Research on Block Chain Service Composition Strategy Based on Big Data

Wei Yang¹,*
¹Faculty of Information and Control Engineering, Shenyang Urban Construction University, Shenyang, PR China, 110167
*Corresponding author e-mail: waye@syucu.edu.cn

Abstract. With the proposal of China's new infrastructure strategy, big data, artificial intelligence and 5G networks are bound to get further rapid development, and the Internet of Things, as a key component, is also getting more and more extensive attention and in-depth research. Wireless sensor network is an important part of the development of the Internet of Things, which is widely used in military, transportation, industry and daily life. Therefore, the security of wireless sensor network is particularly important. Due to the limited resources such as energy, storage and space, existing heavyweight security authentication methods are not suitable for wireless sensor networks. Based on the block chain design idea, a lightweight wireless sensor network security authentication model is proposed to solve the data security problem of wireless sensor network terminal. The model divides the sensor network into two layers: global network and local network. The local network adopts asymmetric encryption for centralized security authentication. The global network uses directed acyclic graph (DAG) and Tangle technology to construct the account books, and uses the key nodes and random walk method to verify the consistency.

Keywords: Blockchain, Cross-Domain Authentication, Public key Infrastructure, Biometric Identification

1. Introduction
As the human society enters into the era of big data, the upsurge of big data application and the multiplication of data value make the big data system and its application present unprecedented complexity. As shown in Figure 1. Traditional protection means can no longer meet the new security requirements under the big data environment, and the security problems of application are increasingly prominent. The research on cross-domain authentication of data and applications is of great significance to the secure sharing of big data across regions, industries and enterprises. As a trust-building machine, the blockchain technology, especially the multi-center architecture of the alliance chain and the scenario of multi-institution cooperation, well meets the needs of cross-domain certification among regions, industries and enterprises. Blockchain technology itself has a data block chain structure that is not easy to tamper with, a consensus mechanism jointly maintained by multiple
parties, open and transparent ledger of distributed storage and other characteristics, which can well solve cross-domain authentication problems [1].

![Blockchain Technology Penetration](image)

**Figure 1.** Blockchain technology penetration

2. **Blockchain technology**

As the most influential hot technology at present, blockchain has got rid of the single application scenario only in the field of digital currency, and has a broad application prospect in the fields of finance, Internet of things, identity authentication and so on. In the academic world, blockchain has also achieved some research results in non-financial fields. Blockchain technology has attracted more and more attention from all walks of life [2].

Blockchain technology integrates the key technologies of distributed storage, modern cryptography, point-to-point network, consensus mechanism and intelligent contract to exchange, store and process data. It is a new technology of security, efficiency and shared intelligence. Therefore, the blockchain technology has multiple layers of concepts. As shown in Table 1: First, block chain is a specific data structure with time sequence and block link mode, and its block data storage is safe, orderly, and verifiable. Second, blockchain is a distributed shared ledger protected by cryptographic means, which cannot be tampered with or deleted. Third, blockchain is a distributed infrastructure and computing paradigm that uses a new way to verify, store, generate, update, transmit, access, program and operate data. Fourth, blockchain establishes distributed credit by means of decentralization, consensus mechanism, encryption algorithm and bookkeeping of the whole network, which is an upgrade of TCP/IP protocol, or will evolve into a new Internet protocol [3].

| blockchain technology | function       |
|-----------------------|----------------|
| storage               | data processing|
| modern cryptography   | data storage   |
| intelligent contract  | data exchange  |

### Table 1. Table of blockchain technology.

3. **Blockchain technology features**

Under the dynamic technical framework, blockchain has developed so far. As a machine of trust, blockchain has basically formed the following five common features: (1) Distributed structure. Blockchain is a distributed system based on the network. The ledger is not centralized in a single node, nor can it be recorded and managed by a trusted third-party authority. The block chain system operates on rules and consensus, and participates in the maintenance of block data through certain rules. The failure of any single node does not affect the system operation. (2) Openness and transparency. The operation and data of the block chain are open and transparent, and all nodes of every transaction are visible. Data and contracts on the chain are protected by cryptography and cannot be changed. Open
and transparent operation rules lay a solid foundation for the establishment of mutual trust between nodes. (3) Credibility and reliability. Blockchain technology realizes the consensus reached and the trust relationship established by all nodes without the guarantee of a trusted third-party authority through the distributed consensus mechanism. (4) The timing sequence cannot be tampered with. In theory, it would take an astronomical amount of time to crack blockchain data protected by cryptography. In addition, even if a certain number of node databases are modified, it still cannot affect the normal operation of the whole system. (5) Automatic performance. At present, most blockchain application systems focus on the field of value exchange, while virtualized digital asset trading contracts are programmed to execute automatically according to pre-agreed rules, which shows great changes in the trust mechanism and forms trust in the system and code. Such automatic performance greatly reduces the transaction cost [4].

