

Focus on Blockchain: A Comprehensive Survey on Academic and Application

YIJUN ZOU¹, TING MENG^{1,2,3}, PENG ZHANG^{2,3}, WENZHEN ZHANG^{2,3}, AND HUIYANG LI⁴

¹E-Commerce Laboratory, School of Economics and Management, Beijing University of Posts and Telecommunications, Beijing 100876, China

²School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

³Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China

⁴Department of Computer Science and Engineering, The University of Texas at Arlington, Arlington, TX 76019, USA

Corresponding author: Ting Meng (mengting@bupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61170273, and in part by the China Scholarship Council under Grant [2013]3050.

ABSTRACT As a decentralized distributed ledger, blockchain has developed rapidly since its birth and has been highly valued by governments, academia, and industry. Start in the financial field, blockchain technology has been rapidly applied to various fields such as the Internet of Things, supply chain, and healthcare. Blockchain technology has made sufficient development and innovation, but it also faces many challenges, such as security, scalability, and waste of resources. This paper starts with the development history of blockchain and combines the characteristics and technical principles of it to analyze the current academic research status and application scenarios. Meanwhile, this paper analyzes the existing outstanding blockchain projects and elaborates on their key advantages and current challenges. With discussing the ongoing development trend of blockchain, the development direction, and the research trend of blockchain in the future, this paper provides a useful reference for related research.


INDEX TERMS Blockchain, academic, application, projects, consensus algorithm, smart contract, security, development trend.

I. INTRODUCTION

Since the concept of blockchain was first proposed in Satoshi Nakamoto's paper [1], it has developed rapidly from a prototype concept into a hot technology in the past decade. Technically, blockchain is a combination of blocks linked by hash functions, and its essence is a distributed ledger based on asymmetric encryption algorithms. It is an integrated and innovative technology which integrates cryptography, distributed system, network security and others. The emergence of blockchain has changed the past pattern of transactions that had to rely on trusted third-party institutions. The central institution can no longer restrict both parties of the transaction, and each transaction is verified by more than half of the participants in the network [2], making a truly distributed peer-to-peer transaction possible. To ensure network consistency in the blockchain, Nakamoto proposed a Proof-of-Work (PoW) consensus mechanism, which means that the more work a miner does, the more likely it is

to mine a block and the higher the chance of obtaining a reward. Nevertheless, the Proof-of-Work (PoW) mechanism still has problems, such as waste of computing resources and low efficiency, so the consensus mechanism of Proof-of-Stake (PoS) [3] and Delegated Proof-of-Stake (DPoS) [4] has been proposed successively. Blockchain is based on a peer-to-peer network, where distributed ledger books are stored on each node to complete peer-to-peer transactions. Based on consensus protocols and P2P networks, to extend the availability of blockchain, the concept of smart contracts was proposed. Generally speaking, smart contract is a contract written in code. If it can meet the conditions, it is automatically enforced without an intermediary's need to establish trust. However, once mistakes are in the smart contract, the consequences can be disastrous [5]. Smart contracts are widely used to defend against distributed denial of service (DDoS) attacks, design voting protocols, and build decentralized applications (DAPPS).

With the continuous development of blockchain technology, the concept of blockchain has expanded from the financial field to other fields, such as healthcare, IoT and

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Yu .

supply chain, etc. It has been continuously combined with other application scenarios, gradually heading in the direction of “blockchain +” [6]. Various universities and research institutions attach great importance to this technology and publish a large number of academic achievements related to blockchain. At present, there are a large number of literature reviews about blockchain techniques, such as the technical architecture [7]–[8], security and privacy [9]–[11], network security [12]. And some discussion on a specific area of blockchain [13]–[15] has been raised. The paper [16] presents a comprehensive introduction to the blockchain’s architecture, principles and applications from a more technical perspective. Unlike the above papers, our paper starts from the perspective of academics and application. It focuses more on academic data information statistics and industry applications to show the development status and blockchain trend. Therefore, this paper is devoted to the holistic research of blockchain, as shown in Figure 1. 1) Comprehensively expound the concept and characteristics of blockchain from the background and development history. 2) Analyze the academic community’s attention to the blockchain, and summarize the latest research results. 3) Analyze the application scenarios and actual implementation projects of blockchain in various fields. 4) Elaborate on the advantages and challenges of blockchain under the current situation. 5) Predict and discuss the technology development trend and industry trend of blockchain. We hope that the work in this paper can provide a useful reference for subsequent studies.

II. BLOCKCHAIN BACKGROUND

A. BLOCKCHAIN CONCEPTS

Satoshi Nakamoto first proposed the concept of blockchain, which is a Proof-of-Work chain based on hash. It is used for online transactions without any financial institution [1]. In this part, we explain the concept of blockchain based on different subject backgrounds and perspectives and summarize the following directions.

At the technical level, blockchain can be regarded as a technology built on the basis of a series of encryption algorithms, storage technologies, and peer-to-peer networks, with features including “unalterable”, “consensus mechanism” and “decentralized”. At the database level, blockchain can be thought as a giant ledger for bookkeeping [17], [18]. At the economic level, blockchain can build a reliable trust foundation for both parties who know nothing about transactions with equal and credible. In summary, blockchain is an innovative integration solution of multiple existing technologies that integrates cryptography technology, distributed consistency protocol, network security, and other related technologies [19].

B. BLOCKCHAIN PAST AND PRESENT

As shown in Figure 2, from “New Directions in Cryptography” published by Diffie and Hellman in 1976 to Libra proposed by Facebook in 2019 [20]–[25], blockchain technology is constantly developing and improving.

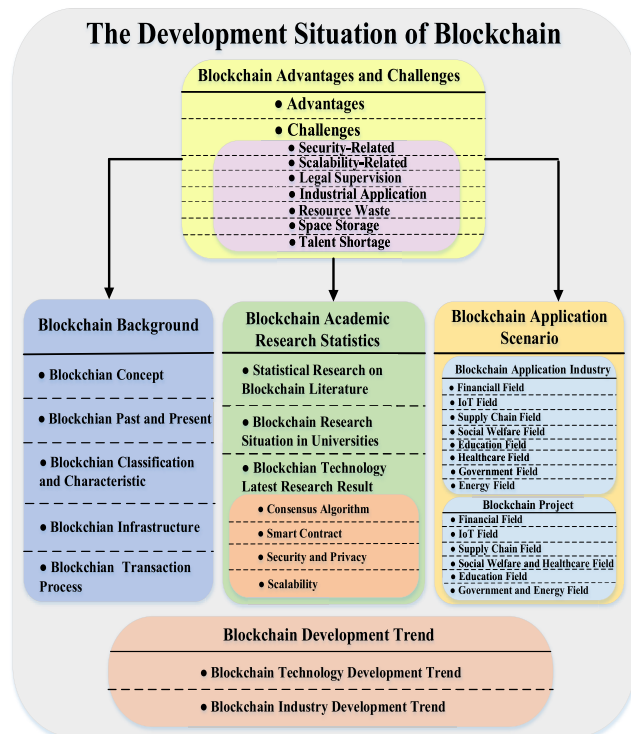


FIGURE 1. The Structure of Blockchain Holistic Research.

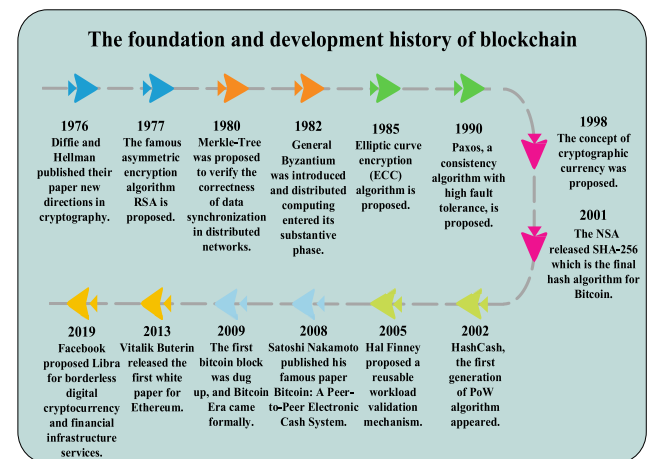


FIGURE 2. The Foundation and Development History of Blockchain.

C. BLOCKCHAIN CHARACTERISTIC AND CLASSIFICATION

There are four of the most important features of blockchain.

- Anonymity:** The anonymity of blockchain means that everyone has a virtual identity on the blockchain. For example, Bitcoin users anonymously hold public keys for transactions, and public keys are not unique [1].
- Decentralization:** The decentralization of blockchain means that no central institution is needed, and every node is equivalent. It has become the core technology

of digital cryptocurrencies, such as Bitcoin and Ethereum [26].

- **Tamper-resistance:** The tamper-resistance of blockchain means that any transaction information stored in the blockchain cannot be tampered during and after the process of block generation [10]. The data structure of the blockchain is formed by orderly linking blocks containing transaction information.
- **Traceability:** The traceability of blockchain means that transaction sources can be tracked through data storage structure and chain structure. L. Xiao *et al.* designed a blockchain-based traceable IP copyright protection algorithm [27], X. Li *et al.* researched critical technologies of the logistics information traceability model [28].

Blockchain can be classified into the public chain, alliance chain, and private chain. These three types of blockchains have some common characteristics: They use a distributed P2P network for transactions. They all rely on the consensus algorithm to synchronize network transaction data and require that each transaction need digitally signed before being added to the chain [30]. The details of the three blockchains are as follows.

- **Public Chain:** It refers to the blockchain where anyone in the world can enter the system at any time to read data, send verifiable transactions, and complete accounting. The public chain mainly includes Bitcoin and Ethereum.
- **Alliance Chain:** It refers to the blockchain with several institutions participating in the management. Each institution runs one or more nodes. The data only allows different institutions in the system to read, write and send a transaction, and record transaction data together. The alliance chain is represented by Hyperledger. Besides, Jingjing Gu *et al.* built an alliance blockchain framework to detect malicious code in malware [31].
- **Private Chain:** It refers to the blockchain whose writing permission is controlled by an organization or institution. The qualification of participating nodes will be strictly restricted, and its writing permission is in the hands of only one organization. Private chains are generally used as internal audits in practical applications. The applications based on private chain technology are mainly the Linux Foundation and R3CEV Corda platforms.

