Li, Q., Xu M., Fang, M., Yang, M., Guo, Y. (2019). A conceptual framework for data property protection based on blockchain. In *Proceedings of The 19th International Conference on Electronic Business* (pp. 501-505). ICEB, Newcastle upon Tyne, UK, December 8-12.

A Conceptual Framework for Data Property Protection Based on Blockchain

(Work in Progress)

Qian Li, Nanjing University, China, qianli@nju.edu.cn
Meng Xu*, China Mobile Information Technology, China, xumeng@chinamobile.com
Miao Fang, Nanjing University, China, fangmiao960323@163.com
Meng Yang, China Mobile Information Technology, China, xumeng@chinamobile.com
Yue Guo, Southern University of Science and Technology, China, guoy@sustech.edu.cn

ABSTRACT

Blockchain is a new decentralized infrastructure and distributed computing paradigm. The blockchain technology has the characteristics of decentralization, time series data, collective maintenance, programmable and secure. This paper addresses the needs of China Mobile's digital intellectual property protection and transaction, and uses the relevant design and technology in the blockchain to propose solutions and ideas for identity authentication and traceability of China Mobile's digital intellectual property transactions. Finally, the design concept of blockchain architecture based on China Mobile digital intellectual property transaction is proposed.

Keywords: Blockchain; Digital asset; Traceability; Smart contract

*Corresponding author

INTRODUCTION

At present, with the emergence of new technologies such as artificial intelligence, blockchain, Internet of things and 5G, the global digital transformation has entered an accelerated period, and human society has gradually entered the era of big data. As an important product of the rapid development of information technology and mobile Internet, big data is beginning a major era transformation. Among them, as the amount of data continues to increase and the field of application becomes more widespread, the value of data is increasing day by day. And more and more industries and fields are committed to pursuing the potential value behind the data. This makes the data transaction demand more and more urgent, and also makes the protection, application and management of data property rights face severe challenges.

As a value-adding tool, big data technology will bring unprecedented data changes, and deeper commercial potential and value can be discovered through data. Big data can help managers to make intelligent and reasonable decisions and improve the efficiency and level of enterprise management. Therefore, both the data demand side and the supply side have strong data transaction willingness, and the formation of the data transaction market is beyond doubt. However, due to the current perfect data trading market has not yet formed, data transactions lack legal channels. Data transactions face legal risks such as unclear property rights, complex authorization, difficult pricing, lack of transparency in transactions, difficulty in ensuring fair transactions, and leakage of privacy (Lafuente,2015).Therefore, a careful analysis of the current data transaction status and data transaction characteristics, clarifying a series of issues related to property rights protection in data transactions, is essential for deepening the innovative application of big data in various industries(Yuan & Wang, 2016).

With the development of Internet technology, in order to realize the transformation of information Internet to value the Internet, blockchain technology emerged as the times require. Blockchain technology is a new type of decentralized infrastructure and distributed computing paradigm with distributed storage, time-series data and non-tamperable, decentralized credit, smart contracts, high privacy protection, etc. (Sun,2016).These make the blockchain technology provide a solution to the problems of high cost, high security and high risk that are common to traditional centralized technologies. Because of the above characteristics of blockchain technology, considering the use of blockchain technology in the data transaction process can help to better trace the source in the data transaction process, locate the data value chain, confirm the data ownership, etc. Solve the security risks in the data transaction process under the era of big data.

LITERATURE REVIEW

Intellectual property rights is an intangible property right that people enjoy in accordance with the results of their intellectual activities and the marks and credits in their business management activities (Wang &Gu,2009). The growth effect of intellectual property protection depends on the gap between China's technology level and the world's technological frontier (Li, 2016).Intellectual property protection is further divided into property rights protection of physical assets and data assets. Nowadays,

watermarking technology, digital copyright protection technology, and related legal such as "The Agreement on Trade-Related Aspects of Intellectual Property Rights" and "The Measures for the Administrative Protection of Internet Copyrights protect intellectual property rights".etc are available.

Data transactions mainly refer to the process of transferring big data as a resource and transferring it to the demander through various trading methods (He, 2018).Big data has become a new strategic highland in a major of industries in China, but its power ownership and system security still plague the development of these industries and industries. At present, the main factors restricting Big Data's role in China are as follows: (1) data standards and sharing issues; (2) data privacy issues; (3) intellectual property framework and protection innovation; (4) technical standards and research and development in key areas (Han *et al.,* 2018) Traditional digital asset transactions require transactions through a third-party trading center during the transaction because of mistrust between users. The user uploads the data to the transaction center, and the transaction center grasps all the data information, and the user's inquiry and transfer of the assets are completed by the transaction center (Ding, 2015).Because the trading center is a centralized system, once hacked, all data will result in lost and irreparable results. In traditional digital asset trading, saving data can only be encrypted by simple data. There is no signature verification mechanism in the transaction transmission process to ensure the security of the data transmission process. The traditional digital asset trading system is a seemingly "trustworthy" central management organization to manage the transaction process. The intermediate link will inevitably lead to managerial negligence and infringement of data property rights. Whether the user's interests are damaged depends mainly on the integrity of the transaction center management degree (Zhang e*t al.,* 2016).

