**探索区块链：由来，现状，与未来**

1120200822 郑子帆

北京理工大学计算机学院07112002班，北京 100081

(1120200822@bit.edu.cn)

#### Exploring Blockchain Technology: Origins, Current Status, and the Future

Zheng zifan

(Class 07112002, School of Computer Science, Beijing Institute of Technology, Beijing 100081)

**Abstract** This comprehensive thesis delves into the core elements and potential applications of blockchain technology. The thesis illuminates the essential components of blockchain. It dissects the blockchain architecture into six distinct layers. The transformative potential of blockchain technology is exemplified in its applications in cryptocurrencies, decentralized applications (DApps), and the healthcare sector, underscoring its capacity to bolster security, efficiency, and decentralization. It also confronts the inherent 'blockchain trilemma' — the challenge of balancing scalability, security, and decentralization, and elucidates contemporary strategies and future prospects for addressing this quandary. The concluding segment underscores the vast potential of blockchain technology in future development, particularly its synergistic interplay with other emerging technologies like Artificial Intelligence(AI), which paves the way for groundbreaking applications and advancements.

**Key words** Blockchain; Virtual Currency; Cryptography; Transactions

摘要 本文深入介绍了区块链技术。首先简要介绍了它的历史发展，然后阐述了区块链的基本组成部分——交易，地址，账本，块，以及区块链本身。然后，文章着重阐述了区块链架构的六层，即数据层，网络层，共识层，激励层，合约层，和应用层。区块链技术的变革潜力在其在加密货币，去中心化应用和医疗保健等领域的应用中得到体现，展现出了它的强安全性，高效率和去中心化的能力。最后，本文探讨了区块链三元悖论，并阐明了当前的策略和应对这个难题的未来前景。结论部分强调了区块链技术在未来发展中的巨大潜力，如与新兴技术AI的协同互动构建智慧城市等，为开创性的应用和进步铺平了道路。

关键词区块链；虚拟货币；密码学；交易；

## 1. Introduction

### 1.1 What is blockchain technology

Blockchain technology originated from the un-derlying technology of Bitcoin and has now become a revolutionary technology with widespread applications. The key features of blockchain technology are decentralization, transparency, and security. It stores data across a distributed and decentralized network of computers. This prevents any central company from manipulating or controlling the entire blockchain as they lack the authority and capability to discover and modify each data block[1].

A blockchain is composed of a series of blocks, with each block containing transaction information. Each block includes encrypted data strings, timestamps, and other relevant data. To ensure the consistency of data displayed on different nodes, a core component of blockchain technology called consensus algorithm plays a vital role. It guarantees data consistency and enables every participant to possess the same version of the data.

### 1.2 The history of blockchain

The development of cryptography[5,15] has played a crucial role in the advancement of blockchain technology. In the 1980s, cryptography experienced rapid growth, and the emergence of hash functions enabled secure communication between two parties over insecure channels.

In 1991, Stuart Haber and W. Scott Stornetta proposed a system that embedded tamper-proof timestamps within documents, ensuring their integrity. This marked the first mention of a technology similar to blockchain.

The introduction of Bitcoin in 2008 expedited the progress of blockchain. Satoshi Nakamoto, a pseudonymous individual, presented a peer-to-peer electronic cash transaction system. Blockchain technology served as a vital com-ponent supporting this system, addressing the risks of double spending in digital currencies while eliminating the need for third-party intermediaries.

In 2014, Vitalik Buterin introduced Ethereum, incorporating the concept of smart contracts that automatically execute transactions under specified conditions. This innovation elevated the functionality and complexity of blockchain technology.

In recent years, blockchain technology has been expanding and maturing. It has been explored for various applications such as decentralized applications(DApps) and secure medical records. Companies like IBM and Microsoft are also actively investigating blockchain technology and considering its applications in areas such as identity verification and voting systems.

## 2. Main Components of Blockchain

In this section, we will explore several crucial technologies or components in blockchain. Section 3.1 will cover encryption-related technologies[1], while Section 3.2 will delve into specific terminologies used in blockchain[4].