D. BLOCKCHAIN INFRASTRUCTURE

The blockchain architecture consists of six different layers, as shown in Figure 3.

- **Data Layer:** This layer encapsulates the chain structure of the underlying data block, and the related digital signature and time stamp technology, which is the most underlying data structure in the whole blockchain technology.
- **Network Layer:** Including P2P network, communication mechanism, and verification mechanism.

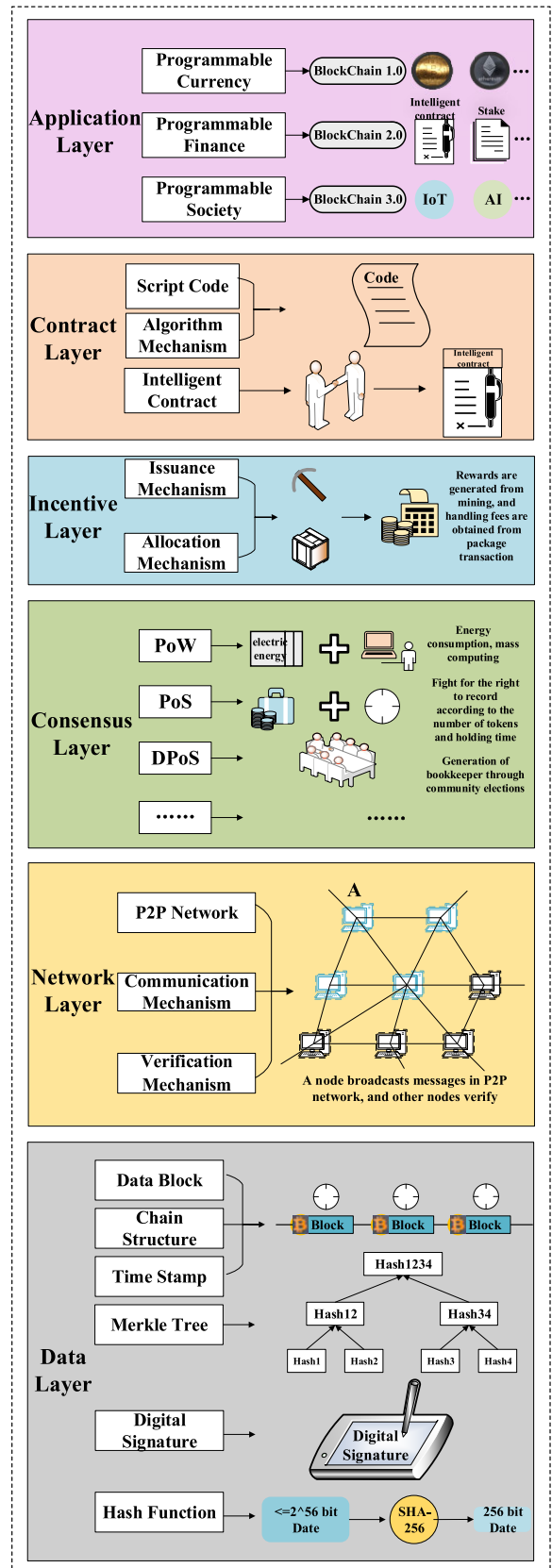


FIGURE 3. The Infrastructure of Blockchain.

- **Consensus Layer:** It is one of the core technologies of blockchain and the blockchain community's governance mechanism to make highly decentralized nodes reach a consensus in the decentralized blockchain network.
- **Incentive Layer:** The incentive layer is the mining mechanism. You can get as many rewards as you contribute to the blockchain system. With this incentive mechanism, nodes in the entire network can be encouraged to participate in data recording and maintenance on the blockchain.
- **Contract Layer:** This layer encapsulates various scripts, algorithms, and smart contracts, which is based on the programmable characteristics of the blockchain.
- **Application Layer:** The "blockchain +" as we know is at the application layer. This layer encapsulates various application scenarios and cases of the blockchain. The transaction's main content includes the formation of blocks by miners' package trading, and the verification of the blocks excavated by miners' mining and broadcasting. To ensure the security and integrity of the transaction in the system, the construction of the transaction address also use multiple hash encryption.

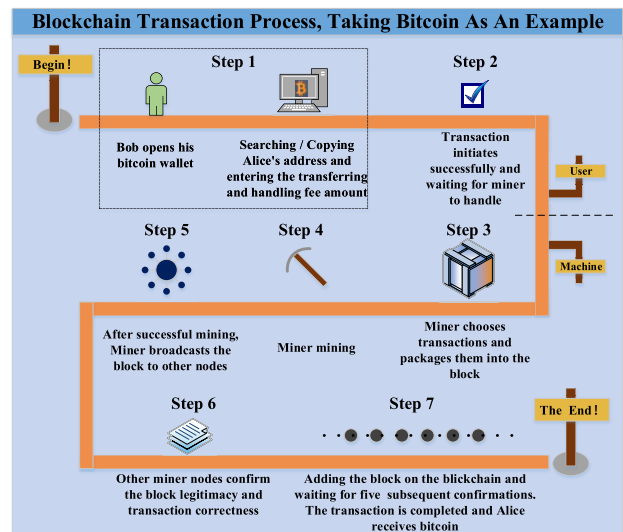


FIGURE 4. The Transaction Process of Blockchain.

achievements published has increased dramatically, especially from 2017 to 2019.

From the survey of IEEE database, there are more and more discussions on blockchain in recent years. And universities and research institutions have invested more scientific research strength in the field of blockchain, which plays an important role in the mature application and further development of blockchain.

b: ACM

This part investigates the total number of blockchain papers in ACM database from since 2008, including the number published by different universities and the collection in different ACM journals and conferences. The research results show in the Figure 6(a)-(c).

According to the ACM library, we can conclude that the number of blockchain related papers has surged in the past five years. Different universities competing to publish papers and putting forward different viewpoints, which have played an important role in the development of blockchain technology.

c: SPRINGER

This part investigates the total number of blockchain related academic achievements published in the Springer database since 2008. The research results show in the Figure 7(a)-(b). According to the papers retrieved from the database, no blockchain related papers were published in 2011 and before. Since 2012, the number of publications of related papers has gradually increased, and it can be seen that the research on blockchain is becoming more and more popular. From only two papers in early 2012 to two thousand in 2019, more than two thousand related papers have been published since 2020, which can be said to be quite popular.

E. BLOCKCHAIN TRANSACTION PROCESS

In addition, taking bitcoin as an example, blockchain transaction has seven steps, as shown in Figure 4. The transaction's main content includes the formation of blocks by miners' package trading, and the verification of the blocks excavated by miners' mining and broadcasting. To ensure the security and integrity of the transaction in the system, the construction of the transaction address also adopts multiple hash encryption.

III. ACADEMIC RESEARCH STATISTICS

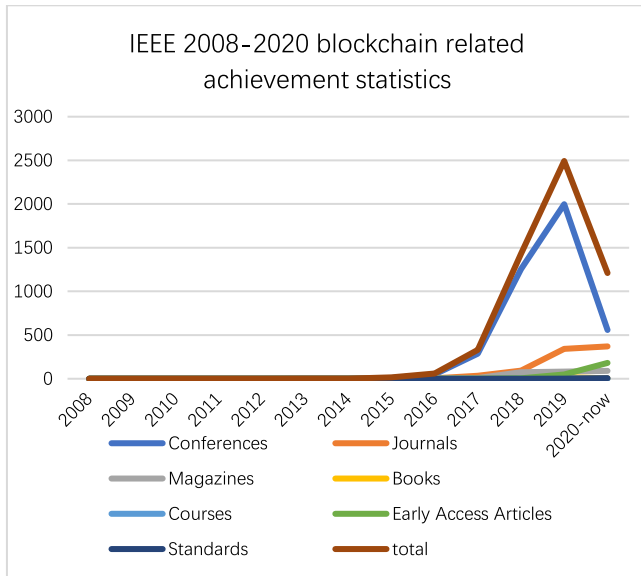
A. STATISTICAL RESEARCH ON BLOCKCHAIN LITERATURE

To make better statistics on blockchain's research status, we searched the four major databases, including IEEE, ACM, Springer and Elsevier. It can help us make a portrait of the blockchain academic research's current situation, and facilitate us to examine the popularity and future trends of the blockchain. The following databases selecting results on academic research achievements of blockchain used advanced search methods to filter achievements. The number of papers from the four databases used blockchain as the keyword, then the other features, such as conferences and journals, universities and institutions, used more search items combining the blockchain keyword with the corresponding labels.