In view of the above drawbacks of traditional data transactions, data property rights cannot be well protected, so this paper proposes a method of data property protection based on blockchain technology. The blockchain technology involves time-stamping, Merkle tree, consensus algorithm, and other technologies to realize the authenticity and traceability of data transactions.

Timestamp: The blockchain technique requires that the node that obtains the accounting rights must be time stamped in the current data block header to indicate the write time of the block data. The timestamp adds time dimension to the future blockchain-based Internet and big data property protection. For suspicious data transactions, auditors can use the blockchain timestamp to trace the source and verify the data to accurately analyze whether the data is Tampering; it also increases the spatial dimension and eliminates the risk caused by information asymmetry. Therefore, the auditor who obtains the authorization key can access the audit data without space restrictions, greatly improving the scope of audit supervision and preventing infringement.

Merkle Tree: The Merkle tree is an important data structure for blockchains. Its role is to quickly summarize and verify the existence and integrity of block data. The hash algorithm is combined with MerkleTree to implement the data storage function of the blockchain, and the information stored in the block is transaction information. This is the main function of the MerkleTree tree. At the same time, the Merkle Tree structure feature can support hash data comparison in a short time; only verifying the root of the Merkle Tree can verify the validity of the data, thus protecting the privacy of the transaction data[i].

The application of blockchains in the field of asset management has broad prospects for enabling the identification, authorization and real-time monitoring of physical and digital assets. For physical assets, by combining IoT technology to uniquely identify and deploy assets to the blockchain, it can form "digital intelligent assets" to realize distributed asset authorization and control based on blockchain; For digital assets, based on the characteristics of time stamp technology and non-tampering, blockchain technology can be applied to intellectual property protection, domain name management, and point management.

IDENTITY AUTHENTICATION DESIGN AND TRACEABILITY PROBLEM

China Mobile's digital intellectual property transactions and protection are mainly studied through blockchain identity authentication and blockchain data anomaly traceability. The following are two parts of the design concept and related research perspectives.

China Mobile Digital Property Rights Identity Authentication Design

The characteristics of China Mobile's digital property rights transaction require that the type of blockchain is different from the public chain type of Bitcoin. The behavior of nodes joining and exiting the blockchain is not free, but is subject to supervision by China Mobile. Based on the above factors, the blockchain type of China Mobile Digital Property Rights Transaction should be selected as the alliance chain.

For the alliance chain, refer to the structural design of the hyperledger to discuss the design of the identity authentication problem in the context of China Mobile Digital Property Rights Trading.

In the hyperledger, the concept of PKI was introduced. What is a PKI? A public key infrastructure (PKI) is a collection of internet technologies that provides secure communications in a network.

Digital certificate

In the hyperledger, the digital certificate is a module for storing user information, which is similar to the citizen's identity document, in which the public key information is stored in the digital certificate, and at the same time, the digital certificate is designed based on cryptography to ensure the content of the digital certificate. Information is not tampered with. China Mobile's digital property rights transaction requires that each node in the China Mobile blockchain network has a unique digital certificate for storing information about the node. At the same time, any node that wants to join the China Mobile blockchain network must hold a digital certificate.

Public and private keys

Authentication and message integrity are important concepts in secure communication. Authentication requires that the parties who exchange messages create the identity of a particular message.

Traditional authentication mechanisms rely on digital signatures, which, as the name implies, allow a party to digitally sign their messages. Digital signatures also guarantee the integrity of signed messages. Technically, the digital signature mechanism requires each party to hold two keys for an encrypted connection: a widely available public key and a private key that acts as an authentication anchor, and a private key that is used to generate a digital signature on the message. The recipient of the digitally signed message can verify the source and integrity of the received message by checking if the additional signature is valid under the intended sender's public key.

Under the China Mobile Digital Trading Framework, due to the characteristics of China Mobile's digital transactions with other different companies, this requires the confidentiality of trading information. Referring to the design of the hyperledger, the transaction is encrypted and decrypted by the public key private key to ensure the security of the transaction.