### 2.1 Encryption Algorithm

In blockchain technology, data protection is of paramount importance. We commonly employ hash algorithms to transform data into fixed-length outputs, which are used to verify data integrity and prevent tampering. Furthermore, we often utilize asymmetric encryption to sign the hash value, ensuring data security and enabling verification of the authenticity of the signature.

#### 2.1.1 Cryptographic hash functions

One crucial component of blockchain technology involves the utilization of cryptographic hash functions for various operations. Hashing entails applying a cryptographic hash function to data, generating a relatively unique output (known as a message digest or simply a hash) for inputs of any size, such as files, text, or images. Cryptographic hash functions possess significant security attributes, including pre-image resistance, second pre-image resistance, and collision resistance.

In many blockchain implementations, specific cryptographic hash functions are employed, such as the Secure Hash Algorithm 256 (SHA-256), which produces a secure hash with a 256-bit output size. These functions play a pivotal role in ensuring data integrity, immutability, and secure verification within the blockchain network.

The simplest form of a hash function can be represented by converting the content to be hashed into ASCII code and using it as input for the hash function. The function can be defined as . However, this algorithm may frequently encounter collisions, where multiple inputs and produce the same hash value, i.e., .

The SHA-256 algorithm is part of the SHA-2 family and serves as a successor to the SHA-1 series. It effectively mitigates collision issues. According to calculations, the SHA-256 algorithm exhibits an average collision probability of approximately one in every  computations.

#### 2.1.2 Symmetric and Asymmetric Encryption

Symmetric encryption and asymmetric encryption are two commonly used algorithms for encryption and decryption. In symmetric encryption, the same key is used for both the encryption and decryption of data. On the other hand, asymmetric encryption utilizes a public key for data encryption and a private key for data decryption. This section will focus on introducing asymmetric encryption algorithms.

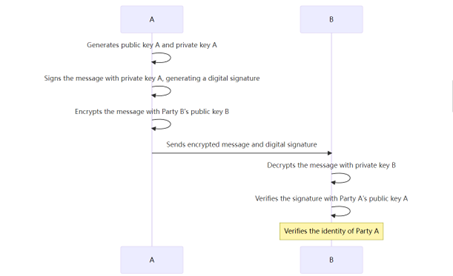
Due to the need for facilitating transactions between two mutually untrusted participants in blockchain technology, asymmetric encryption algorithms are employed. As depicted in Figure 1, in simple terms, if Participant A wants to send confidential information to Participant B, both A and B generate their respective public and private keys. A uses their own private key for digital signing and encrypts the data and generates an address using B's public key. B, on the other hand, decrypts the data using their own private key and verifies the signature and data integrity using A's public key.

图1 非对称加密流程

Fig.1 Asymmetric Encryption Process

### 2.2 Main Components

The content covered in this section rep-resents the foundational and fundamental com-ponents of blockchain technology, including transactions, addresses, ledgers, blocks and blockchains.

Transactions. Transactions are the fundamental units in blockchain, representing in-dividual operations that occur within the system. Each transaction consists of a set of inputs and outputs, which represent the movement of assets. Each input of a transaction references an old, unspent transaction output (UTXO), and each output creates a new UTXO.

Addresses. An address is a unique identifier in a blockchain network used to receive assets. It is typically a hash of a public key and is often represented in a human-readable format, just like the content in section 2.1.2.

Ledgers. The ledger is the core of a blockchain, serving as a database where data can only be added. It records all confirmed transactions, which are organized into blocks and linked together in the order they are added to the ledger.

Blocks. A block is the basic unit of the ledger and contains a set of confirmed trans-actions. Each block includes a link to the previous block, known as the previous block's hash.

Blockchains. As the fig.2 showed, a blockchain is a special type of ledger that stores data in the form of blocks and links them together using hashes. This structure ensures that once a block is added to the ledger, it cannot be altered without tampering with sub-sequent blocks.