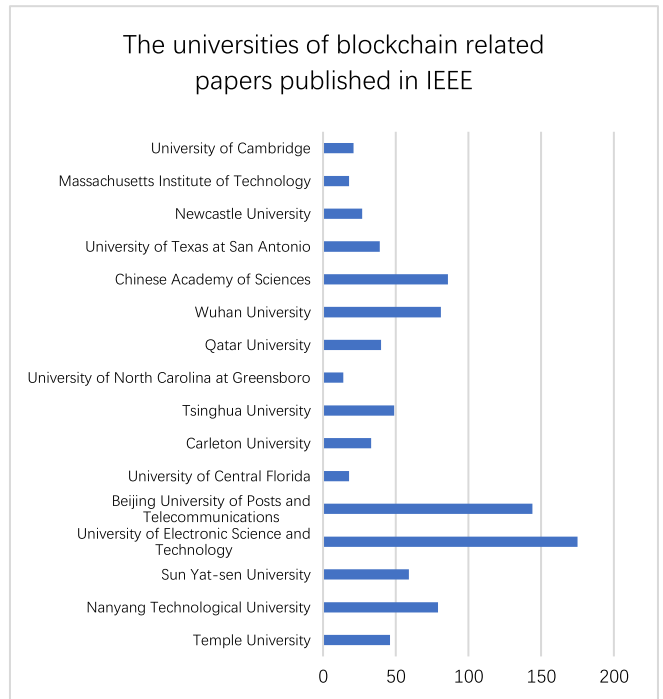
1) LITERATURE ANALYSIS OF EACH DATABASE

a: IEEE

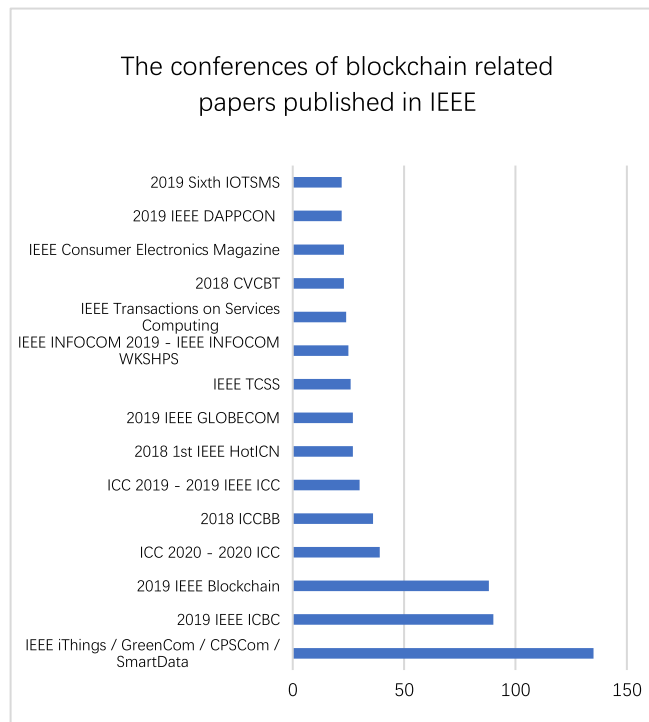
This part investigates the total number of blockchain-related academic achievements published in IEEE database, the publication status of universities, the conferences with more publications, since 2008. The research results show in the Figure 5(a)-(c). Since 2013, the number of blockchain



(a). The number of blockchain related achievements in IEEE.

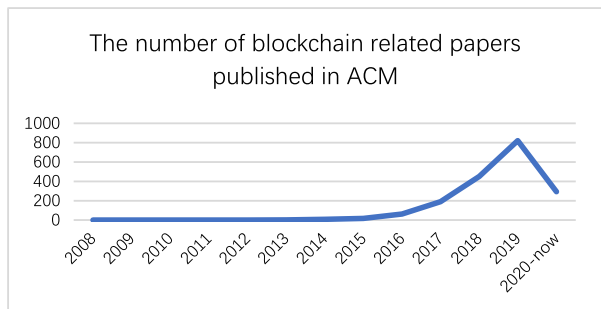


(b). The universities of blockchain related papers published in IEEE.

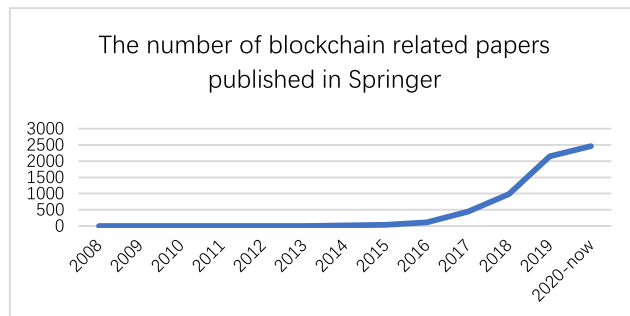


(c). The conferences of blockchain related papers published in IEEE.

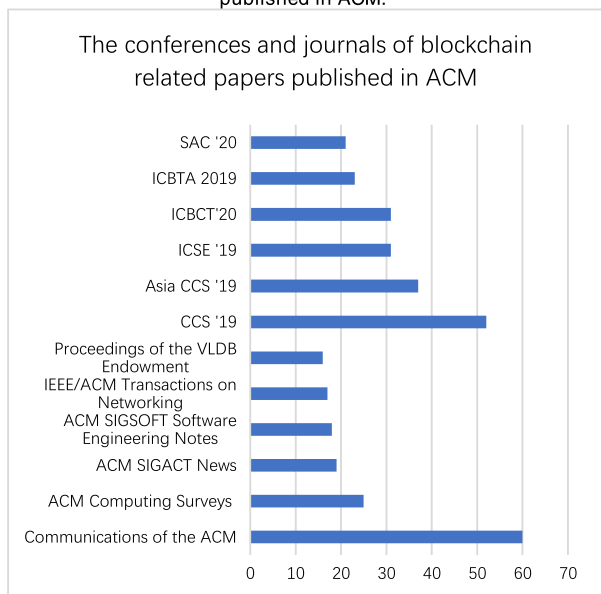
FIGURE 5. (a). The number of blockchain related achievements in IEEE. (b). The universities of blockchain related papers published in IEEE. (c). The conferences of blockchain related papers published in IEEE.



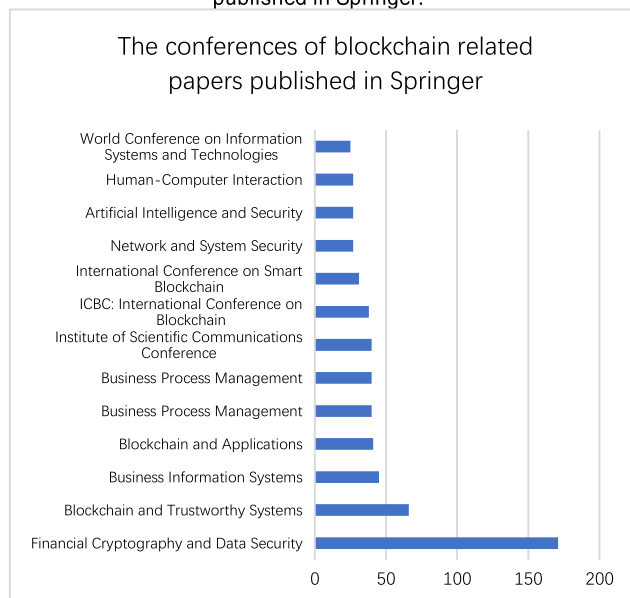
(a). The number of blockchain related papers published in ACM.



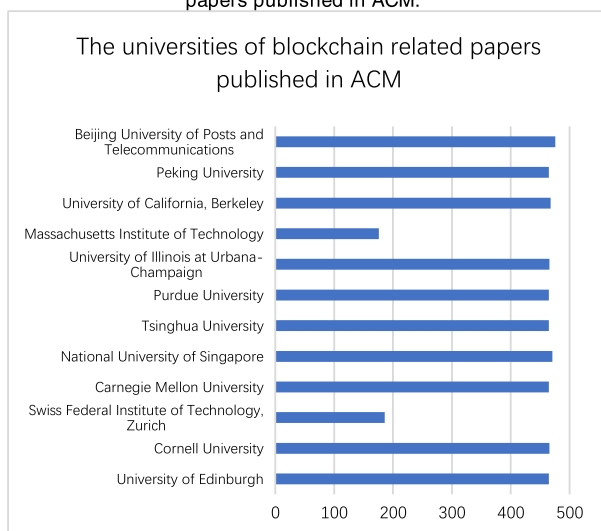
(a). The number of blockchain related papers published in Springer.



(b). The conferences and journals of blockchain related papers published in ACM.



(b). The conferences of blockchain related papers published in Springer.



(c). The universities of blockchain related papers published in ACM.

FIGURE 6. (a). The number of blockchain related papers published in ACM. (b). The conferences and journals of blockchain related papers published in ACM. (c). The universities of blockchain related papers published in ACM.

FIGURE 7. (a). The number of blockchain related papers published in Springer. (b). The conferences of blockchain related papers published in Springer.

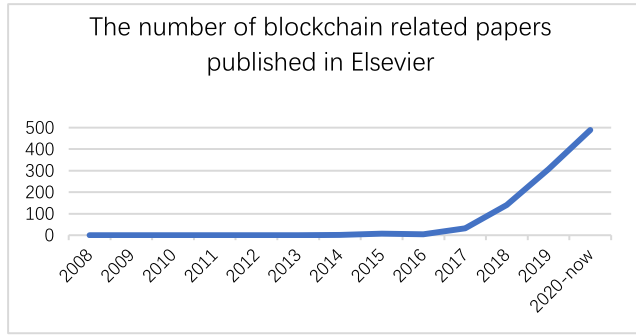
d: ELSEVIER

The research results show in the Figure 8(a)-(b). By August 2020, there were 981 records and 10 journals that had published papers. Academic Research on blockchain has various types of results, most of which are Research Article, and the access type is also developing towards open access.

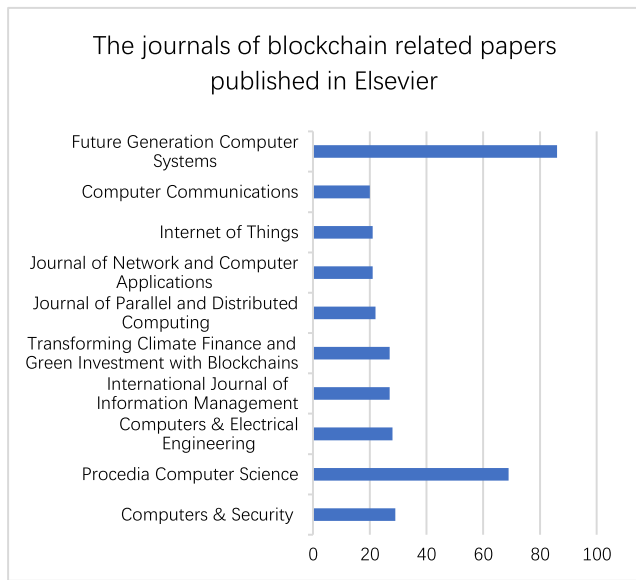
With 2014 as the starting point, attention has been gradually rising, the academic research achievements have been increasing year by year, and the blockchain has been increasingly influential in the world.

