Research on Power Universal Service Access Gateway Based on Blockchain

Shao-peng Wanyan(✉), Peng Jia, and Xiao-yuan Zhang

NARI Group Corporation, State Grid Electric Power Research Institute, Nanjing, China

Abstract. With the development of power Internet of things and energy Internet, the traditional centralized access authentication method of power Internet of things terminal is difficult to meet the application needs. At present, the centralized access authentication mode has brought great computing and communication pressure to the authentication center, especially large-scale concurrent access and mobile access have a serious impact on the authentication efficiency of the system. Based on the decentralized technology of block chain and the characteristics of power communication network, a distributed authentication scheme suitable for power Internet of things is proposed. The power ubiquitous service access gateway based on block chain is developed, and the terminal test is carried out in wired environment and wireless environment. The gateway can realize the terminal access authentication of the typical ubiquitous power Internet of things system, such as distribution automation, new energy and so on. It has the characteristics of good universality and convenient configuration, and can significantly improve the security of the terminal system without affecting the original system topology.

Keywords: Block chain · Distributed authentication · Power Internet of Things · Gateway · Terminal test

1 Introduction

With the increase of the demand of the intelligent service of the power grid and the universal access of the energy Internet, a large number of intelligent terminal devices have been connected [1, 2]. New changes have taken place in information acquisition methods, storage patterns, transmission channels and processing methods. Therefore, the information and communication technology to support the power grid business capacity put forward higher requirements [3, 4]. The growth of power communication network coverage and access services has resulted in an explosion of terminal types and number of terminals. In particular, the large-scale construction of the Internet of things will greatly accelerate this trend [5]. The ubiquitous power communication network is a multi-service integrated carrying network, and the service does not need to pay attention to the composition of the communication network. Because the network handles the massive traffic efficiently, the network resources has obtained the full play. Because of the huge number of terminals, there are a large number of different types of terminals to exit and access the network every day [6]. Access and terminal access must be plug-and-play

Y. Tian et al. (Eds.): ICBDS 2020, CCIS 1415, pp. 458–470, 2021.
https://doi.org/10.1007/978-981-16-3150-4_38

flexible access without cumbersome access processes. The network coverage becomes bigger, and the type and number of terminals increase, which makes the network more vulnerable to attack, and puts forward higher requirements for the security authentication of terminals [7, 8].

The current power communication network is a typical convergent network with almost no data interaction between terminals and terminals [9, 10]. Terminal authentication relies on centralized proxy communication patterns and servers. All devices are verified and connected through a cloud server with strong operating and storage capabilities. With the construction of the energy Internet, such a centralized network faces challenge [11, 12]. First of all, the demand for direct communication between a large number of terminals is becoming more and more prominent due to the construction of the energy Internet and the access of services. The traditional convergent networks should be transformed into interconnected networks [13, 14]. Secondly, as the base of the Internet of energy interconnection, the Internet of things will bring a surge in the number of terminals. Centralized access that relies too much on authentication centers cannot meet the demands of the growing Internet of things ecosystem in terms of effectiveness and security [15].

The key to the above problem lies in the existence of the central node [16]. Decentralization is an important way to solve these problems because it is unable to deal with mass data processing, storage, forwarding, reliability and security risks [17]. For the application of power industry, the above problems can be solved by using blockchain technology [18]. In order to avoid the centralized processing of a large number of transaction information between devices, it can provide a flexible and credible access to protect the privacy and anonymity of users. However, from the existing applications, there are still some problems to be solved in the application of blockchain technology in power systems. In this paper, a distributed authentication scheme for power internet of things is proposed, and a blockchain-based universal access gateway is developed.

2 Distributed Authentication Based on Block Chain

2.1 Features of Power Communication Networks

In the energy Internet environment, there will be different characteristics, different needs of the Internet of things nodes together to apply for access. As shown in Fig. 1, the access scenario is characterized as follows.

