A Decentralized Identity based Energy Trading System over a Blockchain Network

Jia Guo
Beijing State Grid Digital Technology Holding Co.Ltd
Beijing China
guojia1@sgdt.sgcc.com.cn

Wei Yu
Beijing State Grid Digital Technology Holding Co.Ltd
Beijing China
yuwei@sgdt.sgcc.com.cn

Songpu Ai
iF-Labs, Beijing Teleinfo Technology,
China Academy of Information and Communications Technology
Beijing China
aisongpu@caict.ac.cn

Junwei Cao
Beijing National Research Center for Information Science and Technology
Tsinghua University
Beijing China
jcao@tsinghua.edu.cn

***Abstract*—In the field of the energy internet, the consumption of distributed power generation for renewable energy is increasing steadily. Considering either the energy security or the transportation loss, the locally generated power would be the first choice. More frequent and more accurate peer-to-peer distributed energy transactions with complicated quality requirements are a significant challenge for current power trading systems. It would be risky and unnecessary to design and operate a centralized trading system to deal with all local transactions on the entire grid. At the same time, the system also needs vital capabilities like supervision and regulations. In this paper, a decentralized identity based energy trading system is proposed over a blockchain network and the distributed identifier (DID) is adopted to identify different energy entities and participants. The verifiable presentation (VP) is adopted by the system to simplify the detection and supervision process of the participants and to minimize information leakage during the transaction lifecycle. On the blockchain network as a highly trusted universal data registry, the entire workflow of energy trading is immutable and traceable. Simulation results show that the energy trading system could operate well.**

Keywords—energy internet, DID, VP, blockchain, energy trading, microgrid

I. INTRODUCTION

Energy internet is a combination of internet, renewable energy, and the modern power system. It utilizes internet concepts, methods, and technologies to achieve peer-to-peer interconnection between energy units, which is an inevitable trend in the integration and development of information technology and power technology [1]. Energy internet architecture could be a productive integration of conventional centralized power networks and decentralized energy networks to undertake wide access to renewable energy such as solar and wind energy.

Consuming the locally generated power would be a priority in view of both energy security and transportation loss. Microgrid, as a basic component of the energy internet, can realize the transformation and sharing of multiple forms of energy [2]. As an effective interface connecting distributed renewable energy to the energy internet, microgrids should support peer-to-peer (P2P) energy transactions [3-5]. P2P energy trading in microgrids has emerged as a promising research direction. It enables private purchasers and distributed power generators to trade mutually to improve the flexibility of distributed generation and network stability by balancing the supply and demand from the bottom of the network.

Meanwhile, increasingly frequent energy distributed transactions with complicated quality requirements would challenge the current power trading system. It is risky and unnecessary to design and operate a centralized trading system to process all the local transactions on the entire grid, since processing all the trading through a central node may bring massive interaction and decision-making requirements as well as security risks caused by single point failures, while a distributed bottom-up built energy internet would prefer to keep the transaction locally. It should be noticed that as crucial infrastructure for industrial production and citizens' daily lives, energy systems need essential capabilities like supervision and regulation.

Decentralization is a core characteristic of blockchain based technologies [6], which is consistent with the bottom-up thinking of the energy internet. Blockchain technology is capable of supporting the distributed software architecture for the energy market [7]. In the research of next generation energy system, blockchain-based energy transaction system is considered as an exploration tendency [8-14]. The utilization of blockchain technology to build a value-sharing system in the energy internet meets the needs of security, openness, and sharing of energy transactions.

The decentralized commonality forms the basis of blockchain technology being adopted to energy internet microgrid energy transactions. The applications of blockchain technology, especially the decentralized identifier (DID) [15] and verifiable presentation (VP) [16] could simplify the conventional multi-layer trading systems and realize efficient P2P energy transactions by constructing trustable decentralized universal resource identification and distributed credential verification among the energy internet. In terms of trust, a microgrid in the energy internet includes multiple stakeholders such as energy producers, consumers, and prosumers. Trading decisions are made locally among the stockholders. The distributed trust system constructed by blockchain technology could provide proper support for the desired autonomy of microgrids among the energy internet.

