IOP Conf. Series: Journal of Physics: Conf. Series **1168** (2019) 032051 doi:10.1088/1742-6596/1168/3/032051

The Research on Construction Mode of Business Information System Based on Blockchain Technology

Zhouquan Du[1,*], Jun Zhou[1], Hailong Wang[1] and Yang Lei[1]

[1]Institute of Electronic Equipment System Engineering Company, Beijing, China;

[*]Corresponding author e-mail: dzq2006610@163.com

Abstract. In order to explore the application of blockchain technology in business information system, the category feature and core technology of blockchain technology has been analyzed in this paper. Especially, the research has contained the data sharing interaction, tamper resistance, access rights and timeliness via combining the characteristics of business information system. The deployment application mode and miner distribution method were carried out after a lot of explored research, and some difficult problems that need to be solved were put forward too. Gratefully, the multiple advantages of blockchain technology have brought significant opportunities for business information systems to achieve the goal of acceleration and increasing efficiency.

1. Introduction

The blockchain was introduced in 2009 by Nakamoto Satoshi[1]. He also proposed a decentralized electronic currency system called bitcoin. Bitcoin has been actively running since 2009 and getting a large amount of public attention over the last year. As the first cryptocurrency, it was rated as the top performing currency in 2015 and has more than 300K confirmed transactions daily in May, 2017. Bitcoin represents a radical new approach to monetary systems and it could revolutionize the underlying technology of the payment clearing and credit information systems in banks, thus upgrading and transforming them[2].

In recent years, more and more people focus on the analysis and research on the blockchain technology and a lot potential applications based on it have appeared in many fields not only in virtual currency systems. It's also popular with the medical data access and permission management[3], the smart cities accelerating [4], the software engineering exploiting[5], etc. The blockchain technology has shown promising application prospects, and the research and analysis on its security and privacy issues would be on the way[6].

At the same time, the work of making standards for it also attracts people's great concern. The W3C organized a workshop to consider whether there are aspects of the blockchain technology which could be standardized in June 2016[7]. The IEEE announced the establishment of special interest group which works on standards and education about the blockchain technology in August 2016[8]. On October 2016, the International Organization for Standardization (ISO) has established the technical committees (TC) for developing new international standards concerning blockchain and electronic distributed ledger technologies[9]. Similarly, other standards organizations are also considering how to approach this issue[10].

Otherwise, blockchain technology has not yet been clearly defined. Speaking in detail, the blockchain technology is a brand-new distributed infrastructure and computing paradigm which chooses blockchain data structures to verify and store data, chooses distributed node consensus

algorithms to generate and update data, chooses cryptographic methods to secure data transmission and access, and chooses smart contracts to program and manipulate data. In brief, blockchain technology is a chained data structure in which data blocks are sequentially connected in a time-ordered manner, and it ensures non-falsifiable and unforgeable relying on cryptographically.

2. Related knowledge of Blockchain

From the birth of the first blockchain system Bitcoin, the blockchain technology has experienced a great development. In the blockchain 1.0 stage, the blockchain technology is mainly used for cryptocurrency. In addition to Bitcoin, there are many other types of cryptocurrencies, such as Litecoin, Dogecoin and so on. In blockchain 2.0 stage, smart contract is introduced so that developers can create various applications through smart contracts.

2.1The Classification of Blockchain

The UK Government Office for Science provides a report about the classification based on permission regarding the use and maintenance of the integrity of the ledger[11]. They classify the blockchains into three types, and the first one is called unpermissioned blockchain which can be used and maintained by anyone. The second one is called permissioned public blockchain which can be used by anyone, but only maintained by the trusted nodes. The last one is called permissioned private blockchain which can be only used and maintained by their owner. From now on, this type of classification based on permission for read and maintenance functions is widely used and accepted.

Similarly, another classifications considers the source of control for the permission of read and maintenance functions in the system. It also summarized as three categories of blockchains, and the first one is named as public blockchain which can be read or maintained by anyone. The second one is named as consortium blockchain which is under the control of a financial consortium responsible for maintenance functions. The last one is named as fully private blockchain which can be controlled by only one entity[12].

2.2The core Technology of Blockchain

In order to solve the issues of trust and security in the transaction. The blockchain technology makes out four technical innovations which are the core idea of it.

