



REVIEW



# Blockchain Technology Research and Application: A Literature Review and Future Trends

Min An<sup>1,2</sup> , Qiyuan Fan<sup>1,2,\*</sup>, Hao Yu<sup>1,2</sup>, Bo An<sup>3</sup>, Nannan Wu<sup>4</sup> , Haiyang Zhao<sup>1,2</sup>, Xinhao Wan<sup>1,2</sup>, Jiaxuan Li<sup>1</sup>, Rui Wang<sup>1</sup>, Jingyu Zhen<sup>1</sup>, Qinyan Zou<sup>1</sup> and Bin Zhao<sup>5</sup>

<sup>1</sup>*School of Software, Yunnan University, China*

<sup>2</sup>*Engineering Research Center of Cyberspace, China*

<sup>3</sup>*School of Mathematics and Statistics, Tianshui Normal University, China*

<sup>4</sup>*School of Ecology and Environmental Science, Yunnan University, China*

<sup>5</sup>*Gansu Jingmei Energy Company LTD., China*

**Abstract:** Blockchain, as the basis for cryptocurrencies, has recently garnered significant attention. It is a type of immutable distributed ledger technology with key features including decentralization, anti-tampering, transparency, anonymity, and contract-autonomy. These attributes enable transactions to be conducted credibly within a decentralized environment. Such features are instrumental in enhancing services and driving the advancement of blockchain-based applications. The proliferation of blockchain-based applications across various sectors such as financial services, reputation systems, Internet of Things (IoT), among others is evident. However, there remain numerous challenges associated with blockchain technology such as scalability and security that require resolution. This article presents a comprehensive overview of blockchain technology and its applications. It begins by outlining the evolution of blockchain before providing an architectural overview and systematically reviewing the research and application of blockchain technology in diverse fields (including federated learning, reinforcement learning, cloud edge computing, intelligent transportation, power systems, and IoT) from both academic research and industry perspectives. Additionally highlighted are technical challenges alongside recent developments. Finally concluded are some challenges and future directions pertaining to the application of blockchain technology as well as broader perspectives for further study.

**Keywords:** blockchain, federated learning, Internet of Things (IoT), intelligent transportation, reinforcement learning, smart grid

## 1. Introduction

Blockchain is a distributed ledger technology that records and shares every transaction occurring within a network of users. Cryptocurrency has now become a widely discussed topic in both industry and academia. However, digital currencies are just one application of blockchain. There are various evolving applications, including online voting, medical records, insurance policies, property and real estate records, copyrights and licenses, and supply chain tracking [1]. Smart contracts are another example, where contractual conditions are embedded in the blockchain, and payouts between involved parties automatically execute when those conditions are met. It is evident that blockchain technology holds great value and potential as it finds utility across multiple fields.

The concept of blockchain was first proposed in 2008 and implemented in 2009 [2]. Essentially, blockchain is a distributed public

ledger resembling a key-value database. Through the use of asymmetric encryption technology and distributed consensus technology, all transaction data are permanently recorded in an immutable chain. As new blocks are added and the chain grows longer, the cost of tampering or attacking the blockchain also increases, making it more secure. Blockchain possesses key characteristics such as decentralization, persistence, anonymity, and auditability. These attributes contribute to the ongoing popularity of blockchain technology and explain how it significantly reduces costs and improves efficiency.

Blockchain is a distributed digital architecture system that operates within edge networks. It was initially proposed by Scott Stornetta in 1991 [3]. The fundamental concept of blockchain is based on a peer-to-peer (P2P) decentralized network, where each node within the blockchain functions as a peer in a decentralized structure. This design allows all network nodes to collect transactions and record them in blocks. The reward mechanism within the blockchain network incentivizes each node to compete for blocks using a unified consensus algorithm. As a result, a chain structure composed of blocks stored across multiple nodes is formed, eliminating the need for trust between blockchain nodes.

\*Corresponding author: Qiyuan Fan, School of Software, Yunnan University and Engineering Research Center of Cyberspace, China. Email: [fanqiyuan@mail.ynu.edu.cn](mailto:fanqiyuan@mail.ynu.edu.cn)

### 1.1. Blockchain structure

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Figure 1 shows the basic structure of the blockchain, where TX represents a specific transaction on the blockchain. The underlying data structure of the blockchain is shown in Figure 2. The blockchain starts from the genesis block, and the orderly one-way connection in the way of hash pointer constitutes the whole blockchain, and the validity of transactions on the chain is guaranteed according to the longest chain legal principle and consensus algorithm.

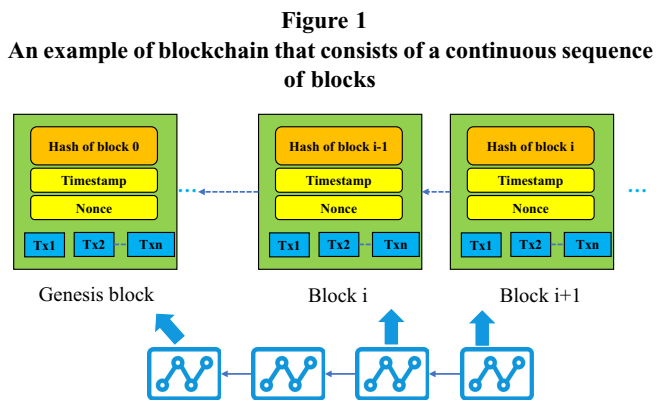
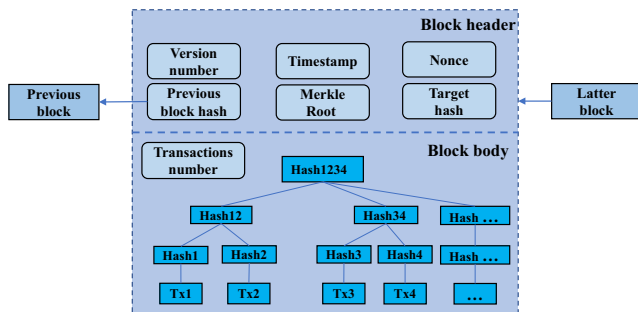


Figure 2 Diagram of the underlying data structure of the blockchain



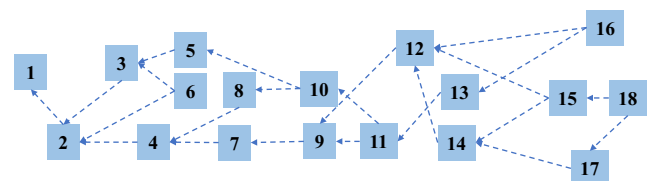
A block on the blockchain is composed of two parts: a block and a block. The block contains data records generated within a certain period of time that cannot be tampered with. Specifically, the block contains information such as the block version, Merkle tree root hash, timestamp, parent block hash, and nonce. A block consists of a transaction counter and all transactions within the block. The maximum number of transactions that a block can contain mainly depends on the size of a single block and the size of each transaction, and the maximum number of transactions essentially represents the throughput performance indicator of the blockchain. The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm [4].