2) OVERALL LITERATURE ANALYSIS

According to the survey of these four major databases, the number of blockchain papers is increasing year by year. As the year 2020 is not over, the number of papers has decreased slightly. The results show in the Figure 9. People’s enthusiasm for blockchain research is also increasing.



(a). The number of blockchain related papers published in Elsevier.



(b). The journals of blockchain related papers published in Elsevier.

FIGURE 8. (a). The number of blockchain related papers published in Elsevier. (b). The journals of blockchain related papers published in Elsevier.

Especially from 2017 to 2019, the number of papers has exploded. But at present, we believe that the development of blockchain is still in the early stage, and the future development prospects are still very broad to explore and study. In addition to theoretical research, practical research also needs more attention.

B. BLOCKCHAIN RESEARCH SITUATION IN UNIVERSITIES

With the continuous development of blockchain technology, various universities and research institutions have also begun to pay attention to blockchain. The number of universities offering blockchain courses is constantly increasing, which also proves the importance of blockchain technology. At present, the world is facing a shortage of blockchain talents. This contradiction between supply and demand has given the market a vast imagination, which is the reason that the current colleges and universities are offering blockchain courses. With the rapid development of blockchain technology in various industries around the world, the imbalance

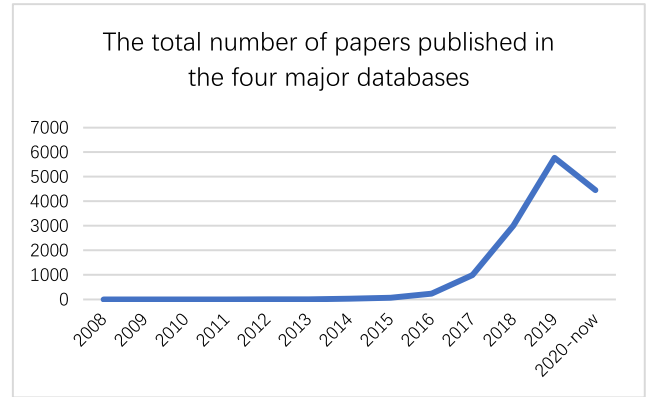


FIGURE 9. The total number of papers published in four major databases.

of talent supply and demand has also become a hot topic in the industry, and the entire industry urgently needs a large number of professionals. In a short period, the situation of talent supply and demand mismatch in blockchain is still difficult to change. In addition, we investigated the situation of blockchain labs opened by universities around the world, and statistically summarized the corresponding websites of the labs, as shown in TABLE 1.

C. BLOCKCHAIN TECHNOLOGY LATEST RESEARCH RESULT

1) CONSENSUS ALGORITHM FIELD

Driven by previous research, the PoW algorithm used by the Bitcoin system came into being. Unfortunately, many other research results show that the PoW algorithm have many defects, such as energy waste and security issues. Philip Daian [32] stated that these huge computing power had no effect on society except for protecting the security of the Bitcoin network. To prevent the generation of large mining pools, Miller [33] proposed a new mechanism to design the PoW puzzles as non-outsourced puzzles. In addition to the security problem of the PoW algorithm, Eyal raised another problem: the payment system using the PoW algorithm is not suitable for real-time payment [34], and proposed a new consensus model called Bitcoin-NG, which speeds up the confirmation time of transactions. Sompolinsky and Zohar [35] proposed the GHOST strategy to reduce the block generation time while being able to handle the problem of forks and prevent double-spending attacks. Vivek Bagaria et al. [36] proposed a new blockchain proof protocol called Prism, which can resist 51% attacks, thereby improving the security of the system.

PoS was proposed because of the unfair mining of PoW. Nxt is the first electronic currency with a 100% Proof of Stake (PoS) mechanism. The more coin miners have, the greater chance to mine the next block. Kiayias et al. [37] used Follow-the-Satoshi program to implement the PoS consensus, claiming that the leader election should be completed randomly by calculating entropy. To overcome the

TABLE 1. Global University Blockchain Lab.

University	Blockchain Lab Name	Blockchain Lab Website Address
Arizona State University	Arizona State University's Blockchain Research Lab	https://blockchain.asu.edu/
Cambridge University	Cambridge Centre for Alternative Finance	https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/
Carnegie Mellon University	CMU Blockchain	http://blockchain.cs.cmu.edu/
Columbia University	Blockchain at Columbia	https://blockchainatcolumbia.com/
Cornell University	IC3: The Initiative for CryptoCurrencies and Contracts	https://www.initc3.org/
Delft University of Technology	Blockchain Lab	https://www.blockchain-lab.org/
Duke University	Duke Blockchain Lab	http://www.dukeblockchainlab.com/
Frankfurt School of Finance & Management	Blockchain Center	https://www.frankfurt-school.de/en/home/research/centres/blockchain
Harvard University	Harvard Blockchain Lab	https://blogs.harvard.edu/blockchain/
Marquette University	Marquette University Blockchain Lab	https://www.marquetteblockchain.com/
Massachusetts Institute of Technology	MIT Cryptoeconomics Lab Media Lab: Digital Currency Initiative	https://ce.mit.edu/ https://dci.mit.edu/
RMIT University	RMIT Blockchain Innovation Hub	https://sites.rmit.edu.au/blockchain-innovation-hub/
Stanford University	The Stanford Center for Blockchain Research	https://cbr.stanford.edu/
Tsinghua University	Center for Block-chain Finance Research	http://cbfr.sem.tsinghua.edu.cn/
University of Amsterdam	Blockchain & Society Policy Research Lab	https://blockchain-society.science/
University of Basel	Center for Innovative Finance Team	https://cif.unibas.ch/en/research/blockchain-dlt-184/
University of British Columbia	Blockchain@UBC	https://blockchain.ubc.ca/
University of California, Berkeley	Blockchain X-Lab Blockchain at Berkeley	https://scet.berkeley.edu/blockchain-lab/ https://blockchain.berkeley.edu/
University of California, Irvine	Blockchain and Cryptocurrency at UC Irvine	https://www.blockchain.uci.edu/
University College London	UCL Centre for Blockchain Technologies	http://blockchain.cs.ucl.ac.uk/
University of Cumbria	Research into Currencies	https://www.cumbria.ac.uk/research/centres/iflas/research-and-publications/research-into-currencies/
University of Edinburgh	IOHK Blockchain Technology Laboratory	http://web.inf.ed.ac.uk/infweb/partners/blockchain-technology-laboratory-iohk
University of Pennsylvania	Penn Blockchain	http://pennblockchain.com/
University of Southern California	Blockchain @USC	https://blockchain.usc.edu/
University of Texas at Austin	Blockchain Initiative	https://www.mccombs.utexas.edu/centers/blockchain
University of Zurich	UZH Blockchain Center	http://blockchain.uzh.ch/
Western University	CryptoEconomics Lab	https://www.ivey.uwo.ca/cryptoeconomics-lab/
Wuhan University	Laboratory of Cryptography and Blockchain Technology in Wuhan University	http://blockchain.whu.edu.cn/
York University	Blockchain.lab	https://blockchain.lab.yorku.ca/

limitations of the existing PoS in terms of fairness and security, Lee *et al.* [38] proposed a new protocol called Proof of Sharing (PoS) based on fairness and dynamic sharing management. Larimer's idea was to use rights and interests as the evidence of voting [4], rather than the opportunity to mine new block. This consensus algorithm is called Delegated Proof of Stake (DPoS). Some people think that the consensus algorithm used by PPCoin is the first variation of PoS. Bentov *et al.* [39] proposed a solution called Proof of Activity (PoA). This PoA consensus combining PoW and PoS not only solves the double spending attack, but also deals with the Tragedy of the commons caused by the PoW consensus. TABLE 2 compares the PoW, PoS algorithm, and the combination of them from multiple angles.

In addition to the above mainstream consensus algorithms used in the blockchains, many scholars have also

developed other types of consensus algorithms in recent years. Blocki and Zhou [40] proposed the Proof of Human puzzle. The ingenious design of this puzzle is to mine a new block. It cannot simply depend on the hardware devices, and human participation is also required. Proof of Space [41] is the other consensus algorithm based on proof types, and they do not use the concepts of PoW and PoS algorithms. In Proof of Burn, miners must send their coins to an address that "burns" them, which means others cannot use these coins. In Proof of Space, miners invest their money in hard drives, which is much cheaper than investing in the equipment used by the PoW algorithm.

This consensus is performed in a special environment called the Trusted Execution Environment (TEE) [42]. Milutinovic [29] proposed the Proof of Luck consensus algorithm, which is also performed in the TEE environment.

TABLE 2. Comparison of Main Consensus Algorithms.

Comparison Items	PoW	PoS	Mixed Form
The Need of Modern Hardware	In Great Need	No Need	Need
Fork	Possible	Difficult	Possible
Double-Spending Attacks	Possible	Difficult	Possible
The Speed of Mining Blocks	Slow	Fast	Slow
Mining Pool	Existing	Existing	Existing
Example	Bitcoin	Nxt	PPCoin

These emerging consensus algorithms have also made outstanding contributions to the development of blockchain.

2) SMART CONTRACT FIELD

The smart contract is similar to the upgraded version of many electronic contracts. When the contract meets the conditions, it will automatically execute. And at the same time, it can receive and store information. Because of the decentralization, tamper-resistance, and traceability characteristics in the blockchain. The developers propose to embed the smart contract into the blockchain to avoid malicious tampering of the contract conditions. However, the widely used cryptocurrencies do not support complex smart contracts. Das *et al.* [43] proposed the practical framework called FastKitten, which is used to execute complex smart contracts at a low cost. In addition, the privacy of smart contracts is the main obstacle to its widespread adoption. Steffen *et al.* [44] proposed zkay language, which introduced the definition of privacy type of private value owners, hid private data with a primitive password, and then enhanced the correctness of update state through Non-Interactive Zero-Knowledge (NIZK) proof, to solve the privacy problem of smart contracts.