Substations where communication sites are physically dispersed and where communication is required. The number of sensors in the substation is large, and there are many kinds of access services for each node equipment.

2.2 Model and Process of Distributed Authentication

The traditional access authentication model is shown in Fig. 2. All nodes with access to the network must be authenticated by a unified authentication center. When the number of nodes is large, the load of CA will be too large [19], which is not suitable for scenarios of a large number of nodes in power communication network.

Block chain-based access authentication includes the following steps.

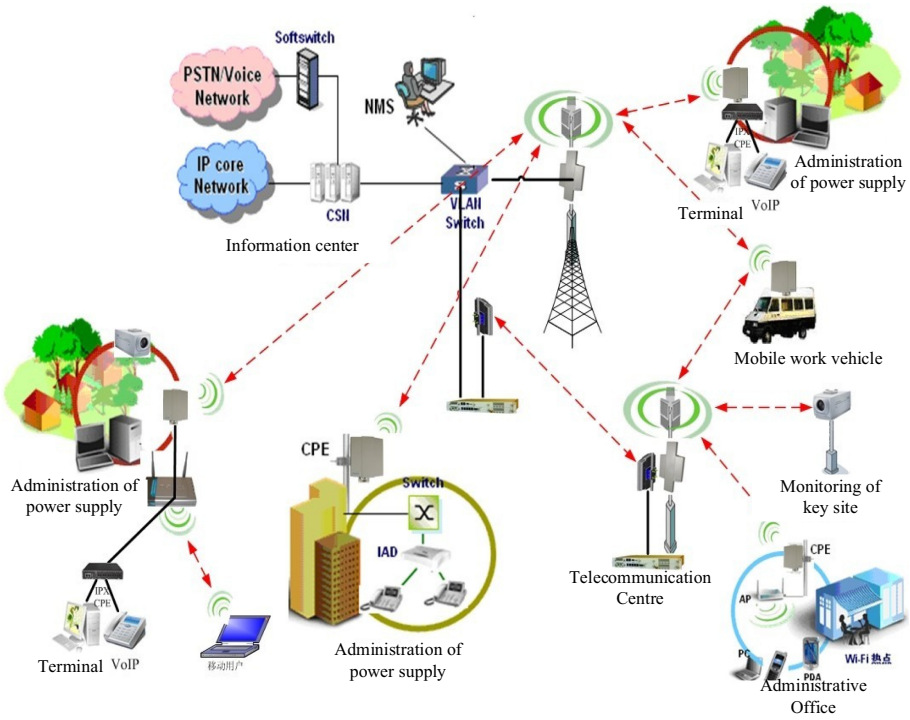

Fig. 1. Schematic diagram of ubiquitous access in power communication network

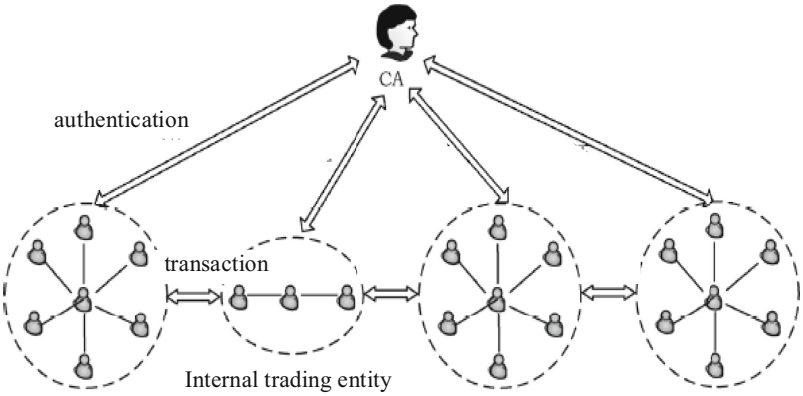

Fig. 2. Access authentication model for traditional services

Step 1. Make sure that each node uses a timestamp to form a block chain. Make sure each node determines the unique public key and the corresponding private key by firmware at the time of shipment.
Step 2. It establishes a consensus mechanism through the PBFT voting mechanism.