In addition, in order to enhance the usefulness of blockchain on resource- and power -constrained devices, people propose a new directed acyclic graph (DAG)-structured blockchain, based on DAG architecture. In chain-structured blockchain, a new transaction must be validated before attached to the main chain, which is called synchronous consensus. Different from it, tangle

adopts an asynchronous consensus, which is more efficient in improving system throughput.

As shown in Figure 3, DAG-structured blockchain is not constrained by the single main chain and forks all the time, the relation among transactions looks like a tangled net. This novel architecture and consensus mechanism can improve network throughput and system response time theoretically. IOTA [5], Byteball [6], and NANO are three representative DAG-structured blockchains.

Figure 3 DAG-structured blockchain



### 1.2. Blockchain type

Blockchain is broadly categorized into three types: public or permissionless blockchain, private or permissioned blockchain, and consortium blockchain [7]. We compare these three types of blockchain from different perspectives. The comparison is listed in Table 1.

In a public blockchain, there is no dominant authority and no party has more power than others in the network. Participants can enter and exit at any time according to their wish. Similarly, any participant can validate the transaction due to its public nature. In Bitcoin, for example, miners can validate the transactions and receive Bitcoins as rewards. With a private blockchain, a centralized structure is followed, where a single entity has full power to validate the transactions and make decisions. The private blockchain is more efficient, easy to implement, utilizes fewer energy resources, and is faster compared to the public blockchain. Besides, with the consortium blockchain, not every member has the same permissions. A few members of the blockchain network are assigned certain privileges to validate the new blocks. Other members can also validate but must reach a consensus before implementation. Different consensus algorithms are implemented depending on the requirements and environment.

Table 1 Comparisons among public blockchain, consortium blockchain, and private blockchain

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Public or restricted	Public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

**Table 2**  
**Comparison of smart contract platforms**

Platform and comparison item	Bitcoin	Ethereum	Fabric	Corda	EOS	Stellar
Language	C++	Solidity, Serpent	Java, Golang	Java, Kotlin	C++	Python, JavaScript
Execution environment	Docker	EVM	Docker	JVM	WebAssembly	Docker
Consensus protocols	PoW	PoW	PBFT	Raft	BFT-DPOS	SCP
Data model	Transaction based	Account based	Key-value pair	Transaction based	Account based	Account based
Permission	Public	Public	Private	Private	Public	Consortium
Turing completeness	Turing incomplete	Turing complete	Turing complete	Turing incomplete	Turing complete	Turing complete
Application	Digital currency	General	General	Digital currency	General	Digital currency

Consensus algorithms play a crucial role in blockchain technology as they determine how the network operates. These algorithms facilitate decentralized decision-making in a collective manner within a decentralized network. They possess properties such as non-repudiation, authentication, decentralized control, transparency, and Byzantine fault tolerance [8].

Several well-known consensus algorithms include proof of work (PoW), proof of stake (PoS), proof of existence, and proof of authority (PoA), among others. These algorithms provide mechanisms for achieving agreement and security within the blockchain network.

Another important concept in blockchain is smart contracts [9]. Smart contracts were first proposed by Szabo [10] and were initially implemented in Ethereum. They are digital agreements between multiple parties that can be executed by a network of mutually distrusting nodes without relying on a trusted authority. Smart contracts are computer programs embedded in blockchains that automatically enforce the terms of an agreement without the need for intermediaries. They can store and process information, generate outputs, and are replicated across multiple nodes in the blockchain to prevent tampering. Smart contracts also enable transaction traceability and irreversibility in certain contexts, such as federated learning (FL) [11].

Regarding the comparison of blockchain platforms, Table 2 compares Ethereum, Fabric, Corda, Stellar, Rootstock (RSK), and EOS based on various aspects, including execution environment, supporting language, Turing completeness, data model, consensus protocols, permission, and applications.

### 1.3. Key features of blockchain

In summary, blockchain possesses the following characteristics.

**Decentralization.** In conventional centralized systems, each transaction needs to be validated through the central trusted agency. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.

**Persistency.** Transactions can be validated quickly. It is nearly impossible to delete or rollback transactions once they are included in the blockchain.

**Anonymity.** Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint (details will be discussed in Section 4).

**Auditability.** Bitcoin blockchain stores data about user balances based on the unspent transaction output model. Any transaction has to refer to some previous unspent transactions. So transactions could be easily verified and tracked.

**Credibility.** Blockchain employs a consensus algorithm to ensure the authenticity of on-chain transactions. The hash value linking mechanism ensures that any modification to on-chain information relies on the contents and calculation order of a series of data in the previous block. The significant cost and uncertain outcomes associated with tampering guarantee the immutability of the data on the chain.

### 1.4. Consensus algorithm of blockchain

The consensus algorithm in blockchain technology is a crucial mechanism that enables decentralized distributed network nodes to achieve consensus. There are three typical consensus algorithms: PoW [12], PoA [13], and PoS [14]. Table 3 provides a comparison of these common consensus mechanisms.

Among them, PoW is the most traditional consensus mechanism, and its consensus process is mainly based on the computing power of each node to carry out mining. However, the method based on computing power will inevitably cause a large amount of computing resources and energy waste in the mining process. The PoS consensus algorithm reduces the waste of computing power compared with the PoW consensus algorithm. The algorithm uses virtual resources such as the number of tokens held by a node or token time to characterize the equity of each node and uses the blockchain node with the highest equity to make the final accounting for the block. Although the PoS speeds up the computing rate, some long-standing nodes are likely to have huge rights, resulting in too much concentration of interests, and it is difficult to fairly carry out block selection. The PoA can effectively reduce the waste of computing power resources and avoid 51% computing power attacks.

Overall, each consensus algorithm has its advantages and limitations. The choice of the consensus mechanism depends on the specific requirements and goals of the blockchain system. It is crucial to strike a balance between security, efficiency, and decentralization when deciding which consensus mechanism to adopt.

Different from the existing blockchain research reviews, which are mostly based on subdivisions, such as blockchain systems in the industrial Internet of Things (IoT) or blockchain and FL, this article starts from the characteristics of blockchain itself, outlines the development status and unique advantages of blockchain, discusses the research and application of blockchain in six fields, and summarizes the main challenges and future development trends. Our main contributions of this article are described as follows:

1) Starting from the structure and technology of the blockchain itself, we outline its role and type, analyze its key

**Table 3**  
**Comparison of major consensus mechanisms**

	PoW	PoS	DPoS	Raft	PBFT
Application scenarios	Public blockchain	Public blockchain and permissioned blockchain	Public blockchain and permissioned blockchain	Consortium blockchain	Permissioned blockchain
Degree of decentralization	Fully decentralized	Fully decentralized	Fully decentralized	Semi-decentralized	Semi-decentralized
Accounting node	Full network	Full network	Selected nodes	Leader based	Semi-dynamic selection
Response time	About 10 minutes	About 1 minute	About 3 seconds	Second level	Second level
Throughput	About 7 TPS	–	About 300 TPS	–	About 1000 TPS
Storage efficiency	Full ledger	Full ledger	Full ledger	Full ledger	Full or partial ledger
Fault-tolerant	50%	50%	50%	50%	33%

characteristics, and then make a brief summary of its consensus algorithm. Moreover, the uniqueness of this article is that it provides a relatively complete comparison of different blockchain types, platforms, and major consensus protocols.

