A Survey of Blockchain Applications in the Energy Sector

Jiabin Bao, Debiao He, Min Luo, and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

***Abstract*—As our fossil fuel reserves are rapidly depleting, there has been an increased focus to explore the utility of renewable energy (e.g., solar energy and wind energy) in replacing fossil fuel. One resulting trend is the energy market gradually shifting toward a distributed market, where renewable energy can be traded, partly evidenced by the number of blockchain-based solutions designed for the (distributed) energy sector. The interest in blockchain is also due to blockchain's underpinning characteristics such as anonymity, decentralized, and transparency. Therefore, in this article, we perform a comprehensive review of how blockchain technology has been, and can be, deployed in energy applications, ranging from energy management to peer-to-peer trading to electric vehicle-related applications to carbon emissions trading, and others. We also study the existing architectures and solutions, and existing and emerging security and privacy challenges, as well as exploring other potential applications of blockchain in the energy sector.**

***Index Terms*—Blockchain, distributed, energy area, privacy protection.**

I. Introduction

ENERGY is a natural resource that has been driving our economy for the past few decades. Increasingly, as our society becomes more digitalized and sophisticated, so does our reliance on energy. For example, according to the "BP Statistical Review of World Energy" [1], it was estimated that global primary energy demand grew by 2.9% in 2018, which is the fastest growth, since 2010. At the same time, carbon emissions from energy use grew by 2.0%, which is reportedly the fastest expansion for many years. The demand for natural gas has also reportedly increased by 5.3%, one of its strongest growth rates for over three decades. Coal demand (1.4%) also increased for the second consecutive year, following three years of decline. Growth in renewable energy (14.5%) decreased slightly but it is still the world's fastest-growing energy source.

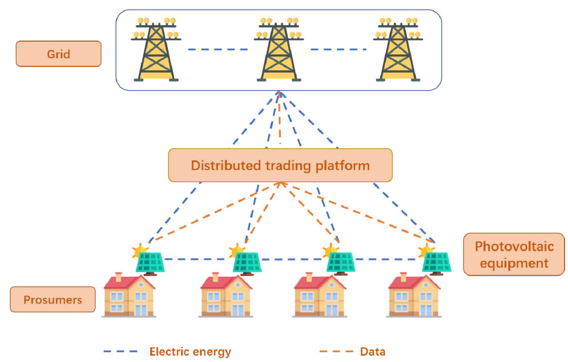

Fig. 1. Distributed trading platform.

Fossil fuels (nonrenewable energy) are limited, and it has been estimated that they will run out in the early 22nd century at the current rate of consumption [2]. This shortage and the known environmental issues associated with carbon emissions, have contributed to an increased focus in explore alternative sources of energy, most notable renewable energy sources such as solar and wind energy. For example, householder owners can install solar photovoltaic power generation system in their own houses for self-use, and the surplus electricity can be uploaded to the grid for financial rebates (i.e., consumers becoming prosumers—see also Fig. 1). One challenge associated with such a trend is the management of the large, dynamic number of prosumers. Conventional grid generally uses a centralized management system, which does not scale well or is not suitable for managing the large number of prosumers. The cost of management and maintenance will also be prohibitively high in a conventional centralized management mode, in addition to the need to deal with challenges due to different (or lack of common) standards, and lack of mutual trust among participants. This necessitates the design of an efficient, safe, fair, and sustainable smart grid system.

In addition, the increasing use of electric cars will compound the challenge of future smart grid system designs. Electric vehicles (EVs) are growing rapidly, with global sales of more than 5.1 million EVs in 2018. It is estimated that global sales of EVs

Manuscript received February 16, 2020; revised May 21, 2020; accepted May 24, 2020. This work was supported in part by the National Natural Science Foundation of China under Grants 61972294 and 61932016 and in part by the Guangxi Key Laboratory of Trusted Software under Grant kx202001. The work of Kim-Kwang Raymond Choo was supported by the Cloud Technology Endowed Professorship and National Science Foundation CREST under Grant HRD-1736209. *(Corresponding author: Debiao He.)*

Jiabin Bao is with the Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China, and also with the Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China (e-mail: jiabin1207@163.com).

Debiao He is with the Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China, and also with the Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China (e-mail: hedebiao@163.com).

Min Luo is with the Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China (e-mail: mluo@whu.edu.cn).

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: raymond.choo@fulbrightmail.org).

Digital Object Identifier 10.1109/JSYST.2020.2998791

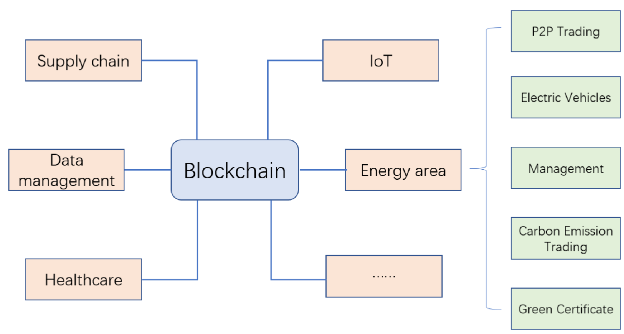

Fig. 2. Applications of blockchain.

will reach 23 million and inventories will exceed 130 million by 2030 [3]. Existing challenges include inadequate supporting infrastructure (e.g., mobile and quick charging), as it is costly to uniformly deploy basic charging facilities. Thus, this also reinforces the importance of developing decentralized mobile charging. Hence, we also need to consider management, pricing, and privacy protection issues associated with the decentralized mobile charging infrastructure.

The carbon emission trading system and green certificate trading system are market mechanisms used to promote global greenhouse gas emission reduction. Carbon trading enables trading institutions that cannot reduce their emissions to compensate by buying credits from others that meet their targets. Green certificates, on the other hand, provide green energy certificates to companies that use renewable energy sources to generate electricity, giving them subsidies to sell green energy. In the promotion of carbon emission trading system and green certificate trading system, users need to consider the safety, transparency and credit data registration of participants in the trading process.

The preceding discussions emphasize the importance of decentralization, one trait commonly associated with blockchain [4]. In recent years, the utility of blockchain has explored in many applications, such as data management [5], [6], healthcare [7], [8], supply chain [9], Internet of Things (IoT) [10], [11], software-defined networking [12], cybersecurity [13], [14], etc. (see Fig. 2).

Another popular application of blockchain is in the energy area [15], [16], partly due to its underpinning characteristics such as anonymity, decentralization, transparency, and reliability. As mentioned above, as the energy sector becomes distributed, there are many issues that need to be addressed, such as distributed storage, control, management, trading, etc. These problems cannot be solved by traditional energy systems, while the features of blockchain can provide solutions. The practical utility is also evidenced by the interest from major technology organizations, such as Siemens (investments in blockchain development), and IBM (setting up a dedicated blockchain lab to develop blockchain applications for various areas, including a carbon tracking platform in China's emissions-trading system and a project with the European power system operator, Tennet, to balance supply and demand for high-voltage grids) [17].

