Using blockchain technology in IoT manufacture environment for intelligence prediction

HongLing Liu

Guangzhou Nanyang Polytechnic College

Yuqiang Chen (✉ chenyuqiang@126.com)

Dongguan Polytechnic <https://orcid.org/0000-0002-5543-2500>

Research Article

Keywords: Intelligence prediction, Edge computing, IoT manufacturing, Blockchain, Internet of Things (IoT)

Posted Date: April 26th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-425158/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Version of Record: A version of this preprint was published at Soft Computing on August 9th, 2021. See the published version at <https://doi.org/10.1007/s00500-021-06044-1>.

Abstract

Blockchain technology has become more important in recent years in Internet of Things (IoT) manufacturing. Many IoT manufacturing factories have successively invested in the blockchain architecture in the system to manage the data of the IoT manufacturing system for intelligence prediction. The blockchain-based system architecture can ensure the process of data transmission and preservation. However, the use of storage space in industrial IoT systems using blockchain architecture will become a major challenge. Since the blockchain itself is based on the concept of a peer-to-peer network, any node must hold complete blockchain information. When there are thousands of nodes, the cost of hard disk space for storing these data will increase drastically as the number of nodes increases. In addition, newly added working nodes must also copy the original complete blockchain information, and will increase in expansion costs. In order to solve the above problems, this paper proposed a blockchain structure to reduce the space and network transmission costs. The architecture divides the traditional blockchain into two parts, which are divided into private blockchain and public blockchain according to the edge and the cloud. Each workshop will manage its own private blockchain, and the cloud will manage itself public blockchain. Under the proposed structure, each working node only needs to maintain the blockchain at its edge node, and does not need to communicate with other edge node. The experimental results, it can effectively intelligence predict the space cost of node expansion, and it can also avoid the unnecessary network communication overhead caused by the traditional architecture. It can improve the space used of blockchain and reduce the network transfer time.

1. Introduction

Industry technology is a brand-new concept in recent years. Its core concept is to connect existing industrial chains through integration, such as factory production lines, distributors, raw material supply, physical channels, etc., Construct a highly adaptable architecture that can flexibly allocate resources in response to various needs. Blockchain is an emerging platform for developing decentralized applications and data storage, over and beyond its role as a platform for cryptocurrencies. The basic tenet of this platform is that it allows one to create a distributed and replicated ledger of events, transactions, and data generated through various IT processes with strong cryptographic guarantees of tamper resistance, immutability, and verifiability. Public blockchain platforms allow us to guarantee these properties with overwhelming probabilities even when untrusted users are participants of distributed applications. Even though blockchain technology has become popularly known because of its use in the implementation of Cryptocurrencies such as Bitcoin, Ethereum, etc. In this architecture, artificial intelligence can realize self-assessment and demand analysis. Upstream and downstream industries can communicate closely with each other, and can adjust the production line of the factory according to different customized orders at any time, as well as automated order distribution and raw materials. Scheduling, which greatly reduces the time cost and labor expenditure of integrating upstream and downstream industrial chains in traditional industries to communicate with each other, and realizes supply-side optimization [1].

With the increasing awareness of data security, blockchain technology [2, 3, 4] has attracted a lot of public attention in recent years. From financial services, media and telecommunications, healthcare to transportation, etc., blockchain has been added. One of the most well-known blockchain applications is Bitcoin [6]. Since Bitcoin became popular globally in 2017, many people have begun to notice the potential and advantages of blockchain technology. Many countries Compete with enterprises to invest technology and funds into the development of blockchain [5, 6]. Of course, there is a reason for the rise of the blockchain. Take Bitcoin as an example. In the traditional gold flow, it is inevitable for any transaction to pass through financial institutions such as banks. But the emergence of Bitcoin has changed this result. Bitcoin Through the cryptography-based blockchain architecture and consensus mechanism [7], it realizes the decentralization of the account data transaction and storage technology, so that the transaction does not need to pass the authentication of any center. It can be established, successfully breaking the centralized structure of traditional cash flow transactions and creating a new safe transaction method. Through its core decentralization mechanism and anti-tampering technology of data, blockchain has gradually been applied to various applications in recent years. In addition to the innovation of blockchain in the cash flow industry, the relationship between blockchain and the Internet of Things (IoT) has also become closer year by year. Many properties of blockchain are quite compatible with IoT applications [8, 9, 10], for example, the distributed architecture of the blockchain requires IoT devices and IoT devices to communicate directly with each other, without the need for coordination or service through a central incoming device. Therefore, each device can directly communicate with each other and establish synchronization records by itself, while maintaining data consistency and tampering prevention. Blockchain is equivalent to stimulating the potential of IoT itself and increasing the industrial environment scalability.

The architecture of edge computing is already a mature technology today [11]. It is already used in many industrial IoT systems to manage the production line in the factory by establishing a cluster of small edge servers located in the factory. The architecture used [12]. In the factory, the current status of the production line equipment and the information of the produced products will be sent to the edge of the factory via the IoT sensors on the production line, and the edge will perform the management and abnormality judgment of the factory At the same time, the edge is also responsible for sending historical information to the cloud, so that the cloud can also have the information on the edge, and the cloud can also manage and maintain the edge.

However, with the increasing trend of the introduction of such smart factories in the manufacturing industry, the subsequent issue is the security of information in the factory [13]. In recent years, there have been frequent incidents of industrial espionage intrusions in factories. Once the servers are invaded, the information of the products in the factory is likely to be easily stolen or tampered with. This will endanger the intellectual property rights of the company and cause serious damage to the company money loss. Therefore, there is an existing design architecture that combines the blockchain architecture with the industrial Internet of Things. In the blockchain, information is packaged into blocks and connected in series, and verified by the blockchain itself. The mechanism can ensure that the block is absolutely not forged or modified [14], and all information and blocks on the chain will be maintained and verified by all

nodes to be maliciously modified or sent by mistake. In addition, the blockchain architecture can also reduce the failure and loss caused by the invasion of important cluster servers through a decentralized distributed architecture.

Although the blockchain architecture itself can effectively reduce the losses caused by data theft or node failures, due to the decentralized architecture of the blockchain itself, all nodes must hold a block of the complete blockchain in order to perform the district. The maintenance and management of the blockchain makes the blockchain architecture face a certain degree of efficiency problems when the number of nodes increases [15]. According to the rules of traditional blockchain, a block must be verified as legal and must be verified by more than 50% of the nodes before it can be legally added to the blockchain, because the block is broadcasted through P2P. For the propagation between nodes, when the number of nodes is extremely large, the propagation speed of the block will therefore decrease, and the processing speed of the block will be slowed down, and a large amount of bandwidth will be used for the propagation of the block. At the same time, since all nodes need to hold a complete blockchain to maintain and manage the blockchain, as long as each machine is a member of the blockchain, it must have the integrity of the entire blockchain. Information, which is also huge for space consumption. Taking into account the data flow in the industrial environment, the generation of blocks will be more frequent than when the blockchain is used for gold flow transactions. Under such a large-scale blockchain architecture, it may be invisible. On the contrary, the edge computing architecture will cause enterprises to bear more hardware costs and performance issues when expanding more factory nodes [16, 17].