- 2) We systematically reviewed the research and application of blockchain technology in various fields from the perspective of academia and industry.
- 3) We summarized the current challenges and research progress of blockchain technology and suggested possible future research trends.

The organizational chart of this article is shown in Figure 4. The remainder of this article is structured as follows. Section 2 briefly summarized the current research status and shortcomings through literature review and gave our suggestions. In Section 3, we summarized the overview of blockchain technology research in multiple fields from both academic and industrial perspectives, including the research and application of blockchain technology in FL, reinforcement learning, cloud computing, edge computing, intelligent transportation, smart grid, and IoT. We described the current challenges about blockchain in Section 4 and introduced the research progress of blockchain technology. Possible future research trends are described in Section 5. Section 6 concluded the paper and showed directions for further work.

## 2. Literature Review

Most of the research on blockchain technology mainly focuses on the security mechanism of blockchain and the blocking rate, in which the blocking rate represents the rate at which blockchain network mining generates blocks. This section will provide a literature review of the current research status of blockchain technology from these two aspects respectively. The literature review table was shown in Table 4.

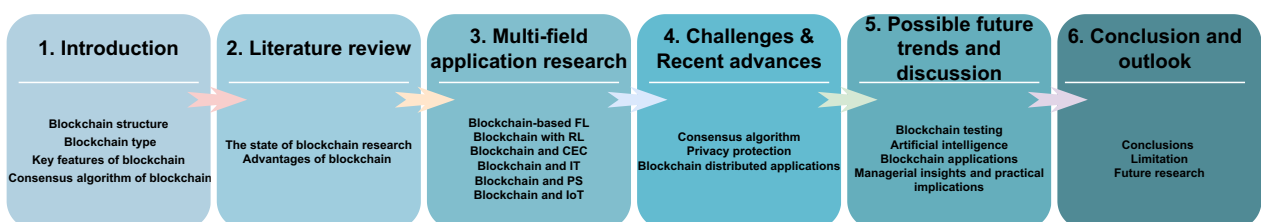
## 2.1. The state of blockchain research

### 2.1.1. Security mechanism of blockchain technology

Blockchain uses consensus algorithm to ensure the security of data, and PoW is a common consensus protocol, but when the attacker’s computing power is greater than half of the blockchain network computing power, the system will be 51% attack, which undoubtedly poses a great threat to the blockchain. Yang et al. [15] proposed a technique that combines the historically weighted information of miners with the total computational difficulty to mitigate the 51% attack problem, based on which the cost of traditional attacks increases by two orders of magnitude. Bae and Lim [16] proposed a random mining group selection technique to reduce the probability of successful double flower attack. In addition to the optimization based on consensus algorithms to resist attacks, some researchers have also developed some novel consensus algorithms. Dorri and Jurdak [17] proposed a fast and scalable consensus algorithm named tree chain. Compared with the existing hash function verification method, tree chain is a leader selection consensus algorithm. Kumar et al. [18] propose a consensus algorithm for public blockchains that shards miners based on their performance. This performance-based consensus algorithm ensures more fairness, avoids hunger, and improves trust among miners and the overall performance of the blockchain network.

Due to the traceability and integrity of its data, blockchain technology can effectively solve major problems such as distributed management and data tampering of complex distributed systems in the current world, but it cannot solve the trust problem of the data itself. Therefore, reputation management has become an important research direction of blockchain. Malik et al. [19] proposed a three-tier trust management framework called TrustChain, which uses consortium chains to track

**Figure 4**  
**Chart of step of this paper**



**Table 4**  
**Literature review table**

Works	Main contributions	Limitations	Suggestions
Yang et al. [15]	Mitigate 51% attacks	Impact decentralization	Reduce system complexity
Bae and Lim [16]	Reduced double spend attacks	Cause trust issues	Ensure fair distribution of rewards
Dorri and Jurdak [17]	Tree-chain consensus algorithm	Impact decentralization	Reduce system complexity
Kumar et al. [18]	Performance-based consensus algorithm	Increase system complexity	Reduce resource consumption
Malik et al. [19]	TrustChain framework	High maintenance cost	Optimized performance
Frauenthaler et al. [20]	New relay scheme	Poor scalability	Increase scalability and reduce costs
Yang et al. [21]	CoDAG (structure optimization)	Increased risk of attack	Enhanced security mechanism
Wang and Kim [22]	FastChain (increase throughput)	Affect system fairness	Optimize cost management
Vera-Rivera et al. [23]	Service-oriented architecture	High latency	Optimized performance

interactions among supply chain participants and dynamically assigns reputation scores based on these interactions. At the same time, there are researchers who have studied the deployment costs of blockchain. Frauenthaler et al. [20] introduced a novel relay scheme, considering that the current blockchain relay scheme requires the target blockchain to immediately verify the size of each relay. The scheme reduces the cost of relaying between Ethereum-based blockchains by 92%, enabling decentralized interoperability between blockchains. There are also studies on the security of distributed FL systems. The model parameters uploaded by the terminal are authenticated and shared through the blockchain, avoiding privacy disclosure and tampering attacks caused by long communication distances. The research focus is mainly on the mechanism of combining blockchain with FL to accelerate the convergence of models through good mechanisms.

### 2.1.2. The blocking rate of blockchain

Due to its decentralized property, blockchain is seen as a promising technology for providing reliable and secure services. However, due to the limited throughput, the current blockchain platform cannot meet the transaction needs in actual use, so researchers have proposed many new solutions. Yang et al. [21] improved on the linear structure of traditional blockchains using DAGs, where blocks are organized by level and width, resulting in a compact DAG structure (CoDAG). Improved security and transaction verification time compared to traditional blockchain architecture. However, due to changes in the structure of the blockchain, the risk of being attacked is increased. Wang and Kim [22] extended the traditional analysis of the basic tradeoff between throughput and fork rate of a blockchain system and further proposed FastChain, which increases the throughput of a blockchain system by reducing block propagation time. This method effectively reduces the propagation delay of block authentication and improves the block rate of the blockchain. However, it may create problems of system unfairness and increase maintenance and management costs.

As can be seen from the above research, it is difficult to optimize the mechanism of the blockchain itself to increase the blocking rate. The application of blockchain in mobile edge computing (MEC) system has aroused great interest among researchers, and collaborative offloading can effectively improve system throughput, which is of great significance for blockchain technology. However, the design and optimization efforts of existing blockchains and MECs are mostly separate, which leads to suboptimal performance. Vera-Rivera et al. [23] proposed a blockchain-based service-oriented architecture that

allows secure and private task offloading collaboration among edge servers in MEC environments to help alleviate processing saturation in dense networks and improve resource utilization of MEC systems. From the above research, it can be seen that computing unloading through edge computing can effectively reduce the block chain blocking rate and improve the system resource utilization rate.

## 2.2. Advantages of blockchain technology

As a distributed data recording system that provides a secure trust mechanism, blockchain technology is of great significance to the development of various fields at present. This technology has the advantages and characteristics of decentralization, multi-party maintenance, smart contract [24], immutable, open consensus, security, and trust. These features are described in detail below.

