2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST)

2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST) | 978-1-6654-0267-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/IAECST54258.2021.9695938

Blockchain Technology for Security and Privacy in Energy Internet

Yongqi ZHU
Department of Mathematical and Physics
North China Electric Power University
Baoding, 071003, China
E-mail: anderna@163.com

Yinghui HAN*
College of Resources and Environment
University of Chinese Academy of Sciences
Beijing, 100049, China
Corresponding author: E-mail: hanyinghui@ucas.ac.cn

Zhiwen XUE
Department of Mathematical and Physics
North China Electric Power University
Baoding, 071003, China
E-mail: Zhiwen13639618514@hotmail.com

Wenkun JIANG
Department of Mathematical and Physics
North China Electric Power University
Baoding, 071003, China
E-mail: Jiangwenkun123456@163.com

Yuanxun ZHANG
College of Resources and Environment
University of Chinese Academy of Sciences
Beijing, 100049, China

Ying ZHANG
Institute of Remote Sensing Application
Chinese Academy of Sciences
Beijing, 100094, China

Zhengqiang LI
Institute of Remote Sensing Application
Chinese Academy of Sciences
Beijing, 100094, China

Ayman AHMED*
Space Imaging Division
Egyptian Space Agency
Cairo, 1564, Egypt
Corresponding author: E-mail: ayman.ahmed@egsa.gov.eg

***Abstract*—Blockchain is an emerging technology, which can solve a series of problems of the traditional energy industry and promote its development, such as peer-to-peer transaction of distributed energy, tracking carbon emissions et al. At the same time, the application of blockchain technology brings some challenges, such as regulatory difficulties and the privacy problems. In this work, the blockchain technology in the application status of Energy Internet was briefly summarized, and the security issue and the lack of privacy protection were pointed out. By analyzing the results of other industries, some methods were summarized and suggested to meet the challenge of blockchain privacy protection in the energy Internet.**

Keywords-Blockchain; Energy Internet; Privacy; Zero-Knowledge Proof

I. INTRODUCTION

In the past ten years, due to the progress of technology, the increasing competition in the industry, and the inclination of national policies, the cost of renewable energy has been continuously reduced, and it has become the cheapest energy source. The Central Committee of the Communist Party of China and the State Council issued the Guiding Opinions on Promoting the Development of the Western Region to Form a New Pattern in the New Era, which pointed out that it is necessary to *strengthen the development and utilization of renewable energy* and *accelerate the local consumption of wind power and photovoltaic power generation*. As the largest energy consumer in the world, China is upgrading its traditional industries to further reform its energy sector. However, to prevent environmental pollution from harming people's health, traditional energy companies usually build power plants in suburbs far away from cities or in western regions witch rich in coal and oil. This leads to a long-distance to transmit electricity, which indirectly increases the price of electricity. At the same time, due to the continuous development of distributed photovoltaic power generation in China and the increasing non-traditional power consumption mode caused by the popularization of new energy vehicles, the existing energy business model is no longer suitable [1].

To meet the needs of new sustainable development, the application of blockchain technology in the energy industry will significantly improve the shortcomings of the existing profit model. However, in the process of applying blockchain technology to the energy Internet, privacy security, regulatory breach, and other issues need a specific specification, which will be discussed in detail in this paper

II. APPLICATION STATUS ANALYSIS

Producing electric energy near the consumers can avoid the loss of electric energy caused by long-distance power transmission, while the current electrical consumers are often intensive household users except in some factories [2]. Traditional electric energy production methods are not suitable for production near residential buildings due to noise and

978-1-6654-0267-5/21/$31.00 ©2021 IEEE

environmental pollution, therefore, local, decentralized and clean new energy production methods are accelerating development. Although the current new energy production is decentralized, for example, in photovoltaic grid-connected systems, especially in photovoltaic systems combined with buildings, the producers of electric energy are consumers themselves, and in many cases, they will be energy providers. Although decentralized power producers can trade surplus power produced by themselves to other power users, this process will still be integrated into the Nation Grid and cannot be directly traded by power producers and power consumers. This concept of peer-to-peer transactions fits perfectly with blockchain technology [3]. As more energy users become consumers who produce their energy and suppliers who consume energy from other users, it is extremely urgent to reform the existing energy trading mode by using blockchain technology [4].