Step 3. It defines the virtual currency and establishes the incentive and punishment mechanism. When the node provides the authentication service, the node acquires a specified number of virtual currencies. When a node applies for a authentication service, it needs to consume a virtual currency.
Step 4. All nodes can download account information. Encryption algorithm ensures that privacy information is not leaked during authentication.

Based on the above steps, the power communication network is established to access the private block chain data structure and intelligent contract. The new equipment is uniquely identified when assembled by the factory, and transfer to a common blockchain after installation deployment. In this block chain, you can interact with other devices autonomously and cooperate with the authentication process without the participation of the certification center. The authentication model is shown in Fig. 3.

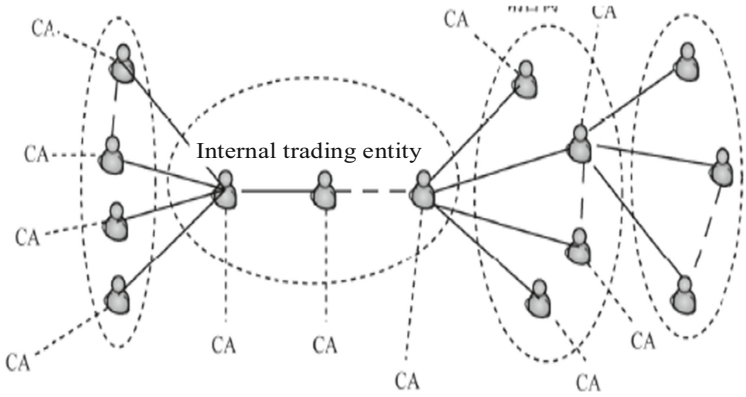

Fig. 3. Schematic of the distributed authentication

Each node in the system has the characteristics of high autonomy, and the nodes are free to connect with each other to form a new connecting unit. Any node may become a stage center but does not have a mandatory central control function. The influence between nodes will form a nonlinear causality through the network. It lets the device know the functions of other devices and the instructions and permissions of different users around these devices.

The first step for an IoT terminal to access authentication is to send an authentication request [10]. The main node requests the packet according to the authentication result, and then retrieves the appropriate node in the access authentication block chain. Appropriate nodes must meet legitimacy and authentication, as well as functional requirements. Legitimacy means that the node has been successfully connected to the system, authentication means that the node belongs to the same business, and functional requirements mean that it has sufficient processing power to run the algorithm. Finally, the request is sent to the authentication group by multicast. The entire access authentication process is shown in Fig. 4.

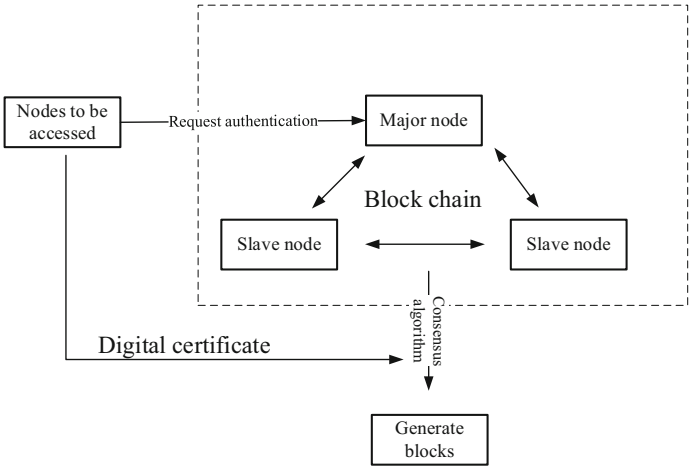

Fig. 4. Schematic diagram of access authentication process

The whole authentication process can be divided into request and confirmation phases.