3) SECURITY AND PRIVACY FIELD

The essential security characteristics of the blockchain come from the advancement of cryptographic technology and the design and implementation of the Bitcoin system. Rui Zhang *et al.* summarized the inherent security attributes of the blockchain and the parts that need to be strengthened [10].

Among them, consistency, tamper-resistance, prevention of DDoS attacks, resistance to double-spending attacks, and the use of pseudonyms are all more common mature security attributes in blockchain, while, unlinkability, confidentiality, and resistance to majority 51% consensus attacks need to be strengthened. In addition, Ganesh *et al.* [45] proposed a privacy-protected version of the PoS protocol, defining the concept of anonymous verifiable random functions, and strengthening the security of the PoS protocol. Zhang and Preneel [46] proposed the future direction of more secure PoW protocols and pointed out several common pitfalls in PoW security analysis.

Rodler *et al.* [47] have proposed a new smart contract security technology that protects deployed contracts in a backward compatible manner through runtime monitoring and

verification. Matetic *et al.* [48] proposed a new Bitcoin protection method for light client competition, which provided significant protection for light clients. Ting Cai *et al.* designed a Blockchain-Assisted Trust Access Authentication System for Solid [49]. With the increasing interest of blockchain in academic research and industry, the security and privacy of blockchain will attract considerable attention gradually.

4) SCALABILITY FIELD

Scalability is defined as the ability of a system, network, or process to handle increasing workloads, or to expand its potentiality for accommodating this growth. For the current blockchain, scalability is a problem that prevents it from being accepted by the mainstream. Currently, Visa, the fastest payment network, can process approximately 24,000 payments per second. However, due to the use of blockchain, the transaction speed of most cryptocurrencies is inferior and cannot meet demand. At present, it seems that increasing the block size and Lightning Network are the only two mode options for expanding the Bitcoin system, but this is actually just the two mainstream methods currently favored by BCH and BTC [50]. In fact, there are many other suggestions for improving throughput, including sidechains, which can ease the pressure on the network without having to switch to a hosting solution similar to Lightning Network. In addition, Payment Channel Network (PCN) has become the most widely deployed solution to alleviate the scalability problem, allowing most transactions between two users to be handled outside the chain. On this basis, Malavolta *et al.* [51] studied and designed a secure and private PCNS. Smart contract is a kind of automatic implementation protocol, and the scalability challenge hinders its further adoption. Based on this, Dziembowski *et al.* [52] proposed State Channel Network (SCN), which can create and close state channels without blockchain interaction, and allow to sign contracts with any number of organizations. Although different blockchains vary in scalability, the differences between projects are increasing in the process. This trend will bring great progress to solve the scalability problem of cryptocurrency, and gradually form a perfect solution.

IV. BLOCKCHAIN APPLICATION SCENARIO

A. BLOCKCHAIN APPLICATION INDUSTRY

The main advantages of blockchain are no intermediary participation, efficient and transparent process, low cost, and high data security. Based on the above advantages, the application of blockchain is very extensive, as shown in TABLE 3, which can penetrate many industries. At present, many literatures divide the application industry of blockchain into financial industry and non-financial industry. A more detailed classification is discussed in this paper.

1) FINANCIAL FIELD

Digital currency is the most widely used and accepted application of blockchain. The most familiar one is bitcoin, which

TABLE 3. Blockchain Application Scenario.

Blockchain Applications	Financial	Global Payments
		Securities Trading
		Cryptocurrency
		Financial Supervision
	Internet of Things	Distributed Device Management
		IoT Ecommerce
	Supply Chain	Information Sharing
		Product Traceability
	Social Welfare	Charity Transparency
		Charity Authenticity
	Education	Certificate Management
		Credit Record
	Healthcare	Drug anti-counter feiting traceability
		Electronic Medical Record
	Government	Identity Management
		Electronic Voting
Energy	Power Sharing	
	Smart Grid	

used to be synonymous with blockchain. Digital currency is the beginning of the combination of the blockchain and financial field.

At present, there are hundreds of digital currencies in the market. PRCash [53], a blockchain currency that can pay quickly and has a good level of user privacy and regulatory control, providing a new regulatory mechanism for transactions using cryptographic promises, and regulating expenditure limits of zero-knowledge proof. It realizes a more effective security method of blockchain in the financial field. Avgouleas *et al.* [55] built a comprehensive blockchain-based framework that can perfectly express the relevant securities trading logic with codes, realize real-time asset transfer, and accelerate the speed of transaction liquidation. Meanwhile, blockchain technology can optimize the global financial infrastructure, achieve sustainable development, and create more effective systems than now. They also explore the challenges and opportunities of implementing blockchain technology in the banking industry [54]. Therefore, the application of blockchain in the financial field has dramatically improved security and speed.

2) IOT FIELD

In addition to the financial field, the Internet of Things may be the field combines with blockchain to produce the most sparks, as shown in Figure 10.

IoT and blockchain are two different technologies. IoT represents a large number of data collection devices, while blockchain ensures that they do not tamper the data. However, the IoT still lacks effective means in the construction of the network credit system and value system, and there are still many problems in equipment security, identity authentication, data privacy and public, etc. In terms of security and privacy, to provide end-to-end security that meets the

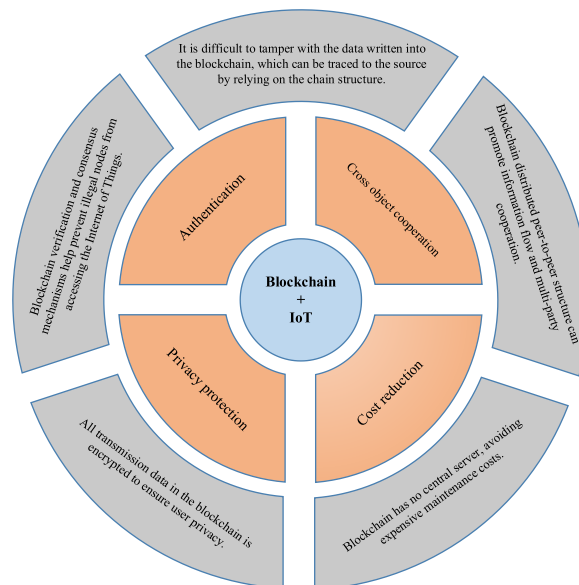


FIGURE 10. The Advantages of “Blockchain + IoT”.

IoT’s needs, a lightweight, scalable blockchain (LSB) is proposed [56], which guarantees the privacy of IoT. In terms of identity authentication, Wazid *et al.* [57] designed the universal authentication key management protocol UAKMP for the IoT security, which protects users’ privacy and identity. In terms of data sharing, the IoT design based on the blockchain can use the blockchain as an auditable storage layer and a distributed access control layer to achieve flexible access control management and secure data sharing [58]. In terms of credibility verification, a framework with layers, intersect, and self-organization Blockchain Structures (BCS) is proposed, helping us build trust, significantly reduce costs, and reduce human errors, to protect data security and privacy better for IoT [59]. Integrating blockchain and IoT will bring many advantages to solving IoT’s shortcomings, which can break the existing multiple information islands, promote the horizontal flow of information, and multi-party collaboration. “Blockchain + IoT” will promote a new round of technology integration and innovation.

3) SUPPLY CHAIN FIELD

It is real that supply chain management systems lack sufficient efficiency and transparency, thus trying to integrate every part in the supply chain is still a difficult problem. Based on blockchain technology characteristics, Li *et al.* [60] proposed a new customs supervision model to solve the problems, the poor customs supervision management, low efficiency and high cost in cross-border import e-commerce retail business. In terms of the supervision system problems from the traditional food industry, such as industrial chain deficiency, data dispersion, and so on, it is a risk and an area of concern for systems where there is a need for a high-reliability solution. The Hierarchical Multi-Domain Block Chain (HMDBC) network structure and the

secondary inspection mechanism proposed by Tao *et al.* [61] is quite appropriate. Moreover, Blockchain technology can solve some of the most pressing issues in the supply chain, as it provides new methods to record, transmit, and share data. It is visible, just like the information on the Internet, for every aspect of the transaction process with blockchain technology used in the supply chain. Blockchain technology can also be combined in the supply chain to throw light on every product [62] for gaining customer confidence from global markets. Schmidt *et al.* [63] used the transaction cost theory to explain how the blockchain affected the supply chain and believed that the effective and transparent nature of the blockchain helped the supply chain reduce transaction costs. Blockchain technology helps the supply chain network establish a shared and secure information flow record and provides a “shared version of events” for supply chain transactions, processes, and partner networks. Therefore, blockchain will combine supply chain with great chemistry.

4) SOCIAL WELFARE FIELD

In recent years, a series of dishonest donations on the Internet has aroused many netizens' attention and enthusiasm. Trust is significant for charity, once people lose trust in others, it is difficult to rebuild. Due to the blockchain advantages of decentralization, transparency, and information traceability, the problems that have been criticized by people in this field will be solved one by one if these advantages are applied to the field of public welfare and charity. According to the above advantages, there is an innovative charity logistics platform [64] based on the Ethereum platform, combined with the unique responsibility system and appraisal report mechanism, for achieving the data consistency of the chain and the real state, as well as the authenticity and transparency of charity logistics data. Once add the data of public welfare projects to the blockchain that the moment user donates to the end, every link in the process will be recorded on the chain in detail and all information process relevant cannot be changed artificially. Sun *et al.* [65] regarded blockchain as an electronic log of transactions and other information in commercial and charitable activities, enabling secure transfers, reducing fraud, retaining tracking evidence, improving transparency, reducing costs, and increasing efficiency. Blockchain-based charitable donations may also be more complicated, donors can design a smart contract to release certain donations in specific conditions [66]. Jain and Simha [67] designed a distributed ledger application and stakeholder incentives, such as accountability, transparency and flexibility, to increase social welfare. For charity, the transparency from blockchain technology can ensure that donors clearly understand and check the flow of their funds. The tamper-resistance ensures that financial information will not be tampered with and anonymity also protects the privacy of donors. Therefore, blockchain technology can be regarded as the best medicine for charity.