In this article, we provide a survey on recent applications of blockchain in the energy sector.

The rest of this article is organized as follows. First, Section II introduces the blockchain technology and the energy Internet. Section III reviews how blockchain is applied in the energy sector, such as in management, P2P trading, EVs, and carbon emissions trading. In Section IV, we summarize and discuss the applications of blockchain technology in the energy sector, and identify a number of research opportunities. Finally, we conclude this article in the last section.

II. Related Work

A. Blockchain Technologies

1) Overview of Blockchain Technologies: Blockchain is a decentralized electronic database (decentralized ledger) that maintains an ever-growing list of records made up of blocks. Each block typically contains transaction data, a timestamp, and a hash pointer to link to the previous block. A chain is formed by linking blocks with each block containing the hash value of the previous block. The use of hash values ensures that changing the contents of a block requires changing all subsequent blocks, which is expensive to do, so it has tamper-proof capabilities. The process of block addition goes like this: the node that has the right to package transactions puts the packaged transactions (block) on the existing blockchain and broadcasts it to the whole network. After the other nodes receive the block, they validate it, and if the block passes validation, all nodes will synchronize this block. Each packaged transaction is called a block, and the blocks are added to each other, extending the blockchain. The decentralized ledger is verified and maintained by all participating nodes according to a consensus mechanism, without the need for a trusted central control. Multiple nodes hold a complete copy of the entire database [18], [19].

2) Consensus Mechanism: Problems can arise when applying blockchain to specific scenarios. For example, the double spending and the Byzantine problem [20]. The double spend problem means the same amount of money is used twice in two different transactions. Traditional currency is the entity, so we do not have the problem of doubling spending when we use traditional currency. There will also be a trust center to avoid this problem in the widely used online trading methods. Since the blockchain currency is not an entity and there is no trusted third party, we need another approach to solve this problem. Blockchain solves this problem by verifying transactions with many distributed nodes. In distributed systems, the Byzantine generals problem is a problem that must be solved. In a distributed system, information is transmitted between nodes in a P2P manner. However, if some nodes are maliciously attacked in the process of information transmission, the information transmitted may be tampered with. Uncompromised nodes need to distinguish between the correct information and the tampered information, and all normal nodes need to get consistent results, so corresponding consensus algorithm needs to be designed. The core objective of the consensus algorithm is to solve the Byzantine generals problem [21], [22].

Blockchain ensures the global ledger maintained by all legal nodes are consistent by the consensus mechanism. There are some different consensus mechanisms such as proof of work, proof of stake, delegated proof of stake, etc. [23], [24].

3) Smart Contracts: The use of smart contracts is a key reason why blockchain is widely used. A smart contract is essentially an executable piece of code that executes automatically when the initial conditions are met, eliminating the need for a trusted third party to monitor the transaction, making it irreversible, secure, and decentralized.

The smart contracts contain all the information about the transaction and only perform the resulting action when the requirements are met. The biggest difference with the traditional paper contract is that the intelligent contract is produced by the computer and executed automatically. It stipulates the trigger conditions and the operations to be performed in advance. Any participant will be forced to perform relevant operations under the condition that the conditions meet, so there will be no evasion or denial.

Smart contracts can be used for trading and any exchange between two or more parties. The contract code contains the conditions required to automatically execute the contract.When the smart contract is written, it is uploaded to the blockchain network, and nodes can invoke it when needed. To write smart contracts, we must use the smart contract language, for example, solidity.

4) Characteristics of Blockchain Technologies: Blockchain technologies have the following characteristics.

a) Decentralized: Blockchain stores data based on a decentralized structure and maintains the database jointly by all participating nodes, without the need for centralized management by a central management agency. And the damage of one node will not affect the normal operation of the whole system.

b) Anonymity: The nodes in the blockchain can be anonymous when exchanging data with each other, so the privacy of each node can be protected to some extents.

c) Untrustworthy: Untrustworthy here means that the nodes in the blockchain do not need to trust each other, but only need to trust the system of blockchain and its trading mechanism. Under the consensus mechanism of blockchain, each participating node can become a supervisor, so there is no need to worry about the occurrence of fraud.

d) Reliability of data storage: Due to the decentralized storage structure of blockchain, each node can have a complete copy of the whole database, so an attacker cannot control the whole database by controlling or attacking a certain node.

e) Smart contracts: The emergence of smart contracts brings the blockchain industry into a new era. A smart contract is actually a program that can be executed by a computer. It uses computer language instead of legal language to record the terms of a contract. When conditions are met, the contract is completed automatically by the computer. Compared with traditional contract signing, smart contract can reduce the cost of contract signing, supervision, and execution.

B. Energy Internet

Due to the shortage of fossil energy and the environmental problems caused by it, people have started to develop renewable energy, such as solar energy, wind energy, etc. However, there are still many problems to be solved in the management of renewable energy. Because the acquisition and use of these energy resources are usually distributed rather than concentrated, the efficiency of management and trading is often low, and unfair trading is easy to occur. Huang *et al.* [25] put forward the concept of energy Internet. The energy Internet is a new type of power grid structure. Based on energy storage technology and the Internet, it is used to manage the generation of renewable energy and optimize the energy supply system.

At present, there are many problems in the energy system, such as the cost and security problems caused by centralized management. Moreover, as many scenarios in the energy sector are moving toward a distributed structure, the traditional centralized management model is clearly no longer applicable. The advent of blockchain technology provides solutions to these problems.

With the development of blockchain technology, the energy Internet has developed rapidly. A truly efficient energy Internet is possible. With the application of blockchain technology in the management, trading, tracking, and other links in the energy area, the management efficiency of the new distributed energy network has been greatly improved.

III. Applications of Blockchain in the Energy Sector

In this section, we review how blockchain is applied in the energy sector, such as in management, P2P trading, EVs, and carbon emissions trading. And we analyze the privacy problems in some systems or structures.

A. Decentralized Storage and Control in Power Grid

As mentioned in Section I, the energy market is gradually shifting to a distributed market. For example, the solar photovoltaic industry has been more and more widely covered. However, with the emergence of a large number of prosumers, how to manage them has become a problem we must face. For example, with the increasing of participants in the energy market, it is difficult to store the massive data of them. Storing large amounts of data in a central management organization will bring many problems. With the increasing number of participants, the data volume will be larger and larger, and the corresponding storage cost will be higher and higher. If all data are stored in one organization, it will be difficult for other participants to access the previous data and the transparency will be difficult to ensure. In addition, all data are at risk of being leaked or lost if central organizations are attacked or compromised. On the other hand, the voltage control is very important in the decentralized power grid, because it will affect the operation stability of the grid. But it seems that it's difficult for the traditional centralized management method to deal with these problems.