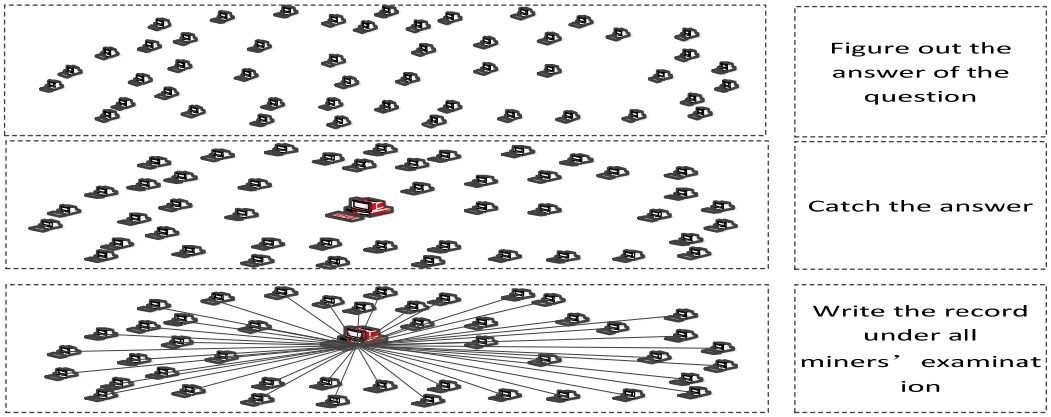

Figure 1. Competing for billing rights

- Distributed ledger is the first key technology, which means that the transaction accounting is performed by multiple nodes which are distributed in different places. Each node will record a complete account so that they can participate in monitoring the legitimacy of the transaction all together and testify for each other. With large different from the traditional centralized billing plan, there is no single node could record the account individually which could avoid the possibility of a single bookkeeper being controlled or bribed to make a false accounting. On the other hand, if the number of nodes is large enough, the account data will not be lost or damaged unless all the nodes are destroyed. The situation will not happen in theory and the account data will be stored completely.

- Another essential technology is asymmetric encryption and authorization technology, which assigns a private key for each agent and a public key shared with all other agents. The transaction information stored on the blockchain is public, but information of the account identity and some private data is highly encrypted. To ensure the security and personal privacy of those data, they could be accessed only when the data owner authorizes it.
- The third core technology is consensus mechanism, which guarantees the reliability and consistency of the data and transactions without a third-party trusted authority. The method can not only solve how to determine the validity of a record but also avoid the data to be tampered. There are many consensus mechanisms [13]such as PoW (Proof of Work), PoS (Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), DPoS (Delegated Proof of Stake), PoB (Proof of Bandwidth) [14], PoET (Proof of Elapsed Time) [15], PoA(Proof of Authority) [16] and so on. Different consensus mechanisms will suit for different application scenarios and achieve a balance between efficiency and security. For example，the bitcoin selects the PoW, and you can forge a non-existent record if more than 51% of the accounting nodes have been controlled by you in the entire network. It will not be an easy work when the nodes is many enough,so it is impossible to forge.
- The last but not least one is smart contract, which can execute some predefined rules and terms automatically based on these trusted and irrevocable data. Taking the insurance as an example, it is easy to apply for claims automatically in some standardized insurance products if everyone's information is authentic and reliable. So the smart contract can function well forever if all factors have been considered when it was designed and put out.

3. The actual problem in business information system

There is an urgent need for information sharing and data fusion between business information systems. And the traditional deployment model has seriously limited the development of business systems. How to realize the interaction and sharing of information with safe, reliable and fast has become the key to maximize the benefits of informatization.

3.1The Sharing and Interacting of Data

The decentralized idea in blockchain technology, there is no centralized hardware or management organization with distributed accounting and storing. The rights and obligations of nodes are equal to each other, and the data blocks are maintained together by the nodes with maintenance functions.