The traditional distributed electricity trading mode is combined with the State Grid, in which the electricity producers merge surplus electricity into the State Grid, and the electricity consumers' trade with the State Grid to obtain electricity [5]. Although there is no direct transaction between electricity producers and consumers in this process, the sensitive information of both parties is only stored in the intermediate medium, and the sensitive private information of their users will not be exposed under normal circumstances. The reason why distributed transactions need to protect the privacy of users is that blockchain is a decentralized, open, and transparent data storage technology. As a result, criminals can easily obtain almost all the data from public information. By using these data, they can analyze all consumers of electric energy sellers, and can analyze the purchase information of electric energy consumers, to obtain the specific identifying information of accounts.

Weiqi et al. proposed a peer-to-peer trading framework based on blockchain to track carbon emissions and achieve regional energy balance. Transactions are conducted under self-executing standardized smart contracts. This kind of smart contract is one of the key technologies of blockchain, which can make the negotiation between the two parties more credible in the case of the decentralized situation, without mentioning the impact of the attack of the third party on the system [6]. Gai et al. put forward a joint blockchain-oriented method, which can solve the privacy leakage problem without restricting the transaction function. The practicability of this method has not been proved yet [7]. Ioan et al. demonstrated how to use blockchain to support the formation and use of energy communities, and proposed an energy framework based on blockchain, which can support the energy exchange of consumer communities. The smart contract proposed by the author meets some requirements of the General Data Protection Regulations (GDPR) to protect privacy. Since this paper only simulates the system, it did not put forward a specific scheme for privacy protection security measures [8]. Zhitao et al. put forward a BC-ETS model, which can only involve the transfer of energy ownership in energy storage equipment, without the specific way for users to produce electricity. Therefore, power producers and consumers in different regions will not know the specific information about each other, which will protect privacy to a certain extent. However, this method cannot guard against the production and consumption habits of users obtained from data analysis by lawless elements [9]. The advantages and disadvantages of current methods are summarized in the following Table I.

TABLE I ADVANTAGES AND DISADVANTAGES OF CURRENT METHODS

Advantages and disadvantages of current methods			
Method	***Pros.***	***Cons.***	***Refs***
Peer to peer trading framework	Transactions are conducted under self-executing standardized smart contracts.	Without mentioning the impact of the attack of the third party on the system.	**[6]**
A joint blockchain -oriented method	Can solve the privacy leakage problem without restricting the transaction function.	The practicability has not been proved yet.	**[7]**
An energy framework based on blockchain	Can support the energy exchange of consumer communities.	Did not put forward a specific scheme for privacy protection security measures.	**[8]**
BC-ETS model	Can only involve the transfer of energy ownership in energy storage equipment.	Cannot guard against the production and consumption habits of users obtained from data analysis	**[9]**

III. DISCUSSION

It can be seen that blockchain workers are very optimistic about the application and promotion of blockchain in the energy industry and are eager for blockchain technology to have a positive impact on the energy field and significantly change the energy industry. However, when a user writes data in the blockchain, the entire link needs a consensus from multiple users to work, so the data written by the user cannot be tampered with. As a result, the data in the blockchain is safer, but the relationship between the data and the data owner is diluted, and the data owner cannot prevent others from acquiring and using their data, because all the data are open and traceable. At present, the energy blockchain technology is still in the experimental stage, and the staff focused on the implementation of the advantages of blockchain decentralization, transparency and data cannot be tampered with [10] but ignored the data security problems, unsupervised and lack of privacy protection of blockchain, which could not be effectively solved for the time being. In some other industries, blockchain has been applied maturely, so we can learn from its privacy protection methods and apply them to energy blockchain. Many schemes have been explored to protect privacy, among which the following schemes are widely used.

A. Front-end data encryption

To protect the privacy of users, data encryption is the most intuitive and simple method. After users encrypt their information, they upload the encrypted data to the blockchain. Meanwhile, recipients need to use the same decryption method to obtain complete data information. In this way, the third party cannot know the specific transaction information.

Anik Islam et al. proposed a blockchain-based secure healthcare scheme (BHEALTH), which uses shared keys to maintain system security during communication. The drones

verify the health data through the hash bloom filter and digital signature algorithm. When the verification is successful, the health data terminal will request the consent of other verifiers to upload to the blockchain [11].

