

Impact of block-chain Technology on Auditing

Zhang Liucheng¹, Zhang Li²

¹School of Accounting Harbin University of Commerce Harbin 150028, China

²Teaching and Experimental Equipment Management Center, Harbin University of Commerce Harbin 150028, China

E-mail: zhangliucheng@126.com

Keywords: block-chain; essential characteristics; audit characteristics; technical aspects

Abstract: It is not the social media, big data, robotics, or even artificial intelligence that may have the greatest impact on the next ten years. It is actually the underlying technology - the block-chain, which exists in bitcoin. I believe it represents the development of the next generation of the Internet. It is vital to society as a whole, to all businesses and each of us. Based on the characteristics and technical aspects of the block-chain, the article analyzes the impact of the block-chain technology on the audit from various aspects and the challenges it brings.

1. Introduction

This template, modified in MS Word 2007 and saved as a “Word 97-2003 Document” for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

In 2008, an anonymous person named Nakamoto, in a paper, devised a digital currency protocol based on Bitcoin, the cryptocurrency that allows people to establish themselves without a third party Trust and trade. Bitcoin is an asset whose value fluctuates up and down, saying that it is a cryptocurrency rather than a state-controlled currency, but the real highlight is its underlying technology, the block-chain. With the development of Internet technology, various technologies emerge in an endless stream, which has both fiery artificial intelligence and robots of various industries. However, in recent years, bitcoin has risen nearly 8 million times from the public transaction in April 2010 to now it is About 8,000 US dollars, its violence to get rich so that people started to pay attention to its underlying technology - the block-chain.

Block-chain can be fully used in the financial industry, insurance industry, art industry, legal industry, open industry, real estate industry, etc.

It not only guarantees the trust and security of the transaction, but also keeps the transaction data permanently, People can make subsequent inquiries. block-chain has also received a lot of attention in the accounting industry. Deloitte, Price water house Coopers and other accounting firms have carried out relevant discussions and plans to develop the accounting and auditing work with the block-chain as the core. In China's accounting industry on the block-chain research is also increasing, many experts and scholars put forward the block-chain in the audit industry development and application of the initiative.

2. The block chain overview

Block-chain, also known as distributed general ledger technology, is a distributed database maintained jointly by decentralized network nodes. This technique mainly allows any number of nodes participating in the system to pass through a series of data blocks generated by using cryptography. Each data block contains all the transaction information of the system within a certain period of time and generates data to verify the validity of the remaining information and link the next data block. From an audit point of view, block-chain can be a new way to reduce credit costs, reduce financial risk, reduce human error, reduce audit costs, and increase data processing speed. block-chain has gone through three stages of development:

1) block-chain 1.0 - Digital currency. As the name suggests is the digital monetization, is a virtual currency represented by bitcoin, although there are many deficiencies, including the price volatility, waste of power and the regulatory restrictions of governments, etc., but he is the bud of the block-chain, block-chain technology is the successful application.

2) block-chain 2.0 - smart contracts. Smart contract is pre-programmed procedures, when the set conditions are met, the contract will be automatically performed. Because it can automatically enforce the terms and eliminate the possibility of human-fraudulent fraud in economic cooperation without human involvement, this phase mainly serves the financial sector, including increasing the efficiency of settlement payments and reducing the cost of cross-border payments, Equity registration and transfer functions.

3)block-chain 3.0 - Decentralized

To decentralization is the node of the block chain to jointly maintain a peer-to-peer network without centralized management. The rights and obligations of any node are equal. It applies to industries other than the financial industry and all aspects of society to make society a programmable society. People no longer need the trust of a third agency. He applies them in all fields to solve the trust problem and improve the efficiency of the *society*.

2.1. The nature and characteristics of the block-chain

The essence of the block-chain is decentralized distributed books, each of which is determined by the mining operations of millions of computers. He would be stored in a central warehouse, spread on top of a global book using advanced cryptography. When someone trades, the miner will generate a block in about 10 minutes with huge computing power on hand, This block includes all previous transaction information. block-chain technology features [2] include:

First, get decentralized. The block-chain system consists of individual nodes, there is no central node, and any single node's corruption does not or disrupts the overall system's operation.