The work in [26] designs a hybrid blockchain system for data storage in the energy Internet. This system is characterized by the use of a mixture of public blockchain and private blockchain, combining the advantages of both, to achieve an intelligent, efficient and secure energy Internet management mechanism. It can meet the requirements of safe and efficient data storage.

TABLE I
HYBRID BLOCKCHAIN

Types	Responsibility	Advantages
Public blockchain	Verify consistence Storage data	Security
Private blockchain	Broadcasr transaction Verify consistence	Efficiency

Even the number of participants in the energy Internet is very large, it can storage and management their data well.

The main feature of the system is the adoption of a hybrid blockchain storage structure. It combines the private blockchain and the public blockchain. The private blockchain is mainly responsible for verifying the accuracy of relevant transactions, while the public blockchain is responsible for ensuring the integrity of data. The hybrid blockchain combines the efficiency of private blockchain and the security of public blockchain (see Table I).

Another application of blockchain in decentralized management is to help control the decentralized grid. When the residential low-voltage grid (for example, the solar photovoltaic power generation facility) has excess power, it needs to upload the excess power to the main grid. If it is not controlled well, it will lead to unstable voltage on the grid, such as a sharp increase of voltage. An effective way to solve this problem is to control the output power reasonably. In [27], a proportional and equitable control scheme based on blockchain and smart contract is proposed. If some prosumers are installed on the same distribution feeder, they will sign a smart contract to decide which participants will act as voltage regulators during the control period. The decision is based on their available credit status and economic strategies.

Compared with this control scheme, the traditional centralized management architectures usually force all participants to participate in voltage control and always limit their output power. It is obviously that it is not fairness or efficient. The blockchain-based solution can not only achieve the control goal of the centralized architecture, but also avoid the problem—the cost and complexity of control increase with the increase of participants. However, the authors point out that because the scheme is based on the private blockchain, there are two potential limitations—mining cost and communication cost.

Mannaro *et al.* [28] proposed a Crypto-trading project. This project mainly considers using blockchain and smart contract to construct smart grid. The smart grid can make electric adjust the relationship between supply and demand so as to promote the creation of a distributed energy market. In the distributed energy market, end-users (prosumers) can manage their own energy supply and the sale of surplus energy. In this project, blockchain has two main functions. One is to act as a distributed ledger to record all the data in the process of energy trading; the other is as a control system to drive intelligent meters.

Based on the sovereign blockchain, Gao *et al.* [29] implement a smart grid management system. The system is mainly used to protect the data of consumers, which can ensure the transparency and integrity of the data and prevent malicious tampering. The system is designed to protect consumer data. In this system, blockchain is used to record consumer data, which can ensure that users' electricity data is integrity and confidentiality and can prevent the electricity data been tampered with by external attackers without permission. At the same time, consumers have the complete authority to control their own data. Smart meters provide users with a detailed record of how much electricity they use and which appliances consume the most. In this system, smart contracts are used to automatically detect operations performed in the grid system and identify potential malicious use of power or malicious use or tampering with power data.

Liang *et al.* [30] proposed a distributed data protection framework based on blockchain to enhance the ability of modern power system to resist external network attacks. The framework can improve the security of data in power system and prevent data from being maliciously tampered with or used. This framework makes use of the distributed security features of blockchain technology, and uses the smart electricity meter as the node in the blockchain to record and store the power data with the distributed ledger, so as to ensure the consistency and integrity of the data.

The blockchain technology and smart contract are also used for monitoring the power consumption of users. The imbalance of power supply and demand may threaten the security of power supply, lead to the overload of power components, and eventually lead to power failure or service interruption. One way to solve these problems is demand side management. The power demand side management based on blockchain can be used in the power supply and demand regulation of smart grid. The method is to respond to peak load by encouraging users to reasonably distribute their power demand to match power demand with supply. Pop *et al.* [31] designed a smart meter to detect the real power consumption of users, and then a smart contract to evaluate the power consumption of users according to the agreed rules, and to give incentives or punishments according to whether users abide by the agreement. Blockchain records the data as a distributed ledger. But the electricity consumption records of consumers in blockchain is public, so one can discover other consumers' daily activity patterns. This is a privacy problem.

To manage the decentralized energy system better, people usually use blockchain to store the huge amount of data, protect consumers' data or make decisions by consensus mechanism and smart contract (see Table II). The blockchain technologies make the management of decentralized energy system simpler and fairer, and reduce the management cost. Most of all, even if the number of participants continues to grow, the decentralized management mechanism can cope well. But the privacy problems we discussed above also should be pay more attention (see Table III).

B. P2P Energy Trading in Smart Grid

Traditional energy transactions are usually managed through a centralized organization. The energy market will become more and more complex as large numbers of prosumers gain access. And the trading between prosumers and consumers will become more complex, too. Take electricity trading for example.

TABLE II
BLOCKCHAIN TECHNOLOGY APPLIED IN DECENTRALIZED STORAGE AND CONTROL

Ref.	Main technologies used	Objective	Contributions
[26]	hybrid blockchain	data storage	Design a data storage system for energy Internet based on hybrid blockchain.
[27]	blockchain smart contract	the decentralized grid control	Achieve the control goal of the centralized architecture and avoid the problem - the cost and complexity of control increase with the increase of participants.
[28]	blockchain	the smart grid control	Blockchain is used to record all the data in the process of energy trading and to drive intelligent meters as a control system.
[29]	blockchain smart meters smart contracts	consumer data protection	Implement a sovereign blockchain-based system on a smart grid system, which can protect consumer data.
[30]	blockchain smart electricity meters	data protection	Improve the security of data in power system and prevent data from being maliciously tampered with and used.
[31]	blockchain smart meters smart contracts	the demand side management of grid	Use blockchain and smart contract to keep balance of power supply and demand.

TABLE III
PRIVACY PROBLEMS IN DECENTRALIZED STORAGE AND CONTROL SYSTEMS

Ref.	Characters of the system	Privacy problems
[26]	Data are stored in public blockchain.	Data in public blockchain can be accessed by anyone not suitable for private data.
[27]	Apply blockchain and smart contract to voltage control.	Not mentioned.
[28]	Blockchain and smart contract are used to adjust the relationship between supply and demand in grud.	All transaction information is stored on the blockchain, which could reveal the electricity habits of some users.
[29]	Blockchain is used to protect the data of consumers, which can ensure the transparency and integrity of the data.	External attackers can't get access to the data without permission. To some extent, the privacy of users is protected.
[30]	Make use of the features of blockchain technology and digital signature to improve the security of data in power system.	Data integrity can be guaranteed, but confidentiality cannot.
[31]	Blockchain and smart contract are used to keep balance of power supply and demand.	The electricity consumption records of consumers in blockchain is public, so one can discover other consumers' daily activity patterns.