First, blockchain, as a decentralized distributed system, uses a multi-centralized consensus approach to establish trust mechanisms. The verification, accounting, storage, maintenance, and transmission of transactions in the blockchain all rely on the distributed system structure. Each blockchain node can distribute the same mathematical problem to select nodes among multiple distributed nodes for the final mining block and complete the verification and verification of transactions through the mining process. Thus, instead of the traditional method of using third-party trust organizations or institutions to build trust relationships, a decentralized and trusted distributed system is established [25].

Second, the blockchain is jointly maintained by all nodes, and new blocks are added to the blockchain by selecting specific nodes through a consensus mechanism, ensuring the robustness and security of the system. Therefore, the blockchain network is a distributed consensus and multi-party maintenance system that guarantees the authenticity and immutability of transactions. Blockchain stores transaction information using a chain structure with a timestamp, so it is possible to track transaction information on the chain. And for any two adjacent blocks in the blockchain, each block contains the information of all previous blocks, so if one block is tampered with, the data information of that block and all subsequent blocks must be modified. Tampering must be done in a limited amount of time, but, in reality, every re-mining calculation requires a huge cost, so the data on the blockchain are immutable.

In addition, blockchain technology can create smart contracts between users who do not trust each other [26], guaranteeing the confidentiality of transactions. Blockchain network is an open consensus network, which encrypts the data on the chain through asymmetric encryption technology to ensure data security and



prevents external attacks from tampering through complex consensus algorithms.

To sum up, blockchain technology has a tamper-proof mechanism and a security and confidentiality mechanism based on encryption, which is of great significance to ensure the safe sharing of data in the network.

### 3. Multi-field Application Research

#### 3.1. Blockchain-based FL

The traditional FL architecture collects and aggregates model information of all participants based on a central server, and then the central server merges and updates the model information to the participants.

This process may lead to the following three problems:

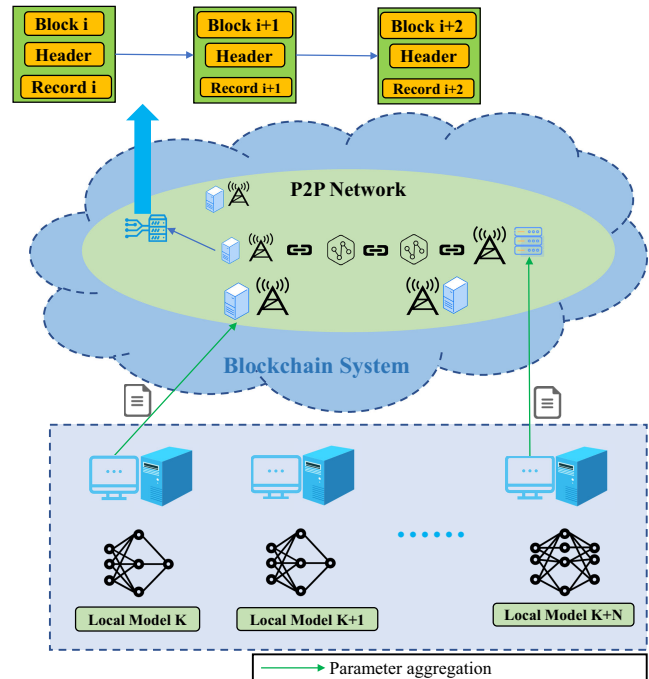
- 1) The central node may be unstable due to the influence of service providers or other computing tasks;
- 2) The central node may favor some clients, resulting in unfair system;
- 3) If the central node is attacked or malicious, the training of the model will be damaged or the data privacy will be disclosed.

In addition, the central node is usually far away from the terminal, and it is easy to be eavesdropped or tampered with by attacks during the interaction process. In order to solve the above problems caused by the central structure, decentralization through the edge network is an effective method. In order to ensure the security and privacy of parameter aggregation in the edge network, FL combined with the blockchain technology in the edge network shows its advantages of security and convenient coordination. In fact, at present, many studies have taken blockchain technology as the infrastructure of FL to realize the task of model aggregation of FL through blockchain technology, and the incentive mechanism in blockchain also provides technical solutions to improve the enthusiasm of participants to participate in the training of FL model.

Once the FL process has decentralized the centralized structure using the edge network, it is difficult for the participants to coordinate and interact safely and effectively under the condition of mutual distrust. Generally, the distributed system builds trust based on trusted third-party institutions or organizations to provide trust authentication and cryptographic interaction. However, in the absence of trusted third-party institutions or organizations, it is difficult for distributed systems to directly establish trust relationships.

Therefore, blockchain technology has important implications for establishing a secure and trusted system for FL [27]. Figure 5 shows the architecture of a FL network based on blockchain. Xu et al. [28] proposed an asynchronous FL framework with dynamic scaling factor based on blockchain. The framework addresses the issue of trust between devices primarily through blockchain and, at the same time, proposes new dynamic scaling factors to help improve FL efficiency and accuracy. The framework mitigates the impact of low-performance devices while being just as efficient as traditional FL and has the added benefit of alleviating trust issues between IoT devices. There are studies using CFL clustering to solve the problem of poor performance of existing blockchain-based FL schemes when data are sparse. CFL is a cross-cluster FL system facilitated by cross-chain technology, which divides a large cluster into multiple smaller clusters, each within its own geographic area and organized by a BFL. It can be seen that the federal learning framework based on blockchain technology has

Figure 5  
Federated learning network architecture based on blockchain



become an important direction for the development and research of federal learning. However, in addition to the blockchain mechanism to ensure the security of data, the throughput rate of blockchain itself is limited, which will limit the efficiency of FL. In the current research, more consideration is given to optimizing the model update process of FL. There is no consideration for the optimization of the blockchain mechanism as well as the mechanism of the system itself.

#### 3.2. Blockchain with reinforcement learning

Currently, reinforcement learning is mainly used to optimize the performance of blockchains. Most IIoT applications rely on centralized servers for data processing and transmission, which exposes data to security risks as well as high operational costs and latency. Therefore, data security and efficiency become key issues for IIoT.

To address the above issues, blockchain is widely recognized as a promising solution for building a secure and efficient data storage/processing/sharing environment in the IIoT. Despite the significant benefits of blockchain technology, traditional blockchain systems struggle to provide the scalability needed to meet the high transaction throughput demands of the IIoT. In fact, scalability has become a key issue for blockchain to be used as a common platform for different services and applications.

In recent years, many teams have been working to achieve a universal, scalable, and deployable blockchain platform. It is mainly divided into two kinds according to different optimization angles. One is on-chain optimization schemes such as adjusting block sizes and intervals, improving the block out process, and proposing new consensus mechanisms. One is the off-chain optimization scheme, which aims to reduce redundancy on the main chain using side chains, multi-chains, lightning networks, payment channels, etc.

In order to deal with the dynamic and high-dimensional characteristics of IIoT systems, Liu et al. [29] proposed a new blockchain vehicle networking performance optimization framework based on deep reinforcement learning (DRL) to maximize transaction throughput while ensuring the decentralization, delay, and security of the underlying blockchain system. In this framework, we first analyze the performance of blockchain systems in terms of scalability, decentralization, latency, and security. DRL technology is used to select block producers and adjust block size and block interval to adapt to the dynamic changes of vehicle networking scenarios. Simulation results show that the proposed framework can effectively improve the throughput of blockchain-enabled vehicle-connected systems without affecting other characteristics.

