China-USA Business Review, June 2017, Vol. 16, No. 6, 294-298
doi: 10.17265/1537-1514/2017.06.006

Will Blockchain Change the Audit?

Zhiyong Li
Jianghan University, Wuhan, China

Blockchain technology is the underlying technology of bitcoin. The bitcoin can be used to consume and exchange real currencies, because the blockchain can provide credit certificate of online transaction, and all transaction related information is encrypted and stored in the blockchain. So, it is safe and decentralized, and it will reduce the transaction cost and be widely used. Another important feature of blockchain is non-modifiable. Since all transaction related information is recorded in blockchain and not changeable, this feature facilitates the audit work. Because audit work is designed to testify whether all transactions and matters are truthfully recorded. It generates the problem whether the blockchain will change and facilitate the audit.

Keywords: blockchain, distributed ledger, audit

Introduction

The WannaCry Virus has recently swept the globe, many computers in the Education Intranet of China were infected. The Bitcoin, a virtual currency created by Satoshi Nakamoto, now stands in the spotlight of China. People are wondering why the virtual currency can be used to consume in the real world, even to exchange real currency all over the world and what makes the Bitcoin trustworthy. The answer is the Blockchain Technology, an innovation by Fintech. This technology is acknowledged for its advantage in recording transactions and events. Many believe that blockchain, like the Internet, will revolutionize how people and organizations will manage transactions and assets (Swan, 2015).

The Blockchain Technology

The blockchain is a distributed database system, which is composed of different data-blocks and participated by different nodes. The data are stored in the data-blocks of the chain. Meanwhile, the data are sealed with a timestamp, encrypted with the timestamp together, and then a hash value will also be generated and stored in a data-block. Every data-block contains the hash value of the last data-block, in this way data-blocks are linked from the genesis data-block to the current data-block and form the blockchain.

The essence of blockchain is under the condition of asymmetrical information people can trade without any credit certificate. For instance, currently people can trade and pay online via Alipay or bank. That means all the trade related information is stored in the database of Alipay or bank. The trade and payment needs the credit certificate of these institutions, and all information is centralized. In contrast, the blockchain has many nodes, every node can supply necessary information. Therefore, the blockchain is a distributed ledger. With this technology, the demand of huge institutions to supply credit certificate is weakened, transaction cost is

Zhiyong Li, assistant, Institute of Business of Jianghan University, Wuhan, China.
Correspondence concerning this article should be addressed to Zhiyong Li, No. 1 Bo Xue Road, Jianghan University, Wuhan 430056, China.

accordingly reduced. So, if anyone or any institution wants to amend any information stored in the data-block, they must do it from the very beginning and on all the nodes. In other words, if there are many participants, it's fast impossible to amend the information stored in the blockchain. It must be costly; hence, this technology solves the credit problem of online trade and has a very good prospect in the financial industry.

