Blockchain Overview

Subjects: Transportation | Computer Science, Information Systems
Contributor: Boyu Liu, Xiameng Si, Haiyan Kang

Blockchain technology integrates a hash algorithm, digital signature, point-to-point transmission, consensus mechanism, and other existing technologies, so it is characterized by anti-fraud, traceability, security, and trust. Supply chain refers to the network chain structure formed by upstream and downstream enterprises involved in the activities of providing products or services to end users in the process of production and circulation.

Keywords: blockchain technology ; supply chain ; application

1. Introduction

In 2008, Satoshi Nakamoto published an article named Bitcoin: A Peer-to-Peer Electronic Cash System in which he proposed the basic concept of the first cryptocurrency, Bitcoin [1]. As a well-known peer-to-peer virtual currency without a third party or a central bank, it is the first application of blockchain technology. With the rise of bitcoin, the technology underlying it has gradually drawn people's attention. Since its birth, it has experienced many times of innovations. In the past ten years, the 'blockchain 1.0' is marked by encrypted digital currency and the version 2.0 is featured by smart contracts [2]. And now, the version 3.0 crosses the threshold into the stage of application, serving as the key technology that extends engagement in many areas such as finance, government affairs, supply chain, and so on [3]. Blockchain technology integrates a hash algorithm, digital signature, point-to-point transmission, consensus mechanism, and other existing technologies, so it is characterized by anti-fraud, traceability, security, and trust.

Supply chain refers to the network chain structure formed by upstream and downstream enterprises involved in the activities of providing products or services to end users in the process of production and circulation. Nowadays, globalization impacts everything, with no exception for the supply chain. The rapid development of economic globalization and the increased market competition could make the supply chain become highly complex and dynamic [4]. In recent years, customers are more demanding, e.g., expecting better-customized products and better customer service, all at an acceptable speed and cost. To effectively adapt to market changes and remain competitive, companies are now focusing on their core functions and are moving towards collective and collaborative efforts [5]. It comprises multiple stakeholders, and they could be worldwide, which leads to the high dispersion of information. Moreover, the global division of labor getting deep, modern enterprise supply chain presents the characteristics of fragmentation, complexity, and geographical dispersion [6]. To manage and share the information among these participants, more costs are needed in the conventional supply chain, but the information asymmetry could not be fully solved. And this kind of information asymmetry could be either intentional or unintentional [4]. Therefore, information sharing and coordination of the supply chain is the key. The efficiency can be improved by enabling real-time information transfer, coordinating inventory management, increasing flexibility, and adapting to changes in demand across the supply chain [7]. However, in the process of information sharing, there may be risks of data manipulation, loss of expertise, weakened bargaining power and information disadvantage [8].

2. Blockchain Overview

2.1. The Origin of Blockchain

In 2008, Satoshi Nakamoto published an article named 'bitcoin: a peer-to-peer electronic cash system', proposing a brand-new concept, bitcoin. Two months later, in 2009, the bitcoin system was published with its source code, and everyone worldwide can be a user of it. At the same time, the first block called Genesis Block was born with the initial fifty bitcoins in the world. For blockchain 1.0, Bitcoin's enabling technology is the Blockchain Technology (BCT) as the underlying structure, which leads to the explosion of all kinds of digital cryptocurrencies based on the system. And this fever has undoubtedly drawn people's attention to blockchain technology, which has greatly made the spread move. Besides bitcoin, people gradually tried to adopt blockchain technology in other areas, but it was hard to realize the implementation without smart contracts. The bitcoin system uses Bitcoin script to support the Unspent Transaction Output (UTXO) model and complete the Bitcoin transfer logic. Bitcoin script is extensible, and additional instructions can be

added to implement more transaction types and segregated witnesses. However, the script is in the data field of the transaction, and the logic part is coupled with the data part, which lacks flexibility. Instruction expansion is likely to cause system security risks. The script's instruction function is Turing incomplete [9].

Smart contracts introduced into blockchain 2.0, the system logic supports users in the custom business. In 2013, the most typical system of blockchain 2.0, Ethereum, was launched. After that, considering the transparency, reliability, openness, security, immutability, and disintermediation, it is possible to adopt blockchain technology into more fields if intensive coordination is required. So far, blockchain technology has gradually expanded engagement to logistics [4], biomedical and health care [10], energy [11], and other fields.

Blockchain 3.0 is the core of the Value Internet which is a globally distributed ledger system. Although the blockchain has been applied in many industries, the blockchain applications in various industries are still independent of each other, forming information silos. However, the goal of blockchain 3.0 is to break the status quo and form an interconnected network from information silos to make big value. Through the innovation of the existing Internet system, blockchain technology will cross the threshold into the value Internet era with 5G network machine learning, the Internet of Things, and other technologies together.