Second, open and transparent. Since the block-chain runs on millions of computers, the system is open and the block-chain is open to the public, but only if the trader's private information is confidential and the other transaction information is public, as long as the private key is available, all information.

Again, timestamp. It is usually a string of characters that identifies the time in real time, just like a digital beeswax thing. The nodes in the block-chain that are required to obtain the account right must stamp timestamps and record the data writing time so as to make future data query easier.

Finally, the information can not be tampered with. Miners through their own computing power to generate a block, and each block is generated on the basis of a block, so once tampered with a transaction information, you must master more than 51% of the entire network to successfully tamper with Information, and this ability is almost impossible to achieve, so the information is highly secure and can not be tampered with.

2.2. block-chain technical level

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This

measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

(1) core technology

Distributed accounting methods. It is a decentralized decentralized accounting, transaction accounting nodes in various regions operate together, and each node will disclose its information, so that everyone can see, you can monitor each other to improve the legal transaction Sex. This database records the information of all traders, each of whom can make changes to the information, the updated content is made public, so that other participants can see and everyone sees the same.

Asymmetric encryption and authorization technology. In order to ensure the security of the transaction information, it is necessary to encrypt the information, generally using the public key and the private key to encrypt, and encrypting with one key, then it needs to be decrypted with another key, for example, Decrypt. And public key generation is irreversible, that is, the private key can not be released through the public key. And only the decryption of people can view, thus ensuring a high degree of confidentiality of information.

Consensus mechanism. Traders through the POW, POS, DPOS, POOL mechanism to form a consensus to determine the accuracy of a message, so that both to confirm the information but also to prevent the information has been tampered with to achieve the balance of efficiency and security.

Smart contract. It's a contract that can be executed on its own, and it can not only execute the plan, but also manage the plan and its daily work and transaction costs. There are a variety of projects in the Ethereum system, some of which may become substitutes for the stock market, and some may become the new model of democracy in which politicians are more accountable to citizens. And in the block-chain financial industry, there is no settlement, because payment and settlement is one thing, just change the books.

(2) related to basic technology

P2P network. P2P (person to person) As the name implies, it is an individual to an individual. No third institution participates in it. Each node has equal status. Traders can communicate directly without intervening intermediaries, and they can share some hardware facilities , These resources can provide services and content over the network.

Hash algorithm. Hash also known as hash is the compression of any length of characters into a fixed length function. The block-chain does not directly store the original data or transaction records, but rather stores its hash function values by performing a hash function on the data. He has a one-way (non-inverse input), fixed-length (regardless of how long the hash value, the result is a fixed length), timing (different length of the function value consumes about the same length), random (One byte will also produce significantly different input values).

Workload proof mechanism. As the name suggests is a proof of workload, he can show how much you have done. For example, in the process of getting bitcoin, we have to find the solution of the function by a hashing algorithm. This process is extremely fortuitous because it can only rely on a random hash collision of computers and how many collisions each miners can make each time To get solution, is to look at the performance of their calculations, which is what we call proof of workload mechanism.

3. Block-chain on the audit impact

The block-chain has brought a considerable impact on the audit. It mainly audits the accuracy, immediacy and reliability of data entry, audits reasonable and lawful compliance of accounting through smart contracts, The accounting security under the chain is audited to prevent attacks from other systems.

3.1. Block-chain on the audit of real-time impact

The real-time audit is to do side trial is also called real-time audit. The operation of the block-chain is that each node gets the block by its own computing power, and the first calculated node needs to pass the consent of all the nodes to verify the correctness. Only the correct ability can be

confirmed as the block data, and the block Between a chain buckle chain, so to ensure the accuracy of a block of data. The use of the audit is done first account, and this account is equivalent to the block-chain using hash function to solve the process, and the accounting entries and the accounting result is the block data obtained, just the accounting results will be Verified by other nodes to see if it is accurate, so as to achieve the effect of real-time audit. Real-time audit can not only improve efficiency, reduce audit costs and audit risks, but also help auditors get audit results quickly and save audit time [3].