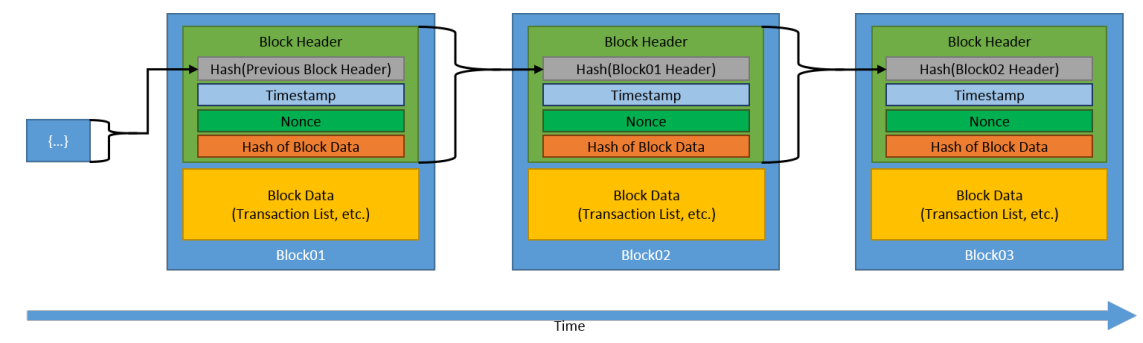


图2 区块链结构

Fig.2 The Structure of Blockchain

## 3. Blockchain Model

Similar to the TCP/IP network model dis-cussed in Section 2, blockchain technology also has its own hierarchical model. Different literature may present different perspectives, but this article adopts a widely accepted layered approach[4, 8].

As the Fig.3 shown, blockchain technology can be divided into six layers, namely the Data Layer, Network Layer, Consensus Layer, Incentive Layer, Contract Layer, and Application Layer. The following sections will provide detailed explanations of these six layers.

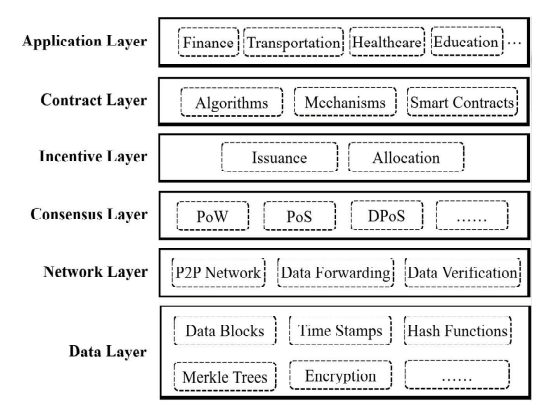


图3 区块链模型

Fig.3 Blockchain Model

### 3.1 Data Layer

Data layer is the foundation of the blockchain model. It's where the actual data is stored in the form of blocks. Just like what has been shared about in section 2.2, each block contains a list of transactions, and these transactions are stored in a cryptographic hash structure. This structure ensures the integrity and immutability of the data. Once a block is added to the blockchain, the data it contains cannot be altered without the consensus of the network.

### 3.2 Network Layer

Network layer is responsible for the communication between nodes in the blockchain network. It ensures that all nodes in the network have the same version of the blockchain. The network layer uses consensus algorithms to validate new blocks and resolve conflicts. This layer is crucial for maintaining the decentralized nature of the blockchain.

The network layer of blockchain utilizes a peer-to-peer (P2P) architecture, also known as a P2P network. Fig.4 is a model of P2Pnetwork. P2P network is a distributed network model where participants (nodes) connect and interact directly, eliminating the need for centralized servers for communication. The P2P architecture offers numerous advantages and distinctive characteristics, such as peer equality, resilient data storage, efficient data trans-mission, and heightened security.

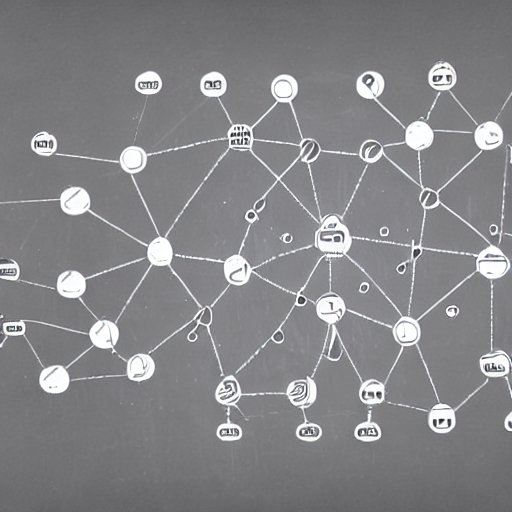


图4 P2P模型

Fig.4 P2P Model

The communication mechanism[14] at the network layer is crucial for the entire blockchain system, as the absence of reliable communication would hinder the implementation of blockchain technology. Under the communication mechanism, the network layer can be further divided into three parts: propagation layer, connectivity layer, and interaction logic layer. The communication mechanism at the network layer builds upon the TCP/UDP protocol stack at the application layer and supports specific interaction logic for peer-to-peer networks, including node handshakes, heartbeat checks, transaction and block propagation, and more.