Rajesh et al. used two hospitals as an example to divide the secure data sharing scheme into five steps [12].

Encrypting the data in the front-end can conveniently protect privacy, but at the same time, the decryption process will take much more time and delay the system because of data encryption. Nowadays, more and more people are using new energy, so the delay of the system will be much higher, which will seriously restrict the trade between energy sources.

B. Mixers

The mixing mechanism can be divided into a centralized mixing mechanism and a decentralized mixing mechanism. For example, the CoinJoin [13] fundamentally dilutes the relationship between input and output address. In a transaction, when a large number of users participate in it at the same time, an extremely large amount of input and output data will be generated. Therefore, when criminals attack a single node or a few nodes, even if they successfully obtain data, they cannot correspond these huge amounts of data to anyone. To obtain a better protection effect, it can even be mixed multiple times and mix a small amount of user data each time. However, the application of CoinJoin is mostly centralized, which leads to the mixed data being saved in the central server, which cannot guarantee the security of user data. Of course, there is also a decentralized mixed mechanism, but due to the lack of supervision, this mechanism is difficult to be accepted by government departments at present. If this mixer is used in the energy Internet, once this unsupervised blockchain technology is used to do some illegal things, it will not only cause losses to the property of the people, but also badly affect the application of blockchain technology in energy, and even lead to a stagnant development.

C. Zero-knowledge proof

Zero-knowledge proof (ZKP) was put forward in the early 1980s, which is very useful and powerful in cryptography. Zero-knowledge proof is a method by which the prover can convince the verifier that one of his assertions is correct without providing any useful information. The zero-knowledge proof system consists of two parts: a prover who claims that the proposition is true and a verifier who confirms that the proposition is true [14].

The security guarantee of zero-knowledge proof is that when the proposition is true, the verifier will be sure that the proposition is true if both of them obey the rules correctly; when the proposition is false, the prover cannot explain that the proposition is true under any circumstances. Another point is that the prover should not disclose any other information to the verifier [15].

Xiaohui et al. improved the existing claim identification model in blockchain by using smart contract and zero-knowledge proof algorithm, this model realized the unlink ability of identity. In addition, they designed a system prototype (BZDIMS) that allows users to selectively provide information to service providers, effectively preventing the information exposure of distributed accounts, thus protecting the privacy rights of users [16], but it takes some time to generate out-of-chain proofs. On the other hand, the operation cost of the BZDIMS system is very high. When applied to the energy Internet, this method needs to improve its logic to reduce the redundancy of the system, or it can reduce the time of generating out-of-chain proofs by generating a dedicated zero-knowledge proof library.

Haiping et al. put forward a secure data sharing scheme for the intelligent medical system, which combines blockchain, intelligent contract, and zero-knowledge proof, and can protect privacy when medical data is shared by multiple entities. And the scheme can also solve the secure data sharing of intelligent medical systems. Generally, the verification of zero-knowledge proof can make the intelligent contract automatically judge whether the patient's specific medical data meets the requirements of the research institution without revealing the patient's privacy and adopt the proxy re-encryption mechanism to transmit the encrypted medical data into intermediate cipher text which can only be decoded by authorized research institutions. After a series of security and privacy analysis, it shows that the sub-scheme can achieve confidentiality, availability, integrity, and privacy protection [17].

Introducing zero-knowledge proof into the energy Internet can hide the specific transaction details between energy producers and energy consumers, such as transaction amount, transaction scale, and transaction time. It plays a very important role in solving data security and privacy security. Therefore, we believe that the application of zero-knowledge proof in the energy Internet can promote the rapid development of the energy industry through the advantages of decentralized blockchain and extremely distributed storage. On the other hand, the application of zero-knowledge proof can ensure that energy transaction data will not be obtained by criminals in the process of circulation and sharing and protect users' data privacy to the greatest extent.