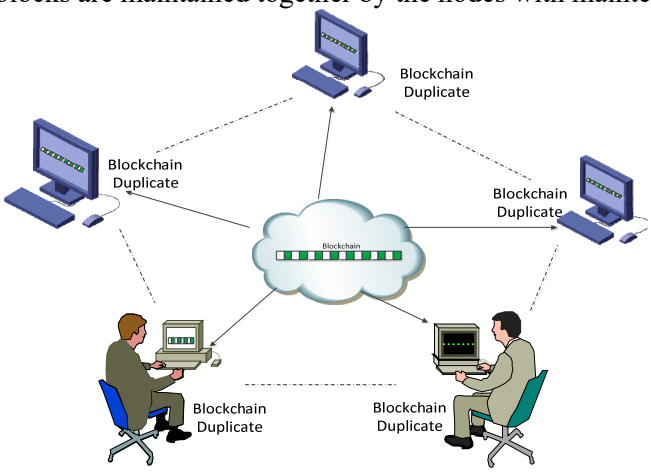

Figure 2. Each miner has the full-scale blockchain

In the application of business information systems, distributed billing technology is adopted, and several typical nodes are selected as the representatives of each business information system to participate in recording the behaviors and data interactions between the business information systems. These nodes and data are existed in one network, and all business systems have nodes to participate in the accounting of the entire network. So each business system node stores the network-wide data

completely, which facilitates the users of each business information system to query or access the corresponding data stored at the billing node directly after gaining the authorization from the data owner. This will reduce the cumbersome process of data exchange, transmission, and conversion.

3.2The Security against Tamper of Data

The blockchain technology has the features of high-redundancy storage, decentralization, high security and privacy protection, which make it be suitable for storing and protecting important private data particularly. It could avoid the data lost and damaged in large scale caused by centralized organizations attacked or improper management of rights. It also could prevent the hidden dangers of being tampered due to data highly centralized, and strengthen the supervision and management of data usage. Each node in the system has the most complete and newest database backup. Falsifying the database a single node is invalid because the system will compare automatically and regard the same data record which appears the most times as truth.

In the business information system, once the blockchain technology has been used for data recording, each accounting node will store a complete network-wide data according to its characteristics. The upload and exchange of information will be under the supervision and inspection of all the participating nodes. Each record will accept the review of all the accounting nodes and reach a consensus, otherwise it will not be wrote in the blockchain. So each accounting node only can make changes to the existed data with the audit approval of all the participated nodes.

In addition, when an accounting node malfunctions or a new node participates in accounting, it could download from other nodes to update the stored data. This mode makes sure the date in each node are consistent with the entire network nodes, and prevents the network-wide data from being tampered and damaged when individual nodes have been attacked or destroyed.

3.3The Access Right of Data

Even though each node will store the network-wide data with the blockchain technology, some of the data are not public and only accessed by few users. This demand of access under control is resolved perfectly through asymmetric encryption and authorization technology. The transaction information stored on the blockchain is public and transparent, which could be look up and applied for developing related applications for everyone. The information of account identity and some data transmitted is highly encrypted, and it could be accessed only when the data owner authorized in order to ensure the security of data and personal privacy.

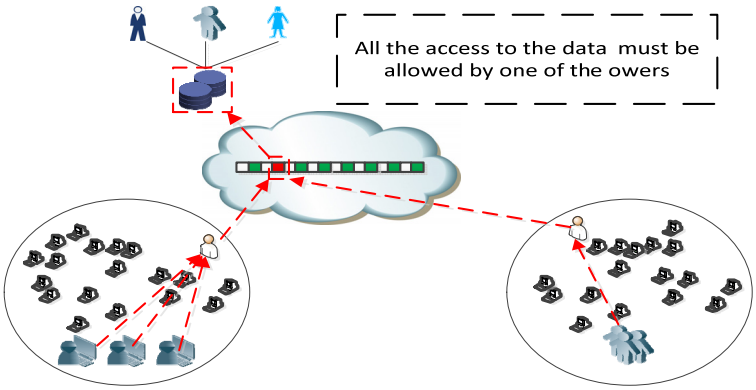

Figure 3. The control of data access right

In the business information system, the records of data interaction and users' behavior are open and transparent, but the business data is highly encrypted as same as the user ID if necessary. The signature technology in blockchain provides an ability to configure the access right flexibly, which could be accepted to achieve the requirement of access under control. With the appropriate rules of private key authorization, it is easy to realize the full-life access monitoring and limited propagation of the information stored in blockchain.

For example, when the data belong to a business system completely, it can decide independently whether provides an authorization for the access and download or not. And it also has the right of the data modification and update all by oneself. When the data is owned by multiple systems together, the data modification and update would be approved by all systems and the access and download of the data would be authorized by one or more systems which has been formulated in advance.

3.4The Timeliness of Data

The timestamp technology of the blockchain will write time information in each data record to form an unchangeable and unforgeable data block. Each block also contains the index information and verification information of the previous one and they are connected end to end sequentially. There are entire history data from the first block to the latest block, and the query function provided by the block chain can be used to trace the source of the recorded data and verify it one by one.