Certification authority

In the hyperledger, the node participates in the blockchain network to have a digital certificate issued by the system trust authority. This system trust organization is called a certificate authority (CA). China Mobile's digital property rights transaction, the certificate issuance work to be completed by China Mobile, the company that cooperates with China Mobile, the transaction company to apply for the digital certificate of the blockchain network to China Mobile. By referring to the design of the identity information content of the hyperledger, China Mobile can solve the identity authentication problem in the digital transaction process, that is, the authorization problem. The specific blockchain transaction process design also needs to be designed according to the characteristics of China Mobile Digital Property Rights Transaction.

Certificate revocation list

A certificate revocation list (CRL) is easy to understand, it is just a list of references to certificates that the CA knows to be revoked for some reason. China Mobile has the right to issue digital certificates in accordance with the relevant applications and also has the right to revoke digital certificates in accordance with the relevant rules. This requires design based on specific circumstances.

Research Concept Based On Blockchain Traceability

Each transaction generated in the blockchain will complete the transaction storage through the consensus mechanism of the blockchain. At the same time, each transaction guarantees the queryable traceability. The new hypothesis of the blockchain traceability problem is proposed below.

Merkletrees is an important part of the blockchain structure. Each block has a Merkle tree starting from the leaf node (bottom of the tree) and a leaf node is a transaction hash (bitcoin uses double SHA256 hash). The advantage of the Merkle tree is that a node can verify that a transaction is included without downloading the entire block. And these only need one transaction hash, one Merkle root hash and one Merkle path.

Based on the merkletrees, it is proposed here whether the problem of blockchain traceability can be based on the characteristics of the merkletrees.

The data of the blockchain is stored in the leaf nodes of the merkletrees, and then the hash operation is continuously performed by the leaf nodes, and finally the root of the tree represented by the hash value is obtained. A change in the value of a leaf node causes

a change in the final root hash value. Based on this feature, the idea of traceability of blockchain anomaly points based on merkletrees is proposed.

BLOCKCHAIN ARCHITECTURE DESIGN MODEL BASED ON CHINA MOBILE

The blockchain model proposed in this paper is designed for the actual business of China Mobile, and it mainly realizes the functions of data security and data source tracking in the process of data asset transfer of mobile companies. In this framework, the service requester and the service provider establish a trust relationship through the blockchain, and use the smart contract to generate and manage new transactions, and broadcast the transaction information to the entire network, and the node receiving the information passes. The consensus mechanism verifies the transaction and protects against malicious attacks, and the verified transaction is written into the blockchain.

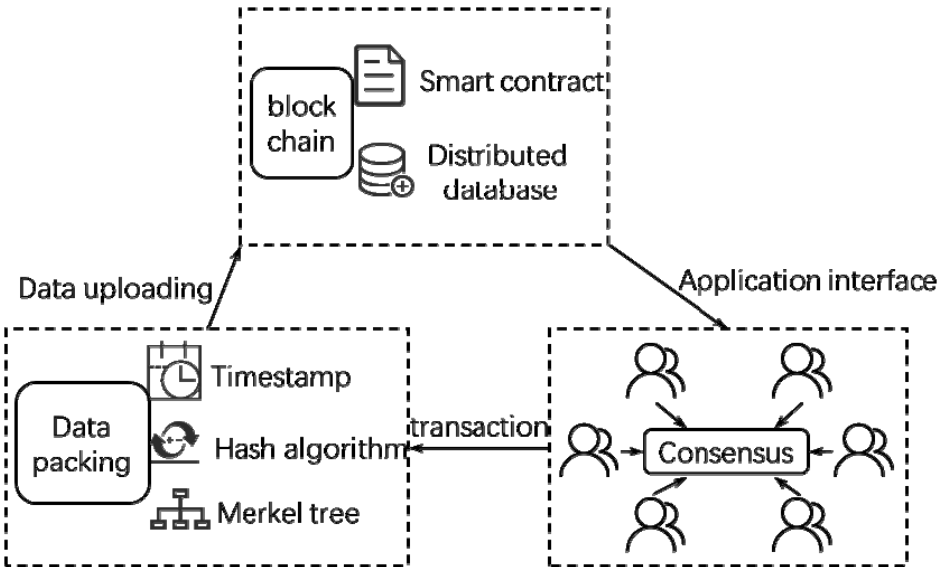

Fig. 1 A blockchain-based digital asset management framework.

In the framework, China Mobile internally forms a Private blockchain of mobile companies by the provincial branch offices according to business needs, and the external business forms Consortium blockchains with other companies. China Mobile Headquarters acts as an intermediary to connect the Private blockchain and the Consortium blockchain. In the given blockchain, according to a set of rules, a legitimate transaction defines how to change the state, and what meaning can be obtained from that state. Therefore, transactions are treated as applications of business logic in the blockchain, so complex applications are often referred to as smart contracts. First, the external company sends a data access request through the API, and then calls the smart contract in the blockchain to extract the relevant data. Finally the external node gets the required data.