The propagation layer facilitates the basic transmission of data between peer nodes and encompasses two data propagation methods: unicast and multicast. Unicast refers to the direct transmission of data between two known nodes without involving other nodes for relaying. Multicast involves the forwarding of data by receiving nodes to neighboring nodes through broadcasting. The blockchain network commonly utilizes the Gossip protocol for flood-based propagation.

The connectivity layer is responsible for obtaining node information, monitoring and altering the connectivity status between nodes, and ensuring link availability. Specifically, the connectivity layer protocol assists newly joining nodes in obtaining routing table data, maintains stable connections through periodic heartbeat checks, and handles connection closure in case of neighbor node failure or other events.

The interaction logic layer is the core of the blockchain network. In terms of major processes, this layer's protocol facilitates information exchange among peer nodes, including ledger data synchronization, transaction and block data transmission, feedback on data verification results, and more. Additionally, the interaction logic layer provides message channels for complex operations such as node election, consensus algorithm implementation, and other extended applications.

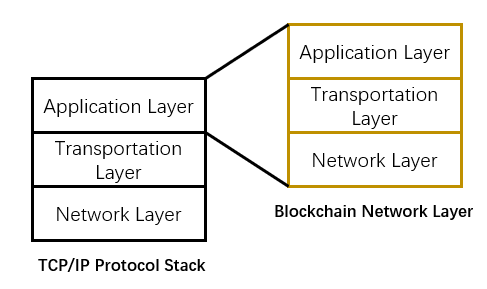


图5 区块链通信机制

Fig.5 The Communication Mechanism of Blockchain

### 3.3 Consensus Layer

Blockchain uses a variety of consensus algorithms to guarantee the data consistency and the fault-tolerant ability of the shared ledger among distributed nodes.

Consensus algorithms serve a crucial role in achieving agreement and consistency within distributed systems. In the context of block-chain technology, these algorithms play a pivotal role in addressing several fundamental challenges: Firstly, consensus algorithms determine the selection of the next block creator, ensuring the continuity and growth of the blockchain. By establishing a mechanism to designate the responsible node, the algorithm ensures the orderly addition of blocks to the blockchain. Secondly, they guarantee data consistency across the distributed network. Despite the presence of potentially malicious nodes or communication failures, consensus algorithms enable all participants to converge on a shared transaction history and state. This fosters a synchronized view of the blockchain's data. Furthermore, consensus algorithms mitigate the risk of double-spending, a critical concern in digital transactions. By validating and confirming each transaction, these algorithms prevent the occurrence of multiple reuses of the same digital asset or currency. Consequently, they ensure the integrity and uniqueness of recorded transactions within the blockchain.

Traditional application scenarios typically are relatively closed ecosystems with entities trusting in each other, where early algorithms such as PAXoS might be sufficient to reach consensus efficiently. Blockchain models, however, mainly focus on open and dynamic environments with a large number of trustless entities with possible Byzantine failures, so that more complex algorithms are needed, such as practical Byzantine fault tolerance for semi-open environments and Proof-of-X (PoX) type consensus for open environments. For example, there are currently many popular consensus algorithms, such as PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PoET (Proof of Elapsed Time), PEFT (Practical Byzantine Fault Tolerance).

Data Layer, Network Layer and Consensus Layer are the most basic and important layers and technologies of blockchain, which is not called "blockchain" if missed any of them.

### 3.4 Incentive Layer

Incentive layer[13] incorporates economic rewards into blockchain systems. By rewarding miners with a portion of digital assets, there is an incentive for them to verify transaction information, thereby sustaining mining activities and the continuous updating of the blockchain ledger. Additionally, relevant protocols and mechanisms are established to ensure clear incentives and penalties, motivating validating nodes and punishing malicious nodes.