5) EDUCATION FIELD

With the general trend in the development and transformation of global education, blockchain technology is expected to play an important role in the construction of the “Internet + education” ecology. An in-depth discussion on the educational application with blockchain technology, and its benefits that blockchain technology can bring to education is conducted by Alammary *et al.* [68]. M. Han *et al.* use blockchain to provide proof of achievements for academic transcripts issued by education providers [69]. There is a global trust education framework [70], based on blockchain to verify the academic certificates and course credits of college students. By means of ensuring the consistency between local education certificates and credits, it can ensure a comprehensive understanding about students' performance. On account of the application of blockchain technology in the education field is still in its infancy, the potential of blockchain in the education field is not consummate yet.

6) HEALTHCARE FIELD

Blockchains can also be applied to many scenarios in healthcare, especially in the data sharing of clinical medicine scenario, which has great potential to overcome the trust problem and technical problems. In the field of “blockchain + healthcare”, the most cases are medical tracing. Chaudhari *et al.* [71] constructed a medical tracking system based on blockchain, which aims to solve the trust problem in the process of data sharing. Xia *et al.* [72] built a medical device traceability system by combining traditional tracking systems with blockchain technology, using alliance chain and smart contract. The blockchain system is able to records the whole process data of drugs, including the product information, logistics data, storage data, sales data, and consumption terminal purchase data. Once the link data is added to the blockchain, it cannot be tampered. Blockchain is mainly used in medical data storage, drug anti-counterfeiting traceability, gene data secure storage, etc. The characteristics of blockchain can help us fully trace the flow of drugs from manufacturers to end-users, and identify the counterfeit drugs [73]. In general scenarios, personal case data is kept by the hospital, while centralized data storage has many advantages, such as high efficiency, easy to operate. However, data stored in this way is highly likely to be lost. Once the data is lost, it will cause very serious consequences. To solve this problem, Rouhani *et al.* [74] proposed a secure distributed medical data asset management system, which can help patients and medical staff effectively exchange medical data while ensuring the security and privacy of private medical data. Abdullah *et al.* [75] introduced a medical data management system based on blockchain technology, which encrypts patients' data to ensure users' privacy. The data stored in a hospital alone is not comprehensive enough. The privacy of medical cases and the anti-counterfeiting of drugs are both crucial links. “Blockchain + healthcare” can gradually solve these problems, expecting to be popularized as soon as possible.

7) GOVERNMENT FIELD

Blockchain can reduce official fraud, improve efficiency, and reduce costs. The ideal state is to achieve a completely paperless digital government and minimize corruption. The use of blockchain in taxation may change how the government collects and disburses funds and improve efficiency [76]. Many countries have adopted blockchain technology to implement the electronic voting system and realize “voter authentication and result saving”. However, the traditional electronic voting system has the risk that the data is not open and transparent enough, and it is easy to be tampered with and forged; the user’s private information is exposed; the voters are unable to verify the voting results [77]. Nadar *et al.* [78] proposed a new method to realize decentralized voting system by using blockchain. Shahzad and Crowcroft [79] proposed a framework to ensure data security by using effective hash technology. The paper introduced the concept of block sealing, which helps make the blockchain more adjustable to meet the security needs of the voting process. In daily life, many scenarios require identity authentication, such as through border customs, airport security, cashing checks or opening bank accounts. The government needs to prove and manage the identity. In many cases, identity is easy to be forged. And blockchain can help to solve the problem of identity authentication. Kuperberg *et al.* [80] conducted a thorough analysis of the opportunities brought by the combination of the latest blockchain technology and the electronic identity document (EID) issued by the government, including the existing implementation and pilot. Odelu [81] proposed a new key management mechanism of blockchain based on user authentication and analyzed the mechanism strictly, which showed that the proposed protocol could resist all kinds of possible attacks. The combination of blockchain and government services can maximize the efficiency of work. Utilizing technical means can increase the people’s trust and build a safer society.

8) ENERGY FIELD

Blockchain technology, as a new database technology, can increase the mutual trust of multi-stakeholders in the energy network. Its decentralization, openness, and transparency are in line with the concept of the energy network and have attracted more and more attention in energy field. At present, the application of blockchain in energy field mainly focuses on distributed intelligent energy systems and energy sharing. Mengelkamp *et al.* [82] provides a distributed market platform for energy producers and consumers to trade energy without centralized institutions. Gao *et al.* [83] combined smart grid with blockchain technology, and use smart contract to establish trading procedures to provide trust between participants on the network. The system is proved to be very effective since users can monitor how to use electricity. When the energy meets the blockchain, the collision and blending of the two are related to the long-term and overall situation, which will have a significant impact on the production and

lifestyle of the whole society and may set off a new energy revolution.

B. BLOCKCHAIN PROJECT

Blockchain technology can help organizations and institutions build trust among, while reducing the cost of trust. In the blockchain boom, technology giants, venture companies, and academic institutions have joined in and launched one project after another. According to the classification of blockchain application industry in the previous section, we sort out the projects of corresponding industries, as shown in Figure 11.

1) FINANCIAL FIELD PROJECTS

- **Digital currency projects:** Digital currency is the project that has the most public contact among blockchain projects, and is mainly used for transactions such as ordinary currency. At present, there are more than one thousand kinds of digital currency in the world. Among them, the more successful projects are bitcoin, ETH, Litecoin, Monero, EOS, Ripple.
- **Global payment projects:** With the continuous development of credit card payments and mobile payments in recent years, the traditional cash payments in reality have been gradually away from people’s lives. Compared with the traditional global payment mentioned above, the global payment system and settlement function of the blockchain is unique and epoch-making. The following is a list of some blockchain global payment projects.

a: InterLedger PROJECT OF RIPPLE

Ripple, American finance and technology company, has launched the InterLedger project. This project is a practitioner of global cross-border payment based on blockchain. The purpose is to create a unified global unified payment standard and a unified network financial communication protocol. At present, banks in more than ten countries have joined the project to cooperate, and in addition, they have received support from companies such as Apple and Microsoft.

b: STELLAR PROJECT OF IBM

IBM launched the blockchain global payment system World Wire, in which Stellar protocol constitutes a key part of the technical framework for real-time cross-border payment. Stellar’s new platform enables real-time clearing and settlement of cross-border transactions. IBM believes that World Wire can integrate with any existing payment system at any time and support payment at any scale, any destination and any asset type in a high security environment.

c: LIBRA PROJECT OF FACEBOOK

Libra’s mission is to build a simple, borderless currency and global payment system for billions of people. Libra is composed of three parts, which will work together to create a more inclusive financial system: a) It is based on a secure, scalable, and reliable blockchain. b) It is backed by asset reserves that give it intrinsic value. c) It is governed by an

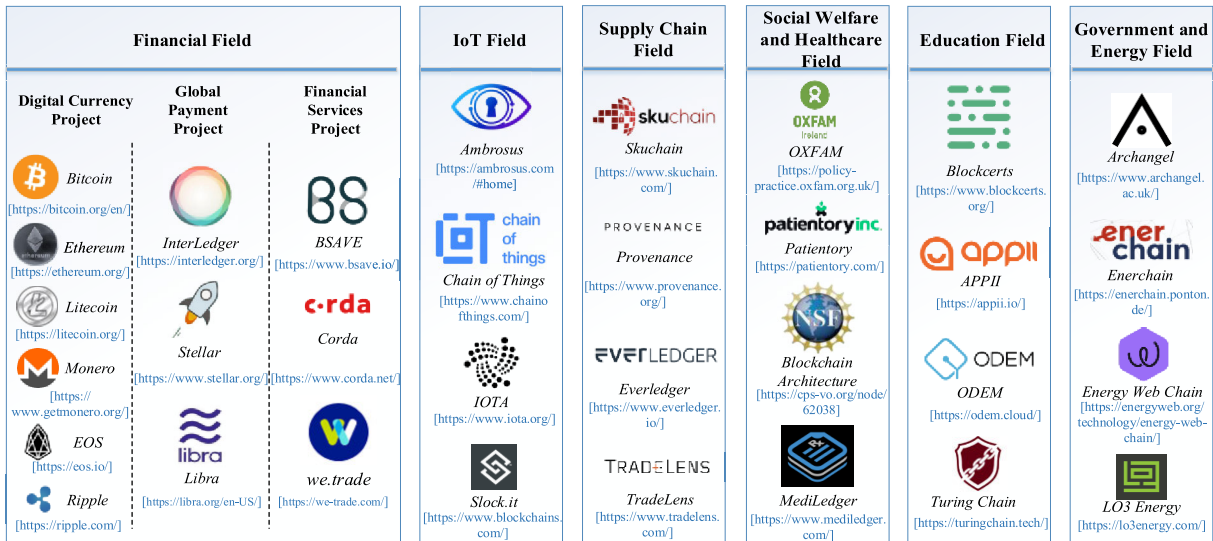


FIGURE 11. Blockchain Project Classification.

independent Libra association whose mission is to promote the development of this financial ecosystem.

- **Financial services project:** Scenarioization of financial services is a trend, and blockchain will make many changes to traditional financial models and business processes. Blockchain reconstructs the financial services scene, connects the bank's financial system and services to the scene, and makes the information more symmetrical and transparent.

d: BSAVE PROJECT

In March 2019, British Basve company launched research on a platform providing users with online storage bitcoin asset, so that users can directly obtain income from their bitcoin assets. The company's goal is to fundamentally simplify the process of online savings and investment, fully exploit the financial service potential of digital currency, and provide convenience for people all over the world.

e: CORDA PROJECT

R3, a global blockchain alliance organization, has been committed to developing a third-party financial transaction platform with the help of blockchain technology. Corda project is a distributed ledger launched by R3 which uses blockchain technology to record and manage financial contracts. Corda is used to recording, manage, and synchronize financial contracts between traditional financial institutions, which is largely inspired by the blockchain system, excluding some designs that are not suitable for banking application scenarios.

f: WE.TRADE PROJECT

We.trade a financial trading blockchain platform jointly developed by nine well-known banks, which aims to provide enterprises with the tracking of fund flow and transaction management, and improve the efficiency of cross-border financial transactions. The We.trade blockchain

platform has completed the first real-time cross-border financial transaction.