In this paper, a decentralized identity based energy trading system is proposed, where DID is adopted to identify different participants. VP is utilized to represent authorization between entities within the microgrid, as well as to be an attempt to expose just necessary information during the transaction lifecycle. The entire workflow of energy trading is achieved on blockchain and is immutable and traceable owning to the blockchain network as a trustable universal data registry. The remainder of this paper is organized as follows. Related works are introduced in Section II. In Section III, the system design is described. Achievable DID and VP mechanisms are provided. A simulation is given in Section V. The paper is concluded in Section VI.

II. Related Works

Blockchain has been considered to construct energy trading networks in recent research and projects. The BMG project could be a pioneer which is operated by LO3 Energy with Siemens empowering P2P energy transactions using blockchain. The project includes a microgrid energy market in Brooklyn, New York [17], implemented on the TransActive Grid private blockchain protocol. The platform is a microgrid scenario that enables prosumers to sell excess solar energy to NYC residents. The later versions of this project support charging stations and electric vehicles (EVs) to sell their surplus energy on the microgrid through blockchain technology.

In some early works, such as the one in [8], researchers applied the blockchain in the energy trading network to record transaction results on-chain as distributed storage networks, to avoid the records being damaged or modified when a single failure happens. Since trust could be built between the stockholders by jointly maintaining transaction records, blockchain as a trust-building infrastructure could have been further applied in the entire workflow of energy trading. For instance, the processes of transaction matching and settlement could be promoted by blockchain to offer more trustable, traceable energy trading services.

Notably, a number of existing blockchain based energy trading solutions are designed on a blockchain layer [9-14,18-21]. The entire workflow of energy trading is recorded and traceable on the blockchain. The consensus among the blockchain nodes in these designs not only provides the foundation of trust for the entire trading network, but also ensures the accuracy and effectiveness of all transactions on the network. This places a challenge on the blockchain infrastructure if mass and rapid requirements of the energy transactions on the trading network are taken into account, not to mention that promoting the efficiency of consensus is yet an ongoing research topic of blockchain technology. One possible solution is conducting special consensuses designed for energy trading scenarios in the energy internet [18-21]. One other option that could be interesting is to decouple the fundamental capability of blockchain which builds trust among the trading network with other expected capabilities that we want the trading network to have, for instance, checking the accuracy and effectiveness of all the transactions. A means of balancing the trustable and efficiency is worthwhile to be explored.

Additionally, it is able to be observed that certain existing blockchain based energy trading solutions are entity based energy trading, which means that transactions are constructed between entities, such as two households, a building and an EV, etc. The transactions are conducted on the energy layer. However, in the real world, trading has more than an energy layer. The business more often takes place between persons including natural persons and legal persons. This is usually manifested as when we want to consider the settlement in the trading network, the roles of the entity owners at the value layer should be introduced into the network. Both entities and owners need to be defined and managed properly, which introduces complexity to the blockchain network.

III. System Design

In order to depict the ownership and authorization among a microgrid properly and efficiently, introducing a certain kind of digital identity seems reasonable. Digital identity provides the identification and trust of persons and things in digital space, adapting to the characteristics of network information system transmission, storage, management and utility, and giving people, institutions and things unique digital identity and credentials. The digital identity system issues and authenticates the owner and the attributes of the object of the digital identity, and then feedbacks authentication results to the application system in order to let the identity provider obtain access authorization and services.

From the perspective of the energy internet, which is a bottom-up built system with the principle that regional consumptions have priority over long-span interconnections, distributed digital identity, especially blockchain network based distributed digital identity system could be a worth option. Distributed digital identity and the traditional centralized one are different in the number of centers of authorization and authentication. The former prefers multi-center authorization and multi-center authentication to build a digital identity system in a larger scope, enabling users to obtain a far more unified digital identity experience and boost the development of the energy internet. The distributed digital identity system empowers persons, institutions and things to obtain and manage their own digital identity, and it could safely store users' digital identity and privacy. An interoperable and portable distributed digital identity can realize interconnection between data silos and build flat and flexible identity trust across different applications, domains, networks, and platforms. In addition, the topology of the blockchain network could be roughly coupled to the structure of the energy internet. Therefore, the blockchain network based distributed digital identity system is adopted in the proposed design.

Moreover, the blockchain network based distributed digital identity takes full advantage of the blockchain infrastructure. Taking using blockchain to build an energy trading system as an example, besides saving the infrastructure construction budget, it also integrates and links energy entities with their owners efficiently in the energy internet based on the different characteristics of different microgrids, and achieves unified management and regulation on a large scale. Through decoupling the fundamental trust-building capability of blockchain to the creation, modification and verification of identity and authorization, the performance of blockchain could be highly expected.