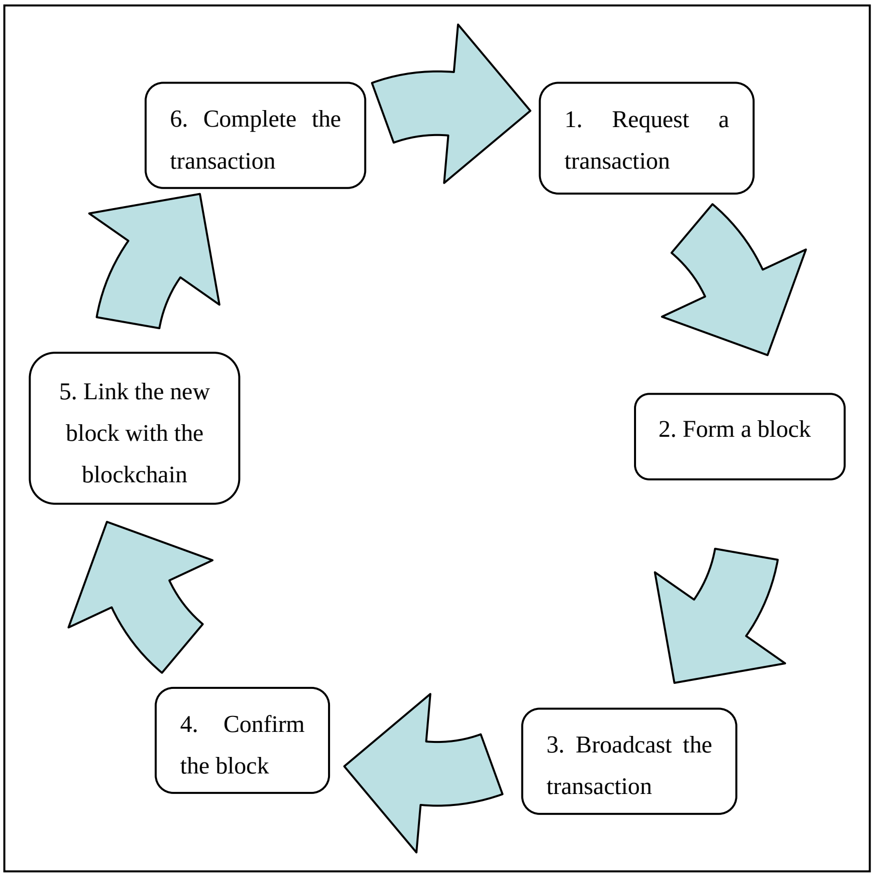
1. Request a transaction
2. Form a block
3. Broadcast the transaction
4. Confirm the block
5. Link the new block with the blockchain
6. Complete the transaction

Figure 1. The operational principle of blockchain.

The Application of Blockchain

The blockchain is an underlying technology of fintech, it can possibly reshape the financial industry, for instance the traditional financial service, P2P, or crowd-funding, even the financial regulation, financial risk and illegal fund-raising prevention. So, it's expected to be widely used, the internet finance may enter "blockchain+" era.

- Blockchain + International settlement. The existing international currency exchange model is mainly through the accession to Society for Worldwide Interbank Financial Telecommunication (SWFIT). Take Ripple for example, Ripple is distributed financial technology which enables banks to send real-time international payments across networks. In Ripple system, not only all real currencies but also virtual currencies can be exchanged and transferred more efficiently and economically. The Ripple is basically a shareable open source database, and no one can completely control Ripple, which is a typical distributed ledger system, a blockchain.

- Blockchain + Credit Investigation. Credit investigation is a blue ocean market. Traditional credit investigation service cannot share the information, so the information of one institution is relatively limited. Besides traditional credit investigation service costs too much. Blockchain provides a new idea to solve the difficulties. Firstly, all information across the Internet can be used, but cannot be falsified, and it enhances credibility of the investigation. Secondly, using the blockchain technology can reduce the cost significantly and supply multi-dimensional data.
- Blockchain + Exchange. The exchange is a market for securities transactions, and it needs a transaction registration institution. Because of the features, such as non-modifiable, shareable, anonymous, open source, economic. Hence, an application of blockchain in the securities transaction can notably improve the efficiency of securities registration, issuance, transfer, and delivery. At the end of 2015, the blockchain technology has already been used by NASDAQ (National Association of Securities Dealers Automated Quotations) and Australia Exchange.

Blockchain and Audit

The objective of an audit is to enable the auditor to express an opinion on whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework. In the assertion level of audit, it is crucial to obtain sufficient and appropriate audit evidence. For example, to confirm a transaction really happened, auditors must collect evidence like invoice, shipping document, customer order, confirmation requests and so on to confirm occurrence of this transaction, all relevant information recorded, the accuracy of the record, the right accounting period, and the right classification.

As mentioned above, any transaction in the world of blockchain will be recorded, encrypted but cannot be falsified. Therefore, the audit evidences in assertion level can all be simply obtained, and this will eliminate the influence of asymmetric information. That will reduce the detection risk. Blockchain is also encrypted, that will help to resist malicious attack and to keep the accounting record accurate. In addition, since data-block is stored in every node, there is no loss risk. That also means every node which can decrypt the data-block can inquire the transaction information, so the auditing is not restricted by space. Because of non-modifiability of blockchain, it is impossible to conduct a financial statement fraud. So, it is clear that, the features of blockchain are in accordance with the function of audit.