At present, the digital asset trading market has problems such as lack of transparency, cumbersome procedures, fraud risks, and public record errors during the transaction period and post-trade process. The application of blockchain technology enables the recording and tracking of digital asset ownership, usage rights, usage records, etc., and ensures the accuracy and verifiability of relevant documents.

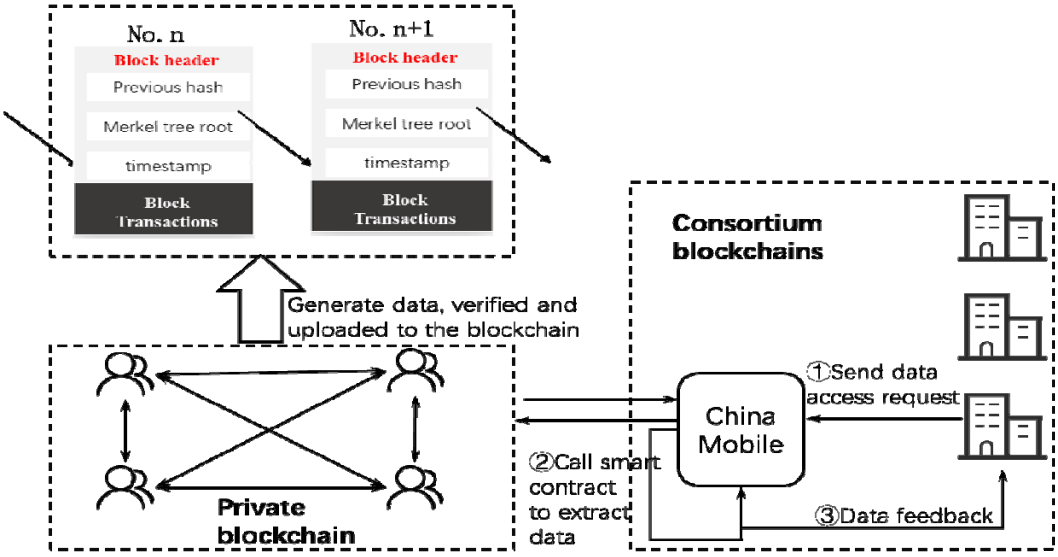

Fig. 2 Blockchain framework of China Mobile Network

In addition, block-chain technology enables real-time paperless and real-time trading. The use of blockchains and smart contracts to verify, bill, store, maintain, and transfer transaction data between service providers and service requesters. As shown in the figure, the blockchain technology is used to realize highly transparent information, non-tamperable information, and high anonymity in the mobile service networking, so that it can manage record transactions and reduce management costs with little or no personnel involvement.

CONCLUSIONS

The blockchain-based China Mobile digital asset management framework proposed in this paper solves the problems of opaque and vulnerable to digital asset transaction transactions by using blockchain, smart contract and consensus mechanism, and realizes decentralization, transaction transparency and security. Traceable service management effectively reduces management costs, improves overall system operation efficiency, and reduces malicious attacks and spoofing.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their valuable comments and suggestions. This work was supported by Ministry of Education - China Mobile Research Fund (MCM20170306) and the National Natural Science Foundation of China [grant numbers 71872061, 71702045]

REFERENCES

Ding, W. (2015). Block chain based instrument data management system. *China Instrumentation*, *10*(1), 15-17.

Han, S., Pu, B.M., & Li S.X.(2018).Application of Blockchain Technology in Digital Asset Security Transaction. Computer system application , 27(3), 205-209.

He,J.(2018). Intellectual Property Protection and Legislation for Big Data： Challenges and Solutions. China Invention & Patent,3,29-33.

Lafuente, G. (2015). The big data security challenge. Network Security,2015(1), 12-14.

Li, J.Y.(2016). The Discussion of Big Data Trading Patterns. Mobile communication, 40(5),41-44.

Sun, Y.R. (2016). The Development of Cultural Industries and Intellectual Property Protection. Journal of Beijing University （Humanities and Social Sciences）, 124(2),22-26.

Wang, L., Gu, J.(2009). Intellectual Property Protection and Economic Growth in Developing Countries: An Empirical Analysis Based on Cross-Country Data. World Economic Research, 5, 48-51.

Yuan, Y., Wang, F.Y.(2016). Blockchain:The State of the Art and Future Trends, *Acta Automatica Sinica*, 42, 481-494

Zhang, N., Wang, Y., Kang, C., Cheng, J. N., & He, D. W. (2016). Blockchain technique in the energy internet: preliminary research framework and typical applications. *Proceedings of the CSEE*, *36*(15), 4011-4022.