In essence, the data verification and block creation process driven by consensus competitions can be considered as a crowdsourcing task to participating nodes that contribute their computing power. These nodes are actually self-interested agents, so that incentive compatible mechanisms must be designed to make individual behavior of revenue maximization aligned with the system-wide target of guaranteeing a secured and trusted ecosystem.

### 3.5 Contract Layer

In this layer, various smart contracts, mechanisms, and algorithms are used to manipulate data. Users can create high-level smart contracts, cryptocurrencies, or other decentralized applications (DApps). For instance, Ethereum (ETH) platform can offer Turing-complete script language and enable users to design any arbitrary smart contracts or transactions that can be precisely defined.

### 3.6 Application Layer

The application layer is where the technologies from the preceding five layers are applied to specific use cases. The specific application scenarios will be introduced in Section 4.

## 4. Applications of Blockchain Technology

### 4.1 Cryptocurrency

The application of blockchain in the realm of cryptocurrencies has revolutionized transactions by providing enhanced security, transparency, and decentralization. It has empowered users with greater control and privacy protection. The most widely used cryptocurrencies are Bitcoin and Ethereum.

Bitcoin was the pioneering cryptocurrency that first leveraged blockchain technology. In the context of Bitcoin, blockchain serves as a decentralized distributed ledger, recording and verifying transactions. Through blockchain, the Bitcoin network enables trustless value exchange, ensuring transaction transparency and security while bypassing the need for intermediaries and exorbitant fees associated with traditional financial systems.

Ethereum, on the other hand, is a more comprehensive blockchain platform. Beyond its role as a digital currency known as Ether, Ethereum supports the programming and execution of smart contracts, a significant highlight and feature. Smart contracts on Ethereum are self-executing contracts executed on the blockchain, enabling transactions and operations to be carried out based on predefined conditions and rules. This versatility has led to a broader range of applications for Ethereum, including decentralized applications (DApps) and more, which will be explored further in Section 4.2.

In summary, the application of blockchain in the realm of cryptocurrencies has made transactions more secure, transparent, and decentralized while granting users greater control and privacy protection. These applications have the potential to reshape the traditional financial system and have propelled the development and widespread adoption of cryptocurrencies.

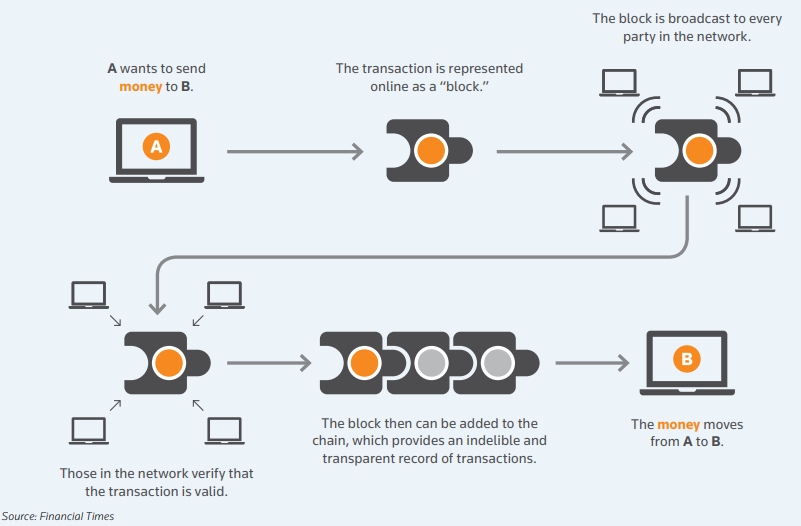


图6 金融交易流程

Fig.6 Financial Transaction Process

### 4.2 DApps

In DApps, the application of blockchain technology is primarily manifested in the following aspects[18, 19].

Smart Contracts. Through smart contracts, DApps can automate transactions, asset management, voting mechanisms, and more, without the need for reliance on third-party institutions.

Decentralized Data Storage. DApps can store data on the blockchain, ensuring the security and immutability of the data.

Cryptocurrency Payments. Many DApps utilize cryptocurrencies on the blockchain as a means of payment. Blockchain-based cryptocurrencies enable fast, low-cost, and decentralized transactions, providing DApps with more flexible and convenient payment options.