4. Identity authentication technology
There are many ways of identity authentication, this section mainly introduces the PKI/CA digital certificate authentication, biometric authentication and password authentication, and introduces the cross-domain authentication and two-factor authentication that this paper focuses on. PKI is a security infrastructure based on public key theory. It has public key management, authentication and encryption, integrity detection, security timestamp and other service functions. The work process of PKI revolves around the life cycle of digital certificates. Its responsibility is to integrate the public key information of users with their identity information through CA (Certificate Authority) to form an authenticated digital certificate which can be used to prove who the user is. Through digital signature, encryption, and key and certificate management, to ensure the security of information transmission [5].

5. Biometric
Biometrics is the use of biological characteristics inherent in the human body to identify individuals. The biometrics used for identity authentication must satisfy the four basic conditions of universality, uniqueness, measurement and stability, as well as the standard requirements of speed, error and nondestructive in practice. Now commonly used biological characteristics are physiological and behavioral, the former is mostly congenital, stable and unchanged. For example, fingerprint identification based on detailed features such as breakpoints, bifurcations and transitions; Face recognition based on stable features of human face. Most of the latter are acquired habits and show up in People's Daily behaviors. For example, recognizing a person's gait by taking advantage of the unique way they walk; Handwriting recognition based on the characteristics of the type form, the order of strokes, the pressure of the pen tip, the inclination and the writing speed [6].

At present, with the help of artificial intelligence technology, the level of fingerprint and face recognition has been breakthrough, has formed a large-scale application. In addition, there are palmprint, hand shape, iris, retina, human ear, DNA, human body temperature spectrum and other biometric recognition technologies have been developed and limited applications to varying degrees. In recent years, the unification of digital identity and physical identity of users has become increasingly prominent, and the theory, method and technology of biometric encryption emerge as The Times demand, which makes up for the deficiency of biometric authentication [7].

6. Password authentication
Password authentication is composed of static password and dynamic password. Static password authentication means that the system makes the user set up and stored in the database password to verify the authentication of the user's login password. Generally, the static password set by people is a set of regular and meaningful strings with moderate length, which is easy to remember, easy to realize and easy to use, and is commonly used in E-mail, daily affairs and other systems. However, static password authentication system has poor security and weak anti-attack ability, so it is difficult to prevent eavesdropping, exhaustive and other password attacks, especially the application of big data
technology, which poses a more serious threat to it. Static password authentication has been limited to be applied in unimportant scenes. At this point, the new method came into being.

7. Cross-domain authentication
Cross-domain authentication refers to authentication of users across security domains. With the wide application of The Internet, the demand for cross-domain access services grows rapidly, and cross-domain authentication becomes more and more prominent. When users access resources across domains, problems such as trust relationship and authentication speed need to be solved, especially the collaborative authentication of users by the two domain authentication systems. At present, more mature cross-domain authentication generally establishes trust relationship between two or more domains with the help of PKI authentication systems. After establishing the trust relationship, first transmits the user's identity authentication result in the starting domain to the authentication system of the access domain, and then the authentication result is verified by the access domain authentication system which has established the trust relationship in advance. The successful cross-domain authentication is deemed as passing the authentication.

8. Conclusion
Wireless sensor networks may contain a large number of nodes, and to ensure scalability, it is assumed that the blockchain is managed by some nodes in the network. Here, DBSCAN clustering algorithm is used to cluster the nodes in the wireless sensor network, and each cluster node is selected as the cluster head. The nodes selected as cluster heads will remain online for a long time and have enough resources to process block calculations. The author divides the wireless sensor network into two layers. One is the local network, that is, the exchange and transmission of information between nodes in each cluster. Centralized authorization management is adopted, and the cluster head node (sink node) is responsible for the wireless sensor network. The other is the global network, and the communication between cluster heads and servers is authorized based on DAG blockchain. Wireless sensor Network architecture. All cluster heads are responsible for block chain management. In addition, each cluster head node is responsible for communication and data transmission between other nodes in the cluster.

References
[1] Qiu Tianyi. Research on using block chain technology to promote the development of new retail innovation [J]. Industrial innovation research, 2020(22): 14-16+19.
[2] Li Jizhong, Zhang Aizhong, Liu Yi, Wang Runze. Construction of dual-use emergency logistics information system based on big data platform [J]. Journal of military communications academy, 2020, 22(11): 53-57.
[3] Li Bowen, Yan Jun. Chinese Collective Economy, 2020(32): 7-10. (in Chinese) the Construction and Prospect of rural Homestead Management Trading Platform based on block chain model [J].
[4] Guo Chongling, Zhao Ye. A review of the application of blockchain technology in the field of spatial information intelligent perception [J]. Computer science, 2020, 47(S2): 354-358+362.
[5] Liang Xi, Zhang Haibo. Analysis on the application mode of blockchain technology in international payment [J ]. Friends of accounting, 2021 (02): 155-160 [2020-12-25] http://kns.cnki.net/kcms/detail/14.1063.F.20201224.1303.050.html.
[6] Zhang Yuanyuan, Chen Li, Zhang Jie, Yan Ruimin. Application Research of green building management platform based on blockchain and BIM Technology [J]. Engineering construction and design, 2020 (24): 248-249.
[7] Chen Han, Zheng Liuzhi, Xiong Jialong, Qiu Dongsheng, Luo Xinyue. Zhongchuang space financial service under blockchain technology [J]. Shangxun, 2020 (36): 59-60.