DID is considered as one of the key components of the distributed digital identity technical stack. The ownership of a DID can be verified by proofing the ownership of a private key, while the public key of the DID is openly accessed by checking the DID's document which is called DID doc [15]. Since the category of DID discussed in this paper is built on blockchain, the DID doc of a DID should be announced by the owner among a blockchain. DIDs refer to persons, institutions or things, workflows, algorithms, abstract entities, etc. can connect with each other at any security level, initialing from exchanging information using the ways described in their DID docs.

In the proposed design, DID is built as a systematic application of the blockchain network. Each node of the network has the capability and responsibility to receive and process requests from a participant of the energy internet to register, amend, or terminate a DID. Consequently, a participant should pick one of the DID methods that the blockchain network supports firstly. The participant should then generate an operation request of a DID, including the proof that can indicate its ownership of the DID, just as the DID method specified. Afterwards, the participant should send the request to one or multiple, random or specific nodes of the blockchain network according to the DID method. Each DID is allocated with a globally unique string of characters and its corresponding DID document is recorded on a blockchain. Appropriate cryptographic design of the DID method ensures that only the owner of a DID can prove the ownership of this DID and manage this document.

As mentioned in Section II, entities undertake the energy layer transactions, while persons undertake the transactions on the value layer. DID can reflect this type of relationship within the system. However, it is hard to realize complex proxy and authorized operations by DID itself. Even though some DID methods support delegation and some allow a DID to have more than one owner, a much more powerful tool is still required to reliably and securely exchange information between participants. For this reason, VP is introduced.

A VP can represent all the same information that a physical credential does. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts. Technically, a VP is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted by the receiver after a process of cryptographic verification. A verifiable presentation might contain data that is synthesized from, rather than contain, the original verifiable credentials (for example, zero-knowledge proofs), which could also minimize the data exposure. By VP, complicated delegation operations can interact among the energy trading lifecycle on both the energy and the value layers, which could provide external flexibility to the trading system.

VP is considered as one of the key components of the distributed digital identity technical stack, which is built on DID. DID is used to identify the issuer, holder and sometimes verifier of the VP. To offer a VP, an issuer should firstly make one or multiple claims for a subject based on the knowledge the issuer has. The issuer should select a proper verifiable credential context from the list that the trading system supports and then it provides properties to form a verifiable credential about the subject. The verifiable credential is sent to the holders to store. When the claims in one or multiple verifiable credentials are required, the holder should select a proper VP context from the list that the trading system supports, and package the required verifiable credentials into a VP, and send it to the verifier through the P2P channel between them. The verification methods should be provided in the VP. Normally, those methods might link to an address owned by the issuer DID on the blockchain network, where the verifier(s) could find more details on how the VP be verified.

In the proposed design, VP is used to provide third party endorsements on the capability or service of energy sellers, for instance the storage capacity, green energy qualification, etc. The energy purchasers may not know the sellers in the real world, they could choose to trust certain third party endorsement agencies by verifying the VPs that the agency issued to trust the energy seller. In this way, the trading system could release the responsibility of detecting and supervising the energy sellers. At the same time, by letting agencies provide necessary information only in the VP as well as introducing zero-knowledge proofs, the energy sellers could keep some of their capability in secret to the trading system as well as to the purchasers. On the other side, energy sellers could also ask energy purchasers to provide VPs to prove that they do have relevant energy needs.

The blockchain infrastructure in the system could be considered as a universal data registry that enables the functionalities of DID and VP among the energy internet, as well as to undertake the operation of energy transaction trading. The introduction of decentralized identity could decrease the workload that requires frequent blockchain consensus, the complexity of trading design, and leave performance of blockchain focused on servicing transactions.

The system fundamentally includes a user management module, a data acquisition module, a blockchain node module, a smart contract module and a contract management module.

The user management module is used to initiate new user registration, perform identity authentication, etc. Each energy layer entity is allocated a global unique DID. The owner of each energy entity should be a person (natural person, legal person, etc.), who is represented in the system by a DID owned by the person her-/him-/itself.