(1) Phase of the request
The power terminal initiates the authentication application, in which the registration information of the terminal is included. After receiving the authentication application, the main node confirms the terminal signature with the terminal public key, and finally forms the authentication protocol request message.
(2) Phase of the confirmation
After the main node receives the authentication application, the authentication block chain is retrieved and then integrated matching is carried out. It is mainly based on the type of node, the running state, the type of business and so on. Finally, the most satisfied node is selected to form the authentication group G = {P1, P2,…, Pt}. It sends authentication protocol request message in G. The node completes the authentication through the consensus algorithm, generates the block, finally the terminal receives the confirmation information.

The consensus algorithm consists of request, preparation, preparation and submission, as shown in Fig. 5.

(1) Phase of startup preparation
Primary node randomly selected $t-1$ elements, let $a_1, \ldots, a_{t-1} \in Z_p^*$,

$$f(x) = R + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \tag{1}$$

$$y_i = f(x_i), 1 \leq i \leq n$$

Assign y_i to slave node i.

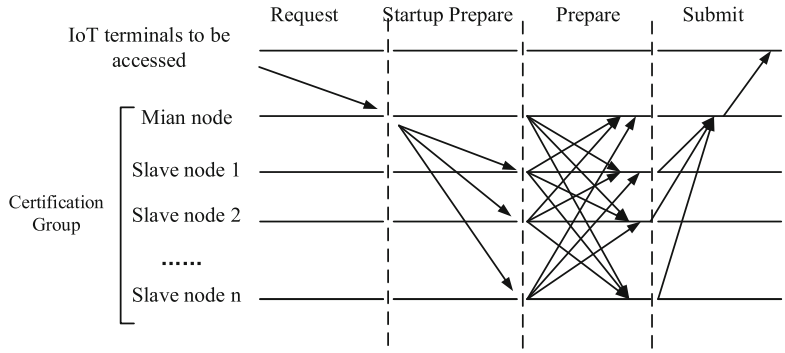

Fig. 5. Interactive process of access authentication based on consensus algorithm

(2) Phase of preparation
When the node receives the request, the recovery algorithm is adopted. The secret share held by the exchange of nodes in G, so we can get t point pairs, $(x_1, y_1), \ldots, (x_t, y_t)$. So the certificate information for the terminal is as follows.

$$R = \sum_{j=i}^{t} y_j \prod_{1<l<t, l\neq j} \frac{x_l}{x_l - x_j} \tag{2}$$

(3) Phase of submission
It submits the authentication results to the main node. The main node completes the authentication of the terminal according to the result of authentication.

3 Design of Service Access Gateway for Electric Communication Network

3.1 Hardware of Gateway System

The system hardware consists of a blockchain authentication server, a programmable switch and a configuration terminal.

(1) Authentication server
The server uses an industrial control computer with an X86 architecture, 8G memory, CentOS 7 operating system, gigabit Ethernet port.
(2) Three layer switch
Switches with remote configuration can receive control instructions from the authentication server. It establishes a connection link when the instruction is passed. When the instruction is blocked, cut off the network access to the corresponding interface.
(3) Certified terminals
The performance of certified terminals is shown in the table below (Table 1).

Table 1. Table of performance parameters for authentication terminals

Parameters of certified terminal	Performance
CPU	Broadcom BCM2837B0 A53 (ARMv8) 64 位@ 1.4 GHz
GPU	Broadcom Videocore-IV
Internal memory	1 GB LPDDR2 SDRAM
Network	Gigabit Ethernet, 2.4 GHz and 5 GHz Dual - frequency Wi-Fi
Bluetooth	Bluetooth 4.2, Low-power Bluetooth (BLE)
Storage	Micro-SD
GPIO	40 pin GPIO dual row pin
Other interfaces	HDMI, 3.5 mm Analog Audio Video jack, 4x USB 2.0, Ethernet, Camera Serial Interface (CSI), Display Serial Interface (DSI)
Size	82 mm * 56 mm * 19.5 mm, 50 g