### 3.3. Blockchain and cloud edge computing

Blockchain is considered to be the prototype of the next generation of cloud computing, and the combination of blockchain and cloud computing is a hot research area. In November 2015, Microsoft proposed the concept of blockchain as a service, deploying blockchain as an application service in the cloud. This is similar to the software-as-a-service model, where users can interact with different technologies in a low-risk environment provided by the Azure cloud platform. Tencent FiT released a white paper on blockchain solutions in April 2017, building an enterprise-class blockchain infrastructure platform.

The limited computing and storage resources of edge servers not only need to provide support for relevant application services but also need to cache data frequently accessed by users, so deploying blockchain should save server resources as much as possible. In a cloud computing environment, multiple copies of data backup are placed in multiple data centers to cope with the access requests of a large number of users in different locations, but the placement of data copies should take into account the storage cost of the data center, the access delay of users, and the transmission cost between servers. The blockchain system oriented to the edge computing field should optimize and improve the blockchain to reduce the overhead of block transmission and storage. Tschorsch and Scheuermann [30] proposed a blockchain system supported by fog computing architecture, but each fog node needs to save complete data, resulting in huge network transmission costs and node storage costs. Ongaro and Ousterhout [31] proposed a decentralized data management system, which uses smart contracts to manage access rights and save the hash of data in blocks, reducing the storage cost of blocks, but storing complete data in additional devices still increases the storage cost. Zeng et al. [32] proposed an edge computing-oriented blockchain system, which realizes the optimal storage strategy on edge devices including mobile devices, improves the PoS mechanism to meet the edge environment, and reduces the storage cost of nodes. However, the device storing blocks are an intelligent device with limited resources and high mobility.

The edge cloud environment of cloud edge aggregate computing meets the distributed requirements of blockchain deployment, and the blockchain can be deployed in the edge cloud to ensure the security and reliability of data uploaded at the edge end. However, the shortcomings of blockchain storage occupation and resource consumption still hinder the deployment of blockchain in the edge cloud. Obviously, this poses a challenge to the deployment of blockchain, and researchers have designed a lightweight blockchain LBlockchainE that is suitable for the edge cloud in the cloud edge-converged computing environment.

### 3.4. Blockchain and intelligent transportation

Blockchain applications in smart transportation are equally widespread. Based on the immutability and traceability of blockchain, some parking reservation solutions can be designed in combination with the reputation mechanism. Currently, the application of blockchain technology in the Internet of Vehicles has received some attention. In order to solve the problems in IoT, some researchers have proposed different combinations of IoT and blockchain solutions (such as privacy protection, vehicle life cycle, vehicle supply chain, vehicle edge computing, electronic toll collection).

Intelligent transportation system (ITS) is critical to cope with traffic events, e.g., traffic jams and accidents, and provide services for personal traveling. Although some researches have investigated the integration of blockchain and ITS, they mainly focus on data sharing, energy delivery, trust management, blockchain-enabled crowdsensing, and blockchain network architecture. However, to the best of our knowledge, existing researches ignore the blockchain safety, the brought latency by blockchain, and the trade-off between these two metrics.

When blockchain and ITS are combined, for transaction selection, we need to consider the data size, waiting time in the transaction pool, and blockchain environment. However, it is rather challenging to select suitable active miners from road side units (RSUs), since the reliability and computing power of RSUs need to be evaluated. To solve the problem, Ning et al. [33] put forward a secure, efficient, and distributed ITS system and formulated it as a multi-objective optimization problem, i.e., minimizing the system latency and maximizing the data safety and user utility. The DRL-based algorithm can make a satisfied trade-off between blockchain security and latency, and the DIADEM algorithm is able to choose task computation modes for vehicles in a distributed way. They experimentally demonstrate the effectiveness of both algorithms, i.e., the DRL-based algorithm can reach higher blockchain safety and lower blockchain latency, and the DIADEM algorithm can obtain larger social welfare than benchmark methods.

### 3.5. Blockchain and power system

Blockchain promises to change the way we execute global value transactions. Therefore, it is very important to explore the application of this new technology in the field of energy. This part mainly expounds the application of blockchain in the energy field from the perspective of energy trading and power grid operation. We see blockchain as a distributed system that can provide trust between different and independent parties. It allows the creation of distributed P2P networks where untrusted members can interact in a verifiable way without a trusted intermediary. With blockchain, transactions can be managed in ledger form, making microgrids more powerful. These transactions may include electricity transactions, currency transactions, or even records of the flow of electricity in the network.

At present, electricity trading has been able to realize online trading, but this trading method is still in a relatively preliminary stage, that is, the use of centralized central database to store and process electricity consumption data and transaction data; this method may encounter network attacks in the Internet, and at the same time, the data center operator as an intermediary between the seller and the buyer in electricity trading. There is no guarantee of trusted transactions, so blockchain technology could enable new power trading systems to solve the above problems.

Moreover, with the continuous expansion of the scale of power and the gradual opening of the power market, the operational stability and security of the power grid tend to decline. In view of this, an efficient and flexible microgrid system integrating power generation, distribution, and sale has emerged. The development of microgrid helps to solve the problem of new energy consumption, and its deployment at the receiving end makes it easy to meet the diversified needs of the receiving end users. Blockchain is known as the “next generation Internet”; as a decentralized, low trust cost, information cannot be tampered with distributed ledger system, and its combination with distributed microgrid system has become a research trend.

### 3.6. Blockchain and IoT

The integration of the IoT and industry is an important means to promote industrial automation and information. IIoT helps reduce errors, reduce costs, improve efficiency, and enhance security in manufacturing and industrial processes, enabling a higher level of integrity, availability, and scalability in the industrial sector. However, security attacks and failures could cause huge headaches for the global IoT network. For example, central data centers are vulnerable to single point failures and malicious attacks such as Distributed Denial of Service (DDoS), Sybil attacks, etc. In addition, there is a risk of leakage of sensor data stored in data centers. In addition, communication between IoT devices may be subject to data interception, and the credibility of the collected data cannot be guaranteed [34].

Leveraging the characteristics of blockchain’s tamper-proof and decentralized consensus mechanism, there is an opportunity to address the security issues in the IIoT systems described above [35].

There are some existing research on this topic, for example, Novo [36] proposes an access control system based on the blockchain technology to manage IoT devices. Li et al. [37] exploit the consortium blockchain technology to propose a secure energy trading system. But they do not consider privacy issues, such as the sensitive data disclosure risk, and thus it cannot guarantee sensitive data confidentiality. The aforementioned systems all adopt chain-structured blockchains in IoT systems, which are overloaded for power-constrained IoT devices. Xiong et al. [38] introduce edge computing for mobile blockchain applications and present a Stackelberg game model for efficient edge resource management for mobile blockchain. In addition, there are some other challenges that also brought in the meantime when introducing the novel design of blockchain into IIoT systems.

## 4. Challenges and Recent Advances

Although blockchain has been widely used in many fields and achieved great success, but at the same time, it also faces many challenges that limit its further application. Below, we list some of the key challenges and recent research developments from the perspective of blockchain application limitations.

