

Research on the Application of Blockchain Technology in the Financial Field

Shuyi Gu*

School of Economics and Management, Beijing Jiaotong University, Beijing, China

*Corresponding author: 20711007@bjtu.edu.cn

Abstract. Decentralization, autonomy, integrity, immutability, verification, fault-tolerance, anonymity, auditability, and transparency are desirable characteristics of blockchain technology. Blockchain technology originated from Bitcoin which is one of the applications of digital currency. From a financial point of view, it is a distributed data storage system. Therefore, it is very important to analyze the current research status in this field, and further sort out the deficiencies of current research and future development direction. This article describes the definition of blockchain technology and hash algorithm first. Besides, it also shows some applications including supply chain finance, digital ticket, and digital currency in the financial field. Privacy and risk are the key points to worry about. This article also introduces how to protect user privacy in supply chain finance. This article analyzes how blockchain effectively protects user privacy from banks and non-banks. It is difficult to take into account all three features of blockchain: security, scalability, and decentralization. However, the integration of finance and technology is an increasingly strong trend.

Keywords: Blockchain technology; User information protection; Supply chain finance.

1. Introduction

Blockchain is a distributed and shared database that comprises hash algorithms, asymmetric encryption algorithms, consensus mechanisms, and distributed ledger technology. It has undergone three major changes since 2008. Blockchain 1.0 is primarily used for peer-to-peer digital currency transactions [1] and users may only modify it according to the rules upon the development of the application system. The entire system is divided into two parts: interaction tools and core nodes. The operating interface is left to the user through the interactive tool, and the core node is only responsible for implementing the functionality. Blockchain 2.0 primarily uses smart contracts. The most significant change from blockchain 1.0 architecture is the addition of smart contract virtual machines and smart contracts. Ethereum is considered to be a pioneer in the era of blockchain 2.0 architecture. A blockchain technology application system does not need to be built from scratch when using smart contracts [2]. Ethereum already has a consensus algorithm, password algorithm, network communication algorithm, etc. Blockchain 3.0 can support the construction of organization-specific private blockchain networks. Hyperledger is a representative project of blockchain 3.0. In addition to digital currencies, blockchain 3.0 supports the construction of customized private blockchain networks for organizations. The blockchain 3.0 architecture also incorporates access gateway control. To increase security, access gateway control can be delegated to specific nodes.

Blockchain is widely used in finance, the Internet of Things (IoT), supply chain, healthcare, energy, voting, education, and many other fields [3]. To identify its shortcomings and potential directions for improvement, it is crucial to evaluate the current state of economic research. As a result, the following mainly introduces the research of blockchain in the financial field and then analyzes the possibility of future research.

2. The basic introduction to Blockchain technology

2.1 The definition of the Blockchain technology

Blockchain technology is a new distributed ledger technology, which has six characteristics: decentralization, global circulation, anonymity, transparency, information that cannot be tampered

with, and autonomy [4]. A blockchain table, which consists of a timestamp table and a data module that records the data in an orderly manner, guided by basic cryptography techniques and machine theory, is created by blockchain technology to ensure the orderly cooperation of data from various network nodes to support its steady growth. Blockchain technology is used in finance and other areas, and as it develops, it even outperforms some older fingerprint data block encryption storage applications.

2.2 The structure of Blockchain technology in the financial field

Fig. 1 shows the structure of the blockchain, and blocks on the figure are connected in a chain structure. The Block Header consists of all fields in the green part of the block. The SHA256 encryption hash is performed on the block header to generate the hash value of the current block [3]. No matter the size of the string, we can get a fixed number of bits, and this value can be used to identify a particular block.

