Decentration transaction method based on blockchain technology

Qi Liu[1]，Kenli Li[2]
(1. College of Information Science and Engineering, Hunan University, Changsha Hunan 410082, China;
(2. College of Information Science and Engineering, Hunan University, Changsha Hunan 410082, China
kanye91635@163.com

***Abstract*—In recent years, the bitcoin has provided great opportunities and challenges for modern financial industry, and then the blockchain technology which supports bitcoin has attracted more and more attention. In this paper, we propose a novel decentration transaction approach based on blockchain technology. Transaction data in the digital monetary system model with blockchain technology contains the transaction information of digital currency circulation, and the account information of the digital currency owner. A blockchain is constructed by a unique sequence through saving the functions of former block. The formation of a chain depends on the system time of each node, which is related to the real sequence obtained the block. A block is made up of block head and block body, and. The block contains all the relevant information about the transaction, and the block head contains the previous block's hash value, timestamp, random number, difficulty coefficient and the Merkle root hash value. Finally, block synchronization between two nodes is given.**

Keywords- Decentration transaction, Blockchain technology, Bitcoin, Hash value

I. INTRODUCTION

With the rapid development of information technology, we have gone into an era of information explosion, interpersonal cooperation, competition and trust has been more and more important [1][2]. As Information resource is the most valuable resource, if information has been lost, it may bring great losses [3]. However, existing methods of recording information is not able to show that the information belongs. Furthermore, as the information is easy to be lost, we live in a world where information cannot be completely trusted, at the same time, the legitimate rights and interests are threatened [4]. Blockchain is regarded a key technology of bitcoin, which is able to handle the mutual trust between people, which has made a meaningful attempt to protect user information security [5][6].

From 2009, the bitcoin suddenly broke into the area of technology and finance. The blockchain technology which supports bitcoin has attracted more and more attention [7][8]. Currently, almost all industry, especially the financial industry, is interested in the blockchain application [9]. Block Chain is regarded as a technical solution, and it denotes a novel application of computer technology, including Distributed Date Storage, Point-to-Point Transmission, Consensus Mechanism, and Encryption Algorithm. The main features of Blockchain lie in that 1) decentralization, 2) safe, 3) effectiveness, 4) reliability, and 5) flexibility especially in financial field. From 2015, Blockchain has experienced fast development from all above the world [10][11]. Many different institutions have concentrated on Blockchain, such as Central Banks, Government Departments, Commercial Banks, IT company [12][13].

II. OVERVIEW OF BLOCKCHAIN TECHNOLOGIES

Transaction data in the digital monetary system model based on blockchain technology is described as two aspects, a) the transaction information of digital currency circulation, and b) the account information of the digital currency owner [14][15]. When the central bank produces the digital currency, it is crucial to simultaneously satisfy the privacy of the protection and main of social order [16]. Hence, in order to achieve this aim, the blockchain is realized using the license chain. Central bank and commercial banks both protect digital currency running books, and are responsible for the verification and saving transactions of commercial banks [17][18]. In addition, the central bank is able to reach transaction information, however, it cannot be permitted to visit the account information [19][20]. In financial supervision, e.g. anti-money laundering, the central bank is able to invite commercial banks to provide particular information to avoid crime. Based on the above analysis, internal framework of the blockchain system is illustrated in Fig.1.

Fig. 2 illustrates that a blockchain is established by a unique sequence through recording the functions of former block. The formation of a chain relies on the system time of each node, which is corresponding to the real sequence obtained the block. Then, new obtained blocks are saved in all network nodes when it has been admitted by the network. As the mathematical properties of the hash algorithm, when the formation of a chain is given, block contents and its sequence should not be changed. A blockchain contains a lot of blocks, and a block is made up of a lot of transactions.

