ATLANTIS PRESS
Advances in Social Science, Education and Humanities Research (ASSEHR), volume 184
2nd International Conference on Education Science and Economic Management (ICESEM 2018)

The Application of Blockchain in Auditing

Xiaozhen Jiang
Fuzhou University of International Studies and Trade, 350202

***Abstract*—As one of the most cutting-edge technologies in Fintech, the application of blockchain has been prevailing across a series of industries. By adopting literature research, this paper analyzes the origin, characteristics and working principle of blockchain. According to the features and requirements of traditional auditing, this paper finds the superiority of blockchain technology, for example, distributed ledger, consensus mechanism and timestamp could facilitate auditing in three ways: (1)improve timeliness of auditing and reduce auditing cost; (2)ensure data integrity and realize automatic auditing; and (3)realize pre-warning and real-time supervision to reduce auditing risk. However, although blockchain has brought unprecedented opportunities to the development and reform of audit industry, the blockchain technology still faces a number of challenges, such as data security, talent and technology support, industry and recognition promotion, and practical application and execution. Concerning these limitations, this paper looks forward to further research field which could contribute to the upcoming improvement of blockchain auditing.**

Keywords—Blockchain; Distributed ledger; Decentralization; Auditing

I. INTRODUCTION

In the 19th National Congress of Communist Party of China, President Xi Jinping put forward the notion that building a powerful nation of science and technology to support the modern economic system. As a cutting-edge technology in the digital era, blockchain fits the strategy perfectly by its technology superiority and features. Auditing, as an indispensable part of the economic activities, is in pursuit of reform and automation with the promotion of Financial Shared Service Center (FSSC) and big data processing. So far, the enthusiasm of blockchain technology has been prevailing throughout a diversity of industries. And the auditing profession has been eyeing blockchain with interest. Therefore, it is of great significance to analyze the application of blockchain in auditing.

In November 2008, a man under the pseudonym Satoshi Nakamoto published the paper titled " Bitcoin: A Peer-to-Peer Electronic Cash System " in the bitcoin forum, which put forward the concept of "blockchain" for the first time. In January 2009, the bitcoin network was formally launched. The first 50 bitcoins were mined by Satoshi Nakamoto, marking the birth of the first block " Genesis Block". Then, Satoshi Nakamoto sent 10 bitcoins to a cryptography expert, which is the first transaction paid by Bitcoin in history. From then on, the Peer-to-Peer electronic cash system was put into practice. In the open protocol project created by Satoshi Nakamoto, the data was stored in different blocks, which are linked together in chronological order to form a chain ,then the "blockchain" came into being. In May 2010, an American programmer in Florida purchased 25 dollars worth pizza coupons with 10 000 bitcoins, resulting in the first fair exchange rate of bitcoin. In 2015, the Nasdaq Stock Exchange launched Linq platform, which uses blockchain digital ledger technology to issue stock and record stock transactions. So far, all the major financial institutions across the world, such as the New York Stock Exchange, Barclays Bank, Deutsche Bank and Citigroup Group, have carried out the blockchain technology applications through different channels to create efficient, convenient and low-cost trading systems.

At present, the development and prospect of blockchain technology are mainly embodied in three stages: blockchain 1.0, 2.0 and 3.0. Block chain 1.0, represented by encrypted digital currencies such as bitcoin, has been the most successful application of blockchain technology until now, making the currency issuance free of reliance on central banks. The blockchain 1.0 applications include payment, exchange and currency transfer. Block chain 1.0, though having a high starting point, is also facing some restrictions such as governments' supervision. The core of blockchain 2.0 is the deep integration of intelligent contract and life scenario. And Ethernet developed in 2013 is representative of blockchain 2.0. At this stage, its application can extend to a series of economics, market and financial activities such as stocks, bonds, property rights and intelligent contracts etc., which go far beyond cash currencies. The application of blockchain 3.0 has surpassed the monetary and financial fields, covering all aspects of social life, such as government, healthcare, art, culture and logistics. In this stage, information doesn't need the trust of a third party any more, but to fulfill self-proof through information sharing, and thus the operation efficiency of the whole social system can be dramatically improved. At present, we have gone through the stage of blockchain 1.0, and are moving steadily from block chain 2.0 to 3.0. KlausSchwab, the founder of the Davos forum, believes that as an important achievement of the fourth industrial revolution, blockchain technology is expected to store 10% of the world's total GDP BY 2025.