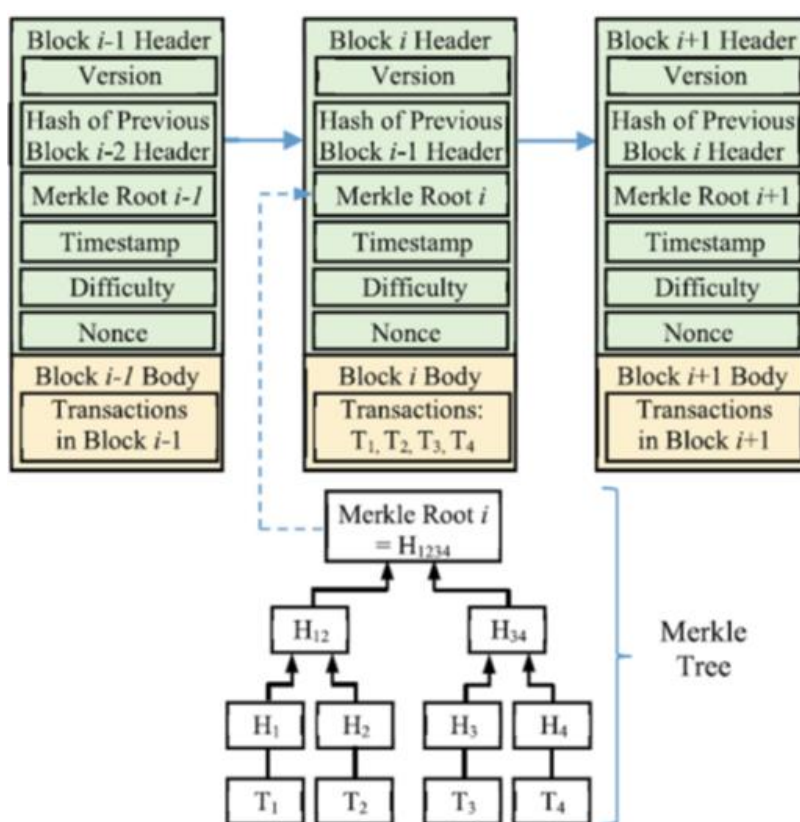


Figure 1. Diagram of the blockchain structure [3]

Hash of Previous records hash of the previous one. Merkle Root Records all transactions in the current block. In Fig .1, hash calculation is done on transaction 1 to obtain H_1 . Similarly, H_2 , H_3 , and H_4 are obtained. H_1 and H_2 are merged to obtain H_{12} . H_3 and H_4 form H_{34} . Then, H_{12} and H_{34} are merged to obtain H_{1234} . The timestamp is the generation time. Difficulty shows the workload. A Nonce is a number that is constantly computed for the hash to meet certain conditions, a process called mining. The Hash algorithm is unidirectional and cannot be modified. On the one hand, entering data can easily get the output value, but the reverse is difficult to achieve. On the other hand, when one of the records is changed, the security check will recognize the error, and the subsequent chain will be broken. Only if the whole values of the hash are known, the modification can be made [3].

2.3 The application of Blockchain technology in the financial field

2.3.1 Supply chain finance

One of the most efficient ways to address the financial challenges faced by small and micro businesses is supply chain finance. The entire supply chain is covered by the blockchain platform, including core businesses, suppliers, distributors, logistics providers, etc. The chain records and stores all transaction data from small and micro businesses, supporting anti-counterfeiting traceability [5].

2.3.2 Digital ticket

Due to its immutable and anti-counterfeiting traceability properties, blockchain technology can successfully address the challenges the bill market faces. Data bills have evolved from paper bills to electronic bills to become new digital assets, and bill transactions are carried out via the blockchain platform [5].

2.3.3 Digital Currency

Advances in technology have affected the way we save money and pay for goods and services. In many countries less and less cash is used, and all transactions are made electronically by credit card, bank transfer, or Venmo, a payment service like Paypal [6]. Blockchain, a technology that emerged from Bitcoin, is the foundation of new digital currencies. The tamper-proof, traceable, and private-key encryption features of blockchain technology can successfully thwart money laundering, fraudulent transactions, and other wrongdoing.

3. The security of privacy protection based on blockchain technology

3.1 Application case analysis of banking financial institutions

Privacy protection is the focus of user concern and the emergence of technical feasibility. The major focus of the part that follows is an analysis of the control strategy and authorization of personal financial information from the standpoint of block technology.