Since the use of traditional blockchain in the Industrial Internet of Things may cause some intangible cost and efficiency issues, this research attempts to propose a hierarchical blockchain architecture. Under this architecture, it is no longer the nodes in all edge servers to jointly maintain the entire blockchain, but instead each edge server has its own private blockchain independently. There will be no interference from the other party's private blockchain. Each edge server will only be responsible for its own private blockchain. In the cloud, there will be a public blockchain. All edge servers will regularly push the blocks to the cloud, and this blockchain will store all the blocks from different edge servers. Through this design, this research attempts to reduce the communication cost between nodes in different edge servers, so as to reduce the transmission time and the purpose. At the same time, under the hierarchical blockchain, each private blockchain only has edge server is used for storage, so only a small number of edge nodes are needed to store the blockchain information, which improves the design method that consumes a lot of storage space in the original distributed architecture. Through the above methods, industrial manufacturers can adopt the blockchain architecture while avoiding the costs caused by the expansion of edge servers or node expansion [18, 19].

This paper has five parts. The first is the introduction, which will explain the research background, research motivation and research purpose, and also summarize the improvement of the traditional methods. The second is the analysis of related technologies and literature discussion. It will explain the basic knowledge of blockchain related technologies, which includes basic blockchain algorithms and theories, and introduces the various types of blockchains. Advantages, disadvantages and

characteristics. At the same time, the consensus algorithm and data storage technology used by the blockchain itself, as well as the communication methods between nodes under the blockchain technology, will be introduced. At the end of this section, we will discuss the existing blockchain technology and research, and explain its help and reference to this paper. The third will explain the system architecture. It will present the hierarchical blockchain architecture, and compare the differences with the traditional architecture, as well as improvements and features, and explain them in a table. Next, explain the block data structure used in this framework and the format of the data received in the experiment. And will explain the physical environment and virtual machine information of the system test, as well as the basic instructions and process of environment construction. The fourth will conduct experimental tests. It will compare the results of the traditional architecture and the architecture under the simulation of the industrial environment data flow, and from the block synchronization speed, block receiving time, block space, etc. To analyze its effect, it will use the number of nodes, data volume, transaction length and other values as variables to analyze the pros and cons of the proposed method and the traditional method in different situations, and present the differences in a chart. Last will summarize this paper. It will explain the specific contributions and future [20, 21].

2. Literature Review

2.1 Blockchain

Blockchain is a decentralized information storage technology that protects and stores data based on the credibility of cryptography. Among them, the most famous application of the blockchain is Bitcoin. Bitcoin may be used as an example for theoretical and explanation. In the blockchain architecture, there is only one blockchain, which is formed by connecting countless blocks. In each block, there is a part called transaction, which represents the data contained in this block [22, 23]. Taking Bitcoin as an example, transaction records represent the records of Bitcoin transferred from user A to user B. Transaction records can have different data storage content with different applications. The method of concatenation between blocks is to concatenate blocks one by one by enclosing the hash value of the previous block in each block. In other words, a blockchain is a data chain composed of multiple blocks, as shown in Fig. 1.

2.1.1 Block data structure

A block can be divided into two parts: a block header and a block body containing transaction data. The block body is usually a list of all transaction records, which is responsible for saving in the blockchain. In the data field, the number of transaction records in a block is not fixed. In terms of Bitcoin, in fact, there will be an average of 3-500 transactions in a block, which records all actual money transaction information [24, 25]. There are three types of metadata in the block header. When verifying the block, you only need to check the block header to complete the verification. The three original materials are as Fig. 2:

- 1) The data of its own hash value and the hash of previous block header .

2) Timestamp (Timestamp), the random number of the proof of work algorithm and the difficulty target of the proof of work algorithm.

3) The transaction records in the current block will use the merkle tree to calculate the hash value of each transaction data, and the block header will store the hash value of the merkle tree root.

When each new block is generated, the current last block of the blockchain will be used as the parent block of the newly generated block, and its hash value will be recorded in the newly generated block, and its own block header. All the fields in will also be connected and hashed to calculate the hash value of its own block header and add it to the end of the blockchain. By analogy, when the next new block is generated, it is also necessary to record the hash value of the current end block before it can be added to the blockchain. The reason why the blockchain is known for its high reliability is that it uses the basis of cryptography to protect data. As mentioned above, the block will save the hash data of the previous block. The hash is a way to calculate the data. The fingerprint method, which means that different data will get different hash values (only a small chance of collision), so each block will have its own unique hash value [26, 27]. Blockchain uses this feature to protect data, which means that if the transaction information (data) of one of the blocks is falsified, the hash value of the block will change together, because each block is above hash data of each block is concatenated. If the hash data of one of the blocks does not match or has been maliciously modified, it can be easily verified. In addition to recording the time stamp when the block is generated, the block header requires a consensus mechanism in Bitcoin to determine who will process the block through proof of work or mining competition. Therefore, random storage is required. The number and the difficulty target of the workload proof algorithm [28, 29, 30]. The detailed method of the workload proof will be mentioned later. Finally, the block header will store the hash data of all transactions. This hash value is the root of the hash tree calculated by the hash tree algorithm. The detailed algorithm will be explained later.

At present, the common hash algorithm used in blockchain is SHA-256 (secured hash algorithm 256). SHA-256 is a single function, given an input value and a result will be obtained. It is almost impossible to calculate the input from the result, because efficient calculation of the inverse function of SHA-256 does not currently exist, and even the possible method of estimating the input value does not exist, which also means blockchain data. It is non-tamperable nature [31, 32]. Different from many current decentralized databases, one of the most famous features of the blockchain is its decentralization. The blockchain uses decentralized information storage technology to store information [33, 34]. The entire blockchain, it is jointly maintained by many nodes. Since all nodes jointly maintain the entire blockchain in this architecture, the entire blockchain is jointly maintained by tens of thousands of nodes, which means that there is no nodes can arbitrarily alter or create illegal data and blocks on their own. The reason is that all newly generated blocks should be verified by most nodes. The method of verification is that 50% of the nodes have verified to be a legal zone. Blocks, only blocks that have passed legal verification can be added to the blockchain. Since the blockchain needs to be maintained by all nodes, each node needs to maintain the information of the entire blockchain. Take Bitcoin as an example. When you use Bitcoin for the first time, you must download the entire Bitcoin blockchain (ledger) to your computer before you can

participate in the maintenance and use of the blockchain network. Each node maintains blockchain information, which also ensures that the data will not disappear due to partial node failures [35, 36].