II. THE APPLICATION OF BLOCKCHAIN IN AUDITING

A. The structure and principle of blockchain

In a narrow sense, block chain is a chain data structure composed of data blocks combined in chronological order. And it's a distributed ledger could not be tampered or forged with the guarantee by cryptography. In a broad sense, blockchain technology is a new distributed infrastructure and computing paradigm that uses block chain data structure to verify and store data, applies distributed node consensus algorithm to generate and update data, makes use of cryptography to ensure the security of data transmission and access, and exploits intelligent contracts composed of automated scripts and codes to program and operate data. As the supporting technology of Internet finance, blockchain integrates the knowledge of mathematics and economics, and combines cryptography, time stamp, distributed technology and consensus mechanism. In essence, blockchain is a decentralized bookkeeping system, which is supported by computer network and consensus mechanism. In the context of trustlessness (with no third party as intermediary),the information and data are recorded and stored through distributed ledger, and finally peer-to-peer transaction is completed and the account book is updated in real time. From the perspective of financial accounting, blockchain, a large network account book with computer programs as the supporting technology, is characteristic of public and transparent information. If we take blockchain as the physical account book, then the digital currency is the bookkeeping unit in the blockchain. Each block is equivalent to the page in the physical account book, and the information stored in a block is equivalent to the transaction activities recorded in the book page.

Block is the storage unit in a blockchain, which includes four major elements, they are the hash value of the previous block, the timestamp of the current block, the generated random number and the number of hash tree in the current block(as shown in Figure 1). Each block links the previous block with the hash value of the previous block, and records the transaction time through timestamp. And the Proof of Work(POW), which is generated by the block calculation, is rewarded to encourage the system participants to provide continuous calculation; finally, the number tree of hash value in the current block represents the key array of the stored transaction information.

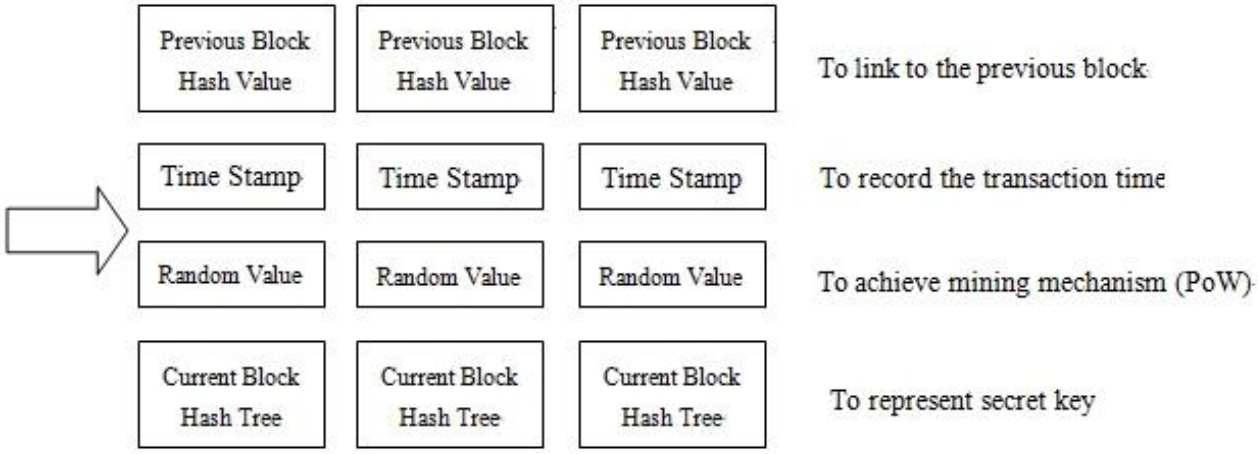

Fig. 1 The structure of blockchain

According to the degree of openness, blockchains can be divided into public blockchain, consortium blockchain and private blockchain. The public chain is represented by bitcoin and Ethernet. It has no access requirements and is open to all, so anyone can participate in it. The consortium blockchain is represented by Hyperledger and R3. Authorization is needed for access and exit, and it is only open to specific organizations and groups. The private chain is represented by Overstock, which is only open to individuals or entities. Because the latter two need authorization for access nodes, they are also known as license chains.