The data acquisition module undertakes the job of monitoring energy entities to collect data on power supply and consumption requirements as well as data about how the transaction is completed. Data should be authenticated by one or multiple third-party endorsements through verifiable credentials. The verifiable credentials should be well organized as VPs and be packaged into blockchain transactions. These blockchain transactions are sent to the blockchain network through nodes to trigger the matching mechanism.

The Blockchain node module is used for specifying data transmission and communication between nodes in the same blockchain as well as with nodes in other blockchains in the blockchain network.

Smart contract module provides all kinds of smart contracts with corresponding functions for each module, and processing smart contract invoking requests for each module. It should be noted it is not necessary to verify every single DID and VP as a default feature, since if the seller and purchaser know each other well, they don't always have to check and verify each other.

The contract management module is used to remotely upgrade and deploy smart contracts. More details about the blockchain and smart contract design are discussed in our previous work on blockchain based power transaction asynchronous settlement systems [18], which were not the core of this paper.

IV. SIMULATION

To limit the scope of the demonstration, a single blockchain was implemented to represent the blockchain network proposed in this work.

The blockchain system was implemented based on the Hyperledger Fabric [22] framework. The electricity transaction system was built on it. Each electricity seller, electricity purchaser, and system administrator corresponded to a Peer node that was responsible for collecting information and encapsulating it into a blockchain transaction and sending it to the Order node. The Order node was responsible for Raft consensus and synchronization of new blocks. The matching mechanism in the transaction matched contract of the Peer node. Since the purpose of the simulation was to build a simple demonstration of the designed trading system, and bilateral matching was selected as the matching mechanism.

BID was adopted as the DID method. BID as one of the DID methods provided in W3C DID Specification Registries [23] is developed by the Chinese Academy of Information and Communication and Beijing Teleinfo Technology for Chinese national level blockchain infrastructure. In the simulation, BID was invoked as a service, which was not directly built on the Fabric chain.

The implementation equipment was a Huawei 2288H V5 server with 40 cores and 64 GB RAM, allocated to 5 virtual machines with 1 core and 2 GB RAM. The system mounted on the virtual machine is CentOS 7.7.1908. One Peer node was deployed on each virtual machine. Each Peer node could connect one or more users.

The longest time required to perform a transaction match was set as 15 minutes. The system was designed to perform a transaction match for the electricity purchasing and selling request within the period every 15 minutes. The match was triggered by the energy provider when submitting the purchasing request. The trigger condition was that the submission time was more than 15 minutes from the last matching start time, and the match was triggered by whoever committed it first. The energy seller and purchaser were set as holding all the required VPs for each of the transactions, which were also properly verified by each other.

500 different electricity purchasers and electricity sellers were generated separately, and information of each electricity purchaser/seller was randomly generated in a set interval. In the microgrid scenario, the simulation data settings were listed in Table I and Table II.

TABLE. I DATA SETTING OF ELECTRICITY SELLING INFORMATION

Selling price	***Supply***	***Energy type***	***Environment-Protection Index***
0.3023 -1.4167	0.01700-0.15751	thermal power/wind power/ hydropower /solar power /bio-energy power	whether it is renewable energy