3.2. Block-chain technology under the characteristics of anonymity audit

Block-chain has a high degree of anonymity, in order to prevent others from posing as auditors, we have a process of identification, so as to ensure that the audit of the job belongs to the right. Although it exposes all the transaction information, it keeps the private information of the traders in good secrecy. The anonymity of the audit can prevent us from accepting bribes and other factors, thereby hindering the fairness and correctness of the audit. For example, in bitcoin, if you access bitcoin through the TOR network, because the TOR network will hide your IP address, you will not be exposed except the public key, thus effectively protecting our personal information. In order to avoid that someone will Your information together, we can set a public key for these information, so as to ensure their own information is not violated.

3.3. Block-chain audit accuracy and security

The results of the audit to the small talk about a business's operating conditions, financial status and its development status, to a big look on the staffing of an enterprise, the development of organizational strategy and even the life and death of an enterprise, the audit results must be accurate and Safety. We need to conduct a systematic independent verification of inspection, so as to ensure the safety of audit. Due to the correctness of the data in the block-chain, coupled with his cohesiveness, the auditing is more efficient and efficient, which improves the auditing accuracy. Asymmetric encryption technology through the public key and the private key, and a key encryption corresponds to the decryption of another key, the public key can not reverse push private key, this double insurance makes audit security has been protected.

3.4. Continuity of audit under the block-chain

Auditing to ensure that the data of the time and can be found, the only way to ensure the continuity of the audit. Each audit under the block-chain will have a specific time, which can ensure the continuity of our audit results, and these audit results will be stored for the convenience of our future data query, which is The charm of the timestamp, which allows us to query the audited matters that have occurred anytime, anywhere. The continuity of audit makes it possible to fully reflect the audit situation so as to fully express the actual situation. This will make our audit results more reliable and will not lack audit data because the audit time is too long.

3.5. Block-chain audit can not be tampered with

The audit report is divided into unqualified audit report, reserved opinion audit report, negative opinion audit report, and rejected opinion audit report. The unqualified opinion is good news for the enterprise, indicating that the financial statements of the Company are more reliable and the opinion of the reservation is reliable as a whole. However, there may be doubts in some matters. The negative audit report is the auditor's opinion that the report is seriously untrue or the accounting The method selection is unreasonable, and there is no reference value. The negative opinion is that the audit procedure can not be carried out and the auditing behavior is blocked at every level, indicating that the enterprise has had major problems and may be suspected of bankruptcy. Audit reports are therefore of crucial importance to the business so that they may have their auditors change their audit results by way of bribes or threats, but this is almost impossible in the block-chain because Once the data is hard to change, you can only edit or modify the information if you reach or control more than 50% of the computers in the world. And although the audit report is open to the public, it is not secret that anyone can edit the data. This will further ensure that the audit can not be tampered

with. Decentralization makes the audit not controlled by one person, but completed under the distribution of each node. Although the audit process and the result are public, the account information is kept confidential, thus avoiding the artificial error. Consensus mechanisms require that all nodes agree to verify audit compliance, thus preventing the possibility of tampering [4].

4. Block-chain itself to the audit impact of the impact

Although the block-chain has brought a lot of convenience to the accounting and auditing profession, its own shortcomings make the audit face some challenges [5].

4.1. Can not be tampered with and revoked

Different perspectives can have different perspectives. Data can not be tampered with to ensure the authenticity and security of the data. In some aspects, this may result in the loss of data. In the block-chain, everything is live, there is no rehearsal, almost impossible to change the data. When we are in the process of auditing, if the address sent by the audit result is incorrect, it will cause permanent loss and there is no way to withdraw it. If we lose the key of an auditor, we can no longer retrieve the key, so that our information may not be retrieved and the corresponding key will disappear. Because the hash of the block is different and the output of the hash is used as the previous citation, this results in you being unable to replace the block in the middle of the block-chain. When the previous block is not unlocked, the last block Can not be solved, so that the fake data tampering difficult, making it even harder. But in reality, this problem does not occur.

4.2. Trading books must be made public

block-chain is decentralized distributed books, which makes the audit will be reflected in different accounts, which is equivalent to every trader knows the company's audit and audit reports of the views and audit Involved in company secrets, which is fatal to enterprises, enterprises will be open after the cost accounting will make the enterprise dilemma, and validation of audit effectiveness need to retrospectively no audit results. So if I know an enterprise's account, then I can know all of its information and the audit of each accounting statement and its audit report comments, which makes the audit completely open, contrary to the professional ethics of auditors, The auditor's position in the industry is affected.