Transaction and block are two components of blockchain. The operation process and working principle of blockchain are shown in Figure 2. When a new transaction is generated, the information will be recorded in one node and be transmitted to other nodes for verification. Therefore, for any new transaction requests, the transaction information should be sealed and encrypted first, and then the hash function is applied to calculate the only hash value representing the transaction to all nodes in the blockchain network. Each node collects the newly generated transaction requests and concentrates them into a block, so each block may contain hundreds of pieces of different transaction information. After receiving the hash value of the to be verified transaction, the first node that figures out the result through the PoW method will finally verify the transaction and get the reward. At the same time, the first node that figures out the result broadcasts the newly generated block to all nodes. Once receive the notification ,the other nodes will confirm the authenticity and validity of the transaction in the newly generated block, then accept the block and connect it to the blockchain if it is confirmed. From then on, the transaction information is irreversible once it is stored. After all the nodes accept the block, the other blocks that do not obtain the authentication power will automatically expire, each node regenerates new

blocks and carries out the next PoW calculation. Through block receipt and verification, the blockchain realizes the distributed management of data decentralization effectively. It is an innovation and breakthrough for the traditional centralized data management.

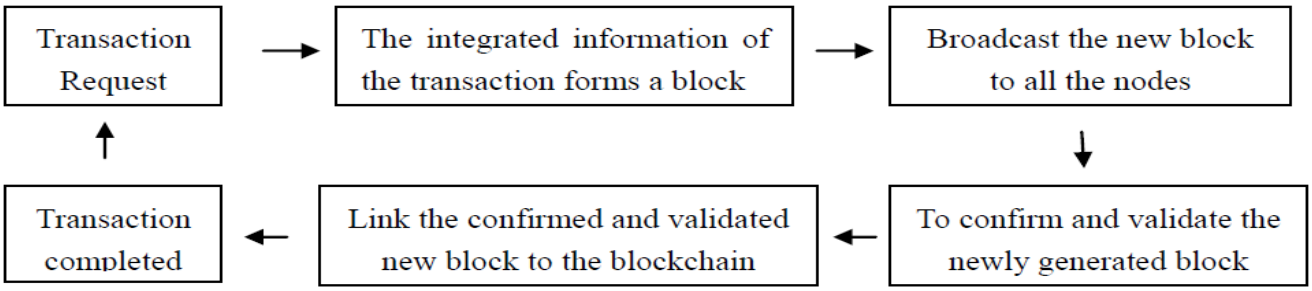

Fig. 2 Working Principle of Blockchain

B. The Characteristics and advantages of blockchain

Decentralization. All nodes in the blockchain network are qualified for record keeping and information storage. The transaction information and record do not need to be processed by the centralized nodes, and no third party agencies participate in the whole process of information processing. Therefore, all the nodes have equal rights and obligations to maintain all the data blocks in the network by decentralized distributed process. It enables the centralized authority credit to transform to decentralized algorithm credit.

Highly transparent and trustless. Unlike the traditional data storage, the open source programs of blockchain ensure that all nodes can update transaction information synchronously when any transaction occurs and provide historical data query and retrieval. Therefore, data information stored in block chains is not only highly transparent and fully shared, but also is under joint maintenance and supervision by all nodes in the network. In this process, no mutual trust between the transaction participants is needed, and the trust mechanism can be realized by synchronous real-time information processing in the blockchain network. This is what we called as trustless.

Collective maintenance. Because all the nodes in the system have the same rights and obligations to maintain and deal with the transaction information together, the data blocks are also under collective maintenance by all nodes in the whole network. Any user cannot easily modify the information, , the whole system will perceive it once any information changes , so that the data security is greatly improved.

Anonymous processing. Because the blockchain technology solves the trust problem, the parties of the transaction do not need to know each other to achieve safe and effective transaction. And there is no need to inform the counterparty the private information such as identity, to realize anonymous transaction.