3.2 Software of Gateway System

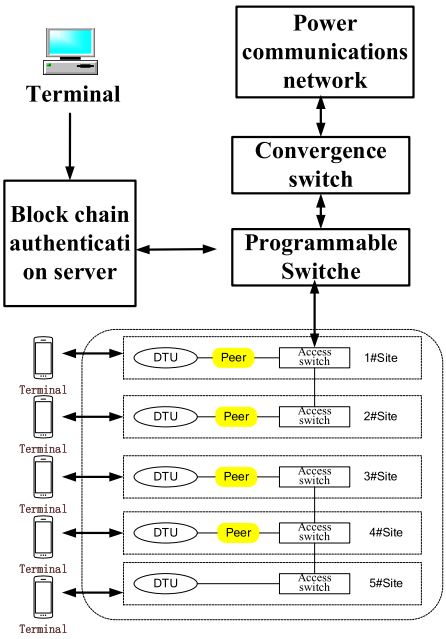

Fig. 6. Deployment of software

Fig. 7. The main interface of the software system (Color figure online)

Access to the home page, system configuration and system management via the navigation bar on the left of the interface. The state of all terminals can be seen in the main interface. The state is divided into three categories, red means denial of access, blue means access, and gray means the device is not online. When in blue, the corresponding device can access the system, otherwise it cannot access the system. The on-off of the device can be controlled manually, showing red or blue (Figs. 6 and 7).

4 Testing and Analysis of Gateway

4.1 Scenario for Testing

The test scenario is a distribution automation system. Distribution automation system is a typical scenario of power Internet of things application. The distribution terminal is mainly connected to the distribution automation system by means of optical fiber and wireless network. Due to the relatively weak security measures and enhanced means of hacking, the distribution automation system is vulnerable to network attacks from public networks or private networks, and then affect the distribution system to the user's safe and reliable power supply. At the same time, the current international security situation has undergone new changes, the attackers have circuitous attacks on the main station by misreporting the fault information at the distribution terminal, thus creating a wider security threat. In order to ensure the safe and stable operation of the power grid, it is very important for the safety protection of the distribution automation system.

4.2 System Topology for Gateway Deployment

The system topology is shown in the following figure. The authentication server verifies the access request of the terminal equipment by connecting the convergent switch to the power communication network. Demonstration verification system is divided into 2 pieces. DTU in slice 1 interworking with convergent switch in layer 2 via access switch,

terminals in slice 2 interworking with convergent switches via 4G network. Before the terminal can access the backbone communication network, it needs to be authenticated by the block chain authentication server and obtain the communication token, otherwise it will not be possible to establish the network layer (three layers) communication link (Figs. 8 and 9).