In general, blockchain 1.0 is the most basic version of blockchain technology, and subsequent blockchain versions 2.0 and 3.0 are implemented based on the 1.0 framework. The blockchain 1.0 system was born to solve the shortcomings of the traditional currency system, but its application is also limited to the decentralized digital currency represented by Bitcoin. Blockchain 2.0 is marked by the development of smart contracts in Ethereum and a Turing-complete virtual machine. The biggest difference between blockchain version 2.0 and version 1.0 is the support for smart contracts. The contract program is developed through development tools, and the written content is finally deployed to the blockchain ledger. The most well-known platform is Ethereum. The function of smart contracts also enables the blockchain to expand from the original currency system to other financial application fields, including applications in securities trading, supply chain finance, banking instruments, payment clearing, anti-counterfeiting, establishing credit systems, and mutual insurance [12]. When entering the era of blockchain 3.0, its application field will go beyond the scope of digital currency or finance, and then expand to any field in need and even the whole of society. **Figure 1** shows the change diagram from blockchain 1.0 to 3.0.

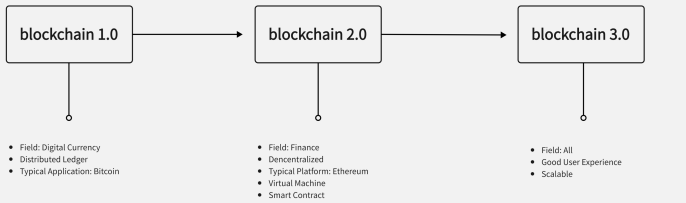

Figure 1. The development of blockchain technology.

2.2. The Structure of Blockchain

A blockchain should be considered as a distributed append-only timestamped data structure [13]. It is a kind of linked data structure connecting each data block in chronological order and the tamper-proof and unforgeable distributed ledger enabled by cryptography. In general, the generated data is stored in blocks, and the block connects with each other end to end in sequence to form a chain structure. At the same time, its structure and the technology within it could make the decentralized distributed ledger tamper-proof, and unforgeable and ensure security when we upload data and access the ledger. Block is the basic unit of chain structure in data storage, so it contains all transaction information. The block has two important parts, the header of the block and the body of the block.

The header of the block consists of the previous block hash, Merkle Tree Root, time stamp, and so on. The previous hash is the hash of the previous block and it is the reason why these blocks could connect with each other. Based on the previous hash, each block could find its previous block and the head is Genesis Block whose previous hash is zero. Therefore, someone could hardly deliberate and capricious alteration of some block because the manipulation would change the hash of the block and cut off the whole chain. A timestamp is complete and verifiable data that can indicate that a piece of data has existed before a certain time, usually a sequence of characters that uniquely identifies the time at a certain moment. Merkle Tree Root is a significant part of the whole block because the Merkle tree is the structure of a block. The body of the block contains all transactions in a period of time. For these transactions, they experience hash and are sorted by size to form the first layer. The value of two consecutive hash values performing the hash calculation is the element at the second layer. Repeating this process till there is only one hash value at a layer and it is Merkle Tree

Root. Based on the structure, blockchain has great potential for data security. **Figure 2** shows the structure of the blockchain.

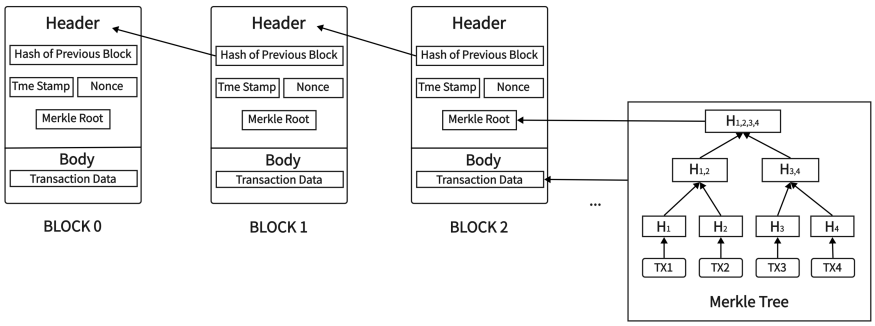

Figure 2. The structure of blockchain.

2.3. Key Features

2.3.1. Trust and Transparency

The blockchain system is decentralized forming a peer-to-peer network. The entire system is transparent to each node so that each node has the same right to send and receive messages, and all transactions in the network are transparent and visible to any node. In addition, all transactions in the network are transparent and visible to any node, and the transaction would record on the block if all nodes reach a consensus, and then each node could also record it to maintain consistency. In this way, the problem of information asymmetry in centralized systems can be easily solved. With the consensus mechanism, the blockchain ensures consistency and reliability while maintaining transparency.