The characteristics of the block chain not only improve the security and effectiveness for the transaction, but also solve the "double-spend problem" and the " Byzantine Generals' Problem" that have been long-troubling in the digital currency field. The "double-spend" problem is an attack where the given set of coins is spent in more than one transaction. Cash is a physical entity, so there will be no double-spend problem. However, in the traditional way, digital money needs intermediaries such as trustworthy banks to guarantee their payment for only once, otherwise the same amount of money will be repeatedly spent for two or even more times. The consensus mechanism of blockchain, which is realized through joint verification by all the nodes in the network, can guarantee that the transaction information (paid by digital currency) will be transferred only once, and the value transfer is realized in the process of information transmission, thus the "double-spend" problem is well solved. The Byzantine Generals' problem originally refers to the problem of reaching a consensus among distributed units if some of them give misleading answers. In the blockchain, it refers to how the users can avoid information transmission error due to system errors in the absence of a trustworthy intermediary or central nodes which ultimately affects the system consistency and causes the loss of both parties. The Byzantine Generals' problem is most frequently faced by the distributed system. Fortunately, the consensus mechanism in the blockchain technology provides a perfect solution for this problem. In the block chain network, all the transaction information will be broadcast to all other nodes in the system once the block is generated, and the transaction information will be stored in the whole network with the same record. Thus, the information is safe and transparent, and the Byzantine generals' problem is readily solved.

With the continuous development of information technology and the Internet, modern auditing is facing unprecedented challenges and reforms. The accounting processing and the output of the financial statements is automatically completed by the financial software by the application of the accounting computerization system. The traditional accounting documents and books are replaced by memories, then the corresponding original audit clues are disappearing. The computerized data is not traceable once modified, which leads to the distortion of the financial information. Therefore, the traditional tracking auditing is no longer applicable. There will be more reliance on the expertise and professional judgment of the auditors. In addition, during the traditional auditing process, data is usually stored on the central server, and a large amount of data will lead to overload and slowdown the software running speed. At the same time, traditional audit is also confronted with high personnel costs,

hardware and software maintenance and upgrading costs. The data stored in the blockchain is irreversible, safe, transparent and integrate, which is consistent with the needs of audit authentication. The features of the blockchain enable it to afford a wide range of applications in the field of accounting and auditing, such as traceable independent audit, property ownership tracing, trading and auditing certification. Professor Zhang Qinglong of National Accounting Institute points out that the blockchain technology has a huge impact on the external audit industry, which will have great influence on the construction of the current financial sharing center and bring drastic changes to the information and accounting flow.

III. THE ADVANTAGE OF BLOCKCHAIN AUDITING

A. Improve timeliness of auditing and reduce auditing cost

In the traditional auditing process, we must first design the interview plan and get the required auditing materials according to specific method and order before the auditing work gets started. In this way, auditors need to spend a lot of time and resources in collecting information and analyzing data, and cannot guarantee whether the information is correct and reliable. Even with the help of financial software, the process of identifying problems and coming to conclusions is still time consuming and costly. The blockchain technology can support the information authenticity and integrity, thus by applying the blockchain technology to auditing, the auditors do not need to confirm and verify the financial information anymore, which can greatly improve the timeliness of audit and accelerate audit projects. Auditing cost mainly includes one-time cost and recurrent cost, such as auditors' salary, software and hardware maintenance and upgrading cost, risk control cost etc. The blockchain technology doesn't require centralization, so the data processing capability of the central server is no longer the main threshold of audit work, thus reducing the requirements for hardware and software and saving the corresponding maintenance and upgrading cost. As long as the blockchain can run effectively, the transaction information stored in the block is timestamped and unmodified. The auditors and external regulators can monitor financial information in real time through blockchain, and inquiries and correspondence procedures are no longer needed to ensure the authenticity and accuracy of financial information, and then reduce the audit workload and thus the auditing cost.

B. Ensure data integrity and realize automatic auditing

In the traditional auditing, once the financial software is experiencing failure or hacker attack, the system is paralyzed and unable to recover. But the distributed ledger of blockchain ensures that the related transaction contents and information are recorded by all nodes and blocks in the network. Thus, if a node or block is experiencing failure or attack, the other nodes or blocks on the blockchain can still provide a complete and valid account book copy. At the same time, the specific encryption technology of blockchain can also greatly improve its ability to resist attacks, which reduces the auditing risk and ensures data integrity. Moreover, blockchain supports triple entry bookkeeping which could not only record the amount and content of a certain transaction ,but also the original documents. With the support of blockchain, we can improve audit efficiency and achieve audit automation. In this way, the transparency of transaction records is greatly improved, and all the information of transactions can be checked in the blockchain in real time. In addition, all the financial activities could be traced back according to the timestamp, which can eliminate the information asymmetry in the traditional audit.