IV. Conclusion

In general, blockchain is a new technology, and applying blockchain to the energy field is a more forward-looking idea. While carrying forward the advantages of blockchain technology, it is also something we need to consider to avoid its disadvantages from damaging traditional industries. At present, the privacy problem of blockchain needs to be solved urgently. The three mature methods to protect user privacy mentioned in this paper have their advantages and disadvantages. The cost of front-end data encryption is low, but the security is insufficient; the Mixing mechanism needs a partially centralized base station server, its data is not safe; the proposal of zero-knowledge proof may enable us to find the strongest way to protect users' privacy in blockchain in the future. Although it is difficult to realize in technology, if the blockchain platform providing zero-knowledge proof privacy technology can be developed in the energy industry, it will greatly promote the development of the energy industry. Of course, the zero-knowledge proof is also a new technology, and it also has shortcomings, such as the need to establish trust

rules and the inefficiency of generating proof, etc. We also need to constantly explore whether there are other solutions to the privacy problem of blockchain, and finding a perfect way is our future work direction.

DECLARATION OF COMPETING INTEREST

There are no conflicts to declare.

ACKNOWLEDGMENT

This research was support by the Chinese Academy of Sciences Network Security and Information Special Project-Advanced Informatization Technology Application Demonstration Cultivation Project; and National Key Research and Development Program of China (No.2017YFC0210202-1)

REFERENCES

[1] Ayman Esmat, Martijn de Vos, Yashar Ghiassi-Farrokhfal et al. A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. Applied Energy V.282, Part A, 15 Jan 2021, 116123

[2] Shuai Zhu, Malin Song, Ming Kim Lim et al. The development of energy blockchain and its implications for China's energy sector. Resources Policy Volume 66, June 2020,101595

[3] Qiang Wang, Min Su. Integrating blockchain technology into the energy sector — from the theory of blockchain to research and application of energy blockchain. Computer Science Review V.37, Aug 2020,100275

[4] Bernd Teufel, Anton Sentic, Mathias Barmet. Blockchain energy: Blockchain in future energy systems Journal of Electronic. Science and Technology V.17, Issue 4, December 2019, 100011

[5] Konstantinos Christidis, Dimitrios Sikeridis, Yun Wang, Michael Devetsikiotis. A framework for designing and evaluating realistic blockchain-based local energy markets. Applied Energy V.281, 1 Jan 2021, 115963

[6] Weiqi Hua, Jing Jiang, Hongjian Sun, Jianzhong Wu. A blockchain based peer-to-peer trading framework integrating energy and carbon markets. Applied Energy V.279, 1 December 2020, 115539

[7] Gai, K. Wu, Y. Zhu, L. Qiu, M. Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Transactions on Industrial Informatics.V.15, Issue 6, June 2019,8613816, pp 3548-3558

[8] Ioan Petri, Masoud Barati, Yacine Rezgui, Omer F. Rana. Blockchain for energy sharing and trading in distributed prosumer communities. Computers in Industry V.123, December 2020, 103282

[9] Zhitao Guan, Xin Lu, Naiyu Wang, Jun Wu, Xiaojiang Du, Mohsen Guizani. Towards secure and efficient energy trading in IIoT-enabled energy Internet: A blockchain approach Future Generation Computer Systems V.110, September 2020, pp 686-695

[10] Wei Hu, Huanhao Li. A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things. Alexandria Engineering Journal Available online 9 October 2020

[11] Anik Islam, Soo Young Shin. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. Computers & Electrical Engineering V.84, June 2020, 106627

[12] Rajesh Kumar, WenYong Wang, Jay Kumar Ting Yang,Abdullah Khan,Wazir Ali,Ikram Ali.An Integration of Blockchain and AI for Secure Data Sharing and Detection of CT images for the Hospitals Computerized Medical Imaging and Graphics Available online 10 November 2020, 101812

[13] M. Möser Anonymity of bitcoin transactions Münster Bitcoin Conference (2013), pp. 17-18

[14] S. Goldwasser, S. Micali, C. Rackoff The knowledge complexity of interactive proof systems SIAM J. Comput., 18 (1) (1989), pp. 186-208

[15] Li Peng, Wei Feng Zheng Yan, Yafeng Li, Xiaokang Zhou Shohei Shimizu. Privacy preservation in permissionless blockchain: A survey Digital Communications and Networks Available online 25 June 2020

[16] Xiaohui Yang, Wenjie Li. A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers & Security V.99, December 2020, 102050

[17] Haiping Huang, Peng Zhu, Fu Xiao, Xiang Sun et al. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. Computers & Security V.99, December 2020, 102010