2.1.2 Genesis Block

As mentioned above, the blockchain is formed by concatenating many blocks, and each block will record the hash value of the previous block as a check for block forgery. Among them, the first block is called the genesis block. The genesis block is the ancestor and starting point of all blocks. Since the genesis node is the earliest zone, the hash value of the previous block stored in it is 0. All blocks can be accessed to the genesis block by looking for the hash value of the previous block [37, 38].

2.1.3 Consensus mechanism

Consensus mechanism is a method used in computer science to maintain the operating sequence and fairness of the system, and it is now mostly used in blockchain applications [3]. Since all working nodes in the blockchain are equal, the consensus mechanism must be used to determine who is responsible for the generation of the block when processing the block. Take Bitcoin as an example: In Bitcoin, there is a famous term called mining. In the past few years, it has attracted a large number of users to join the ranks of Bitcoin. Among them, mining is one of the consensus mechanisms, proof of work:

• Proof of Work

This is a way to solve a large number of service and resource abuse, or block service attacks. The core idea is to require users to pay relatively heavy costs before obtaining the services they want to prove that they are sincere or trustworthy. The general workload proof usually requires the user to perform some complicated calculations that take a certain amount of time, but this answer can be easily calculated by the service party quickly, and the user pays the time and cost as a guarantee to make the service party convinced of the user's Resource access is meaningful. Mining in Bitcoin requires users to perform some complex calculations to obtain the right to package new blocks. In the proof of work, the hash function is most commonly used. Since any value n of the input hash function $h()$ will correspond to a result of $h(n)$, and if n changes by one bit, it will cause an avalanche. Therefore, it is almost impossible to reversely deduct n from $h(n)$. Therefore, by specifying the characteristics of $h(n)$ and allowing users to perform a large number of exhaustive calculations, the proof of work can be achieved. In Bitcoin, mining is to ask the user to find a hash value of raw data plus an integer, and the result is exactly the N digit 0. For example, the original data is Hello World, and the SHA256 function is used as authentication. The server requires the user to find a hash value $h(n)$ with the first 4 digits of 0, then the user must find an integer and connect with Hello World. After that, the first 4 digits of its hash value are all 0s, so starting from Hello World0, the user will eventually get a specified $h(n)$ at Hello World107105:

After completion, tell the server the value of n (where n is the Nonce mentioned above). After the server checks, if the result is correct, the user can get the service. The server only needs to substitute Hello World107105 into the SHA256 function to verify the calculation.

Bitcoin uses a consensus mechanism to ensure that the nodes responsible for packaging are trustworthy. However, Bitcoin is a public blockchain. All nodes that maintain blocks are public users. No one is willing to handle transactions for others without compensation. At the same time, it also costs energy and time to prove the workload. Therefore, Bitcoin Coins use an incentive mechanism to encourage nodes to invest in the maintenance of the blockchain. To put it simply, if you can successfully obtain the packaging rights and complete the packaging of the block, you will be rewarded with a certain amount of Bitcoin upon completion. This is the overall system of mining: through rewards, public nodes are encouraged to spend resources to maintain overall blockchain. The uncertainty of the hash algorithm results in the possibility of being selected as the packer is full of variables. The reason is that the block packer can only be responsible for the first to calculate the random number, which also leads to the competition of the pack block (mining). Sexually, it enables more people to invest in packaging in order to obtain rewards, and at the same time increases the cost and time required for forging blocks or fraudulently obtaining rewards, and improves the security of the blockchain.

- **Proof-of-stake (Proof-of-stake, PoS)**

This consensus mechanism is usually used in consortium chains or private chains (mentioned below). Under this mechanism, every node holding currency has the opportunity to be selected as a new block producer, but the more equity, they have People with will have a higher probability of being selected as a packager. The reason is that people with more currencies usually have completed multiple packages. It is a friendly node that will not maliciously damage the block or forge. Compared with the proof of work, this algorithm does not require time-consuming and high-cost proof of work. It only needs to select the packager based on the equity. Of course, such a system results in a relatively low chance for nodes with low rights to obtain the right to package, which also increases the equity of all shares. The risk of being held by a specific node.

2.1.4 Types of Blockchain

In the current environment, blockchains can be roughly divided into three types based on their functions and permissions, namely, public blockchain, consortium blockchain, and private blockchain. The public chain is the most traditional blockchain. In the initial application of blockchain, Bitcoin is a public chain. Its nature is public as its name implies, which means that all information (such as transactions) in its blockchain is public. Similarly, any information in the block is also jointly maintained by everyone. Under this structure No node has higher power than other nodes. All behaviors on the blockchain are determined through a consensus mechanism. This decentralized mechanism is also one of the reasons for the flourishing of the blockchain. Of course, in some environments, it is not hoped that the information of the blockchain can be accessed by anyone at will. At this time, the alliance chain and the private chain are produced. In the alliance chain, only people or groups specially selected in advance can participate in the consensus mechanism. A private chain is a chain with more restricted permissions, in which only the specified nodes can participate in the consensus decision, which makes the blockchain better controlled.

2.2 Hash Tree

A merkle tree is a tree-like data structure. As shown in Fig. 3, this tree only stores the hash value of the data at the leaf nodes. In the case of the blockchain, it will calculate the hash of all transaction content separately after the value, it is stored in the leaf node; the hash value of the non-leaf node is obtained by concatenating the hash values of other child nodes and calculating the hash. As mentioned above, the blockchain will first calculate the hash value of all transactions and store it in the leaf node. Since the blockchain is usually a binary hash tree, the hash value of the leaf node will be connected in pairs, and calculate the hash value. The result obtained is the hash value of the parent node. The parent node remaining after repeating the above actions is the Merkle Tree Root, because this root node passes all the leaf nodes are obtained layer by layer, so as long as the data of any leaf node is modified or does not match the actual data, it will be easily identified.

In the theory, even if you don't use a tree structure and just concatenate all the transaction records together to hash the hash value, you can still distinguish the transaction records, but you need to pay more for verification.. The advantage of using the hash tree structure is that when verifying the legitimacy of the leaf nodes, it only needs to verify a few of them to complete the verification. For example, in the case of Bitcoin, suppose we want to confirm whether TxD exists in this block. Then we only need to download the three values of Hash (C), Hash (AB), and Hash (ABCD) of this block to complete the verification. The verification method is:

- 1) Calculate the hash value Hash (D) of TxD.
- 2) Calculate the hash value Hash (CD) of Hash (D) and Hash (C).
- 3) Calculate the hash value Hash (ABCD) of Hash (AB) and Hash (CD).
- 4) Confirm that the calculated Hash (ABCD) is consistent with the hash tree root or Hash (ABCD) in the block.
- 5) Consistency means that the transaction does exist in this block, disagreement means that the transaction does not exist

2.3 Blockchain fork

The consensus proof algorithm; One is to reduce the risk of block tampering or forgery, the other is to reduce the probability of blocks being generated at the same time and added to the end of the blockchain. Due to the characteristics of consensus proof, even if there are many nodes, the probability of calculating a legal random number at the same time is very low. However, sometimes it happens that two blocks are generated at the same time, and the last block is regarded as the parent block at the same time. In this case, it will fork, since when a node generates a block, the transaction information contained in it is broadcasted by neighboring nodes. So the transaction information contained in the block generated by different nodes will also be different, which means when two blocks are generated at the same time, these two blocks will have the same transaction data at the same time and are legal blocks at the same time, resulting in repeated additions of transactions. According to the basic principles and

security of the blockchain, it is not allowed to have sidechains under normal operation conditions. At this time, the blockchain will usually adopt the longest chain principle to deal with.