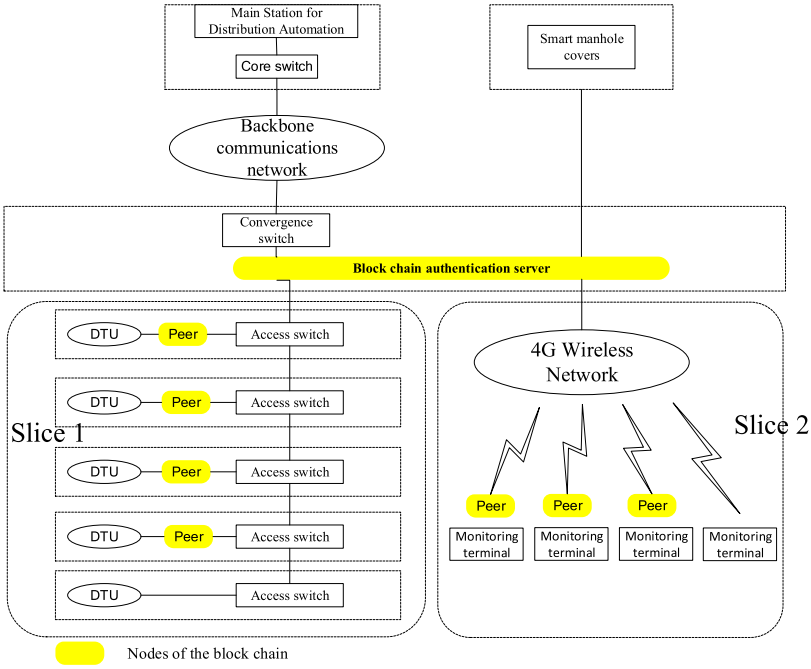

Fig. 8. General topological diagram of the system

4.3 Terminal Testing Under Wired Communication

This test scene is the monitoring service of the distribution automation terminal. The system uploads the monitored data to the monitoring center server via a three-tier switch via the Ethernet interface, and then the server acquires the data. If the authentication does not pass, the server sends blocking instructions to disconnect the bridge of the authentication terminal and realize the blocking function of the illegal terminal. In this field test, the blockchain authentication server is deployed in the computer room to communicate with the authentication terminal through the three-layer switch.

The IP address distribution table for the terminal is as follows (Table 2).

The deployment of the blockchain authentication server in the computer room is shown below (Fig. 10).

The test results are shown in the table below.

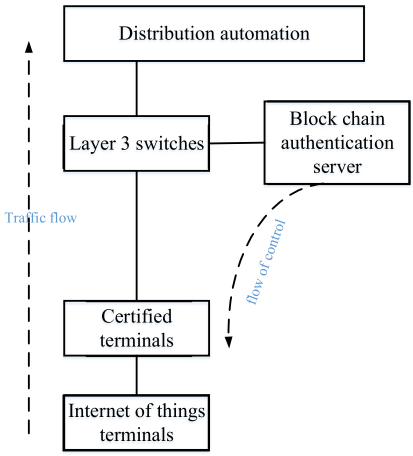

Fig. 9. Deployment diagram of equipment

Table 2. Address assignment for terminals

Terminal for testing	Parameters of gateway
Server: 10.10.0.2/29	10.10.0.1
Terminal 1: 0.10.0.18/29	10.10.0.9
Terminal 2: 10.10.0.18/29	10.10.0.17
Terminal 3: 10.10.0.26/29	10.10.0.25
Terminal 4: 10.10.0.34/29	10.10.0.33

Fig. 10. On-site deployment diagram of servers and gateways

Table 3. Test results of terminal access (wire communication)

	Access status	Address	Time
1	On	1# Station	2019 09 09 10:17:21
2	On	2# Station	2019 09 09 10:17:46
3	Off	3# Station	2019 09 09 10:19:25
4	On	4# Station	2019 09 09 10:26:13

As you can see from Table 3, four sites can be authenticated by block chain. The authenticated terminal can access to the network, has no impact on the service, and the uncertified terminal cannot access the network. In the table, the terminal showing the on status is authenticated and therefore accessible to the network. Terminals showing off status are not authenticated and therefore cannot access the network.

5 Conclusion

In this paper, a distributed authentication scheme for power Internet of things is proposed, and a blockchain-based gateway is developed. The gateway can realize the terminal access authentication of distribution automation, new energy and so on. It has the characteristics of good universality and convenient configuration, and can improve the security of the terminal system without affecting the original system topology. This paper makes an in-depth research on the power communication network technology based on information communication, introduces the blockchain technology, and extends the technology across fields. Through the necessary research and development, the technology is applied to all kinds of power service access application scenarios to improve the data transmission performance of the power communication network, and to solve the bottleneck problem of the network performance of the power communication. The next step is to continue to explore the unique advantages of blockchain in information security, combining with the specific application scenarios of the Internet of things, and to study the method of realizing high-efficiency access and fine-grained access control based on blockchain technology.

Acknowledgments. The authors would like to thank the anonymous reviewers and editor for their comments that improved the quality of this paper. This work was supported by science & research project of SGCC. (Research and application of terminal layer architecture and edge eIoT agent technologies in full service ubiquitous SG-eIoT. Project No. 5700-201958240A-0-0-00.)