Nowadays, electricity is usually a monopoly industry in most countries. All consumers have to buy electricity through the electric power company. And the price of electricity is uniform, consumers cannot independently choose the most economical energy purchasing plan. Blockchain technologies provide a new opportunity for the decentralized market. Blockchain technologies can help build a transparent and credible market for electricity trading. Consumers and prosumers can participate in electricity trading in a distribute manner.

The emergence of a new decentralized energy trading system based on blockchain will change the role of traditional power companies in the energy market, there will be no need for them to invest high cost to deploy infrastructure management facilities for the large number of prosumers. Consumers and prosumers will have more choices of energy purchasing schemes in a truly low-cost energy trading environment. The application of blockchain technologies will solve the problems which will appears in the trading process in the distribute energy market and bring some other advantages. For example, it can improve the transparency of the trading process, enhance the smooth operation of the power grid in the process of point-to-point energy trading, optimize demand response, bill and other transaction process, and provide privacy and security protection [32]–[35].

Some P2P energy trading markets based on blockchain mainly use blockchain to realized market auction mechanism. The work in [36] proposed a decentralized market platform for consumers and prosumers in local energy markets based on the private blockchain. A central intermediary is never need to manage local energy transactions. This article focuses on the local transaction system for residential photovoltaic power generation and implements a 100-user proof-of-concept model on Ethereum. The system uses the market auction mechanism to regulate supply and demand. In its proposed market platform, the market auction mechanism is realized through the deployment of smart contracts in the blockchain, and the payment is also completed in the blockchain. The demand and production capacity of each agent (user) are automatically measured and predicted by smart meters and broadcast to each agent. Based on this information, excess demand or excess supply is calculated and sent to the corresponding blockchain account of the agent, but detailed private data is still kept locally to protect users' privacy to a certain extent. When designed this decentralized market platform, the authors had paid some attention to the privacy issues of participates. As they mentioned in the article, the detailed private data are kept locally and would not be broadcast to the blockchain. Only the demand and production capacity of each participate will be measured and broadcast to other users. But in some cases this data may also lead to disclosure of participants' privacy. For example, the malicious people may infer a user's electricity usage habits based on these data.

Hahn *et al.* [37] proposed a decentralized energy auction system based on blockchain. Based on this distributed auction system, buyers and sellers can complete online auctions and realize reliable, safe and transparent power exchange. There are two main categories of identity in the system, seller and bidder, as well as two technologies, smart meters, and smart contracts. When a seller has excess available power and wants to sell it, he can launch a new auction and publish his available power in the blockchain. Bidders in need of electricity can bid after receiving the new auction. The auction and payment processes are automated by smart contracts. Smart meters detect and report the flow of electricity during the transaction, verifying that the transaction is completed. All data from vendors, bidder, and smart meters will be stored on the blockchain. Privacy problems are not mentioned in this article. But if the auction data from sellers, bidders and smart meters stored on the blockchain is not encrypted, some private information may be compromised. And if the final price of each auction can be retrieved in the blockchain, the subsequent auctions may be affected.

The work in [38] mainly deals with security problems in distributed energy transactions in smart grid by using some privacy protection technologies. Instead of completing a transaction through an auction mechanism, this article implements a private distributed energy trading system based on tokens. Through this system, consumers can negotiate electricity prices anonymously without revealing their identities, and their privacy information is well protected during the transaction. The trading system uses blockchain technology, multiple signatures, and anonymous encrypted information flow to provide privacy protection. There is no trusted third party in this trading system so that the price can be negotiated by participates themselves. But they are anonymous at all times, and the data are encrypted to protect their privacy. This article analyzes a series of security and privacy requirements to be achieved by the blockchain-based trading system in detail, and gives corresponding countermeasures in the system proposed in this article. This article can be used for reference to the design of blockchain-based trading system.

Some other blockchain-based trading platforms adjust energy prices according to energy storage, trading and current energy prices, rather than through market auction mechanism.

Park *et al.* [39] proposed a P2P energy trading platform based on blockchain, which realized efficient electricity trading between users. This article proposed using blockchain to store and verify energy labels. Energy labels will identity where energy is generated and consumed. The trading process includes the following steps. First, IoT devices will automatically detect whether consumers or prosumers have the need to buy or sell energy, and generate a buy/sell label. Then, the label will be sent to all participants in the trading platform. When a participant wishes to trade with the consumer/prosumer who issued the label, the label is confirmed and the two parties complete the trading process. Finally, the transaction record of the two parties is generated and added to a block, which will be broadcast to all participants.

The trading platform is able to compare and adjust the current market prices of electric energy according to the trading situation. And it will provide an algorithm to help consumers/prosumers determine which energy is the most cost-effective and high-quality energy choice, enabling consumers/prosumers to trade more effectively than before. The ultimate goal of the authors is to propose an electronic energy trading platform that allows high-quality and low-cost energy trading between consumers and prosumers at anytime and anywhere.

In [40], a distributed trading platform based on blockchain technology is constructed and distributed pricing and P2P trading are realized. The work first proposes a decentralized power market trading framework based on blockchain and then develops a pricing mechanism to promote the balance of supply and demand between consumers. At the same time, this article also compares the traditional power trading methods with blockchain-based power trading methods. By contrast, the significant advantages of blockchain-based power trading are the transparency and security of trading information. In the power trading mode based on blockchain, all transaction information is recorded and maintained by all participating nodes, and all transaction records can be viewed by each node, so the transaction is transparent and traceable. In addition, the data are stored in the blockchain and blockchain is synchronized by all the participating nodes, so it is more secure. In the traditional way of electricity trading, trading information is stored in the central management agency, and only the central management agency can view the users' transaction information. However, once the central management agency is subjected to malicious attacks, it may cause the disclosure of users' privacy information and lead to its malicious use, resulting in serious consequences.

Cheng *et al.* [40] mainly focus on the security and transparency of transaction information. All nodes record and can view all transaction information. This can ensure the transparency of transactions and avoid the single point of failure, but may expose the users' private information contained in the transaction.