2.3.1 The longest chain principle

Since the network has a delay in communication in the actual environment, different nodes receive these two blocks in a sequential order, and when a node generates a new block, it tends to receive the first one blocks are connected. So after a period of time, there will always be one branch chain that is longer than the other. At this time, the shorter chain will be discarded according to the longest chain principle, as shown in Fig. 4, and the longest chain as the main chain continues to extend. At this time, the discarded branch chain transactions must be recalculated by each node and packaged into blocks before they can be recorded in the block chain again. Take Bitcoin as an example, Bitcoin takes a long time to verify transactions. One of the reasons is to wait for the block where the transaction itself is located on the longest chain in the blockchain. Usually it will wait for about six blocks to be connected. Make sure that your block is not in the short chain, then the transaction can be considered as successful.

2.4 Review of related research

In this section, we will briefly review the current research on blockchain. In [19], the method of applying blockchain technology to the edge computing environment is introduced. This paper focuses on the blockchain application of mobile devices and edge computing devices. At the same time, it provides a relatively basic architecture model. Deep learning is used to improve the resource allocation and communication between mobile devices and edge computing, and to improve communication efficiency. It points out that communication traffic is a major cost in the edge computing environment. This shortcoming of block chain is temporarily store blocks instead of directly syncing to the cloud was proposed. It solves the problem of traffic overload that blockchain may face in the industrial IoT environment, and uses edge terminals The network temporarily stores the generated information, and transfers the block to the cloud for storage until the traffic permits. This architecture provides the idea of a hierarchical blockchain. Compared with the former, our paper will focus on space utilization and node cost.

3. System Architecture

3.1 Architecture definition

Since the proposed paper is a system designed specifically for the edge computing environment of the blockchain architecture as Fig. 5, we define the architecture diagram of traditional edge computing first, and then define the architecture that blockchain computing is applied to. First, the architecture diagram of the traditional edge computing system, which is divided into the cloud and the edge. Here, it is assumed that each factory is an edge computing unit. Each edge end contains all the machines in the factory and multiple working nodes that can perform calculation processing. The machine will periodically generate product information and the status data of the machine itself during product production. These data will

device of the Internet of Things are passed to the working nodes in the factory, and these nodes can store and process the data. The cloud can communicate with each edge node and obtain information about a specific machine. If necessary, the cloud can also implement operations on a specific machine.

Blockchain is essentially a decentralized storage technology. It stores data in blocks by means of blocks, and connects each block in a concatenated manner. In Fig. 6, we define the traditional area Blockchain technology uses the architecture diagram of the edge computing system. The architecture of the cloud and the edge is the same as in the Fig. 5. Each edge server represents a factory. In the blockchain architecture, every working node in the factory will be added to the maintenance of the blockchain, and every work in the cloud nodes will also join the maintenance of the blockchain, which means that all nodes can see and maintain the information on the blockchain, and all nodes will save the complete information of the blockchain. If any node tries to tamper with or lose the block Information can be corrected by other nodes immediately. And the machines in each factory will also generate data, which will be processed by the nodes in the factory and then packaged into newly generated blocks and synchronized to the blockchain. Since the information of the blockchain is shared and maintained by everyone at the same time, no matter whether the node is located in the cloud or on the edge after the block is updated, the latest block can be held.

In Fig. 6, it demos the architecture of the current blockchain technology applied to the edge computing environment. Under the architecture, all nodes maintain the blockchain. According to the nature of the blockchain, this architecture can indeed provide good protection and tampering protection function. However, due to the nature of the blockchain itself, in order for any node to participate in the maintenance of the blockchain, the node must download the complete information of the blockchain, which will not cause any problems in the short term, but as time evolves, it uses space will increase rapidly, which leads to any node must have enough hardware space, otherwise it will not be able to maintain the blockchain and add new blocks. At the same time, when the manufacturer decides to expand a new edge computing terminal, since new nodes must also join the maintenance of the blockchain and have complete blockchain information, as the length of the blockchain increases, and the new cost of adding new edge computing units will also increased. In addition to some shortcomings in hardware cost, it is mentioned that after a block is successfully packaged and added to the blockchain, it must be authenticated by more than 50% of the nodes before it can be recognized as a legal block, Since all nodes maintain the blockchain at the same time, this means that at least half of the working nodes must pass authentication before a block is successfully added to the blockchain. This will happen when there are many factory nodes. This leads to serious efficiency problems. At the same time, broadcasting this block to other nodes will also cause a lot of network resource consumption, which is a relatively serious problem for the factory environment.

3.2 Blockchain system architecture

The architecture of traditional blockchains applied to edge computing environments and pointed out some of the shortcomings that may occur. Therefore, this paper proposed a system architecture that can optimize the efficiency of blockchain technology in edge computing environments and space usage. It

will first explain the architecture of the system and the environment configuration of the built system, and explain the details of the different modules one by one, and finally explain the operation process of the overall system.

Figure 7 is the system architecture proposed in this paper. It is an improvement of the system in Fig. 6. This architecture uses hierarchical blockchain technology. The purpose is to reduce some space and time efficiency problems. Describe the difference between this architecture and traditional blockchain.

3.2.1 Architecture description

First of all, it is called hierarchical blockchain technology, which means that the blockchain is hierarchical. This architecture is that all nodes jointly maintain the only blockchain. All management and block additions are shared by all nodes. What this paper proposes in the architecture that each edge computing unit independently, its own blockchain. Here we refer to each edge unit's own private blockchain as a private chain, and the cloud itself holds a public chain. Taking Fig. 7 as an example, there are three edge private chains and one cloud public chain. The private chain means that its blocks can only be maintained and controlled by specific nodes. Under this architecture, each edge unit can only access the private chain of its own edge unit and cannot access the private chain of other edge units. It means that the edge units are completely independent; while the cloud holds a public chain. Although it is called a public chain, it does not mean that nodes on other edge units need to participate in the maintenance of the blockchain. Only the cloud is involved in the maintenance of this chain. The reason why it is called a public chain, because the blockchain holds all the blocks at the edge. In this method, all blocks on the edge private chain will eventually be synchronized to the public chain in the cloud. It will describe the module functions of each working node and the process of synchronizing blocks in detail below, as shown in Fig. 8.