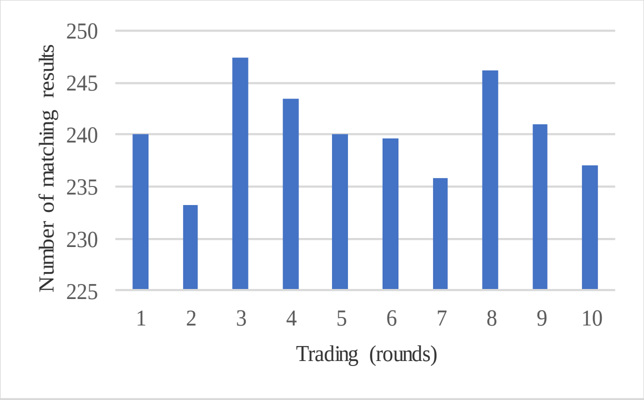

Fig. 1. The number of matching results

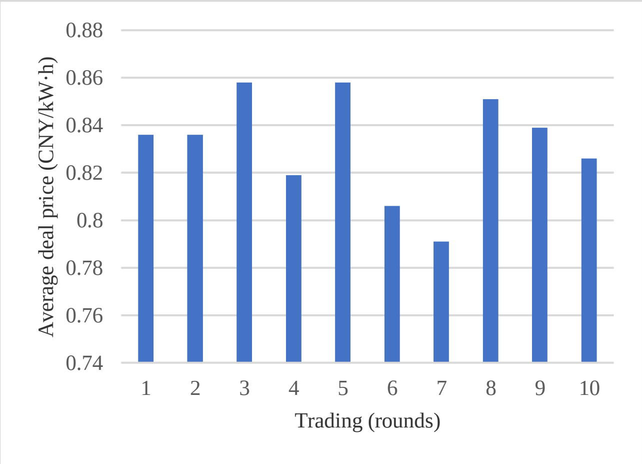

Fig. 2. Average deal prices.

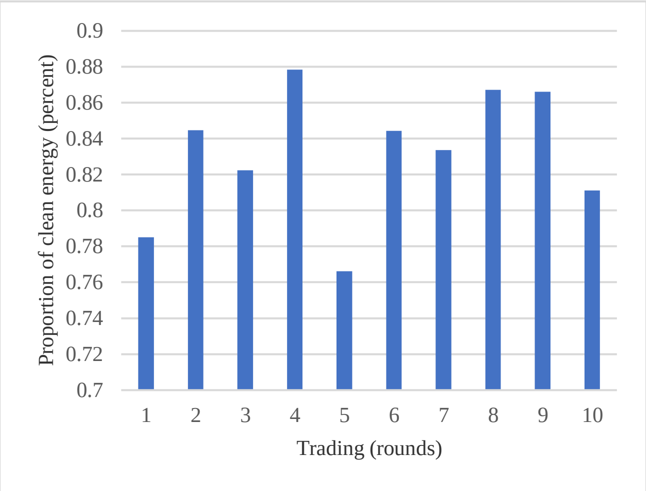

Fig. 3. Proportion of renewable energy.

TABLE. II DATA SETTING OF ELECTRICITY PURCHASING INFORMATION

Purchasing price	***Demand***
0.3023-1.4167	0.01700-0.15751

The application scenario of this work was set to include general industrial and commercial electricity and its price range was wider, so price was utilized as the basis for setting the price interval. The valley price and peak price of electricity for general industrial and commercial electricity in urban areas of Beijing when the voltage level was 1-10kv were 0.3023 CNY/kW·h and 1.4167 CNY/kW·h respectively [24]. Hence, $Price_{min}$ = 0.3023 CNY/kW·h and $Price_{max}$ = 1.4167 CNY/kW·h were set for the simulation. The electricity purchasing and selling price is randomly generated ranging from $Price_{min}$ to $Price_{max}$.

The monthly electricity consumption per capita for non-urban and rural residents in the highest month (December) and the lowest month for urban and rural residents (May) are utilized as the upper and lower limits of the demand range, the demand range is 48.96-453.62 kW·h, according to the National Energy Administration [25]. To every 15 minutes, the demand range was 0.01700-0.15751 kW·h. The range of electricity supply and demand range were hence set as 0.01700-0.15751 kW·h.

The type of energy was set as thermal power, wind power, hydropower, solar power, or bio-energy power, which was marked by an environment-protection index to illustrate whether the energy was renewable or not.

The simulation was set up and operated for 150 minutes. Results are shown in Figure 1-3. It is observed that during the operation time, 10 rounds of trading were successfully conducted.

V. CONCLUSION

In this paper, a decentralized identity based energy trading system is proposed over a blockchain network. DID is adopted to identify different participants. VP is adopted to release the responsibility of detecting and supervising the energy sellers. At the same time, VPs protect the privacy of the participants of the system by providing just necessary information. The entire workflow of energy trade is achieved on a blockchain network and is immutable and traceable, while the blockchain network as a universal data registry is trustable. Simulation results show that the energy trading system could operate well.

REFERENCES

[1] J. Cao, J Sun. “Energy internet and energy systems”. Beijing: *China Electric Power Press*, 2016.

[2] J. Cao, et al. “Energy Internet—Integration of information and energy infrastructure”. *Southern Power System Technology*, 2014,8(04):1-10.

[3] D. Shah, and C. Saibal, "A comprehensive review on day-ahead electricity market and important features of world's major electric power exchanges." *International Transactions on Electrical Energy Systems* (2020): e12360.