With the development of battery energy storage technology, the cost of solar photovoltaic power generation will be lower and lower, so more and more people are willing to install photovoltaic power generation system and become a prosumer. Solar power will gradually occupy a larger market due to its advantages in environmental protection and price. More local electricity markets will emerge for their own use or for sale. Some of them may access to the main grid. The rapid development of distributed generations brings new challenges for the energy trading market. Therefore, it is necessary to do some research on the relevant management scheme and market mechanism and propose some new trading schemes for the distributed energy market based on the advantages of blockchain. But in the blockchain-based decentralized energy trading systems that we discussed above (see Table IV), many of them have not paid enough attention to the privacy protection of participants. Most designers mainly focus on the transparency of transactions,

TABLE IV
BLOCKCHAIN TECHNOLOGY APPLIED IN P2P TRADING

Ref.	Main technologies used	Pricing mechanism	Contributions
[36]	private blockchain smart meters	market auction mechanism	Propose a decentralized market platform based on the private blockchain, uses the market auction mechanism to regulate supply and demand.
[37]	blockchain smart meters smart contract	market auction mechanism	Realize reliable, safe and transparent energy exchange, auctions and payments are automated through smart contracts.
[38]	blockchain multiple signatures anonymous encrypted information flow	negotiate energy prices anonymously	Privacy protection technology is used to solve security problems in distributed energy transactions in smart grid.
[39]	blockchain IoT	adjust prices of electric energy according to the trading situation	Propose an electronic energy trading platform that allows high-quality and low-cost energy trading.
[40]	blockchain	distributed pricing mechanism	Construct distributed trading platform, realize distributed pricing and point to point trading.

TABLE V
PRIVACY PROBLEMS IN P2P TRADING SYSTEM

Ref.	Characters of the trading system	Privacy problems
[36]	The detailed private data is kept locally, only the demand and production capacity of each participate will be measured and broadcast to other users.	Malicious people may infer a user's electricity usage habits based on these data.
[37]	The auction data from sellers, bidders and smart meters stored on the blockchain.	If the the final price of each auction can be retrieved in the blockchain, the subsequent auctions may be affected.
[38]	Use multiple signatures and anonymous encrypted information flow to provide privacy protection.	Achieved many security and privacy requirements.
[39]	Not mentioned.	/
[40]	All nodes record and can view all transaction information.	Focus on the security and transparency of transaction information, but may expose the users' private information contained in the transaction.

which is sometimes opposite to the privacy protection (see Table V).

C. *Electric Vehicles*

The invention of cars makes people's daily travel more convenient, but also brings a series of problems. Cars not only accelerate the consumption of fossil energy, but also emit a large number of greenhouse gas, which will cause environmental problems. European Parliament committed to cut its emissions of greenhouse gas to 40% below 1990 levels by 2030 and 80%–95% by 2050 [41], [42]. The transport sector is typically the fastest consumer of fossil energy and the biggest emitter of greenhouse gases, so many European countries are pushing hard to let EVs replace internal-combustion vehicles. The large-scale use of EVs has not only greatly reduced greenhouse gas emissions, but also reduced the fuel cost of drivers. And it also promotes the development of renewable energy technology. According to [3], global sales of EVs will reach 23 million and inventories will exceed 130 million by 2030.

The surge in the number of EVs has also brought a series of problems, such as the construction of charging infrastructure, the choice of charging mode, and the safety issues in the charging transaction process. If the centralized management is adopted, the construction of charging infrastructure will cost a lot of money. It is also unrealistic to have such a large number of EVs managed by a single department. Therefore, people are looking for distributed EV charging management methods, most of which are based on the blockchain technology. However, the adopting of distributed charging method also requires consideration of pricing methods and the privacy protection in the process of power transaction. The leakage of some private information such as the driving path of EVs and their preference for charging station will bring a lot of troubles to the owners.

Electric cars can be replenished in a variety of ways, such as direct battery exchanges with charging stations, without the need to stop for a long time for recharging. However, using this method may cause the fairness problem in the transaction. Different battery brands and wear levels will affect the fairness of the transaction. With a traditional centralized management system, this information will be stored on a central server, making it difficult to ensure fair trading. Therefore, Hua *et al.* [43] proposed a battery exchange mechanism based on decentralized blockchain system. In this mechanism, the battery information are stored in the blockchain, and smart contracts will automatically complete the payment process, including price difference compensation. The fairness problems in the transaction process can be solve in this way.

Another way for EVs to recharge is using infrastructure such as charging piles. Besides pricing method, charging station selection and transaction method, information security of EVs should also be considered in the design of such schemes. In the process of using charging facilities, some privacy information, such as vehicle information, location information, and habitual travel route may be acquired and used for improper purposes [44], which brings troubles to owners.

Kim *et al.* [45] proposes a lightweight mobile charging system based on blockchain technology. In particular, the system uses (simple payment verification) SPV technology. The node only needs to download the blockchain header to verify whether the transaction exists, so as to reduce the storage space and the burden of the terminal. In addition, a technique to reduce block data size is proposed to solve the problem of blockchain data size accumulation. In this system architecture, mobile chargers are organized as groups, with a parent node for each group. In each group, only the parent node keeps a complete blockchain, and the other nodes are SPV nodes, thus reducing the burden on these nodes.

In [46], a reliable, automatic and privacy-protected EV charging platform based on blockchain technology is proposed. EVs release the request for charging demand and then charging stations issue their own quotations. Electric cars can choose the appropriate charging stations according to the pricing and the distance of charging stations. Trading on blockchain improves the reliability and transparency of the trading process. Meanwhile, the geographical location information of EVs will not be leaked, thus protecting their privacy.

The transaction process includes the following four phases: exploration phase, bidding phase, evaluation phase, and charging phase. Through these four phases, EVs can complete the selection of the most suitable charging station and the charging process, and their privacy information will not be leaked. First, because each user is anonymous in the blockchain, no identity information is disclosed. Second, the geographical location in the demand message released by the user is a regional range. An appropriate range size can not only not disclose the location information, but also facilitate the arrival of EVs to the target area. Moreover, most of the transaction process does not need to be performed in the blockchain, and other users cannot know which charging station the user has chosen and the transaction has been completed at what price.

Huang *et al.* [47] also focus on the security of transactions between charging piles and EVs during charging. They propose a security model to improve the security of transactions between EVs and charging piles. This model mainly makes use of lightning network and intelligent contract. The model mainly includes four stages: registration, scheduling, authentication and billing, and can be integrated with the existing scheduling mechanism to improve the security of it.

Different from other work, paper [48] takes many different EV charging scenarios into account, including G2V, V2V, MCV2V, etc. G2V refers to that EVs charge from the grid, V2V refers to that EVs charge from other EVs with spare power, and the MCV2V is the product of a new type of EVs called gridable electric vehicles. This type of EVs has bidirectional chargers, which is similar to a car's mobile charging station. Based on the consortium blockchain, the authors propose a double-objective optimization model charging scheduling algorithm. This scheduling algorithm considers the charging demand of EVs, the power supply of the grid or mobile charging vehicles, as well as location, waiting time, travel speed, and other factors. Using this framework can ensure the security of power transactions, and due to the consensus mechanism used by the consortium blockchain—the consensus algorithm is performed by some preselected nodes instead of all nodes, it saves a lot of time.