Identity Verification. Blockchain can be utilized as a decentralized identity verification system, safeguarding users' privacy information.

### 4.3 Applications in the medical field

Blockchain technology offers promising solutions to address various challenges in the healthcare system[3], improving its security, reliability, and convenience.

First and foremost, safeguarding medical data security and ensuring privacy protection have always been paramount concerns within the healthcare industry. Conventional storage and sharing methods are susceptible to hacking and data breaches. In contrast, blockchain leverages robust encryption techniques and decentralized storage, ensuring data integrity and immutability. Sensitive medical data can be securely encrypted and access can be granted only to authorized participants, effectively safeguarding patients' privacy.

Moreover, traditional practices of medical record sharing often involve time-consuming and complex processes, necessitating data exchange and verification among multiple healthcare entities. Blockchain provides a decentralized platform that enables secure and efficient sharing of medical records among authorized participants. This accelerates the diagnostic and treatment processes, minimizes redundant tests and redundant data entry, and enhances overall efficiency in healthcare collaboration.

Additionally, blockchain technology facilitates the integration of patient data from diverse sources, enabling healthcare institutions and professionals to obtain comprehensive and meaningful insights. By filtering out irrelevant information and presenting the most relevant data for diagnosis, blockchain enhances diagnostic efficiency and accuracy, ultimately improving patient outcomes.

## 5. Challenges and Future Trends

### 5.1 Blockchain trilemma

As stated in section 1.1, the blockchain's three primary characteristics are scalability, security, and decentralization. Scalability refers to the ability of blockchain technology to handle an increased volume of transactions, allowing for more efficient processing within a given time frame. Security pertains to safeguarding the data on the blockchain from a wide range of potential attacks. Decentralization ensures that the network remains resilient and not under the control of a limited number of entities.

The Consistency, Availability, and Partition Tolerance Theorem, introduced in 1980[6], highlights that decentralized data storage can only fulfill two out of the three aforementioned properties. With the emergence of the blockchain concept, the blockchain trilemma[7] has come to the forefront, asserting that public blockchain infrastructure must make trade-offs by sacrificing at least one aspect among security, decentralization, or scalability. The degree of decentralization directly impacts the network's performance, as a higher number of participants leads to longer processing times and reduced scalability. Conversely, stronger security, indicated by a higher hash rate and shorter confirmation times, contributes to enhanced scalability. These interdependencies demonstrate the inherent constraints and conflicts among the three pillars.

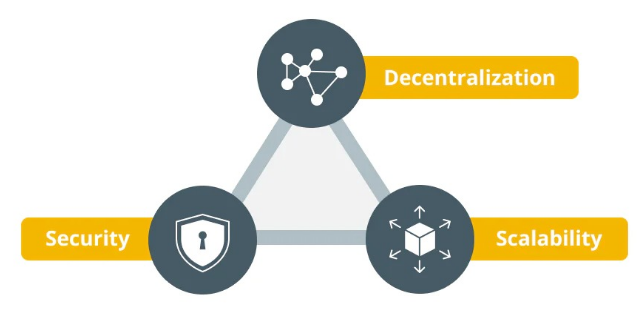


图7 区块链三元悖论

Fig.7 Blockchain trilemma

Thus, enterprises involved in the blockchain space must strive to strike a delicate balance between these factors. Currently, two main approaches are pursued. The first involves improving network speed and security to tackle these challenges. The second revolves around advancing the underlying blockchain technology itself, such as implementing solutions like Bitcoin Cash to increase block sizes and enhance scalability, among other innovations.

### 5.2 Future trends

In the future, blockchain technology still has ample room for improvement and expansion, with its application domains set to expand further.

Firstly, at the technical level, as discussed in Section 5.1, blockchain technology needs to strike a better balance in terms of resource efficiency, processing efficiency, and privacy and security. As blockchain ventures into larger markets, issues such as increased network participants and heightened security vulnerabilities become critical concerns that need to be addressed effectively.

Secondly, in terms of application domains, blockchain has the potential to create even greater value by integrating with current advancements in AI. It can be applied to various sectors such as education, food safety, gaming, and beyond, contributing to the development of smart cities and unlocking new possibilities.