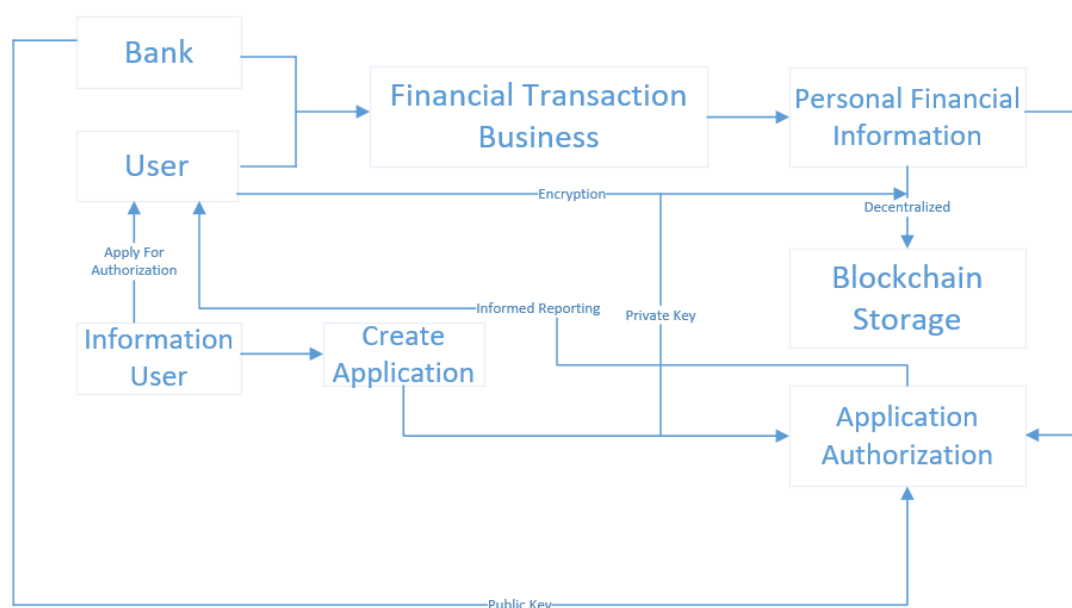


Figure 2. Application ideas of blockchain technology in banking financial institutions
(Photo credit: Original)

As an illustration, consider the two scenarios that can occur when workers of commercial banks disclose personal financial information (see Fig. 2).

First, commercial banks' internal personnel sell clients' financial information for financial gain. Even with a rigorous internal control system and technology security, it is challenging to fully resolve the issue of information leakage. This type of circumstance can occur in information collection, information processing, and information storage of numerous linkages. On the one hand, the traditional method of protecting the privacy of personal financial information typically involves disciplining employees who break the law following the commission of criminal crimes, but it is unable to alter the fact that personal financial information is leakable. On the other hand, the fact that personal financial information is not clearly owned and instead is managed by the bank as internal data amounts to a violation of personal rights [7].

Second, external hackers assault the personal financial data that commercial banks maintain, leading to data leaks. Commercial banks can partially address this issue by expanding firewalls and technical security investments, however, even the strictest firewall cannot 100% ensure information security. According to blockchain technology, a user owns and is the owner of their personal financial information stored in a bank or other financial institution. Every time a person or organization uses personal financial information, they must first create an application, which must be authorized by the user and disclose its intended use. Abnormal applications will be flagged by the blockchain's information feedback mechanism and reported to the user, who can then stop authorization or sound an alarm. This lessens the issue.

3.2 Application case analysis of non-bank financial institutions

In the conventional institutional supervision mode (see Fig. 3), non-bank financial institutions have the authority to handle users' financial information, but due to insufficient internal management, it is simple for users' private financial information to be compromised. In addition to the two methods used by commercial banks to leak personal financial information, there are illicit uses of personal financial information stored by non-bank financial companies as well as benefits exchange. Data is valuable in the age of big data, and personal financial data in particular has significant economic worth. Due to their level of management of clients' private financial information and the lack of significant government regulation, nonbank financial organizations have enormous incentives to break the law.