4.3. Data increase with

Because everyone has a complete audit report, and due to the consistency of the audit, when we analyze this situation, we need to consider the previous situation and need us to query the previous information. When we use computers to do audits, we may need to download the information before, because they are a whole, when we do audit research must be based on previous research. With the passage of time, the data will be more and more, so we need our computer performance requirements are relatively high, so as to ensure the timeliness of our data. In bitcoin, for example, we need to calculate the balance of the pen trade in order to decide whether there is enough balance to pay this time. Although computer performance problems are improving and memory is getting larger, the storage needs for a robust block-chain need to continue to grow.

4.4. Block-chain processing capacity

When we audit matters, we usually deal with a variety of data, and these data include not only all aspects of production, management, management, which means that we need to deal with huge data, which requires our computer with high-speed Processing speed, in order to meet the efficient audit requirements. In bitcoin, for example, it takes years for a single computer to guess a block, and when all computers in the bitcoin network are guessing, it takes 10 minutes on average for a machine to succeed Guess the answer, although has greatly reduced the processing speed, but compared with the bank, its processing speed is too low, a computer in the block chain can handle an average of about seven transactions per second, and the bank about every Seconds can handle 1000, this difference will affect the block generation, and if you encounter hundreds of millions of

orders for 11-11 seconds, the block-chain system probably will collapse, so I'm boring to be committed to improving the block-chain data processing speed.

4.5. Block-chain delay

The formation of the block-chain block is determined by the competition among a series of nodes. When the audit confirms, it needs to wait for the first node to calculate the result, and only after most nodes approve the result, can the result be confirmed. If Two or more nodes calculate the results at the same time, they need to compete for the next step, the final block chain from the longest branch to determine which branch records are correct, which may take a long time , Will affect us to make a decision, billing cycle longer and longer, will affect the timely output of the results.

5. Conclusion

The block-chain has brought about a dramatic change in our lives. It not only brings a lot of convenience to the enterprise but also greatly enhances every aspect of our life. To know that the largest capital flow from the developed countries to the developing countries is not business investment or even foreign aid but remittances. This is a global migration. It is currently one year of 600 billion U.S. dollars and is still growing. These international Banks are on the hook, and in the block-chain, we transnational transposing not only reduced transaction costs about 5 times, but the time is also greatly reduced, in addition the block-chain will save all the information we have before, they will Based on these transaction data, we simulate a virtual we can remember the information we can not remember, and after the transaction we will clean all the data, so it greatly helps us to protect our privacy. While the block-chain's own shortcomings have had some impact on our audits, its convenience has made our audits more efficient, less costly, more secure, and more confidential. Once the block-chain is widely used, its decentralized, hashed computing, cryptographic encryption, and non-tamper-proof features make the computing power greatly reduced the need for manual auditing and may eventually subvert the entire accounting and auditing profession. Faced with opportunities and challenges, accounting audit industry how to deal with that? In my opinion, the actual situation in our country is rather complicated and needs to be taught according to aptitude. First of all, we must pay close attention to changes in the business environment, market environment, political environment and even the global environment, and actively identify opportunities and challenges in a timely manner. Secondly, we should increase investment in science and technology and promptly explore the development of market orientation and emerging technologies Trend, and strengthen the contact with technology companies in a timely manner to focus on R & D products; Finally, we should do a good job of self-positioning, develop a steady development strategy, find suitable for the company's own technology products.

Acknowledgment

This work is supported by National Social Science Fund Project 15BJY017.

References

- [1] Zhou Heng. "Research on the application store business model", "Beijing University of Posts and Telecommunications master's thesis", 2011
- [2] Shen Xin. "block-chain Technology Review." Journal of Network and Information Security, 2016,2 (11)
- [3] Zhang Xiaojing. "Research and Development of Online Auditing." "Finance and Economics", 2013 (20): 243-243
- [4] Wei Wei. "block-chain technology in the application of accounting outlook." Friends of Accounting, 2016 (17): 122-125

[5] Qin Rongsheng. "block-chain technology in the accounting and auditing industries." "High Technology and Industrialization", 2017 (7): 64-67