The future holds promising prospects for blockchain technology, and as it continues to evolve, addressing technical challenges and exploring novel applications will be key to unlocking its full potential and creating meaningful impacts across diverse industries.

## 6. Summary

This thesis delves into the intricacies of blockchain technology, explaining its fundamental components and layered model. It elaborates applications of blockchain in cryptocurrencies, DApps, and the healthcare sector, highlighting the transformative power of this technology. It also discusses the inherent challenge in the blockchain trilemma of balancing security, decentralization, and scalability. Hope it can provide inspiration for people who are interested in understanding blockchain.

**参 考 文 献**

[1] Yaga D, Mell P, Roby N, et al. Blockchain technology overview[J]. arXiv preprint arXiv:1906.11078, 2019.

[2] Michael J, Cohn A, Butcher J R. Blockchain technology[J]. The Jour-nal, 2018, 1(7): 1-11.

[3] Mettler M. Blockchain technology in healthcare: The revolution starts here[C]//2016 IEEE 18th international conference on e-health net-working, applications and services (Healthcom). IEEE, 2016: 1-3.

[4] Singhal B, Dhameja G, Panda P S. Beginning Blockchain: A Beginner's guide to building Blockchain solutions[M]. New York: Apress, 2018.

[5] Popovski L, Soussou G, Webb P B. A brief history of blockchain[J]. Online access: February, 2018, 1: 2019.

[6] Gilbert S, Lynch N. Perspectives on the CAP Theorem[J]. Computer, 2012, 45(2): 30-36.

[7] Abadi J, Brunnermeier M. Blockchain economics[R]. National Bureau of Economic Research, 2018.

[8] Yuan Y, Wang F Y. Blockchain and cryptocurrencies: Model, tech-niques, and applications[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 48(9): 1421-1428.

[9] Guo Y, Liang C. Blockchain application and outlook in the banking industry[J]. Financial innovation, 2016, 2: 1-12.

[10] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportuni-ties: A survey[J]. International journal of web and grid services, 2018, 14(4): 352-375.

[11] Abou Jaoude J, Saade R G. Blockchain applications–usage in dif-ferent domains[J]. Ieee Access, 2019, 7: 45360-45381.

[12] Yuan Y, Wang F Y. Towards blockchain-based intelligent transportation systems[C]//2016 IEEE 19th international conference on intelligent transportation systems (ITSC). IEEE, 2016: 2663-2668.

[13] Wang J, Li M, He Y, et al. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications[J]. Ieee Access, 2018, 6: 17545-17556.

[14] Antwi R, Gadze J D, Tchao E T, et al. A survey on network optimization techniques for blockchain systems[J]. Algorithms, 2022, 15(6): 193.

[15] Sarmah S S. Understanding blockchain technology[J]. Computer Science and Engineering, 2018, 8(2): 23-29.

[16] Abou Jaoude J, Saade R G. Blockchain applications–usage in dif-ferent domains[J]. Ieee Access, 2019, 7: 45360-45381.

[17] Cai W, Wang Z, Ernst J B, et al. Decentralized applications: The blockchain-empowered software system[J]. IEEE access, 2018, 6: 53019-53033.

[18] Miraz M H, Ali M. Applications of blockchain technology beyond cryptocurrency[J]. arXiv preprint arXiv:1801.03528, 2018.

[19] Hashemi Joo M, Nishikawa Y, Dandapani K. Cryptocurrency, a successful application of blockchain technology[J]. Managerial Finance, 2020, 46(6): 715-733.

[20] Abou Jaoude J, Saade R G. Blockchain applications–usage in dif-ferent domains[J]. Ieee Access, 2019, 7: 45360-45381.

[21] Yang W, Garg S, Raza A, et al. Blockchain: trends and future[C]//Knowledge Management and Acquisition for Intelligent Systems: 15th Pacific Rim Knowledge Acquisition Workshop, PKAW 2018, Nanjing, China, August 28-29, 2018, Proceedings 15. Springer International Publishing, 2018: 201-210.

[22] Zheng X R, Lu Y. Blockchain technology–recent research and future trend[J]. Enterprise Information Systems, 2022, 16(12): 1939895.