In the business information system, each interaction information record has timestamp, and the delivery and sharing of business data can be traced back to the specific time and source. At the same time, the rules for data sharing and publishing should be setting to check whether the data is still effective. And the time-stamp technology could be used to analyze and sort the published information to remind the relevant users with a data invalidation notification.

4. The consideration of applying the blockchain in business system

In the bitcoin, each miner is encouraged to join transaction accounting and only the one that successfully solves a cryptopuzzle is allowed to record a set of transactions and to collect a reward. The more mining power a miner applies, the better are its chances to solve the puzzle first. This reward structure provides an incentive for miners to contribute their resources to compete the accounting rights. All the miners consume large resources, but only one could gain the reward.

From the perspective of avoiding serious waste of resources, it is necessary to optimize the mechanism of mining. For example, making a new certification rule for miner can reduce the number and regulate the distribution and composition. And make an alternation mechanism to change the miner periodically ensuring majority of them are honest that is the miners follow the bitcoin protocol as prescribed[17]. The new miner could be generated randomly or recommend, and it is better to be different from the previous one. When the term of one miner is expired, the new one will take over its job and download the network-wide data. Each miner keep the network-wide data, while the lightweight nodes served by the miners would download relevant data on-demand to save space.

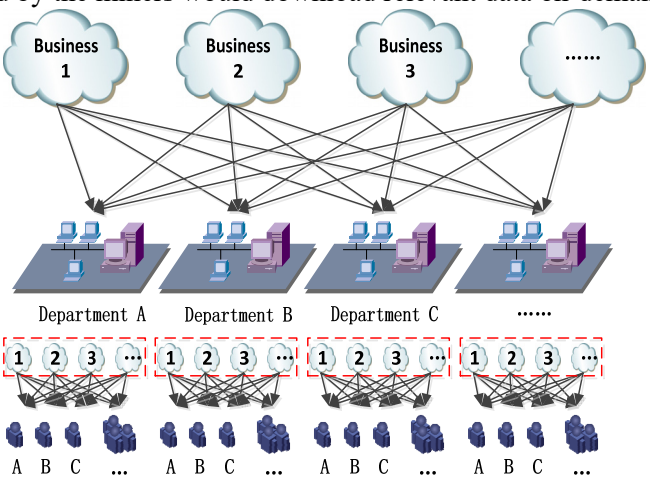

Figure 4. The deployment mode of business information system

In the business information system, it is similar to the consortium blockchain. Each business information system would be deployed in different department for more than one person, and each person would make use of more than one business information system. Considering the decentralization and the practical application scenario, the idea of decentralization-centralization-decentralization is

feasible. First, it could divide the users into clusters through drawing up some rules relying on the regional, the category of business information system and so on. Then, assign some places of miner for each cluster combining with the actual situation. The miners are decided by each cluster and changed regularly. After then, make a rule for the miners to participates in recording the information. The right of recording a set of transactions is distributed to one of the miners randomly and each transaction will be examined and verified by all miners.

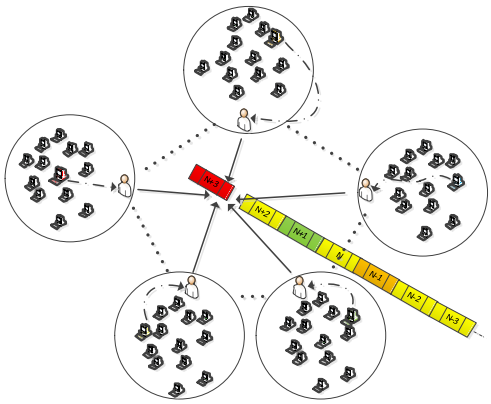

Figure 5. The transactions record based on the clusters

The several situation is considered as follows and the events occurred are called as transactions.

- When a transaction occurs in one cluster, all the participants in the cluster will verify and record, then submit it to their miners. One of the miners will apply a data record for intra-cluster transaction and write it into the blockchain after summarizing and analyzing the messages from the participants.
- When a transaction takes place in clusters, all the participants in the related clusters will confirm and record, then submit it to their miners. And all the miners will make a note of it to check the request for data record from one miner of the related clusters.