### 4.1. Consensus algorithm

Blockchain is essentially a P2P distributed database that maintains the consistency of the data through consensus algorithms. PoW is a proof-of-work consensus mechanism and one of the core technologies of Bitcoin. However, with the continuous innovation of blockchain technology, the defects of PoW consensus algorithm in performance and security are more and more obvious, and improved protocols based on PoW

consensus algorithm are constantly proposed. In the PoW, new coin rewards and transaction fees protect the security of the Bitcoin network. The shortcomings of PoW consensus algorithm are mainly in the following three aspects:

- 1) Waste of resources.
- 2) The network performance is low.
- 3) Computing power centralization.

The core contradiction of PoW algorithm is the block size and block interval. Increasing block capacity can improve throughput, but too many blocks will cause network congestion, increase the time and efficiency of inter-node consensus, and may reduce block efficiency. Reducing the outgoing block interval can also increase throughput, but the shortening of the outgoing block interval will cause more frequent chain forks and increase security issues such as double flowers.

Therefore, with the development of public chain consensus mechanism, PoW consensus algorithm has produced many variants. There are two ways to improve its performance and security. One is to transform the growth mode of the chain, redistribute accounting rights, and reduce disorderly competition and block interval without changing the core of PoW. One is controlling the transaction volume on the chain through the off-chain expansion mechanism to improve the efficiency of the blockchain.

### 4.2. Privacy protection

The blockchain-based-distributed ledger integrates a variety of technologies such as asymmetric encryption systems, P2P networks, consensus algorithms, and smart contracts to ensure the consistency and immutability of transaction records. However, the ledger sharing mechanism in blockchain technology also brings privacy threats, and the privacy protection of user identity, account address, transaction content, and other information has become the focus of research.

In the actual use of the blockchain system, in order to ensure the traceable, verifiable, and other characteristics of the recorded data on the blockchain, all data must be disclosed to all nodes in the blockchain network. By analyzing the transaction data recorded in the blockchain ledger, the attacker discovers the rules, associates the different addresses and transaction data of the user, and further corresponds to the real identity of the user. Such attacks mainly rely on address clustering and identity information mining. In order to prevent the disclosure of personal privacy, the existing research is similar to the method of network privacy protection, which realizes information concealment by mixing personal information with other users’ information.

### 4.3. Blockchain distributed applications

Recently, there has been research into the use of persistent practices in the delivery and deployment of distributed applications and blockchain networks. Górski [39] described a continuous delivery approach for generating complete node deployment packages for blockchain systems, proposed BinCD, a solution that provides the latest deployment scripts and smart contract applications for DLT node configuration, and provided UML modeling support for deployment architecture views. They suggest that researchers focus on the source code and test generation of smart contracts. Tran et al. [40] proposed the Network Deployment and Evaluation framework (NVAL), a software framework that implements a novel architecture-driven, which enables automated deployment and evaluation of blockchain networks. NVAL utilizes



a new architecture-driven and community-supported approach to automate the deployment and evaluation of complex multi-channel blockchain networks.

However, the components and technologies involved in blockchain technology and distributed applications are more complex, including a variety of different consensus mechanisms, smart contracts, decentralized applications, etc., which brings great challenges to automated delivery and deployment tools. At the same time, the security of the blockchain network is of paramount importance and needs to be protected against various types of attacks, including 51% attacks, double spend attacks, malicious nodes, etc. When deploying and running distributed applications and blockchain networks, various security factors need to be considered to ensure the security and stability of the system. This part remains to be studied. In addition, blockchain-distributed applications and networks require the support and maintenance of the community to ensure their stability and sustainability. Therefore, it is necessary to establish a good community ecology.

## 5. Possible Future Trends and Discussion

Blockchain has shown its potential in both industry and academia. In this section, we discuss possible future directions from three aspects: blockchain testing, artificial intelligence, and blockchain applications.

### 5.1. Blockchain testing

Many different types of blockchains have emerged recently. When incorporating blockchain into their business, users must select the type of blockchain to meet their business requirements. Therefore, there is a need for a recognized and universally applicable blockchain testing mechanism to test different blockchains. At the same time, blockchain performance is an important indicator of blockchain application, and blockchain testing is also conducive to objectively evaluating the stability, scalability, security, and other performance indicators of a blockchain.

The design, deployment, and evaluation of blockchain networks and smart contracts are also important. A blockchain network is a distributed system set up by participants who do not trust each other to operate the blockchain. The quality attributes of the blockchain network, such as latency and throughput or simulation, are evaluated by benchmarking after network deployment. Unfortunately, blockchain network deployment and evaluation are time-consuming, error-prone, and platform-dependent. Therefore, it is necessary to automate the deployment and evaluation of blockchain networks. Tran et al. [40] have proposed various methods for automatically deploying blockchain networks and evaluating the effects of deployment, while also implementing relevant deployment tools. However, common tools and cloud service deployment tools do not reduce operational complexity, so there are fewer applications. Their applicability and longevity are also limited by heterogeneous networks and platforms.

Smart contract testing refers to the detailed analysis and evaluation of smart contracts to assess the quality of their source code during the development cycle. We investigated about 40 literatures on smart contracts and found that the main causes of smart contract code defects include non-standard contract coding, immature contract implementation language, and Ethereum Virtual Machine (EVM) mechanism. The smart contract execution engine of Ethereum is the EVM. We also looked for papers on smart contract design and testing. Bartoletti and Pompianu [41] analyzed common design patterns for Ethereum smart contracts. Dolev and Wang [42] proposed SodsMPC, a quantum-secure

smart contract system, to ensure the correctness of contract execution through multi-party computation, while protecting data privacy. Tikhomirov et al. [43] proposed SmartCheck, a scalable static analysis tool for detecting code problems of smart contracts, which provides a comprehensive classification of code problems. Rodler et al. [44] implemented EVMPatch, a framework that integrates many static analysis tools to detect vulnerabilities, to provide automatic methods to patch detected vulnerabilities. Fortunately, good smart contract design patterns can avoid the above problems, so smart contract design patterns are also one of the future research directions. For example, create a structured design pattern library for the Solidity language that covers common coding scenarios.

### 5.2. Artificial intelligence

The combined application of AI and blockchain technology is still in the exploratory stage, but from the point of view of reinforcement learning methods being used to optimize blockchain performance, AI technology is bound to be able to assist blockchain. As a law and regulation on the blockchain, the essence of smart contract is to reach a contract call through a transaction, so it can be seen that its essence is not a smart contract. And AI technology helps build intelligent prophecy machines so that smart contracts can become smarter.

### 5.3. Blockchain applications

Most blockchain applications are currently in the financial sector, and more and more applications in different fields are emerging. In the future, blockchain will definitely be applied to more fields to support the development of the field or enhance the system in the field, and the combination of blockchain and reputation mechanism makes the possibility of malicious nodes to do evil greatly reduced, which is conducive to the more general promotion of blockchain to autonomous systems and other fields.