3.2.2 System module

The difference between the responsibilities of the edge work node and the cloud work node, as shown in Fig. 8. The following will start with the introduction of the module of the edge-end working node, and at the end explain the difference in behavior between the cloud-end working node and the edge-end working node.

- **Raw Data Generator:** In order to simulate the process of actual factory data generation, a raw data generation module is set in each edge working node. This module will periodically generate raw data. The content includes various status messages of production line machines, product process information, time stamps, and other information. This module will send the generated raw data to the raw data receiving module.
- **Raw Data Reciever; Raw Data Sender:** These two modules belong to the Raw Data Interface. The raw data receiving module will receive the raw data generated. The original data of the module, and the received data is transferred to the original data conversion module for conversion. In this system, all data

should be saved in the form of blocks, so all the original data will be parsed in the original data conversion module and converted into the form of transactions, and packaged into a block Blocks, and these blocks will be sent to the block receiving module.

- Block Reciever, Block Synchronizer: These two modules are collectively called Block Interface, where the block receiving module will receive the original data conversion module packaged. The block is completed, and it is verified and hashed. The transaction in each block will be checked to ensure that it has not undergone any tampering. After confirming that the block is correct and is a legal block, the block will be synchronized to other nodes through the block synchronization module. The synchronization will prioritize the synchronization to the working node of the same edge. Try to keep all nodes on the edge side holding the same block information. At the same time, the block synchronization module will synchronize the older block to the cloud block interface and send. The block receiving module accepts the received old blocks. The cloud block synchronization module and the block receiving module have roughly the same functions as those on the edge, but the synchronization range of the synchronization module is limited to the cloud The other working nodes do not include the edge nodes. After being accepted by the block receiving module, the private blockchain and public blockchain will be stored in the hard disk of the working node in the form of blocks at the same edge In the end, all the working nodes will hold the private blockchain information at the edge end at the same time. This enables this architecture to prevent data tampering, and also achieve the effect of redundant backup, ensuring that information will not be lost. Dividing blocks into edge private chains and cloud public chains is the main feature.

3.2.3 Block synchronization mechanism

The private chain block synchronization method of a single edge is shown in Fig. 9.

Figure 9 depicts that the original data is first generated from the factory machine, and then passed through the component named Data Interface. Correct after the original data is preprocessed, it is packaged into a new block and broadcast to each working node. The worker responsible for packaging is determined through a consensus mechanism. Because of the industrial environment, consensus mechanisms such as workload proof are not suitable for this. Therefore, the method of holding proof is used to determine who is responsible for this packaging. Each worker node holds and maintains private blockchain, and it can only be accessed by the worker nodes on the edge. After that, monitor the private chain through the Block Synchronizer, and synchronize the old block generated earlier to the public chain in the cloud. This action will occur at every edge, so the cloud, the order of blocks received by the public chain is not fixed, as shown on the right in Fig. 9. In the end, the public chain in the cloud will hold all the blocks at the edge, and the edge will only save the blocks it generates.

3.2.4 Architecture characteristics

The advantages and disadvantages of the architecture compared to the traditional architecture. The difference between the traditional method and the proposed method is compared in Table 3.1. In this architecture, one of the biggest differences between the traditional method and the proposed method is the number of blockchains. This architecture divides the blockchain into different independent

blockchains by taking the edge and the cloud as the unit. The most obvious improvement under this architecture is the use of storage space. Under the traditional blockchain, all nodes must maintain a single blockchain, and this blockchain must store all received data. In this case, the data generated by each edge will be stored in the same blockchain, and each node must bear its storage cost. After the blockchain is divided by this architecture, each edge only saves itself edge [18, 19].

The generated blocks do not interfere with each other at the edges, which improves the aforementioned space usage problem. Since the only cloud holding all blockchain information, storage costs will become controllable and will not increase due to the number of edge nodes. Moreover, because the edge terminals do not interfere with each other, the coupling degree of the system is also improved, and there is no need to communicate with other edge terminals, the bandwidth cost and processing delay are also reduced. It is worth noting that this architecture is the biggest In addition to the improvement in space, the benefit is that it can reduce the cost of node expansion. Under the traditional architecture, whenever a new node is expanded, the new node must synchronize the existing block information and maintain it together. This leads to As the number of nodes increases, the space cost will also increase significantly, which seriously affects the cost of manufacturers to expand new edge terminals. With this system architecture, the new node does not need to store the old blockchain information, because each edge terminal is independent, so the newly created edge terminal does not need to synchronize the old block, but only needs to maintain itself. The information generated is sufficient, so the cost of expanding nodes can be greatly reduced. Compared with the above advantages, these efficiency and cost advantages are achieved through the reduction of security. Since the traditional blockchain is maintained by all nodes, it is very difficult to tamper with the information of any node. It is difficult, but after changing the layered architecture proposed, since the number of nodes maintained by each blockchain is reduced, the risk of tampering will also be relatively higher.

Table 3.1
Comparison of proposed architecture and traditional architecture

Item	Traditional architecture	Proposed architecture
Number of blockchains	only one public chain	Each edge has a private chain and the cloud holds a public chain
Maintenance method	All nodes are jointly managed	Private chain is only managed by the edge, and cloud public chain is managed by the cloud
Storage space cost	higher	lower
Bandwidth cost	higher	lower
Processing delay	higher	lower
Expansion node cost	higher	lower
Data security	higher	lower

3.2.5 Block data structure

According to the application of the blockchain, the data structure of the block will be different. The block structure used in this system is shown as Fig. 10. Since this experiment does not use proof of work as a consensus algorithm, there will be no difficulty target and not required for verification.

- Block Hash: This block stores the hash value of all the fields of the Block Header concatenated with the conventional blockchain. because SHA-256 is usually used as the hash function, this block field basically has 256 bits
- Previous Block Hash: Store the hash value of the previous block, with 256 bits
- Timestamp: The time when this block was packed
- Merkle Root hash: In the blockchain, a hash tree is used as a data storage method, in which the hash value of the tree root can simply represent the fingerprint of the overall data.
- Merkle Tree: Located in the part of the block body, the hash tree will store data in the part of the leaf node, and calculate the hash value of each layer through the hash operation.

Transaction data generally refers to the data stored in the blockchain as Fig. 11. The environment used in this experiment is on the edge computing environment. The goal is to save the state information of the machine through the blockchain, so its data structure will be similar to the conventional. The blockchain is different and will be shown below.

- Transaction Serial Number: There will be multiple transaction data in a block. This field is used to indicate which transaction is the first.
- Timestamp: The time when this transaction was generated.
- Machine ID: Used to distinguish the machine from which the data is sent.
- Machine Status: The actual data field to be saved in the transaction data can be different according to the application, or there are even multiple data fields to be saved.
- Record Timestamp: The time stamp when the machine status is generated.
- Machine Serial Number: The serial number when the machine generates this message.