In the field of EVs, blockchain technology is mainly used for the selection of charging piles, charging pricing, etc. (see Table VI) The use of blockchain technology and smart contracts can help EVs to choose the most suitable charging place after comprehensive consideration of the distance, cost, and other factors. At the same time, in bidding, choosing charging pile, and charging process, many applications also consider the protection of user data privacy, to prevent the malicious acquisition of users' private information and preferences. But there are also many people ignore this problem (see Table VII).

D. *Carbon Emission Trading and Green Certificate*

In 1997, more than 100 countries signed the Kyoto Protocol due to global warming. The Kyoto Protocol stipulated the duty of developed countries to reduce carbon emissions and put forward three flexible emission reduction mechanisms. Carbon emission trading is one of them. In 2010, carbon emissions accounted for 75% of global greenhouse gas emissions, and from 2015 to 2040, this proportion will continue to grow at an annual rate of 0.6%, most of which comes from the burning of fossil fuels [49], [50]. Global energy-related carbon emissions are expected to increase by 16% from 2015 to 2040 [50].

Carbon emission trading is a market mechanism to reduce global carbon emissions and promote global greenhouse gas emission reduction. Reducing the impact of climate change is the core objective of carbon emission trading. Government departments set carbon emission quotas for companies. Due to various factors, different companies have different ability to control carbon emissions. Some companies cannot keep their carbon emissions within limits, while others may have plenty to spare. For those companies that do not meet the rated emission reduction targets, they can purchase carbon emission permits from other companies that can exceed the targets under the carbon emission trading mechanism.

At present, there are many problems in the carbon emission trading market, such as the allocation of carbon emission allowances, the detection of real emissions, the setting of trading rules and prices, and the regulation. Specifically, due to the large number of companies, it would be a huge amount of work for the government to certify the carbon emission quota of each power producer. In addition, government departments need to track the emission quotas handed over by all companies to ensure their authenticity. The frequent trading of carbon emission permits makes the tracing process extremely complicated. Therefore, records of carbon emission quotas should be traceable and cannot be tampered with. Blockchain technology can provide some solutions.

Khaqqi *et al.* [51] proposes an emission trading system based on blockchain technology, which takes credit trading system as trading mechanism. In this trading framework, smart devices

TABLE VI
BLOCKCHAIN TECHNOLOGY APPLIED IN EVS

Ref.	Charging scenarios	Main technologies used	Contributions
[43]	direct battery exchanges	blockchain smart contract	Propose a battery exchange mechanism which can solve the fairness problem.
[45]	charging piles	blockchain SPV(simple payment verification)	Propose a lightweight mobile charging system and solve the problem of blockchain data size accumulation.
[46]	charging piles	blockchain	Propose a privacy-protected EV charging platform.
[47]	charging piles	lightning network smart contract	Propose a security model to enhance the security of trading between EVs and charging piles.
[48]	G2V(charging piles) V2V MCV2V	consortium blockchain	Propose a double-objective optimization model charging scheduling algorithm.

TABLE VII
PRIVACY PROBLEMS IN EV MANAGE SYSTEMS

Ref.	Characters of the system	Privacy problems
[43]	The battery's life cycle information and all of its operational history will be permanently stored in the blockchain network, increasing information transparency and enhancing trust.	The detailed usage information of the battery can lead to privacy leakage .
[45]	Only charging piles participate in blockchain.	No private information of EVs is stored in blockchain.
[46]	All participants are anonymous, the location information provided by the car is not accurate, and the final choice is known only to the user.	Private information of users can be protected well.
[47]	The operator needs to know the car's location and other information to give the recommended charging location.	Sensitive information such as the location of the car is made available to others.
[48]	Agents need know the location, speed and other information of the car.	Same as above.

are used to monitor emission transactions, while blockchain technology is used to report, verify, and record emission transactions, ensuring their transparency and unforgeability. Based on the bitcoin system, the work in [52] proposed an architecture model of a distributed carbon emission trading system. It mainly aims to solve the problem of anonymous trading among carbon emission trading subjects. This architecture model pays attention to the issues of privacy protection and transaction security in the process of emission credits trading. The role of blockchain in this model is to register and record emission credits.

Green certificate is an electronic certificate issued by the government agency to those companies who use renewable energy to generate electricity. These companies can sell their green certificates. In order to solve the security problem of energy asset trading in industrial systems, Imbault *et al.* [53] designed a system based on blockchain to manage environmental certificates and emission permits. The application of blockchain technology in industrial operating system makes the transaction of energy assets have good traceability. Castellanos *et al.* [54] designed and simulated a GoOs trading platform based on ethereum and smart contracts. By trading GoOs, prosumers and consumers can subsidize renewable energy producers and encourage the development of renewable energy. GoOs is also a kind of green certificate.

IV. DISCUSSION

In the energy area, both the management and trading of energy are gradually changing from centralized mode to distributed mode. In the decentralized energy system, many problems will be encountered, such as the storage of consumer data, the guarantee of data security, and the fairness and transparency in the transaction process. In the previous sections, we discussed the application of blockchain technology in distributed management, P2P trading, EVs, carbon emission trading, and green certificate trading.

In the distributed management, blockchain technology is mainly used to manage the storage of users' data, improve the security and privacy of the data. It also used to control the decentralized grid. In P2P trading, blockchain help to price, regulate supply and demand, and ensure transparency, security and consumers' privacy in the transaction process. When blockchain is applied to EVs area, it is mainly used for the selection of charging piles and charging pricing. The price is sometimes set through bidding, sometimes controlled by smart contracts that automatically adjust to market conditions. In carbon emission trading and green certificate trading, blockchain technology is mainly used for the traceability and privacy protection in the trading process.

Blockchain has such a wide application in the energy area, precisely because it meets the requirements of distributed energy system with the following characteristics.

1) Decentralized: This feature of blockchain conforms to the requirements of distributed energy system in user decentralized management and data distributed storage, which can reduce the management cost and improve the security of user data storage.

2) Anonymity: This feature can help protect consumers' privacy when they are participated in the distributed energy trading.
3) Transparency: Data on the blockchain are synchronized to all nodes, so each node can query all transaction records, ensuring the transparency of transactions. This will reduce fraud in distributed energy transactions and improve the transparency of energy trading.
4) Democracy: The use of consensus algorithms makes transaction decisions in blockchain more democratic. Under the consensus mechanism of blockchain, each participating node can become a supervisor, so there is no need to worry about the occurrence of fraud. This approach also makes energy management more democratic and efficient.
5) Security: Due to the decentralized storage structure of blockchain, each node can have a complete copy of the whole database, it is difficult to have a single point of failure. So, an attacker cannot control the whole database by controlling or attacking a certain node. Thus, the network security is enhanced. And when it applied to decentralized energy systems, the security of consumers' data will also be enhanced.