## 6. Conclusion and Outlook

### 6.1. Conclusions

Blockchain shows its potential to transform traditional industries with its key characteristics such as decentralization, persistence, anonymity, and auditability. As an innovative technology, blockchain technology has now become the cornerstone of the field of information technology and has also had a huge impact on many academic research directions.

In this article, we present a comprehensive overview of blockchain. We begin with an overview of blockchain technology, including blockchain architecture and key features of blockchain. Then the research and application of blockchain in various fields are analyzed and summarized from different angles. In addition, we list some of the challenges and issues that are holding back the development of blockchain, offer some ways to address these issues, and suggest some possible directions for the future. We summarize the bullet points of our conclusions as follows:

- 1) Many studies have identified blockchain technology as the underlying infrastructure for FL, but the introduction of blockchain also brings issues such as high latency and energy consumption.
- 2) Reinforcement learning is primarily used to optimize the performance of blockchains. Scalability has become a key issue for blockchain as a different service and common platform.

- 3) Blockchain is the prototype for the next generation of cloud computing, and the combination of blockchain and cloud computing is a hot research area.
- 4) Based on the immutable and traceable characteristics of blockchain, blockchain is widely used in the field of transportation.
- 5) As the Internet of value, the combination of blockchain and distributed microgrid systems has become a research trend.
- 6) Blockchain tamper-proof and distributed consensus mechanisms can solve the security problems of IoT systems.
- 7) With the application and development of blockchain, consensus algorithms need to be continuously optimized and updated.
- 8) The ledger sharing mechanism in blockchain has brought privacy threats, and the privacy protection of user transactions and other information has become a research hotspot.
- 9) Using persistent practices to deliver and deploy distributed applications and blockchain networks is also one of the major challenges ahead.
- 10) Blockchain testing, the design, deployment, and evaluation of blockchain networks and smart contracts, blockchain combined with artificial intelligence, and blockchain applications are possible research trends in the future.

## 6.2. Limitation

By discussing the application and advantages and disadvantages of blockchain in many fields, this article aims to give researchers a more comprehensive vision of blockchain technology and the combination of different fields.

However, the field discussed in this article is limited, and the application of blockchain technology combined with multiple fields is far more than these, which is also the direction we need to continue to explore in the future. At the same time, this article does not do a survey of the platform applied in the field and only considers a single field when analyzing the application of the blockchain field and does not study the cross-field.

## 6.3. Practical implications and future research

This article can help blockchain researchers have a more comprehensive understanding of the application status and challenges of blockchain in multiple fields and provide reference solutions to the challenges.

The application of blockchain technology in combination with different fields still faces many challenges. Future research directions include coming up with new solutions to address these challenges and studying the performance issues that exist when blockchain is combined with different fields. In the future, we will conduct in-depth research on blockchain-based applications based on the principle that technology benefits mankind.

## Funding Support

This work was supported by the Research and Innovation Fund for Recommended Postgraduates without Examination of Yunnan University under Grant TM-23236809 and in part by the 14th Postgraduate Research Innovation Project of Yunnan University under Grant KC-2222958.

## Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

## Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

## Author Contribution Statement

**Min An:** Conceptualization, Methodology, Software, Formal analysis, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration, Funding acquisition. **Qiyuan Fan:** Methodology, Resources, Supervision. **Hao Yu:** Methodology. **Bo An:** Conceptualization, Software, Data curation. **Nannan Wu:** Conceptualization, Data curation, Visualization, Project administration. **Haiyang Zhao:** Methodology, Validation, Resources. **Xinhao Wan:** Validation, Investigation. **Jiaxuan Li:** Validation, Investigation. **Rui Wang:** Validation, Investigation. **Jingyu Zhen:** Software, Formal analysis. **Qinyan Zou:** Software, Formal analysis. **Bin Zhao:** Software, Formal analysis.

## References

- [1] Wang, J., Wang, Y., Zhang, X., Jin, Z., Zhu, C., Li, L., . . . , & Lv, S. (2024). LearningChain: A highly scalable and applicable learning-based blockchain performance optimization framework. *IEEE Transactions on Network and Service Management*, 21(2), 1817–1831. <https://doi.org/10.1109/TNSM.2023.3347789>
- [2] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>
- [3] Dhobale, J., & Mishra, V. (2020). Blockchain theories and its applications. In S. K. Panda, A. A. Elngar, V. E. Balas, & M. Kayed (Eds.), *Bitcoin and blockchain: History and current applications* (pp. 183–192). CRC Press. <https://doi.org/10.1201/9781003032588-11>
- [4] Johnson, D., Menezes, A., & Vanstone, S. A. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, 1(1), 36–63. <https://doi.org/10.1007/s102070100002>
- [5] Sabbagh, P. (2021). Optimizing blockchains structures based on entropy and TOPSIS model. *Journal of Service Science and Management*, 14(1), 115–131. <https://doi.org/10.4236/jssm.2021.141008>
- [6] Xu, J., Wang, C., & Jia, X. (2023). A survey of blockchain consensus protocols. *ACM Computing Surveys*, 55(13s), 278. <https://doi.org/10.1145/3579845>
- [7] Niranjnamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology: Pros, cons and SWOT. *Cluster Computing*, 22(6), 14743–14757. <https://doi.org/10.1007/s10586-018-2387-5>
- [8] Seibold, S., & Samman, G. (2016). *Consensus: Immutable agreement for the internet of value*. KPMG. [https://kpmg.com/ky/en/home/insights\\_new/2016/09/blockchain-consensus.html](https://kpmg.com/ky/en/home/insights_new/2016/09/blockchain-consensus.html)
- [9] Khan, S. N., Loukil, F., Guegan, C. G., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking Applications*, 14(5), 2901–2925. <https://doi.org/10.1007/s12083-021-01127-0>
- [10] Szabo, N. (1996). Smart contracts: Building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought*, 16, 1–11.
- [11] Huang, H., Li, K. C., & Chen, X. (2019). Blockchain-based fair three-party contract signing protocol for fog computing.