2.3.2. Immutability and Traceability

Immutability is a very significant part of the blockchain, which means that there is no risk of fake data or records. Immutability can attribute to two parts blockchain structure and mechanism. According to the blockchain structure we learned above, if some data is changed in a block, the information of this block would also change which leads to the next block could not find it and destroying the whole blockchain. Moreover, Merkle Tree Root is derived from all transactions through complex hash which means changing one transaction would have a totally different Merkle Tree Root. From the perspective of mechanism, the blockchain network is bound to have a consensus mechanism. Taking PBFT as an example, if someone wants to have cyber attacks, he should control more than 51-percent central processing unit (CPU) power to reach the consensus. However, the cost often outweighs more than the return, making this attack nearly impossible.

Immutability guarantees the authenticity of transactions on the blockchain, which shapes a sound environment for traceability. All transactions in the blockchain have a complete and correct record so that participants can query all relevant information of the transaction in a certain state as needed.

2.3.3. Privacy Security

The blockchain system is a decentralized system that can achieve user privacy and security without relying on third-party protection. Through cryptography, and asymmetric encryption algorithms, users' privacy could be well protected and transactions can be carried out without the need of disclosing their identity. Each user performs identity control through a private key, and a unique corresponding public key generates an address as a unique identity. The public key is generated from the private key, but the private key cannot be worked out from it. In the transaction process, the public key is open to other users, which can be used to encrypt the information that could only be decrypted by the corresponding private key. The private key is private and unique and is held and kept by the user. In addition to decryption, it can also act as a signature to be the user's authorization for transactions or data.

2.4. Blockchain Type

2.4.1. Public Blockchain

The public chain, in brief, is open to everyone. In a public blockchain, each one has the right to take part in the maintenance and reading of the blockchain without the control of some central institution. The data is completely open and transparent. The public chain system is not managed by a central organization, and runs through agreed rules, and these rules can build a trusted network system in an untrusted environment. Systems that usually require public participation and maximize the transparency of data disclosure are suitable for public blockchains. For example, the

bitcoin system which is one of the most well-known public blockchain systems, and its updated version Ethereum. However, in the public environment, the number of nodes is uncertain, the actual identity is unknown, and the network status is hard to confirm, these factors would also affect its reliability.

2.4.2. Consortium Blockchain

A consortium chain is usually built between multiple organizations with known identities to each other. Therefore, the alliance chain system generally requires strict identity authentication and authority management, and the number of nodes is often determined within a certain period of time, which is suitable for dealing with businesses that need to reach a consensus between organizations. Its advantages make it more popular than public blockchain. First of all, compared with the public chain, the efficiency of the consortium chain has been greatly improved. Because each participant in the consortium chain knows each other's identities, and the number of participants is determined within a certain period of time, the number of nodes is less, and the operating efficiency of the consensus algorithm is going to be improved. Second, privacy-preserving will be more secure. The data is only accessible to the members and not accessible to non-members of the alliance. And in the same alliance, different businesses will also have isolation to a certain extent. Last, it does not need tokens to stimulate the work of the whole chain.

2.4.3. Private Blockchain

After the public chain, this part talks about the private chain. 'Private' means the system is not public and only serves some organizations. It is another kind of consortium blockchain that only has one member which is the organization. Private blockchain has an elaborate authority management system that all users need to carry out the authentication. In the private blockchain, everything is under control such as the number of users, and the condition of each node. Its nodes are much fewer than the public chain, and it is more efficient with safer private preserving. However, it does not fit the concept of blockchain, so it does not draw too much attention.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://www.Bitcoin.org/bitcoin.pdf (accessed on 16 October 2022).
2. Aggarwal, S. Blockchain 2.0: Smart contracts. Adv. Comput. 2021, 121, 301–322.
3. Maesa, D.D.F. Blockchain 3.0 applications survey. J. Parallel. Distr. Com. 2020, 138, 99–114.
4. Wan, P.K.; Huang, L.; Holtskog, H. Blockchain-enabled information sharing within a supply chain: A systematic literature review. IEEE Access 2020, 8, 49645–49656.
5. Tejpal, G.; Garg, R.; Sachdeva, A. Trust among supply chain partners: A review. Meas. Bus. Excell. 2013, 17, 51–71.
6. Lou, M.; Dong, X.; Cao, Z.; Shen, J. SESCF: A secure and efficient supply chain framework via blockchain-based smart contracts. Secur. Commun. Netw. 2021, 2021, 8884478.
7. Dolgui, A.; Ivanov, D. 5G in Digital supply chain and operations management: Fostering flexibility, end-to-end connectivity and real-time visibility through internet-of-everything. Int. J. Prod. Res. 2022, 60, 442–451.
8. Yu, M.C.; Goh, M. A multi-objective approach to supply chain visibility and risk. Eur. J. Oper. Res. 2014, 233, 125–130.
9. Sheth, H.; Dattani, J. Overview of blockchain technology. Asian J. Converg. Technol. (AJCT) 2019, 5, 1–3.
10. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. 2017, 24, 1211–1220.
11. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019, 100, 143–174.
12. Xu, M.; Chen, X.; Kou, G. A systematic review of blockchain. Financ. Innov. 2019, 5, 1–14.
13. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telemat. Inform. 2019, 36, 55–81.