References

1. He, P., Yu, G., Zhang, Y., Bao, Y.: Survey on blockchain technology and its application prospect. Comput. Sci. **44**(4), 1–7 (2017)
2. Xiao, Z., Chen, N., Wei, J., Zhang, W.: A high performance management schema of metadata clustering for large-scale data storage systems. J. Comput. Res. Dev. **52**(4), 929–942 (2015)
3. Sun, Y., Yu, Y., Li, X., Zhang, K., Qian, H., Zhou, Y.: Batch verifiable computation with public verifiability for outsourcing polynomials and matrix computations. In: Liu, J.K., Steinfeld, R. (eds.) ACISP 2016. LNCS, vol. 9722, pp. 293–309. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-40253-6_18
4. Lou, J., Zhang, Q., Qi, Z., Lei, K.: A blockchain-based key management scheme for named data networking. In: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, pp. 141–146 (2018)
5. Samaniego, M., Deters, R.: Blockchain as a service for IoT. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, pp. 433–436 (2016)
6. Kan, L., Wei, Y., Hafiz Muhammad, A., Siyuan, W., Linchao, G., Kai, H.: A multiple blockchains architecture on inter-blockchain communication. In: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, pp. 139–145 (2018)
7. Li, H., Tian, H., Zhang, F., He, J.: Blockchain-based searchable symmetric encryption scheme. Comput. Electr. Eng. **73–78**, 32–45 (2019)
8. Andoni, M., et al.: Blockchain technology in the energy sector: a systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. **100–105**, 143–174 (2019)
9. Ji, B., Mo, J., Wang, J.: Study on communication reliability of weakly centralized electricity mutual transaction based on blockchain technology. Guangdong Electr. Power **32**(1), 85–92 (2019)
10. Yuan, Y., Ni, X., Zeng, S., Wang, F.: Blockchain consensus algorithms: the state of the art and future trends. Acta Automatica Sinica **44**(11), 2011–2022 (2018)
11. Yihua, D., James, W., Pradip, K., et al.: Scalable practical byzantine fault tolerance with short-lived signature schemes. In: Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering, CASCON 2018, pp. 245–256 (2018)
12. Min, X.P., Li, Q.Z., Kong, L.J., et al.: Permissioned blockchain dynamic consensus mechanism based multi-centers. Chin. J. Comput. **41**(5), 1005–1020 (2018)
13. Luu, L., Narayanan, V., Zheng, C., et al.: A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS 2016, pp. 17–30 (2016)
14. Castro, M., Liskov, B.: Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. Assoc. Comput. Mach. **20**(4), 398–461 (1999)
15. Pan, C., Liu, Z., Liu, Z., Long, Y.: Research on scalability of blockchain technology: problems and methods. J. Comput. Res. Dev. **5**(10), 2099–2110 (2018)
16. Zhang, J.-Y., Wang, Z.-Q., Xu, Z.-L.: A regulatable digital currency model based on blockchain. J. Comput. Res. Dev. **55**(10), 127–140 (2018)
17. Guo, J.-W., Chu, J.-J., Cai, P., Zhou, M.-Q., Zhou, A.-Y.: Low-overhead paxos replication. Data Sci. Eng. **2**(2), 169–177 (2017)
18. Wang, J., Li, L., Yan, Y., Zhao, W., Xu, Y.: Security incidents and solutions of blockchain technology application. Comput. Sci. **45**(z1), 352–355,382 (2018)

19. Xu, Z.-H., Han, S.-Y., Chen, L.: CUB, a consensus unit-based storage scheme for blockchain system. In: Proceedings of IEEE 34th International Conference on Data Engineering, Paris, France, pp. 173–184 (2018)
20. Li, Y., Zheng, K., Yan, Y., et al.: EtherQL: a query layer for blockchain system. In: Proceedings of International Conference on Database Systems for Advanced Applications. Suzhou, China, pp. 556–567 (2017)