing for mobile blockchain. *arXiv* **2017**, arXiv:1710.01567.
105. Xiong, Z.; Feng, S.; Niyato, D.; Wang, P.; Han, Z. Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks. *IEEE Internet Things J.* **2018**, 1. [CrossRef]
106. Long, C.; Wu, J.Z.; Zhou, Y.; Jenkins, N. Peer-to-peer energy sharing through a two-stage aggregated battery control in a community Microgrid. *Appl. Energy* **2018**, *226*, 261–276. [CrossRef]
107. Tushar, W.; Saha, T.K.; Yuen, C.; Liddell, P.; Bean, R.; Poor, H.V. Peer-to-Peer Energy Trading With Sustainable User Participation A Game Theoretic Approach. *IEEE Access* **2018**, *6*, 62932–62943. [CrossRef]
108. Poon, J.; Dryja, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Available online: https://nakamotoinstitute.org/static/docs/lightning-network.pdf (accessed on 22 November 2018).
109. Erdin, E.; Cebe, M.; Akkaya, K.; Solak, S.; Bulut, E.; Uluagac, S. Building a Private Bitcoin-based Payment Network among Electric Vehicles and Charging Stations. In Proceeding of the 2018 IEEE International Conference on Blockchain (Blockchain-2018), Halifax, NS, Canada, 30 July–3 August 2018.
110. Luo, F.J.; Dong, Z.Y.; Liang, G.Q.; Murata, J.; Xu, Z. A Distributed Electricity Trading System in Active Distribution Networks Based on Multi-Agent Coalition and Blockchain. *IEEE Trans. Power Syst.* **2018**, 1. [CrossRef]

111. Blom, F. A Feasibility Study of Blockchain Technology as Local Energy Market Infrastructure. NTNU. 2018. Available online: http://hdl.handle.net/11250/2502356 (accessed on 20 October 2018).
112. Khorasany, M.; Mishra, Y.; Ledwich, G. Market framework for local energy trading a review of potential designs and market clearing approaches. *IET Generat. Transm. Distrib.* **2018**, *12*, 5899–5908. [CrossRef]
113. Blom, F.; Farahmand, H. On the Scalability of Blockchain-Supported Local Energy Markets. In Proceedings of the 2018 International Conference on Smart Energy Systems and Technologies (SEST), Sevilla, Spain, 10–12 September 2018; doi:10.1109/SEST.2018.8495882. [CrossRef]
114. Lin, C.C.; Deng, D.J.; Kuo, C.C.; Liang, Y.L. Optimal Charging Control of Energy Storage and Electric Vehicle of an Individual in the Internet of Energy With Energy Trading. *IEEE Trans. Ind. Inf.* **2018**, *14*, 2570–2578. [CrossRef]
115. Silvestre, M.L.D.; Gallo, P.; Ippolito, M.G.; Sanseverino, E.R.; Zizzo, G. A Technical Approach to the Energy Blockchain in Microgrids. *IEEE Trans. Ind. Inf.* **2018**, *14*, 4792–4803. [CrossRef]
116. Wu, Y.; Chen, X.X.; Shi, J.J.; Ni, K.J.; Qian, L.P.; Huang, L.; Zhang, K. Optimal Computational Power Allocation in Multi-Access Mobile Edge Computing for Blockchain. *Sensors* **2018**, *18*, 3472. [CrossRef] [PubMed]
117. Liu, H.; Zhang, Y.; Yang, T. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. *IEEE Netw.* **2018**, *32*, 78–83. [CrossRef]
118. King, S.; Nadal, S. Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Available online: https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf (accessed on 22 March 2019).
119. Vasin, P. Blackcoin's Proof-of-Stake Protocol v2. Available online: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed on 23 March 2019).
120. Pike, D.; Nosker, P.; Boehm, D.; Grisham, D.; Woods, S.; Marston, J. PoST White Paper. Available online: https://cdn.vericonomy.com/documents/VeriCoin-Proof-of-Stake-Time-Whitepaper.pdf (accessed on 10 March 2019).
121. Daian, P.; Pass, R.; Shi, E. Snow White: Provably Secure Proofs of Stake. Cryptology ePrint Archive, Report 2016/919. 2016. Available online: http://eprint.iacr.org/2016/919 (accessed on 15 October 2018).
122. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; Springer: Cham, Switzerland, 2017; pp. 257–388.
123. Schuh, F.; Larimer, D. Bitshares 2.0: General Overview. Available online: http://docs.bitshares.org/_downloads/bitshares-general.pdf (accessed on 15 March 2019).
124. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Programm. Lang. Syst.* **1982**, *4*, 382–401. [CrossRef]
125. Castro, M.; Barbara, L. Practical Byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation (USENIX OSDI), New Orleans, LO, USA, 22–25 February 1999; pp. 173–186.
126. Cachin, C. Architecture of the Hyperledger Blockchain Fabric. Available online: https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf (accessed on 12 March 2019).
127. NEO Blockchain. Available online: https://docs.neo.org/zh-cn/index.html (accessed on 20 March 2019).
128. Kwon J. Tendermint: Consensus without Mining. Available online: https://cdn.relayto.com/media/files/LPgoWO18TCeMIggJVakt_tendermint.pdf (accessed on 20 March 2019).
129. Schwartz, D.; Youngs, N.; Britto, A. The Ripple Protocol Consensus Algorithm. Available online: https://static.coinpaprika.com/storage/cdn/whitepapers/10565703.pdf (accessed on 20 Match 2019).