C. Realize pre-warning and real-time supervision to reduce auditing risk

The blockchain technology could also upgrade auditing by improving auditing pre-warning mechanism. In the traditional auditing, we can only achieve early warning effect through auditors' supervision, but it is sub-real-time pre-warning. The blockchain technology could supervise all the data anomalies and modifications in real-time and make corresponding judgment. The pre-warning process is shown in Figure 3. Taking insurance business as an example, if the information provided by the policyholder is confirmed as true and valid, then a new block will be generated and connected to the blockchain. The transaction records are marked with timestamp, and are recorded by all the other participants in the blockchain network to make the data irreversible, unmodified, and traceable on the timeline. However, if the policyholder provides false information, the nodes and blocks in the network can detect the abnormal record in real time according to the data stored in the blockchain,, thus eliminating false information in real time and terminating the transaction before the establishment of the insurance business, so as to realize pre-warning. In the blockchain auditing, through the standard setting of key indicators and opening to the supervision department or the auditors, then the supervision department or the auditors can detect the potential risks in real time and take the timely countermeasures in any business activity recording process, so as to realize the real-time supervision and reduce the audit risk.

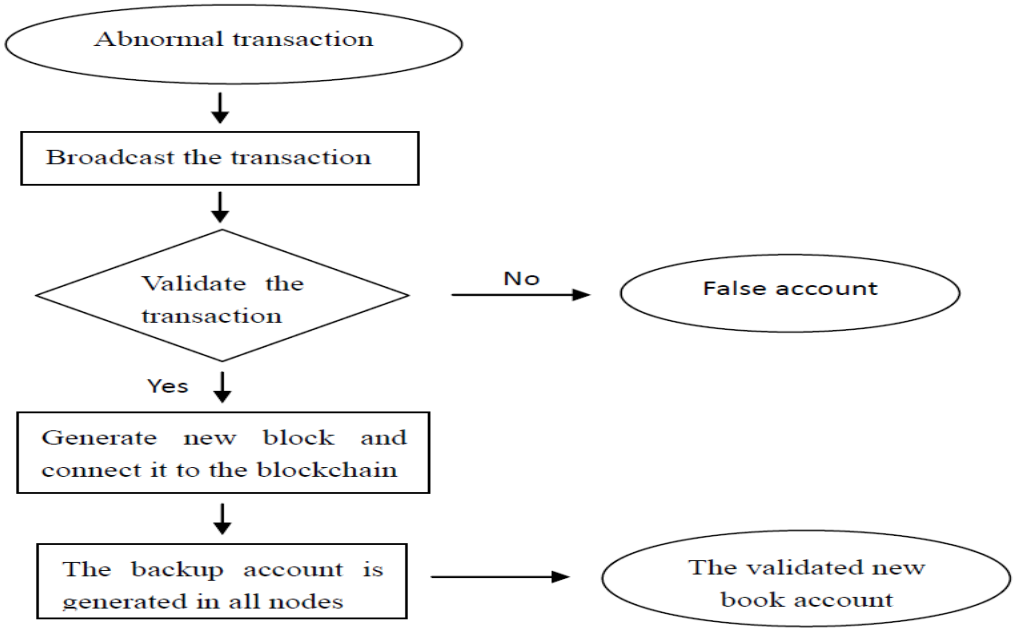

Fig. 3 The pre-warning mechanism of blockchain auditing

IV. THE PROBLEMS OF BLOCKCHAIN AUDITING

Block chain has brought unprecedented opportunities to the development and reform of audit industry by its features of distributed ledgers, consensus mechanism, trustless and encryption technology. However, blockchain technology is currently in the 2.0 stage, and still faces a number of challenges in practical application and execution.

A. Data security

The encryption technology , consensus mechanism and timestamp of blockchain can ensure that the data is unmodified. But the premise is data security, which is also the most critical challenge that blockchain is facing at present. If any node data in the blockchain network is modified or destroyed, the copys of account books recorded by other nodes or blocks could serve as backups. However, in theory, if the nodes in the blockchain system have more than 51% of the computing power in the whole network, then the data in the system can be modified and forged, that is what we called "51% computing power" attack risk. Although the possibility is slim, but with the rapid development of computer technology and the widespread of blockchain technology in auditing, if there is no sound solution to secure data, then the blockchain auditing can hardly be put into practice.