Due to the combination of many characteristics of blockchain with the demand of distributed energy market, its application in the energy field will become more and more extensive, and relevant technologies will become more and more mature. However, there are also some problems or challenges we have to solve when we apply it to the energy area.

First of all, we must pay enough attention to the privacy protection issue when we design a management or trading platform based on blockchain. In most platforms, blockchain is used to record important data to ensure the transparency and tamper-proof, but the protection of users' privacy is often ignored. In some grid management plat, users' electricity consumption records are recorded in the blockchain, which may lead to the leakage of their daily electricity consumption habits. In the distributed point-to-point trading platform, users' detailed demands and quotes are broadcast to the blockchain, which will also lead to their privacy disclosure. In the EV charging management platform, the specific location and driving route of the EV and other sensitive information may also be used for malicious purposes. These problems are caused by the designer's indifference to the user's sensitive data protection. We suggest that when solving problems with blockchain, some privacy protection technologies in cryptography and other fields can be combined to solve users' privacy protection problems. For example, there are many signature and encryption schemes designed to improve privacy protection, as well as some identity authentication and key agreement schemes designed for the IoT, that can be used in blockchain-based energy systems [55]–[59].

Additionally, we should choose the appropriate consensus mechanism and improve it to avoid excessive cost in the implement of the consensus mechanism. And we must concern how to design the appropriate smart contracts in the trading process to improve the market mechanism of distributed market so that it can complete the functions of traditional market.

What's more, if there are too many users in a blockchain-based system, it may produce a relatively large amount of data. The sheer volume of data will certainly raise the bar for users. How to improve the performance of blockchain in data storage or the application of low storage framework has also become the focus of this article.

Finally, in the process of applying blockchain technology to the energy area, we will encounter some other problems such as government intervention and legal supervision, which also need our attention.

In addition to exploring some solutions to the above problems, there are other scenarios, where blockchain applications in the energy sector are also worth exploring. In addition to the energy management and transaction involved in this article, in terms of energy supply, the future energy supply will tend to be a combination of distributed and centralized. Real-time information update based on the blockchain technology will help realize the information sharing between the two modes and reduce the waste of the energy supply system. In the field of energy transportation, there are generally many roles involved in the process of energy transportation, and there are games and competitions among them. The blockchain technology can realize the trust and transaction transparency among multiple roles, promote healthy competition and improve transportation efficiency.

V. Conclusion

We surveyed the existing and potential applications of blockchain in the energy sector, such as those in the distributed renewable energy market (e.g., distributed energy market management, P2P energy trading, EV charging scheme, carbon emission trading, and green certificate management). Through the reviews of these existing applications, we identified how the characters of blockchain (e.g., decentralized, anonymity, transparency, and tamper-proof) can be utilized in the design of the next generation of distributed energy solutions. Meanwhile, we discussed the privacy protection of users in some of these schemes. In addition, we also identified a number of existing and emerging challenges, which will hopefully inform future research efforts.

References

[1] BP, "Bp statistical review of world energy," 2019. [Online]. Available: https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2019-full-report.pdf

[2] M. F. Hossain, "Solar energy integration into advanced building design for meeting energy demand and environment problem," *Int. J. Energy Res.*, vol. 40, no. 9, pp. 1293–1300, 2016.

[3] "Global EV outlook 2019 - International Energy Agency," 2019. [Online]. Available: https://www.iea.org/publications/reports/globalevoutlook2019/

[4] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE EUROCON 17th Int. Conf. Smart Technol.*, 2017, pp. 763–768.

[6] W. Dai, C. Dai, K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: A secure blockchain-based data trading ecosystem," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 725–737, Jul. 2019.

[7] T. McGhin, K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, 2019.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Proc. IEEE 2nd Int. Conf. Open Big Data*, 2016, pp. 25–30.

[9] F. Tian, "An agri-food supply chain traceability system for china based on RFID & blockchain technology," in *Proc. IEEE 13th Int. Conf. Service Syst. Service Manage.*, 2016, pp. 1–6.

[10] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.

[11] T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 17 6935–17 6951, 2019.

[12] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. R. Choo, "P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking," *Comput. Secur.*, vol. 88, p. 101629, 2020.

[13] A. Singh, R. M. Parizi, Q. Zhang, K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Comput. Secur.*, vol. 88, p. 101654, 2020.

[14] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *J. Netw. Comput. Appl.*, vol. 149, p. 102471, 2020.

[15] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K. R. Choo, "*BEST*: Blockchain-based secure energy trading in sdn-enabled intelligent transportation system," *Comput. Secur.*, vol. 85, pp. 288–299, 2019.

[16] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient sdn controller architecture for IoT networks with blockchain-based security," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2020.2966970.

[17] D. Ellis, "Promising blockchain applications for energy: Separating the signal from the noise," 2019. [Onine]. Available: https://www.energycentral.com/c/ec/promising-blockchain-applications-energy-separating-signal-noise

[18] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K. R. Choo, "Best: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Comput. Secur.*, vol. 85, no. AUG., pp. 288–299, 2019.

[19] X. Li, Y. Wang, P. Vijayakumar, D. He, and J. Ma, "Blockchain based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11309–11322, Nov. 2019.

[20] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[21] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, 2019.

[22] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "Dcap: A secure and efficient decentralized conditional anonymous payment system based on blockchain," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2440–2452, 2020.

[23] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 2017, no. 4, 2017.

[24] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, 2017, pp. 2567–2572.

[25] A. Q. Huang, M. L. Crow, G. T. Heydt, J. P. Zheng, and S. J. Dale, "The future renewable electric energy delivery and management (FREEDM) system: The energy internet," *Proc. IEEE*, vol. 99, no. 1, pp. 133–148, Jan. 2011.

[26] L. Wu, K. Meng, S. Xu, S. Li, M. Ding, and Y. Suo, "Democratic centralism: A hybrid blockchain architecture and its applications in energy internet," in *Proc. IEEE Int. Conf. Energy Internet*, 2017, pp. 176–181.

[27] P. Danzi, M. Angjelichinoski, Č. Stefanović, and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2017, pp. 45–51.

[28] K. Mannaro, A. Pinna, and M. Marchesi, "Crypto-trading: Blockchain-oriented energy market," in *Proc. IEEE AEIT Int. Annu. Conf.*, 2017, pp. 1–5.

[29] J. Gao *et al.*, "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[30] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.