3.3 System Information

This system uses three physical computers for simulation. Because the performance comparison between this architecture and the original method can only be simulated in a multi-node environment, the number of available machines will be increased by setting up virtual machines to simulate a real edge computing environment. In Table 3.2, the computer equipment used, the resource configuration information of the virtual machine, and the development tools used are listed.

Table 3.2
System information of machine 1 and its virtual machines

Machine name	OS	CPU	Number of CPU cores	Memory	OS
Computer 1		4.8GHz	Eight core, Eight threads	24GB	Windows 11 64 bit
Virtual Machine 1(Edge1)	-		Two core, two threads	6GB	Linux
Virtual Machine 2(Edge2)	-		Two core, two threads	6GB	Linux
Virtual Machine 3(Edge3)	-		Two core, two threads	6GB	Linux
PS: Computer 2: 4.8GHz; Computer 3: 4.8GHz.					

3.4 System configuration

The tools used to develop this architecture system and the method of setting up the environment. Refer to the diagram for the process. First of all, because this framework needs to simulate the situation in the edge computing environment, it is inevitable to use virtual machines as an alternative when there are insufficient physical machines. The hardware virtualization software, we use VMware Workstation, It is one of the commercial software products sold by VMware. It allows users can create and execute multiple virtual machines at the same time, and each virtual machine can execute its installed operating system. To configure three virtual machines for each physical machine and set the resources to be allocated to the virtual machines, and then install the Ubuntu OS system in sequence. After the installation is completed, because the communication between virtual machines in the experimental

environment is necessary, the network interface card of each virtual machine must be set before use. After setting the bridge interface card for each machine, each machine can have an independent IP under the local network and can communicate with each other, simply use the built-in Linux Ping command to test.

4. Experimental Test

In order to really analyze and test the performance comparison between the proposed architecture and traditional methods, we will build a simulated edge environment, and the hardware devices. The following experiments are performed by a total of ten virtual machines, and are divided into three edge ends according to the different physical machines: Edge1, Edge2, and Edge3. All nodes except the virtual machine Cloud work as working nodes and only maintain their own private Blockchain. The virtual machine Cloud is responsible for the processing of the cloud and is responsible for receiving blocks from each edge. Among them, the virtual machine Edge11, the virtual machine Edge21, and the virtual machine Edge31 not only serve as the work node, but are also responsible for simulating the behavior of the factory machine, responsible for the generation of raw data and outputting the data to the work node on the edge of its own.

4.1 Test items

The performance comparison between traditional blockchain architecture and hierarchical blockchain architecture in the following projects, and analyze the differences:

- 1) The original data is generated by the virtual machine Edge11, the virtual machine Edge21, and the virtual machine Edge31, and other virtual machines serve as working nodes. These data will be converted into blocks by each working node and saved in the form of blockchain, and finally stored on the hard disk. This experiment will analyze the comparison of the hard disk space consumed by the traditional method and the proposed method as the total amount of processed data increases.
- 2) The original data is generated by the virtual machine Edge11, the virtual machine Edge21, and the virtual machine Edge31, and other virtual machines serve as working nodes. After receiving sufficient data, these data will be packaged into blocks by each working node and broadcast to other working nodes. Since the nodes are fully connected in the traditional method, the method proposed in this paper is to take each edge terminal as private Therefore, this experiment will analyze the number of attempts to broadcast the zone to other nodes in different methods as the total amount of processed data increases.
- 3) The original data is generated by the virtual machine Edge11, the virtual machine Edge21, and the virtual machine Edge31, and other virtual machines serve as working nodes. This experiment sets the variable as the number of transactions that can be recorded in each block, and analyzes the speed difference between the traditional method and the proposed method under different transaction numbers.

4.1.1 Comparison of hard disk space consumption

The explains why the traditional blockchain consumes a large amount of hard disk resources in a multi-node environment, as shown in Fig. 6, which shows that all nodes in the traditional blockchain must hold block information, resulting in a large number of hard disks occupied. The hierarchical structure proposed is shown in Fig. 12. Since each edge end only needs to maintain its own blockchain, compared to the traditional architecture, only the cloud must hold all blockchain information, so it can significantly reduce the space occupation of the block.

The comparison of space occupancy under quantitative data through charts. First, the quantitative data will be generated by the data generation nodes: virtual machine Edge11, virtual machine Edge21, and virtual machine Edge31. The transaction list size of the block tested in this experiment is 1024, which means that a block can store 1024 pieces of data. After that, the total amount of data generated by each data generating node is 200, 300, 400, 500 and 600 blocks of data. These data will be received by each working node and converted into blocks. In addition, the data generating node will only send data to the working nodes at the same edge, that is, the virtual machine Edge11 will only send data to the virtual machine Edge11, virtual machine Edge12, and virtual machine Edge13. After completing the data generation and synchronization of all blocks, compare the space usage in the two methods. In order to analyze the resource usage under different architectures, this experiment uses functions in the Java language to obtain the target blockchain and the space used by the block. Since there is no method to obtain the actual size of the object in the native methods of the Java language, this article uses the external library java-sizeof to obtain the size of the blockchain object. In Fig. 13, the comparison of space under different amounts of data is shown. It can be found that, in general, the architecture proposed in this article is superior to the traditional architecture for spatial optimization, the data at each edge is isolated by using a hierarchical blockchain architecture. It can reduce the space problem of rapid expansion due to the increase of nodes in the traditional method.

There is a feature in this architecture. When there are more edge ends, it can save more space consumption. The reason is that the hierarchical structure will cut the original data more finely due to the increase of edge ends, and share it evenly among each edge end. And each edge end only needs to maintain its own data, so it can be more efficient than traditional methods that have to maintain all data. The experiment is shown in Fig. 14, the total data volume range is constant, all are 100 blocks range, and all edge ends are three working nodes. Because of the limited number of machines, only 2, 4, 6 edge-end conditions were initially tested. First of all, the situation where there is only one edge is the same as the traditional method. After gradually increasing the edge, a significant reduction in space consumption. Therefore, this method can effectively reduce the space cost that enterprises need to bear in the face of a large-scale industrial environment.

4.1.2 Comparison of data volume and transmission time

The different architectures to complete block synchronization and transmission under quantitative data. First, the virtual machine Edge11, the virtual machine Edge21, and the virtual machine Edge31 are also used to generate the original data. Under the two architectures, the original data will be packaged into blocks by each node and broadcast to the other nodes. In the next experiment, this article will distinguish

the system architecture strategy used by the nodes by code names. The nodes using traditional methods are NodeA1 to NodeA9 in Cloud A, and the nodes using the hierarchical architecture are NodeB1 to NodeB9 in Cloud B. Corresponding time cost must be spent in the process. The count of the time spent and the transmission time of each node, each edge end and the cloud.