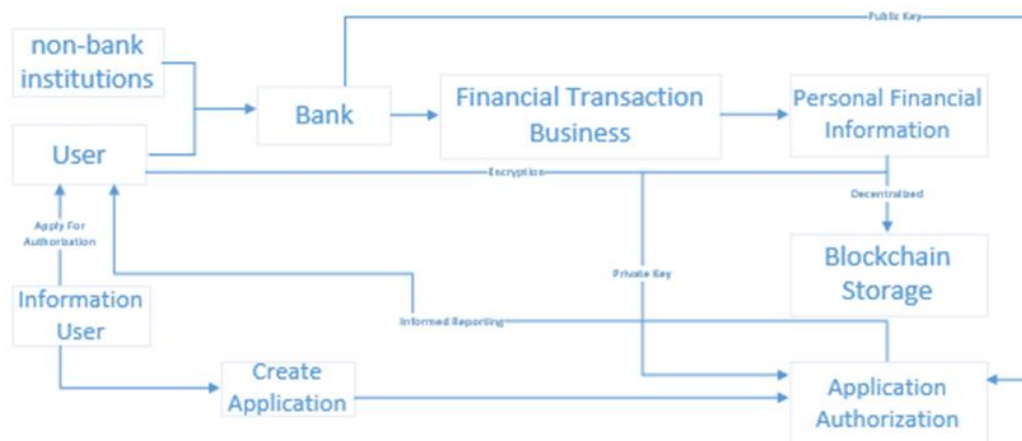


Figure 3. Application ideas of blockchain technology in non-bank financial institutions
(Photo credit: Original)

Users' private financial information is recorded in the blockchain and belongs to them under blockchain technology. A user's name, gender, and other basic information are managed by non-bank financial institutions, but their fundamental financial information is encrypted by them and kept on the blockchain as a result of their financial transactions. Like other information users, a non-bank financial institution must first request information authorization before using such information, and it must also tell the consumer of its intended use. The user can then utilize the personal financial

information with the public key and choose whether to authorize the information based on the application's purpose and duration. This can successfully guard against non-bank financial firms mismanaging personal financial information and causing its sale, theft, or other commercial exploitation [7].

4. Blockchain technology and supply chain finance

The second section of this paper's research on blockchain technology reveals that there is significant compatibility between blockchain technology and the modernization of the financial industry. There is a lot of overlap between blockchain technology and supply chain finance, thus it can effectively address the challenges facing its development [8].

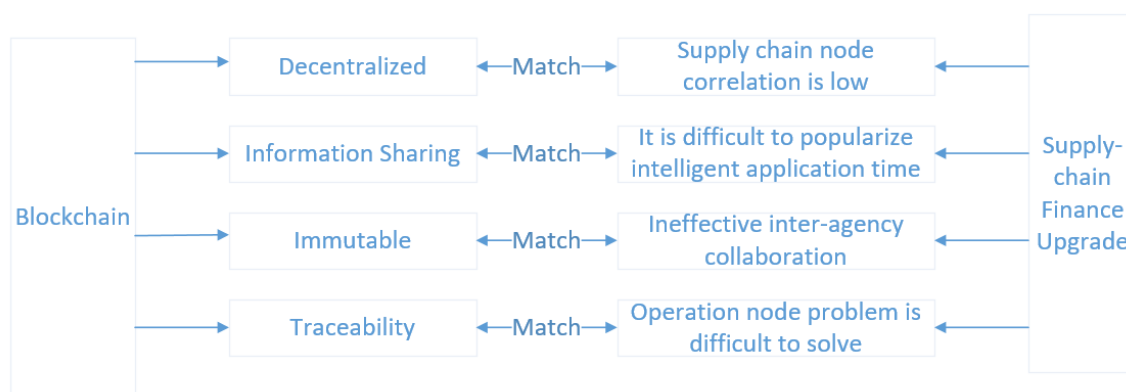


Figure 4. Correlation between Blockchain and Supply-chain Finance Upgrade
(Photo credit: Original)

The characteristics of supply chain financing are shown in Fig. 4 as follows: It is event-driven, to start. Events in the physical supply chain, such as orders, invoices, accounts receivable, other claims, and associated processes before and after shipment, serve as triggers for financial demands [9]. The finance strategy meets these requirements. As a result, supply chain finance is "event-driven" to a great extent. Automated supply chain finance interventions are now possible because of the advancement of corporate systems for recording and regulating events and physical supply networks (financing, risk mitigation, or payment).

Multi-agent coordination is the second. There are numerous groups of buyers and sellers involved in the supply chain's transaction relationship chain. A variety of financing themes are also involved in supply chain finance, including banks and other financial institutions, supply chain service companies, core businesses, logistics firms, regulators, and other pertinent parties. It is important to clearly define the "responsibilities, rights, and interests" of each role in the wealth management and credit creation process with the involvement of multiple actors, coordinate the behaviors of the various actors, and record the behavior track of each role as the evidence of disputes in the future [9]. Following the law, carrying out the terms of the contract, and timely documentation are the only ways to guarantee the smooth functioning of supply chain financing.