B. Talent and technology support

With the popularization and application of blockchain technology in auditing, the skill requirements of auditors will change. Auditors not only should be equipped with auditing knowledge, but also qualified in technology, such as blockchain setting, blockchain security evaluation and so on, which set higher requirements for the blockchain audit personnel. Moreover, the departments and institutions that provide external audit, such as the accounting firms, need to keep up the path of the development of the blockchain technology. Therefore, blockchain audit is a great challenge to both audit institutions and auditors.

C. Industry recognition and promotion

The "Big Four" have seen the broad business opportunities triggered by the blockchain technology. In August 2016, the Distributed Ledger Alliance chain was set up by the "Big Four" to explore how to develop the blockchain application standards in the accounting field so as to promote the blockchain application in the accounting field. Deloitte has launched the blockchain software development platform Rubix which is applied in the enterprise level. The platform can provide customers with a variety of functions supported by blockchain technology, such as real-time nodes monitoring in the system, compiling intelligent contracts, and developing protocols. Deloitte also established the DCC (Deloitte cipher community) research group to study how to take advantage of blockchain technology to provide solutions for audit, accounting, and taxation. In 2016, Ernst &Young launched the "Entrepreneurial Challenge" project to establish a blockchain solution of the financial sector, and published an industry report entitled "The application of block chain technology as a digital platform in the insurance industry." PWC has set up a strategic alliance with the blockchain company named Blockstream, and jointly develops a high quality digital service supported by blockchain technology. KPMG is also unwilling to lag behind. It has worked with an investment research institute named CB Insights and set up a special team to explore the blockchain technology.

The blockchain technology has been standing on the tip of the Internet era, and known as the representative of the fourth industrial revolution. However, according to a recent survey conducted by the Reuters and the Chartered Institute of Management Accountants(CIMA), only 4% of the

practitioners in the field of accounting and auditing believe that the blockchain will have a significant impact on the industry. At present, the whole industry is insensitive to the blockchain technology and even lag behind the trend. It is also a major obstacle to the blockchain technology promotion in the audit field.

V. CONCLUSION

As the latest technological achievement in the era of Internet and information, blockchain has been a hot topic in academia and industry. Blockchain technology, with its characteristics such as decentralization, consensus mechanism, transparent information and non compilation, facilitates its application in auditing to improve audit efficiency, reduce audit costs, realize independent audit and pre-warning and supervision in real time. It is expected to bring new reforms and developments to the audit industry. But at the same time, the problems of data security, talent and technology support and industry recognition and promotion have brought severe challenges to the comprehensive development and wide promotion of blockchain auditing.

REFERENCES

[1] Anderson, N.: Blockchain Technology: A Game-Changer in Accounting? Deloitte (2016).

[2] Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek. (2015). On the malleability of bitcoin transactions. International Conference on Financial Cryptography and Data Security (pp. (pp. 1-18).). Berlin, Heidelberg.: Springer.

[3] Chen Fang. Financial Audit Based on Blockchain Analysis [J]. Accounting Learning, 2017(18):145.

[4] Chen Xu, Ji Chenghao. Real-time Auditing Based on Blockchain Technology [J]. Journal of Certified Public Accountants, 2017 (4): 67-71.

[5] Dai, W.b-money, a scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help[EB/OL].[2016-7-26].http : //www.weidai.com/bmoney.txt.

[6] Dwork C. and Naor M. 1992. Pricing via Processing or Combating Junk Mail [C]. International Cryptology Conference on Advances in Cryptology, Springer-Verlag, 1992.

[7] Ethereum White-Paper. Online: https://github.com/ethereum/wiki/wiki/White-Paper, 2017.

[8] Greenberg, A. 2017. The Little Black Book of Billionaire Secrets Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius [N].Forbes, 2017-4-17.

[9] Huang Guanhua. Blockchain Improve the Network Audit Approach [J] .Financial Science, 2016 (10): 84-91.

[10] Kehoe, L., Dalton, D., Leonowicz, C., Jankovich, T.: Blockchain Disrupting the Financial Services Industry? Deloitte (2015).