In a word, the miner participates in all the transactions, the participants only take part in the cluster which is related to them. It is decentralized among the participants in a cluster just like the relationship among the miners, while it is centralized between the participants in one cluster and their miners.

5. The hidden danger

5.1How to ensure the security of data

The character of anonymous can only guarantee the anonymity within the blockchain. In the blockchain, it is not necessary to check the information of the participants, so it is not easy to contact the account with its actual user. But the data is public and transparent in blockchain, there are many methods to analyze the connection between anonymous accounts and actual users with the information from the network environment. For example, there are some connection among the data of user's transaction status, IP address, habits, etc. A little traces could be found and exploited by the hackers especially.

In the business information system, the privacy of each miner is also significant. It could be public in a limited range if necessary in the same system, but it is a secret for others. Otherwise, all the miner would be in danger if one of them has been controlled by attacker. At the same time, the data stored in each miner is also a security hidden danger. The illegal access need more detail and reliable research. It would be a great issue about applying the blockchain technology in the business information system.

5.2How to record unverifiable information

In the business information system, how to judge whether an information from a business system is true or not. Is there any way to help the related system to make a select? Because of the speciality of the

business information system, some data are produced by itself without any relationship with others. In another word, they say it is what, and it is. If the miner in each system is one of the few, there is a big risk on the security if one of them has been attacked and captured. In addition, there are differences in the limits of authority for different department, which means the information from a department with higher authority would not be verify by the miner from a department with lower authority. So it is a question to make sure the accuracy of each information before wrote in blockchain.

6. Conclusion

In general, blockchain technology brings new opportunities and challenges to business information system. There are many advantage features which can resolve a lot of difficult problems and provide more than one solution. However, it is necessary to choose the appropriate methods for specific problems instead of blindly following. In addition, the experience should be accumulated continuously and the measures of safety protection should be paid more attention, which are good to ensure security and reliability at the same time of increasing convenience and efficiency.

Acknowledgments

We would like to thank the anonymous referees for their valuable comments on our paper.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.
[2] Ye G, Chen L. Blockchain application and outlook in the banking industry[J]. Financial Innovation, 2016, 2(1):24.
[3] Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using Blockchain for Medical Data Access and Permission Management[C]// International Conference on Open and Big Data. IEEE, 2016:25-30.
[4] Sun J, Yan J, Zhang K Z K. Blockchain-based sharing services: What blockchain technology can contribute to smart cities[J]. Financial Innovation, 2016, 2(1):26.
[5] Xu X, Pautasso C, Zhu L, et al. The Blockchain as a Software Connector[C]// Software Architecture. IEEE, 2016:182-191.
[6] Li X, Jiang P, Chen T, et al. A Survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2017.
[7] W3C, "Blockchains and the Web Report," Jun-2016. [Online]. Available:https://www.w3.org/2016/04/blockchain-workshop/report.html.
[8] IEEE, "Getting Linked to the Blockchain,"The Institute, Aug-2016. [Online]. Available:http://theinstitute.ieee.org/technology-topics/computing/getting-linked-to-the-blockchain.
[9] MEXT, "The ISO Will Start Discussion on International Standardization of Blockchain Technologies,"Oct-2016. [Online]. Available: http://www.meti.go.jp/english/press/2016/1007_05.html.
[10] Anjum A, Sporny M, Sill A. Blockchain Standards for Compliance and Trust[J]. IEEE Cloud Computing, 2017, 4(4):84-90.
[11] Parkin A, Prescott R. Distributed ledger technology: Beyond the hype[J]. Journal of Digital Banking, 2017.
[12] V. Buterin, "On Public and Private Blockchains,"2015. [Online]. Available:https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.
[13] Zheng Z, Xie S, Dai H, et al. Blockchain Challenges and Opportunities: A Survey[J]. International Journal of Web & Grid Services, 2017.
[14] Jansen R. A TorPath to TorCoin:Proof-of-Bandwidth Altcoins for Compensating Relays[J]. 2014.
[15] Chen L, Xu L, Shah N, et al. On Security Analysis of Proof-of-Elapsed-Time (PoET)[J]. 2017.
[16] Angelis S D, Aniello L, Baldoni R, et al. PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain[C]// Italian Conference on Cybersecurity. 2018.

[17] Eyal I, Sirer E G. Majority Is Not Enough: Bitcoin Mining Is Vulnerable[J]. 2014, 8437:436-454.