5. Limitations & Future outlooks

Beyond digital currencies, blockchain technology's application has grown, becoming crucial to new market customs and modes of consumption. The financial sector has a high degree of compatibility with blockchain technology due to its inherent benefits. With the advent of the digital age, the key to the use of blockchain technology lies in the integration with diverse industries to build the industrialization of blockchain. Everyone needs reliable data to support their decisions, whether it be in the everyday financial management of individuals, the investment and financing activities of

businesses or financial organizations, or the capital control of the central bank. As a result, there are many different ways that blockchain technology is being applied in the financial sector, and it has a significant impact.

The distributed system has an "impossible triangle," in accordance with Eric Brewer's CAP Theorem [10]. It is impossible to accomplish consistency, availability, and partition tolerance at the same time [10]. Two items can only be checked off at once. The triplet paradox has limitations as well, especially for distributed systems like blockchain. Security, scalability, and decentralization are only two options that can be utilized to decide how frequently new blocks are generated in the blockchain network, regardless of the consensus process employed.

A development that has happened and is happening is the introduction of blockchain technology into the financial system to hasten the merger of finance and technology. Technology and algorithms are transforming the financial sector (blockchain). An ever-growing trend is the fusion of finance and technology. The sharing economy and the digital economy both heavily rely on future finance. Fintech competition will be a key area of national competitiveness at the national level. Additionally, the openness and transparency of blockchain data offer fresh approaches to issues that conventional technology is unable to tackle. Users' information is more in their hands, and their privacy is better protected.

6. Conclusion

Blockchain still has privacy protection issues. There are two possible outcomes when bank employees divulge personal financial information: internal staff selling customers' financial information to achieve financial benefits, or outside hackers assaulting personal financial data kept by commercial banks. Non-bank financial institutions also face the illicit use of their stored customer financial information and interest exchange, in addition to information leakage brought on by internal staff and outside hackers. Blockchain technology and supply chain financing have a lot of potentials together.

In the financial field, the blockchain has achieved digital currency, electronic bills, supply chain finance, and other achievements. Banks and non-bank financial institutions use its immutability to a certain extent to protect the privacy of users. In addition, the financial characteristics of the supply chain match the characteristics of the blockchain, and it is worth further strengthening the connection between the two. Despite the difficulty of using all the characteristics of blockchain technology, it provides a possible solution to the problems of information storage security and high intermediate cost existing in traditional centralized institutions and has a very wide application prospect. Introducing it into the supply chain finance business can bring advantages such as solving the problem of information asymmetry, and data traceability, improving the efficiency of clearing, and eliminating intermediate steps by using smart contracts.

References

- [1] Leila Ismail and Huned Materwala, A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry*, 2019.
- [2] Y. Zhu, X Zhang, Zh Y Ju, et al. A study of blockchain technology development and military application prospects, *Journal of Physics: Conference Series*, 2020, 1507 (5): 52018.
- [3] Guo, Huaqun, and Xingjie Yu, A Survey on Blockchain Technology and Its Security. *Blockchain: Research and Applications*, 2022, 3 (2): 100067.
- [4] Xiaohui. Zhao, Research on the application of blockchain technology in the financial industry, *Financial Technology Time*, 2022, 30 (12): 26 - 30.
- [5] Yuxi. Liu, Research on the application path of blockchain technology in the financial industry *Sci-Tech & Development of Enterprise*, 2021, (09): 104 - 106.

- [6] Halaburda, Hanna, et al. Beyond Bitcoin Economics of Digital Currencies and Blockchain Technologies. Springer International Publishing, 2022.
- [7] Zhengzheng Wang. Application of blockchain technology in personal financial information privacy protection, Communication of Finance and Accounting, 2021, (14): 150 - 153.
- [8] D. Xu, Research on the Application of Blockchain Technology in Supply Chain Finance, Southwest Finance, 2019, (02): 74 - 82.
- [9] Sheng Manman and Ma Li. Analysis of the application status and countermeasures of blockchain technology in the field of supply chain finance, Financial View, 2021, (29): 128 - 130.
- [10] Wei. Sheng, Blockchain Financial Supervision in the Digital Economy Era: Current Situation, Risks and Responses, Frontiers. 2022, 250 (18): 52 - 69.