[31] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, 2018, Art. no. 162.

[32] P. R. J. W. C. Burger and A. Kuhlmann, *Blockchain in the Energy Transition. A Survey Among Decision-Makers in the German Energy Industry*. Berlin, Germany: Deutsche Energie-Agentur GmbH, 2016.

[33] K. Ioannis *et al.*, "Blockchain in energy communities, A proof of concept," JRC Tech. Rep. JRC110298, Office Eur. Union, Eur. Commiss. Joint Res. Center, 2017, doi: 10.2760/121912.

[34] G. Dütsch and N. Steinecke, "Use cases for blockchain technology in energy and commodity trading, Snapshot of current developments of blockchain in the energy and commodity sector," PricewaterhouseCoopers GmbH, Berlin, Germany, 2017. [Online]. Available: https://www.pwc.com/gx/en/industries/assets/blockchain-technology-in-energy.pdf

[35] G. Kyriakarakos and G. Papadakis, "Microgrids for productive uses of energy in the developing world and blockchain: A promising future," *Appl. Sci.*, vol. 8, no. 4, p. 580, 2018.

[36] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, no. 1-2, pp. 207–214, 2018.

[37] A. Hahn, R. Singh, C.-C. Liu, and S. Chen, "Smart contract-based campus demonstration of decentralized transactive energy auctions," in *Proc. IEEE Power Energy Soc. Innovative Smart Grid Technol. Conf.*, 2017, pp. 1–5.

[38] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.

[39] L. Park, S. Lee, and H. Chang, "A sustainable home energy prosumer-chain methodology with energy tags over the blockchain," *Sustainability*, vol. 10, no. 3, 2018, Art. no. 658.

[40] S. Cheng, B. Zeng, and Y. Huang, "Research on application model of blockchain technology in distributed electricity market," in *Proc. IOP Conf. Series, Earth Environ. Sci.*, 2017, vol. 93, Art. no. 012065.

[41] "European commission. climate action policies. 2030 framework for climate and energy policies," 2014. [Online]. Available: https://ec.europa.eu/clima/policies/strategies/2030/

[42] "European commission. climate action policies. roadmap for moving to a low-carbon economy in 2050," 2019. [Online]. Available: https://ec.europa.eu/clima/policies/strategies/2050/

[43] S. Hua, E. Zhou, B. Pi, J. Sun, Y. Nomura, and H. Kurihara, "Apply blockchain technology to electric vehicle battery refueling," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018, pp. 4494–4502.

[44] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Secur. Privacy*, 2011, pp. 247–262.

[45] N. H. Kim, S. M. Kang, and C. S. Hong, "Mobile charger billing system using lightweight blockchain," in *Proc. IEEE 19th Asia-Pacific Netw. Oper. Manage. Symp.*, 2017, pp. 374–377.

[46] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Comput. Sci.-Res. Develop.*, vol. 33, no. 1–2, pp. 71–79, 2018.

[47] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[48] X. Huang, Y. Zhang, D. Li, and L. Han, "An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains," *Future Gener. Comput. Syst.*, vol. 91, pp. 555–562, 2019.

[49] "Global greenhouse gas emissions data," 2014. [Online]. Available: https://www.epa.gov/ghgemissions/global-greenhouse-gas-emissions-data.

[50] "International energy outlook 2017," *US Energy Information Administration*, 2017.

[51] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, and M. Kraft, "Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application," *Appl. Energy*, vol. 209, pp. 8–19, 2018.

[52] E. Al Kawasmi, E. Arnautovic, and D. Svetinovic, "Bitcoin-based decentralized carbon emissions trading infrastructure model," *Syst. Eng.*, vol. 18, no. 2, pp. 115–130, 2015.

[53] F. Imbault, M. Swiatek, R. De Beaufort, and R. Plana, "The green blockchain: Managing decentralized energy production and consumption," in *Proc. IEEE Int. Conf. Environ. Elect. Eng. IEEE Ind. Commercial Power Syst. Eur. (EEEIC/I&CPS Eur.)*, 2017, pp. 1–5.

[54] J. A. F. Castellanos, D. Coll-Mayor, and J. A. Notholt, "Cryptocurrency as guarantees of origin: Simulating a green certificate market with the ethereum blockchain," in *Proc. IEEE Int. Conf. Smart Energy Grid Eng.*, 2017, pp. 367–372.

[55] Q. Feng, D. He, Z. Liu, D. Wang, and K.-K. R. Choo, "Multi-party signing protocol for the identity-based signature scheme in IEEE P1363 standard," *IET Inf. Secur.*, vol. 1, no. 99, pp. 1–10, 2020.

[56] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Netw.*, vol. 27, pp. 159–194, 2015.

[57] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Gener. Comput. Syst.*, vol. 63, pp. 56–75, 2016.

[58] S. Kumari, X. Li, F. Wu, A. K. Das, K.-K. R. Choo, and J. Shen, "Design of a provably secure biometrics-based multi-cloud-server authentication scheme," *Future Gener. Comput. Syst.*, vol. 68, pp. 320–330, 2017.

[59] S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Farash, and M. K. Khan, "An improved smart card based authentication scheme for session initiation protocol," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 92–105, 2017.

Jiabin Bao received the bachelor's degree in information security from Xidian University, Xi'an, China, in 2019. He is currently working toward the master's degree with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China.

His research interests include blockchain, cryptography, and information security.

Debiao He received the Ph.D. degree in applied mathematics from the School of Mathematics and Statistics, Wuhan University, Wuhan, China, in 2009.

He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols. He has authored or coauthored more than 100 research papers in refereed international journals and conferences, such as IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, and *Usenix Security Symposium*.

Dr. He is the recipient of the 2018 IEEE Sysems Journal Best Paper Award and the 2019 IET Information Security Best Paper Award. His work has been cited more than 7000 times at Google Scholar. He is on the editorial board of several international journals, such as *Journal of Information Security and Applications*, *Frontiers of Computer Science*, and *Human-centric Computing & Information Sciences*.

Min Luo received the Ph.D. degree in computer applications technology from Wuhan University, Wuhan, China in 2003.

He is currently an Associate Professor with the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University. His main research interests include information security, trusted software, data mining.

Kim-Kwang Raymond Choo (Senior Member, IEEE) received the Ph.D. degree in information security from the Queensland University of Technology, Brisbane, QLD, Australia, in 2006

Dr. Choo currently holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio (UTSA), San Antonio, TX, USA. In 2015, he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP Journal on Wireless Communications and Networking Best Paper Award, Korea Information Processing Society's JIPS Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, Inscrypt 2019 Best Student Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, and Co-Chair of IEEE Multimedia Communications Technical Committee's Digital Rights Management for Multimedia Interest Group.