0-7695-6368-6/18/$31.00 ©2018 IEEE
DOI 10.1109/ICITBS.2018.00111

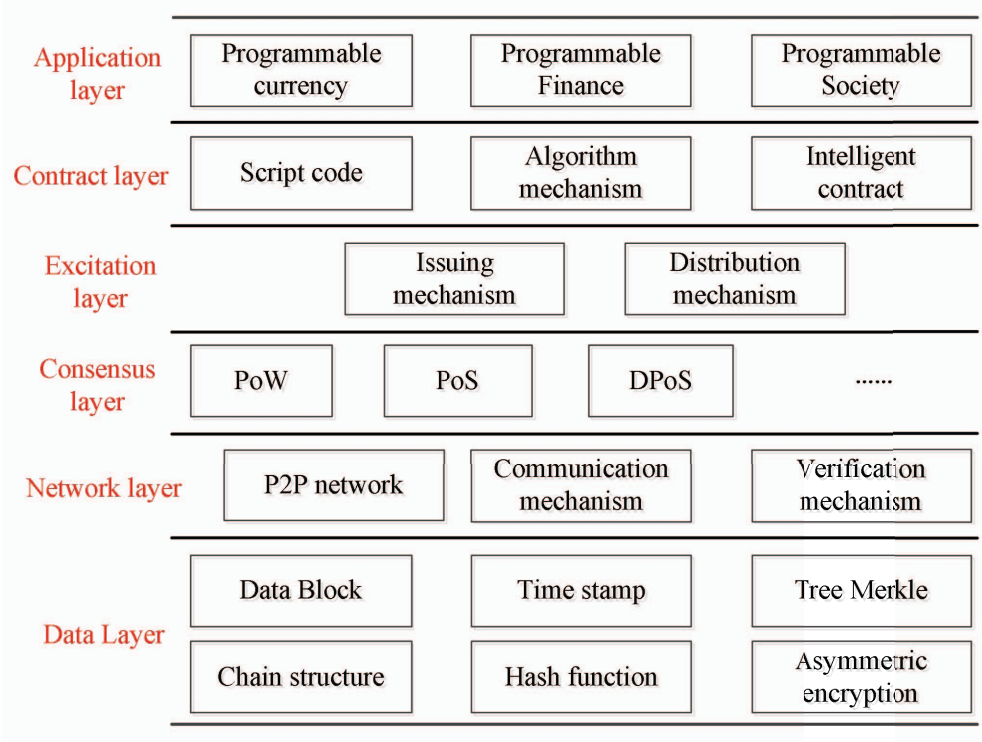

Figure 1. Framework of the blockchain system

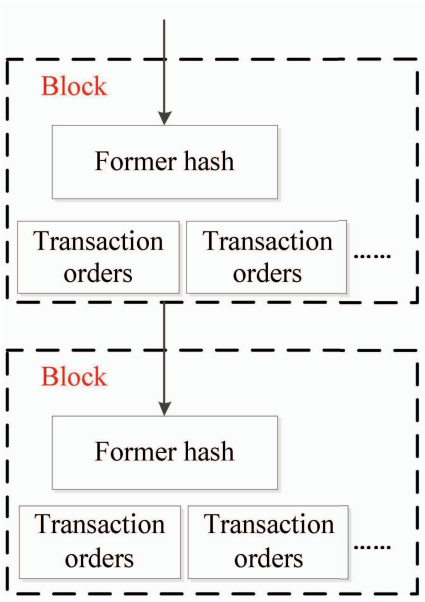

Figure 2. Internal structure of the blockchain.

III. DECENTRATION TRANSACTION METHOD BASED ON BLOCKCHAIN

The data layer encapsulates the data structure of the block and the content related to the data encryption. The block structure is shown in Fig. 3. A block is divided into two parts: 1) the block head and 2) the block body. The block contains all the relevant information about the transaction, and the block head contains the previous block's hash value, timestamp, random number, difficulty coefficient and the Merkle root hash value. Merkle tree is used to identify a unique transaction in the block. These elements can generate hash values with hash generation algorithm, the chain structure is constructed by matching the hash value and parenthash. In addition, the longest chain is called as main chain. The time stamp in the block ensures the order of the block, and has a certain preventive effect on the tampering or forgery of the block data. The difficulty coefficient is used to dynamically adjust the difficulty, and maintain a time floating in the expected time on at the same time. Furthermore, the coefficient of difficulty represents the workload of verification basis.

Various blockchain systems may utilize various block synchronization processes. In the proposed system, node A is able to request block synchronization from node B, and the block synchronization process is illustrated as follows.

(1) Node A requests the header of the latest block from node B. This step is completed via transmitting a GetBlockHeaders message. Then, Node B should answer to node A. In addition, a BlockHeader message which includes the block header requested by A.
(2) Node A requests MaxHeaderFetch blocks to search ancestor from node B. The default value of MaxHeaderFetch is set to 256. However, the number of block headers transmitted from node B to node A is allowed to be smaller than it.
(3) If A cannot detect ancestors, node A sends GetBlockHeaders message
(4) When node A has found a common ancestor, Node A requests block synchronization from the common ancestor.

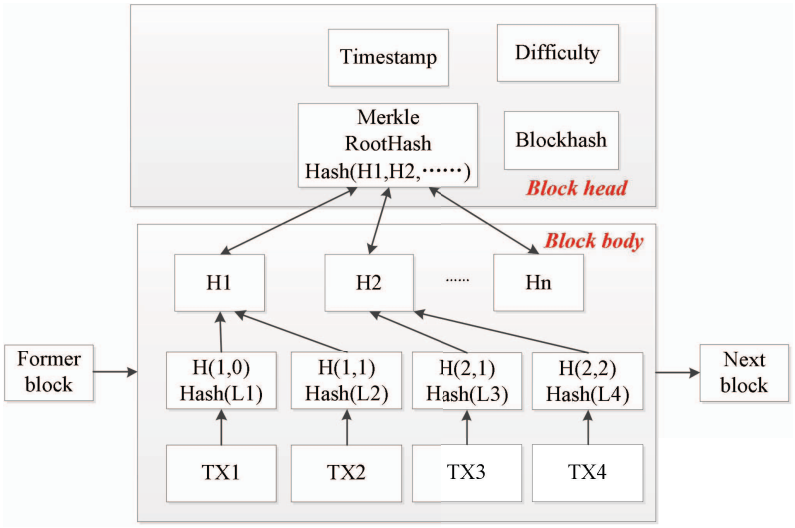

Figure 3. Structure of the block

Block synchronization between two nodes is shown in Fig. 4.