Figure 15 directly shows the time it takes for all nodes to transmit under different amounts of data. Node-A1 to Node-A9 in this experiment represent nodes with traditional architecture and hierarchical approach. The nodes of the architecture, it can be observed that as the amount of data increases, the amount of transmission spent will increase by the same amount, and the hierarchical architecture can reduce the transmission time by a certain amount compared with the traditional architecture. The reason is that the nature of the blockchain itself. When the blockchain is broadcasting, the block must be synchronized to all nearby nodes. At the same time, the block needs to be broadcast to half of the nodes to receive and verify that it is correct before it can be added to the blockchain. This means that if the area is maintained more nodes in the block chain, the longer the verification time will be spent. In this experiment, since the private chains are segmented, and each private chain is maintained by only three nodes, this means that each time a block is synchronized, it only needs to broadcast the block to the other two nodes. On the contrary, in the traditional architecture, all nodes need to know each other, so in the experiment, any node will need to broadcast the block to the other eight nodes and the cloud when broadcasting, which is a more transmission than the hierarchical blockchain. In most cases, the blockchain still broadcasts in a P2P manner, so this cost will only be affected by nearby nodes. The quantity is also affected. The hierarchical blockchain avoids some communication costs through the hierarchical structure, and reduces the time cost of verification.

In order to be able to compare the difference in transmission time more clearly, Fig. 16 calculates the average of the time spent by each node under different architecture methods. This data makes it easier to see that this architecture method is slightly better than the traditional method. Figure 17 lists the transmission difference between each edge end, basically the reason for the result is the same as described above. Figure 18 shows the time it takes for the cloud node to receive the last block. In the experiment, the cloud is only the recipient of the final block, and there is no further calculation optimization.

In addition to analyzing the impact of the number of blocks in time, we also experimented with the impact of different block transaction list sizes on time under the constant number of blocks. In the experiment, the time spent under different block transaction list lengths is tested by fixing the number of blocks range to 100 blocks. The code names of the nodes are the same, which distinguish traditional architecture nodes from hierarchical architecture nodes. Generally speaking, the results are similar to the results. The difference is that the time saving effect is slightly reduced. The reason is that the optimization and improvement of the processing time of this architecture lies in the number of blocks. When changing, therefore, the number of blocks does not significantly affect the time gap as Fig. 19 and Fig. 20.

4.1.3 Comparison of communication times

In IoT environment, bandwidth is also a very tight resource. Most of the bandwidth in many factories is used for equipment communication and data transmission. Therefore, whether the system architecture has a good bandwidth usage architecture is worth considering. To monitor the nodes of different architectures and observe their behavior during regional synchronization, and analyze whether the architecture is a bandwidth-friendly system. The system architecture is to analyze the number of times that the work node communicates with other work nodes in different areas. The results of the experiment are shown in Fig. 21 and Fig. 22. It shows that the architecture can basically retain a relatively small number of communications. The reason is the hierarchical architecture design of the system. Due to the privatization of the chain, each time the node that must communicate is only its own other nodes; on the contrary, the traditional architecture must synchronize blocks with the other eight nodes and the cloud. This is not a bandwidth-friendly behavior. In fact, the block synchronization performed in the experiment may not necessarily add a new block, because it is very likely that the node that receives the broadcast already holds the block, and the newly received block will be discarded immediately. However, the sending action is still performed. It can be seen that when there are more nodes, more blocks will actually be broadcast, but they are actually nodes that do not need to be synchronized, resulting in bandwidth waste. By dividing and privatizing the blockchain, bandwidth waste can be effectively reduced.

5. Conclusion

Through the reliability of cryptography, blockchain technology provides a more reliable choice for today's data storage solutions. At the same time, due to the characteristics of using P2P network communication, it can also be used as a secure distributed storage of data lib. This paper proposed a new blockchain technology architecture based on the viewpoint of industrial security and cost. It optimized the existing blockchain system to make it more suitable for practical industrial Internet of Things applications. The layered architecture uses private chains to separate different industrial environments, which not only improves the overall system The manageability and reliability of the blockchain has improved some of the shortcomings of the blockchain itself, such as the massive consumption of space, the slowdown in processing speed caused by multiple nodes. This paper uses a hierarchical structure to solve the shortcomings of the traditional blockchain, and increases the operating efficiency of the overall system and reduces the transmission cost.

For future work, blockchain as an emerging technology may still have many immaturities. In the face of actual industrial and business networking applications, it still needs to be discussed regarding the completeness of the system architecture. In addition, considering that the current blockchain environment also lacks a set of consensus mechanism algorithms suitable for industrial and business networking, it is also limited to a certain degree in transaction processing speed.

Declarations

Ethical approval

No need ethical approval.

Funding details

This work was supported in part by Guangdong Natural Science Youth Fund under Grant (No.2020A1515110162), Key projects of social science and technology development in Dongguan under Grant (No. 2020507156156), in part by Special fund for science and technology innovation strategy of Guangdong Province under Grant (No. pdjh2020a1261).

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed Consent

No need informed consent.

Authorship contributions

HongLing Liu: Conceptualization, Methodology, Validation, Investigation, Writing, Funding acquisition, Formal analysis, Software, Resources, Visualization, Funding acquisition.

Yuqiang Chen: Methodology, Validation, Writing -Review & Editing, Supervision.

References

1. Barenji AV, Guo H, Tian Z, Li Z, Wang WM, Huang GQ, "Blockchain-based cloud manufacturing: Decentralization", *Proc. 25th Int. Conf. Transdisciplinary Eng. (ISTE)*, pp. 1003–1011, Jun. 2018, [online] Available: <http://ebooks.iospress.nl/publication/49887>
2. Abeyratne S, Monfared R (2016) Blockchain ready manufacturing supply chain using distributed ledger. *Int J Res Eng Technol* 5(9):1–10
3. Li Z, Barenji AV, Huang GQ, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform", *Robot. Comput.-Integr. Manuf.*, vol. 54, pp. 133–144, Dec. 2018, [online] Available: <http://www.sciencedirect.com/science/article/pii/S073658451830022X>
4. Lavanya BM, "Blockchain technology beyond bitcoin: An overview", *Int. J. Comput. Sci. Mobile Appl.*, vol. 6, no. 1, pp. 76–80, 2018, [online] Available: <http://www.ijcsma.com>
5. Crosby M, Pattanayak P, Verma S, Kalyanaraman V, "Blockchain technology: Beyond bitcoin", *Appl. Innov.*, vol. 2, no. 6, pp. 71, 2016, Available:<http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf>
6. Karame G, Androulaki E, Capkun S, "Double-spending fast payments in bitcoin", *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 906–917, Oct. 2012
7. Cai W, Wang Z, Ernst JB, Hong Z, Feng C, Leung VCM (2018) Decentralized applications: The blockchain–empowered software system. *IEEE Access* 6:53019–53033