- Concurrency and Computation: Practice and Experience*, 31(22), e4469. <https://doi.org/10.1002/cpe.4469>
- [12] Garay, J., Kiayias, A., & Leonardos, N. (2015). The Bitcoin backbone protocol: Analysis and applications. In *34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 281–310. [https://doi.org/10.1007/978-3-662-46803-6\\_10](https://doi.org/10.1007/978-3-662-46803-6_10)
- [13] Manolache, M. A., Manolache, S., & Tapus, N. (2022). Decision making using the blockchain proof of authority consensus. *Procedia Computer Science*, 199, 580–588. <https://doi.org/10.1016/j.procs.2022.01.071>
- [14] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, 3(2), 100067. <https://doi.org/10.1016/j.bcr.2022.100067>
- [15] Yang, X., Chen, Y., & Chen, X. (2019). Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In *2019 IEEE International Conference on Blockchain*, 261–265. <https://doi.org/10.1109/Blockchain.2019.00041>
- [16] Bae, J., & Lim, H. (2018). Random mining group selection to prevent 51% attacks on Bitcoin. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, 81–82. <https://doi.org/10.1109/DSN-W.2018.00040>
- [17] Dorri, A., & Jurdak, R. (2021). Tree-chain: A lightweight consensus algorithm for IoT-based blockchains. In *2021 IEEE International Conference on Blockchain and Cryptocurrency*, 1–9. <https://doi.org/10.1109/ICBC51069.2021.9461098>
- [18] Kumar, A., Sangoi, A., Raj, S., & M, K. (2021). ShardCons—A sharding based consensus algorithm for blockchain. In *2021 IEEE International Conference on Electronics, Computing and Communication Technologies*, 1–6. <https://doi.org/10.1109/CONECCT52877.2021.9622529>
- [19] Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). TrustChain: Trust management in blockchain and IoT supported supply chains. In *2019 IEEE International Conference on Blockchain*, 184–193. <https://doi.org/10.1109/Blockchain.2019.00032>
- [20] Frauenthaler, P., Sigwart, M., Spanring, C., Sober, M., & Schulte, S. (2020). ETH relay: A cost-efficient relay for ethereum-based blockchains. In *2020 IEEE International Conference on Blockchain*, 204–213. <https://doi.org/10.1109/Blockchain50366.2020.00032>
- [21] Yang, S., Chen, Z., Cui, L., Xu, M., Ming, Z., & Xu, K. (2019). CoDAG: An efficient and compacted DAG-based blockchain protocol. In *2019 IEEE International Conference on Blockchain*, 314–318. <https://doi.org/10.1109/Blockchain.2019.00049>
- [22] Wang, K., & Kim, H. S. (2019). FastChain: Scaling blockchain system with informed neighbor selection. In *2019 IEEE International Conference on Blockchain*, 376–383. <https://doi.org/10.1109/Blockchain.2019.00058>
- [23] Vera-Rivera, A., Refaey, A., & Hossain, E. (2021). Blockchain-based collaborative task offloading in MEC: A hyperledger fabric framework. In *2021 IEEE International Conference on Communications Workshops*, 1–6. <https://doi.org/10.1109/ICCWshops50388.2021.9473763>
- [24] Rivest, R. L., Shamir, A., & Tauman, Y. (2001). How to leak a secret. In *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast*, 552–565. [https://doi.org/10.1007/3-540-45682-1\\_32](https://doi.org/10.1007/3-540-45682-1_32)
- [25] Yuan, Y., & Wang, F. (2016). Qū kuài liàn jìshù fāzhǎn xiànzuàng yǔ zhǎnwàng [Blockchain: The state of the art and future trends]. *Acta Automatica Sinica*, 42(4), 481–494. <https://doi.org/10.16383/j.aas.2016.c160158>
- [26] Shao, Q., Zhang, Z., Zhu, Y., Zhou, A. (2019). Qiyè jí qū kuài liàn jìshù zǒngshù [Overview of enterprise blockchain technology]. *Journal of Software*, 30(9), 2571–2592. <https://doi.org/10.13328/j.cnki.jos.005775>
- [27] Kalapaaking, A. P., Khalil, I., Rahman, M. S., Atiquzzaman, M., Yi, X., & Almashor, M. (2023). Blockchain-based federated learning with secure aggregation in trusted execution environment for Internet-of-Things. *IEEE Transactions on Industrial Informatics*, 19(2), 1703–1714. <https://doi.org/10.1109/TII.2022.3170348>
- [28] Xu, C., Qu, Y., Eklund, P. W., Xiang, Y., & Gao, L. (2021). BAFL: An efficient blockchain-based asynchronous federated learning framework. In *2021 IEEE Symposium on Computers and Communications*, 1–6. <https://doi.org/10.1109/ISCC53001.2021.9631405>
- [29] Liu, M., Teng, Y., Yu, F. R., Leung, V. C. M., & Song, M. (2019). Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle. In *2019 IEEE International Conference on Communications*, 1–6. <https://doi.org/10.1109/ICC.2019.8761206>
- [30] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3), 2084–2123. <https://doi.org/10.1109/COMST.2016.2535718>
- [31] Ongaro, D., & Ousterhout, J. K. (2014). In search of an understandable consensus algorithm. In *Proceedings of the 2014 USENIX conference on USENIX Annual Technical Conference*, 305–319.
- [32] Zeng, S., Huo, R., Huang, T., Liu, J., Wang, S., & Feng, W. (2020). Qū kuài liàn jìshù yánjiū zǒngshù: Yuánlǐ, jìnzhǎn yǔ yìngyòng [Survey of blockchain: Principle, progress and applications]. *Journal on Communications*, 41(1), 134–151.
- [33] Ning, Z., Sun, S., Wang, X., Guo, L., Guo, S., Hu, X., . . . , & Kwok, R. Y. K. (2022). Blockchain-enabled intelligent transportation systems: A distributed crowdsensing framework. *IEEE Transactions on Mobile Computing*, 21(12), 4201–4217. <https://doi.org/10.1109/TMC.2021.3079984>
- [34] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops*, 618–623. <https://doi.org/10.1109/PERCOMW.2017.7917634>
- [35] Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2019). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal*, 6(2), 1495–1505. <https://doi.org/10.1109/JIOT.2018.2836144>
- [36] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184–1195. <https://doi.org/10.1109/JIOT.2018.2812239>
- [37] Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2018). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8), 3690–3700. <https://doi.org/10.1109/TII.2017.2786307>
- [38] Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2018). When mobile blockchain meets edge computing. *IEEE Communications Magazine*, 56(8), 33–39. <https://doi.org/10.1109/MCOM.2018.1701095>

- [39] Górski, T. (2022). Continuous delivery of blockchain distributed applications. *Sensors*, 22(1), 128. <https://doi.org/10.3390/s22010128>
- [40] Tran, N. K., Babar, M. A., & Walters, A. (2022). A framework for automating deployment and evaluation of blockchain networks. *Journal of Network and Computer Applications*, 206, 103460. <https://doi.org/10.1016/j.jnca.2022.103460>
- [41] Bartoletti, M., & Pompianu, L. (2017). An empirical analysis of smart contracts: Platforms, applications, and design patterns. In *Financial Cryptography and Data Security: FC 2017 International Workshops*, 494–509. [https://doi.org/10.1007/978-3-319-70278-0\\_31](https://doi.org/10.1007/978-3-319-70278-0_31)
- [42] Dolev, S., & Wang, Z. (2020). SodsMPC: FSM based anonymous and private quantum-safe smart contracts. In *2020 IEEE 19th International Symposium on Network Computing and Applications*, 1–10. <https://doi.org/10.1109/NCA51143.2020.9306699>
- [43] Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E., & Alexandrov, Y. (2018). SmartCheck: Static analysis of ethereum smart contracts. In *Proceedings of The 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, 9–16. <https://doi.org/10.1145/3194113.3194115>
- [44] Rodler, M., Li, W., Karame, G. O., & Davi, L. (2021). EVMPatch: Timely and automated patching of ethereum smart contracts. In *Proceedings of the 30th USENIX Security Symposium*, 1289–1306.

**How to Cite:** An, M., Fan, Q., Yu, H., An, B., Wu, N., Zhao, H., . . . , & Zhao, B. (2026). Blockchain Technology Research and Application: A Literature Review and Future Trends. *Journal of Data Science and Intelligent Systems*. 4(1), 1–12, <https://doi.org/10.47852/bonviewJDSIS32021403>