The blockchain has been used in Fintech, Consulting, and Audit. Deloitte has already developed an application platform Rubix, which can provide service, such as counterparty confirmation, real-time auditing, land registration and so on. According to the Chief Advisory Officer of Deloitte, “since all transactions were uploaded to related data-block, the auditing can be accelerated. On the other hand, the data in the blockchain are non-modifiable and with timestamp, the auditors can easily audit all the transaction of the clients.”

Risk Analysis

The 51% Attack

As mentioned above, it is fast impossible to modify the data, but it doesn’t deny the possibility. Because data modification in blockchain needs the approval of 51% participators. Normally when the number of participators is big enough, 51% attack cannot happen, because it costs too much money. But it does not eliminate the possibility. So, if the participators are many enough or the hash value is too short, it may be attacked and data may be modified, the detection risk will consequently increase.

ID Theft

Although every data in blockchain is encrypted, if the private key is stolen, no third party can recover it. Consequently, all the assets which belong to this person will vanish, and the theft cannot be identified because of the anonymity. That leads to the problem that the auditor may obtain the audit evidence of the existence of an online asset of the audited party, but due to the loss of the private key, this asset vanishes. This fact may lead to inappropriate audit conclusion. Also, current cryptography standards are not completely uncrackable. With the advent of quantum computing, it is not impossible for cryptographic keys to be cracked quickly, demolishing the foundation of blockchain technology.

Illegal Activities

Blockchain technology can to some extent protect illegal transactions. The Silk Road website is a market place, where all sellers and buyers are anonymous. They can trade with bitcoin. So, if they trade illegal drugs or weapons, these illegal activities cannot be traced. This feature can also facilitate money laundering.

System Hackling

It is difficult to hack and modify records stored in a blockchain, but not the programming codes and system that implement its technology. MtGox, a bitcoin exchange, was hacked in 2014, and bitcoin which is $700 million was stolen. More recently, the DAO incident, the assets worth $60 million were stolen.

Risk Response

Firstly, although the “51% attack” may happen theoretically, there is still no attack of this type. Because if people want to control 51% participators, huge resources are needed to reach such extent of control. There is no need to consider this problem.

Secondly, cryptographic keys and anonymous transactions make blockchain vulnerable, because the assets of an online ID are only protected by its private key. If the key is lost, then the assets banded to the ID are lost. One solution is to build a life and reputation system using a blockchain (Baxter, 2016). This chain records events like births, schooling, bank accounts and so on. In this way, the other chain becomes a digital identity that is difficult to steal. So, to handle the “ID theft” problem, auditor can only seek the expert’s help.

Thirdly, the world of blockchain is still autonomy, to avoid illegal activities it needs regulations and laws, specially the cooperation of different countries, when international trade occurs.

At last, blockchain itself can prevent fraudulent behaviors, but it cannot detect fraud by itself (Ngo, 2016). Existing techniques using machine learning and data-mining algorithms may find new applications in detecting fraud and intrusions in blockchain-based transactions.

Conclusion

This paper has briefly introduced the blockchain technology. Blockchain technology will due to its features heavily facilitate the audit work and change the way of audit work to be done, e.g. traditional audit work is implemented after balance sheet day, with blockchain the audit work can be done immediately after a transaction is completed. But the blockchain itself still has some problem to solve. Auditors should not totally count on it. To keep quality of an audit and to facilitate an audit work, auditors should consider and assess risk from ID theft, illegal activities, and system hackling, if blockchain technology is widely used in auditing.

References

Baxter, A. (2016). Blockchain—Unchanging the world from fraud? http://www.thepaypers.com/expert-opin/blockchain-unchaining-the-world-from-fraud-/763845

Ngo, D. (2016). How blockchain technology can enhance fraud detection, interview with Feedzai's CTO. http://coinjournal.net/how -blockchain-technology-can-enhance-fraud-detection-interview-with-feedzais-cto/

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Beijing: O'Reilly.