8. Bahga A, Madiseti V (Jan. 2016) Blockchain platform for industrial Internet of Things. *J Softw Eng Appl* 9:533–546
9. Sevilla M, "Does blockchain hold the key to a new age in supply chain transparency and trust?", 2018, [online] Available: <https://www.capgemini.com/research/does-blockchain-hold-the-key-to-a-new-age-in-supply-chain-transparency-and-trust/>
10. Zheng Z, Xie S, Dai H, Chen X, Wang H, "An overview of blockchain technology: Architecture consensus and future trends", *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, pp. 557–564, Jun. 2017
11. Toyoda K, Mathiopoulos PT, Sasase I, Ohtsuki T (2017) "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain". *IEEE Access* 5:17465–17477
12. Yin W, Wen Q, Li W, Zhang H, Jin Z (2018) An anti-quantum transaction authentication approach in blockchain. *IEEE Access* 6:5393–5401
13. Wang X et al., "Survey on blockchain for Internet of Things", *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019
14. Christidis K, DevetsikloTis M (2016) Blockchains and smart contracts for the Internet of Things. *IEEE Access* 4:2292–2303
15. Teslya N, Ryabchikov I, "Blockchain-based platform architecture for industrial IoT", *Proc. 21st Conf. Open Innov. Assoc. (FRUCT)*, pp. 321–329, Nov. 2018
16. Du L, Chen L, Zhang L, Dai L, Shen Y (2018) Security architecture based on blockchain for smart cloud manufacturing. *Inf Technol Netw Secur* 37:34–38
17. Nakamoto S, Bitcoin: A Peer-to-Peer Electronic Cash System, Feb. 2019, [online] Available: <https://bitcoin.org/bitcoin.pdf>
18. Singhal B, Dhameja G, Panda PS, Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Berkeley, CA, USA:Apress, 2018
19. Zhang Y, Deng RH, Shu J, Yang K, Zheng D, "TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain", *IEEE Access*, vol. 6, pp. 31077–31087, 2018
20. He Y, Li H, Cheng X, Liu Y, Yang C, Sun L (2018) A blockchain based truthful incentive mechanism for distributed P2P applications. *IEEE Access* 6:27324–27335
21. Kiayias A, Russell A, David B, Oliynykov R, "Ouroboros: A provably secure proof-of-stake blockchain protocol", *Proc. Int. Cryptol. Conf.*, pp. 357–388, 2017
22. Li Z, Barenji AV, Huang GQ, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform", *Robot. Comput.-Integr. Manuf.*, vol. 54, pp. 133–144, Dec. 2018
23. Lin Q, Yan H, Huang Z, Chen W, Shen J, Tang Y (2018) An ID-based linearly homomorphic signature scheme and its application in blockchain. *IEEE Access* 6:20632–20640
24. Daniel F, Guida L, "A service-oriented perspective on blockchain smart contracts", *IEEE Internet Comput.*, vol. 23, no. 1, pp. 46–53, Jan./Feb. 2019

25. Karati A, Islam SKH, Karuppiyah M, "Provably secure and lightweight certificateless signature scheme for IIoT environments", *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, Aug. 2018
26. Banerjee M, Lee J, Chen Q, Choo K-KR, "Blockchain-based security layer for identification and isolation of malicious things in IoT: A conceptual design", *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, pp. 1–6, Jul./Aug. 2018
27. Wu L, Du X, Wei W, Lin B, "An out-of-band authentication scheme for Internet of Things using blockchain technology", *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, pp. 769–773, Mar. 2018
28. Samaniego M, Deters R, "Internet of smart things—IoST: Using blockchain and clips to make things autonomous", *Proc. IEEE Int. Conf. Cogn. Comput. (ICCC)*, pp. 9–16, Jun. 2017
29. Xiong Z, Zhang Y, Niyato D, Wang P, Han Z, "When mobile blockchain meets edge computing", *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018
30. Miller D (2018) "Blockchain and the Internet of Things in the industrial sector". *IT Prof* 20(3):15–18
31. Liang X, Zhao J, Shetty S, Li D, "Towards data assurance and resilience in IoT using blockchain", *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, pp. 261–266, Oct. 2017
32. Mandolla C, Petruzzelli AM, Percoco G, Urbinati A, "Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry", *Comput. Ind.*, vol. 109, pp. 134–152, Aug. 2019
33. Al-Jaroodi J, Mohamed N (2019) Blockchain in industries: A survey. *IEEE Access* 7:6500–36515
34. Angrish A, Craver B, Hasan M, Starly B (Jan. 2018) "A case study for blockchain in manufacturing: 'FabRec': A prototype for peer-to-peer network of manufacturing nodes". *Procedia Manuf* 26:1180–1192
35. Vujičić D, Jagodić D, Randić S, "Blockchain technology bitcoin and Ethereum: A brief overview", *Proc. Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, pp. 1–7, 2018
36. Fernández-Caramés TM, Fraga-Lamas P (2019) "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories". *IEEE Access* 7:45201–45218
37. Kurpjuweit S, Schmidt CG, Klöckner M, Wagner SM, "Blockchain in additive manufacturing and its impact on supply chains", *J. Bus. Logistics*, Oct. 2019
38. Barenji AV, Li Z, Wang WM, Huang GQ, Guerra-Zubiaga DA, "Blockchain-based ubiquitous manufacturing: A secure and reliable cyber-physical system", *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2200–2221, Apr. 2020

Figures

Old Block

New Block

Figure 1

Blockchain

Figure 2

The detailed data structure of blockchain

Figure 3

Hash tree structure, the hash value of each parent node is calculated from the child node

Figure 4

The longest chain principle

Cloud

Edge

Figure 5

Architecture diagram of edge computing server

Figure 6

Traditional blockchain used in edge computing servers

Figure 7

Hierarchical blockchain used in edge computing servers

Figure 8

Module of edge work node and cloud work node

Figure 9

Flow chart from edge private chain to cloud public chain

Figure 10

Block data structure diagram

Figure 11

Transaction data structure diagram

Figure 12

Hierarchical blockchain improves space occupation

Figure 13

Comparison of space occupation under different data volumes

Figure 14

Comparison of number of edge nodes to the space occupied under the same amount of data

Figure 15

Node transmission time of different architectures under the same amount of data

Figure 16

Transmission time of each edge end under the same amount of data

Figure 17

Transmission time of nodes with different architectures under the same amount of data (each node).

Figure 18

Node transmission time of different architectures under the same amount of data (average of each node)

Figure 19

Under the same number of blocks, the impact of transaction list length on time.

Figure 20

Under the same number of blocks, the impact of transaction list length on time (average of each node)

Figure 21

Block synchronization times of different architectures under the same amount of data

The frequent of block synchronization

Figure 22

Block synchronization times of different architectures under the same number of blocks