2) IOT FIELD PROJECTS

a: AMBROSUS

Ambrosus is a blockchain-powered IoT network for food and pharmaceutical enterprises, enabling secure and frictionless dialogue. The core technology is a decentralized protocol by combining various sensors, smart contracts on AMB-NET, secure storage and robust developer tools components for tracking, storing and transmitting, thus it can be used in supply chain, IoT and health-care application scenarios.

b: CHAIN OF THING (CoT)

Chain of Things (CoT) plays an important role of bitcoin and blockchain technology in providing a better foundation for securing IoT and securing data from IoT devices. Dubbed the 4th industrial revolution, the 'Internet of Things' will consist of a vast network of sensor nodes that will generate an unprecedented flow of global data. These devices will quietly execute smart contracts with physical actuators that will manage many aspects of our future lives.

c: IOTA

It is not only a blockchain but also a feeless and open secure trust layer, protocol for IoT and scalable distributed ledger. The tangle, characteristic of its network, immutably records the exchange of data and value for ensuring the trustworthy and tamper-resistance of information. It enables new possibilities in many fields and will continue to enrich technological maturity and others.

d: SLOCK.IT

Based on the Ethereum network, Slock.it with the name of a Universal Sharing Network (USN) is an open marketplace for real and virtual products renting, sharing or selling. It enables humans and machines to securely participate in the evolving

economy of things. Slock.it brings a better transaction environment, and benefits IoT and financial industry.

3) SUPPLY CHAIN FIELD PROJECTS

a: SKUCHAIN

It is a pioneer of empowering enterprises using blockchain to strengthen collaboration across supply chains. By using Popcodes traceability, brackets smart contracts and ZK-collaboration technologies, it helps customers solve transparent problems of products with their various infrastructure developed tools. There is no doubt that Skuchain is an outstanding achiever with its products and a vigorous assistor for empowering in supply chain scenario.

b: PROVENANCE

It is a platform brings the supply chain to the shopper with the concentration on products' story. Using digital passport for product traceable and the blockchain based platform for transparency, it unites of citizens and businesses in a system to build trust and meaningful relationships with customers in supply chain scenario.

c: EVERLEDGER

It is a digital platform based on blockchain secure technologies, the aim is to contribute greater clarity and confidence in transparent marketplaces with the help business surface and converge information. Based on blockchain, combined AI, Intelligent labelling and nanotech together, it attaches transparency and temper-resistance to IoT and supply chain among produce and transmit process.

d: TradeLens

It is one of interconnected ecosystem of supply chain, absorbed in freeing people from legacy data systems and making trade easy. Using IBM Blockchain Platform which is based on Hyperledger Fabric is to let goods accessible and traceable by every part the goods relevant. It benefits many industries including ports, ocean carriers, shippers, etc., and brings vitality to supply chain.

4) SOCIAL WAELFARE AND HEALTHCARE FIELD PROJECTS

a: OXFAM

It is a charity dedicating to help people beat poverty. It is partnered to carry out a blockchain program that permitted blockchain-backed vouchers to deliver credit and introduces blockchain into rice which known as BlocRice program. It is delighted to know that social welfare can make use of blockchain technology for effective and credible assistance.

b: PATIENTORY

Founded for making a difference in healthcare improvement, it combines people who could be doctors, patients, caregivers etc. together for better treatment. Applied in healthcare scenario, it will gain more new form of relevant technology that could be regarded as healthcare future tense.

c: BLOCKCHAIN ARCHITECTURE

In October 2019, National Science Foundation (NSF) funded the University of California, Berkeley to research blockchain architecture for resource-constrained devices. The goal of this project is to develop a new framework and protocol toolkit so that resource-constrained computers can play an important role in ensuring the security of distributed systems. This resource constrained blockchain architecture will enable innovation and development in the IoT, healthcare, supply chain and other fields.

d: MEDILEDGER

The MediLedger Project was launched in 2017 and it became a fully decentralized peer-to-peer and blockchain network. MediLedger meets the emerging needs of the prescription medicine supply chain through redefining the potential of blockchain for the pharmaceutical sector, it plays an important role in healthcare field.

5) EDUCATION FIELD PROJECTS

a: BLOCKCERTS

Blockcerts Project set up an open standard for creating, issuing, viewing, and verifying blockchain-based certificates. This project aims at helping individuals to process and share their own official records like academic credentials professional licenses, workforce development and more.

b: APPII

APPII is a subproject of Applied Blockchain, which designed a platform underpinned by blockchain and digital signatures as a way to create a single immutable record of an individual's experience. APPII develop a smart contract data store for each user with controls over third party access to that data. APPII is a meaningful practice of combining blockchain with the education industry.

c: ODEM

It is an on-demand education market built on the Ethereum blockchain. The platform brings together students, educators, and service providers who develop and participate in education programs. Once students and educators begin their education programs ODEM smart contract can seamlessly manage payments from the beginning to the end of a long-term contract. ODEM is revolutionizing the way educators and students plan, connect, and book educational programs.

d: TURING CHAIN

Turing Chain Project aim to use AI and blockchain technology to construct a public chain of natural language communication to realize Turing test. Turing Chain is capable of redefining traditional educational certificates and eventually enabling unified and sustainable records tracking for educational industry.

6) GOVERNMENT AND ENERGY FIELD PROJECTS

a: ARCHANGEL

Archangel Project can deliver long-term sustainability of digital archives through new transformational blockchain

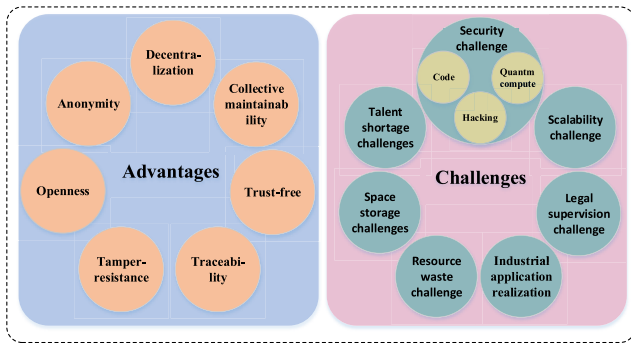


FIGURE 12. Advantages and Challenges of Blockchain Technology.

technology solutions that will ensure both accessibility and integrity of digital archives. By deploying Archangel, the credibility of archives was improved, which not just for study reference, but for matters as serious as legal cases, official investigations.

b: ENERCHAIN

Enerchain is a blockchain based application developed by POTON company. The Enerchain Project has shown that applying blockchain technology in energy markets promises more efficient operational processes and less transaction cost.

c: ENERGY WEB CHAIN

The Energy Web Chain is a public blockchain platform designed for the energy industry, launched in 2019. It implements a virtual machine like public Ethereum, which allow developers to write smart contracts and decentralized application on the platform. The Energy Web Chain provides the foundational digital infrastructure for the energy industry with the advantages of blockchain.

d: LO3 ENERGY

It builds a blockchain based platform named Exergy, to record and process grid edge data. They combine industry expertise with advancements in blockchain technology to deliver a new frontier in energy.

V. BLOCKCHAIN ADVANTAGES AND CHALLENGES

With the continuous development of blockchain applications, blockchain technology becomes more and more popular. This strong development power from the requirements of various industries makes the blockchain technology progress with each passing day, and the achievements of various industries more attractive. However, there are advantages and disadvantages, we summarize the advantages and challenges faced by the blockchain shown in Figure 12 and describe them in detail below.

A. BLOCKCHAIN ADVANTAGES

Blockchain is equipped with decentralization, collective maintainability, trustless, traceability, tamper-resistance, openness, and anonymity etc. advantages.

- **Decentralization:** decentralization is a decentralized distributed structure. The whole network has no central hardware or mechanism, which is the core advantage of blockchain. Decentralization is a key selling point of most public blockchain platforms [84]. Decentralization removes the existence of intermediaries and reduces the cost of intermediaries, which makes blockchain widely used.
- **Collective maintainability:** collective maintainability is built on the basis of decentralization. Without the participation of the third party, all nodes need to be united, and all parties have clear rights and responsibilities to maintain the normal operation of the blockchain. It can better maintain the stability and security of the entire blockchain system [85].
- **Trust-free:** Trust-free is to remove the third-party trust [84], which is manifested in two aspects: one is to trust the authenticity of the historical behavior of the data on the chain; the other is to trust the future behavior constrained by rules and mechanisms.
- **Traceability:** traceability means that the data on the chain can be found. Currently, many studies take advantage of the traceability of blockchain [87-88]. We can track the data in the blockchain, which is convenient for supervision and tracking.
- **Tamper-resistance:** Blocks are linked by hash values, and the ledger is stored on multiple nodes, making the tamper-resistance advantage possible [89]. Tamper-resistance can ensure that we have enough trust in the blockchain data. We do not need to spend time and energy to verify the authenticity of the data, but unconditionally trust the authenticity of the data, which is determined by the tamper-resistance of the blockchain.
- **Openness:** openness ensures the openness of the system. Apart from the fact that the private information of all parties to the transaction is encrypted, the blockchain data is open to everyone. Anyone can query the blockchain data and develop relevant applications through an open interface, so the information of the whole system is highly transparent [90].
- **Anonymity:** the nature of anonymity in blockchain is different from our traditional understanding. More accurately, blockchain has pseudonyms, not real names. Everyone has a virtual identity independent of the real identity on the blockchain. The decentralized model determines the transparency of data disclosure, but all the things the virtual identity does are transparent, and transparency directly leads to privacy problems. The form of anonymity ensures our privacy to a certain extent [91].