[4] T. Sousa, T. Soares, P. Pinson, F. Moret, T. Baroche, and E. Sorin, "Peer-to-peer and community-based markets: A comprehensive review," *Renewable Sustain. Energy Rev.* vol. 104, pp. 367–378, 2019.

[5] C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long. "Peer-to-Peer energy trading in a Microgrid." *Applied Energy* 220 (2018): 1-12.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." *Bitcoin. – URL: https://bitcoin. org/bitcoin. pdf* (2008).

[7] X. Xu *et al*., "The Blockchain as a Software Connector," *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, Venice, 2016, pp. 182-191, doi: 10.1109/WICSA.2016.21.

[8] S. Zhao, B. Wang, Y. Li, and Y. Li, "Integrated Energy Transaction Mechanisms Based on Blockchain Technology." *Energies* 2018, *11*, 2412.

[9] Z. Zeng, et al., "Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application. "*Energies* 2020, *13*, 881.

[10] B. Wang, Y. Li, S. Zhao, et al., "Key technologies on blockchain based distributed energy transaction." *Automation of Electric Power Systems* 2019, 43.14: 53-64.

[11] B. Li, Q. Qin, B. Qi, et al., "Summary of Design of Distributed Energy Trading Scheme Based on Blockchain," Power System Technology, 2019,43(03):961-972.

[12] N. Wang, W. Xu, Z. Xu, and W. Shao. Peer-to-Peer Energy Trading among Microgrids with Multidimensional Willingness. Energies 2018, 11, 3312.

[13] J. Wang, Q. Wang and N. Zhou, "A Decentralized Electricity Transaction Mode of Microgrid Based on Blockchain and Continuous Double Auction," *2018 IEEE Power & Energy Society General Meeting (PESGM)*, Portland, OR, 2018, pp. 1-5, doi: 10.1109/PESGM.2018.8586322.

[14] F. Luo, Z.Y. Dong, G. Liang, J. Murata, and Z. Xu, "A distributed electricity trading system in active distribution networks based on Multi-Agent coalition and blockchain," *IEEE Trans. Power Syst.*, to be published, doi: 10.1109/TPWRS.2018. 2876612.

[15] "Decentralized Identifiers (DIDs) v1.0, " 2023. [Online]. Available: https://www.w3.org/TR/did-core/.

[16] "Verifiable Credentials Data Model v1.1, " 2023. [Online]. Available: https://www.w3.org/TR/vc-data-model/.

[17] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid. " *Applied Energy*, 2018,*210*, 870-880.

[18] S. Ai, D. Hu, T. Zhang, Y. Jiang, C. Rong and J. Cao, "Blockchain based Power Transaction Asynchronous Settlement System," *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, Antwerp, Belgium, 2020, pp. 1-6, doi: 10.1109/VTC2020-Spring48590.2020.9129593.

[19] D. Wang *et al*., "PBFT-based Regional Energy Internet Blockchain Transaction Consensus," *2021 IEEE International Conference on Energy Internet (ICEI)*, Southampton, United Kingdom, 2021, pp. 191-196, doi: 10.1109/ICEI52466.2021.00038.

[20] S. Ai, D. Hu, J. Guo, Y. Jiang, C. Rong and J. Cao, "A Blockchain-based Distributed Controllable Electricity Transaction Match System," *2020 IEEE International Conference on Energy Internet (ICEI)*, Sydney, NSW, Australia, 2020, pp. 56-62, doi: 10.1109/ICEI49372.2020.00019.

[21] C. Zhao, J. He, P. Cheng, and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2049–2061, Sep. 2017.

[22] E. Androulaki, A. Barger, V. Bortnikov, et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains[J]. 2018.

[23] "DID Specification Registries, " 2023. [Online]. Available: https://w3c.github.io/did-spec-registries/#did-methods

[24] "Notice of Beijing Municipal Development and Reform Commission on Relevant Issues concerning the Adjustment of Electricity Prices for General Industrial and Commercial Sales in this Municipality, " 2019. [Online]. Available: http://www.bj.sgcc.com.cn/html/files/2020-05/12 /2020051209310 9482734957.pdf.

[25] "National Energy Administration releases electricity consumption for the whole society in 2019," 2020.01.20. [Online]. Available: http:// www.nea.gov. cn / 2020-01/20/c_138720881.htm