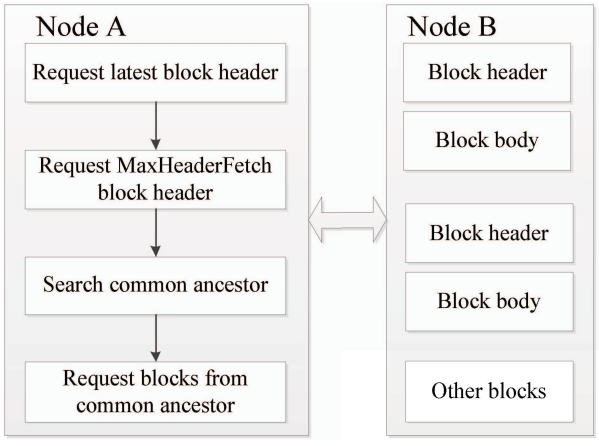

Figure 4. Block synchronization between two nodes.

IV. CONCLUSION

This paper proposes a new decentration transaction method based on blockchain technology. Transaction data in the digital monetary system model with blockchain technology contains the transaction information of digital currency circulation, and the account information of the digital currency owner. In addition, the construction of a chain greatly relies on the system time of each node, which is influenced by the real sequence obtained the block. A block is made up of all information about the transaction, and the block head contains the previous block's hash value, timestamp, random number, difficulty coefficient and the Merkle root hash value. We also provide the block synchronization process.

REFERENCE

[1] T. Aste, P. Tasca and T. Di Matteo, Blockchain Technologies: The Foreseeable Impact on Society and Industry, Computer, 2017, 50(9): 18-28

[2] I. Eyal, Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities, Computer, 2017, 50(9): 38-49

[3] Z. C. Kennedy, D. E. Stephenson, J. F. Christ, T. R. Pope, B. W. Arey, C. A. Barrett and M. G. Warner, Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology, Journal of Materials Chemistry C, 2017, 5(37): 9570-9578

[4] J. Kogure, K. Kamakura, T. Shima and T. Kubo, Blockchain Technology for Next Generation KT, Fujitsu Scientific & Technical Journal, 2017, 53(5): 56-61

[5] T. T. Kuo, H. E. Kim and L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, Journal of the American Medical Informatics Association, 2017, 24(6): 1211-1220

[6] M. Orcutt, The System Behind Bitcoin Is Easing the Plight of Refugees Finland's digital money system for asylum seekers shows what blockchain technology can offer the unbanked, Technology Review, 2017, 120(6): 24-24

[7] M. E. Peck, Do You Need a Blockchain? This chart will tell you if the technology can solve your problem, IEEE Spectrum, 2017, 54(10): 38-+

[8] J. J. Sikorski, J. Haughton and M. Kraft, Blockchain technology in the chemical industry: Machine-to-machine electricity market, Applied Energy, 2017, 195(234-246

[9] P. Treleaven, R. G. Brown and D. Yang, Blockchain Technology in Finance, Computer, 2017, 50(9): 14-17

[10] Y. Zhang and J. T. Wen, The IoT electric business model: Using blockchain technology for the internet of things, Peer-to-Peer Networking and Applications, 2017, 10(4): 983-994

[11] A. F. Bariviera, M. J. Basgall, W. Hasperue and M. Naiouf, Some stylized facts of the Bitcoin market, Physica a-Statistical Mechanics and Its Applications, 2017, 484:82-90

[12] A. Beall, Bitcoin energy bill matches Ecuador's, New Scientist, 2017, 236(3150): 8-8

[13] Wang wenchao, liao xiaobing, luo jun.Journal of power science and technology,2015,30(4):91-95

[14] E. Bouri, R. Gupta, A. K. Tiwari and D. Roubaud, Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions, Finance Research Letters, 2017, 23:87-95

[15] A. S. Hayes, Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin, Telematics and Informatics, 2017, 34(7): 1308-1321

[16] K. Hong, Bitcoin as an alternative investment vehicle, Information Technology & Management, 2017, 18(4): 265-275

[17] H. Huang, X. F. Chen, Q. H. Wu, X. Y. Huang and J. Shen, Bitcoin-based fair payments for outsourcing computations of fog devices, Future Generation Computer Systems-the International Journal of Escience, 2018, 78:850-858

[18] P. Katsiampa, Volatility estimation for Bitcoin: A comparison of GARCH models, Economics Letters, 2017, 158:3-6

[19] T. Kim, On the transaction cost of Bitcoin, Finance Research Letters, 2017, 23:300-305

[20] G. Psaila and P. Garcia-Bringas, Blockchain: challenges and opportunities beyond bitcoin, Dyna, 2017, 92(5): 517-521

[21] M. B. Taylor, The Evolution of Bitcoin Hardware, Computer, 2017, 50(9): 58-66