130. Ripple. Available online: https://ripple.com (accessed on 20 March 2019).
131. Proof-of-Authority Chains. Available online: https://wiki.parity.io/Proof-of-Authority-Chains (accessed on 25 March 2019).
132. IOTA. Available online: https://iota.org/ (accessed on 20 March 2019).
133. Zhang, Y.; Wen, J.T. The IoT electric business model: Using blockchain technology for the Internet of Things. *Netw. Appl.* **2017**, *10*, 983–994. [CrossRef]
134. Zhang, Y.H.; Deng, R.H.; Liu, X.M.; Zheng, D. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Inf. Sci.* **2018**, *462*, 262–277. [CrossRef]
135. Li, G.L.; Wu, J.; Li, J.H.; Guan, Z.T.; Guo, L.H. Fog Computing-Enabled Secure Demand Response for Internet of Energy Against Collusion Attacks Using Consensus and ACE. *IEEE Access* **2018**, *6*, 11278–11288. [CrossRef]

136. Mannaro, K.; Pinna, A; Marchesi, M. Crypto-trading: Blockchain-oriented energy market. In Proceedings of the 2017 AEIT International Annual Conference, Cagliari, Italy, 20–22 September 2017. [CrossRef]
137. Wu, L.J.; Meng, K.; Xu, S.; Li, S.Q.; Ding, M.; Suo, Y.F. Democratic Centralism A Hybrid Blockchain Architecture and Its Applications in Energy Internet. In Proceedings of the 2017 IEEE International Conference on Energy Internet (ICEI), Beijing, China, 17–21 April 2017. [CrossRef]
138. Wang, Y.P.; Saad, W.; Han, Z.; Poor, H.V.; Başar, T. A Game-Theoretic Approach to Energy Trading in the Smart Grid. *IEEE Trans. Smart Grid.* **2014**, *5*, 1439–1450. [CrossRef]
139. Ilic, D.; Silva, P.G.D.; Karnouskos, S.; Griesemer, M. An energy market for trading electricity in smart grid neighbourhoods. In Proceedings of the 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), Campione d'Italia, Italy, 18–20 June 2012. [CrossRef]
140. Faqiry, M.N.; Das, S. Double-Sided Energy Auction in Microgrid: Equilibrium Under Price Anticipation. *IEEE Access* **2016**, *4*, 3794–3805. [CrossRef]
141. Bokopane, L.; Kusakana, K.; Vermaak, H.J. Energy Management of a Grid-Intergrated Hybrid Peer-to-Peer Renewable Charging Station for Electric Vehicles. In Proceedings of the 2018 Open Innovations Conference (OI), Johannesburg, South Africa, 3–5 October 2018. [CrossRef]
142. Hajiesmaili, M.H.; Chen, M.H.; Mallada, E.; Chau, C.K. Crowd-Sourced Storage-Assisted Demand Response in Microgrids. In Proceedings of the e-Energy '17, Shatin, Hong Kong, 16–19 May 2017. [CrossRef]
143. Perica, I.; Ivan, R.; Zlatko, Z.; Lin, H.; Slavko, K. Decentralised electricity trading in the microgrid Implementation of decentralized Peer-to-Peer Concept for Electricity Trading (P2PCET). In Proceedings of the 11th Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, Dubrovnik, Hrvatska, 12–15 November 2018.
144. Sun, Y.N.; Lampe, L.; Wong, V.W.S. Smart Meter Privacy: Exploiting the Potential of Household Energy Storage Units. *IEEE Internet Things J.* **2017**, *5*, 69–78. [CrossRef]
145. Huang, X.H.; Zhang, Y.; Li, D.D.; Han, L. An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains. *Future Gener. Comput. Syst.* **2019**, *91*, 555–562. [CrossRef]
146. Tushar, W.; Chai, B.; Yuen, C.; Smith, D.B.; Wood, K.L.; Yang, Z.Y.; Harold, V.P. Three-Party Energy Management With Distributed Energy Resources in Smart Grid. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2487–2498. [CrossRef]
147. Lee, J.; Guo, J.; Choi, J.K.; Zukerman, M. Distributed Energy Trading in Microgrids A Game-Theoretic Model and Its Equilibrium Analysis. *IEEE Trans. Ind. Electron.* **2015**, *62*, 3524–3533. [CrossRef]
148. Goranović, A.; Meisel, M.; Fotiadis, L.; Wilker, S.; Treytl, A.; Sauter, T. Blockchain applications in microgrids an overview of current projects and concepts. In Proceedings of the 43rd Annual Conference of the IEEE Industrial Electronics Society—IECON 2017, Beijing, China, 29 October–1 November 2017; pp. 6153–6158.
149. Imbault, F.; Swiatek, M.; Beaufort, R.; Plana, R. The green blockchain Managing decentralized energy production and consumption. In Proceedings of the 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Milan, Italy, 6–9 June 2017. [CrossRef]
150. Jia, Y.Q. Op Ed: The Many Faces of Sharding for Blockchain Scalability. Available online: https://bitcoinmagazine.com/articles/op-ed-many-faces-sharding-blockchain-scalability/ (accessed on 20 March 2019).
151. Huobi Global. Available online: http://www.huobi.br.com/en-us/ (accessed on 12 March 2019).
152. Yeoh, P. Regulatory issues in blockchain technology. *J. Financ. Regul. Compliance* **2017**, *25*, 196–208. [CrossRef]
153. Zhang, R.; Preneel, B. Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security. Available online: https://www.esat.kuleuven.be/cosic/publications/article-3005.pdf (accessed on 22 March 2019).