B. BLOCKCHAIN CHALLENGES

1) SECURITY-RELATED CHALLENGE

a: BLOCKCHAIN UNDERLYING CODE

There are several specific security holes in the architecture and implementation of blockchain technology. Blockchain

security vulnerabilities are usually related to the consensus mechanism used to confirm and validate transactions. These security vulnerabilities include DDoS, block discarding, eclipse attack [92], selfish mining, Sybil attack [93], 51% attack, double spend attack [94]. Blockchain projects are open-source. The characteristics of open source are conducive to the development and promotion of blockchain, but also provide opportunities for attackers. The lack of code evaluation in blockchain leads to frequent security events, which limits the development of blockchain.

b: POTENTIAL HACKING

Blockchain design limits the attack of some hackers. For example, if a hacker wants to tamper with the blockchain's data, he needs to have 51% computing power. But the benefits of using 51% computing power to attack the whole system are not as much as the benefits of using 51% computing power to mine normally, so, hackers will not choose to attack blockchain in an ideal state. Due to the immense attacking cost to perform the 51% attack, it was considered very unlikely for a long period [95]. However, we just have to consider such a situation. Hackers are not only trying to obtain benefits, but only want to destroy or show their own technical advantages. Under strict planning and organization, the possibility of blockchain system being broken is also theoretically there.

c: THREATS FROM QUANTUM COMPUTERS

In data storage, blockchain uses public-key encryption, digital signature, hash function and other cryptographic components. To meet the needs of higher privacy protection, some blockchain schemes also need ring signature, zero knowledge proof and other privacy protection technologies. The security of these cryptographic components directly affects the security of blockchain data. In the short term, these cryptography technologies will not be threatened, but with the rise of quantum computing, the existing cryptography algorithms may face a devastating blow.

2) SCALABILITY-RELATED CHALLENGE

Due to the increase in the number of participants in the blockchain system, there is another challenge in the scalability and computing resources of the system. Scalability is still a key barrier when the blockchain technology is widely used in real business environments [96]. With the increasing scale of nodes in the blockchain system, the broadcast mode adopted by blockchain technology may lead to data delay and network performance degradation, or even paralysis. In addition, with the increase in data volume, the efficiency of query and data mining has been difficult to meet people's needs.

3) LEGAL SUPERVISION CHALLENGE

As blockchain technology has been widely concerned in recent years, the corresponding legal provisions are not perfect. Many countries and regions have different attitudes towards blockchain, lacking a unified regulatory standard.

At the same time, due to the anonymity of the blockchain digital currency, bitcoin often appears in the dark network transactions, money laundering crimes and virus blackmail programs. Laws and regulations could impact how far and how fast the technology could develop [97]. The events indicate that our blockchain related regulatory system and means are not advanced enough, which provides an opportunity for crime.

4) INDUSTRIAL APPLICATION CHALLENGE

The slow promotion of standardization and the lack of innovation in business models are the biggest obstacles to implementing blockchain technology in the industry. Currently, the blockchain implementation still lacks industry best practices and standards for reference. At the same time, the application of blockchain faces policy risks. By summarizing the existing implementation difficulties, it is hoped that it will help the implementation and landing of subsequent blockchain solutions.

5) RESOURCE WASTE CHALLENGE

Blockchain is a large ledger of distributed storage, each node keeps a ledger, but repeated data storage will cause serious waste of storage resources. Taking bitcoin as an example, the mining process will produce high power consumption. Cambridge University uses the Cambridge bitcoin electricity consumption index (CBECI) to track the use of bitcoin power, which shows that the electricity consumption of bitcoin accounts for 0.20% of the total electricity consumption of the world every year, 0.17% of the total electricity production of the world every year, which exceeds the total electricity consumption of Austria or Colombia and other countries electricity.

6) SPACE STORAGE CHALLENGE

Each node in the blockchain must save complete backup data. As the amount of transaction data increase, the storage space it takes up is also increasing. Taking bitcoin as an example, there are more than 600000 blocks on the main chain at present, and the synchronous and complete block data needs more than 200G of space, which has a very high demand for storage space resources. It is a crucial problem restricting the development of the blockchain.

7) TALENT SHORTAGE CHALLENGE

The whole blockchain industry is still in the early stage of development, similar to the Internet industry in the 1990s or the early 21st century, few people really understand blockchain. Moreover, blockchain is the integration of various technologies, including cryptography, economics, and computer science, which is more complicated than the Internet and has a higher threshold for in-depth research. Therefore, blockchain related technical talents have been very scarce, which is the pain point restricting the development of the whole industry.

VI. BLOCKCHAIN DEVELOPMENT TREND

A. BLOCKCHAIN TECHNOLOGY DEVELOPMENT TREND

Blockchain itself is a comprehensive technology, and it hasn't been around for a long time, so there is still a long way to go. From a technical perspective, the future development trend of the blockchain is roughly as follows.

1) UNSTRUCTURED CHAIN STORAGE

Structured block data in blockchain storage has certain advantages. But like today's big data technology, it uses unstructured data processing technology. Therefore, once the blockchain can efficiently accept and process unstructured data, a blockchain technology belonging to the future Internet will come. However, improving the chain structure is a very high technical threshold, and it is also a significant challenge to the technical level of the research and development team.

2) CONSENSUS ALGORITHM

Consensus algorithm is the key part to the development of blockchain technology, is the foundation of the whole blockchain trust, and affects the transaction processing ability, security and scalability of blockchain. The PoW consensus algorithm used by Bitcoin has strong anti-attack ability, and good performance in solving data consistency, but consuming too much energy is the disadvantage. Some consensus algorithms proposed in the later stage can solve the problem of energy consumption to a certain extent, but they still have significant limitations and functional degradation. Consensus algorithm plays an important role in the whole blockchain, and any progress of consensus algorithm could dramatically change the development process of blockchain in the future. The future consensus algorithm will develop to superior performance, high adaptability and scalability [98].

3) CROSS-CHAIN TECHNOLOGY

A single blockchain is an information island, and there are two completely closed worlds between one chain to another. To realize the mutual communication of blockchain, cross-chain technology emerged. However, the existing blockchain technology is not mature, it is impossible to expand in the infrastructure. At present, there are many researches on cross-chain technology [99-100], but most of them are studying cross chain exchange between digital currencies, which is not revolutionary. The actual cross-chain technology is far from what we expected. Perhaps, when we break through the fixed block structure, cross-chain technology will have a qualitative leap. Therefore, cross-chain technology is the direction we should strive to study in the future.

B. BLOCKCHAIN INDUSTRY DEVELOPMENT TREND

1) BLOCK DATA APPLICATION DEVELOPMENT

Block data can be used not only as data records, but also as input of programs to help other applications, such as

social tools, games, trading platforms, etc. We can develop DApp directly on the basis of the valuable resource of data.

2) FROM DIGITAL CURRENCY TO NON-FINANCIAL FIELD

In the future, blockchain can be used as a general-purpose technology to accelerate the penetration of digital currency into other fields and carry out innovative integration with various industries. The development of blockchain mainly will be involved by two camps. The first camp is cryptocurrency. Starting from currency, it will gradually advance to the field of asset management, deposit and certificate, and penetrate the field of credit investigation. The second is the IT camp, starting from information sharing, to build the credit core at low cost, and gradually cover all fields.

3) IOT AND BLOCKCHAIN

Blockchain provides a secure and scalable framework for communication between IoT facilities, and therefore brings many advantages [101]–[103]. Undoubtedly, blockchain and the IoT are one of the best combinations in this era. We believe that, in the future, the contribution of the two technologies to human beings and the whole society will be endless and hard to inestimable.

4) BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

The cooperation between AI and blockchain can make a difference in privacy protection, energy consumption, scalability, efficiency and security [104]. Artificial intelligence is to cultivate the centralized intelligence on the closed data platform, while blockchain is to promote the centralized application in the open data environment. If we can find the right way to make two technologies work together, a little collision can produce a huge spark in an instant.

5) BLOCKCHAIN DATA ANALYSIS

Since blockchain technology has been widely concerned, accumulated a large amount of user transaction data. In this age when data represent value, all data are our wealth. The data of blockchain has the characteristics of openness, which provides unprecedented opportunities for researchers to analyze blockchain data and solve related problems [105-107]. Nowadays, there are some worrying problems in blockchain, such as private information disclosure, illegal financial activities, and so on. On the basis of blockchain value mining, analyzing the privacy of blockchain and discovering the characteristics of illegal behavior can help us build a safe and legal blockchain environment.

VII. CONCLUSION

Blockchain technology, with its characteristics of anonymity, decentralization, traceability and non-tampering, has set off a wave of research in academic and social applications. This paper introduces the development background and basic concepts of blockchain, analyzes and summarizes the eight application scenarios of blockchain by investigating the blockchain related researches of many universities and research institutions, and then investigates the physical imple-

mentation projects of blockchain in various fields. Finally, we summarize the advantages and challenges of blockchain technology and put forward the future development trend of blockchain technology. Through the above analysis, we draw the following conclusions. In recent years, the research on blockchain technology has been widely carried out in various universities, and the quantity and quality of published papers have been further improved. As a result, a variety of blockchain projects have been generated in different fields, with a wide range of application scenarios, which can be combined with the Internet of Things, supply chain, medical and other fields. But the technology still faces challenges such as security, scalability, and waste of resources. We, therefore, proposed the future blockchain development trend. In terms of technology, it will develop towards unstructured chain storage and cross chain technology. While in industry, it will develop in the direction of “blockchain +” and integrate more closely with different fields. The development of blockchain relies on the close connection between academia and industry and focuses on the combination of industry and research, to make it better and faster for the benefit of mankind.

REFERENCES

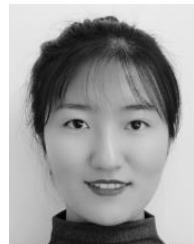
- [1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” *Appl. Innov.*, vol. 2, pp. 6–10, Jun. 2016.
- [3] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of activity: Extending bitcoin’s proof of work via proof of stake,” *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.
- [4] D. Larimer, “Delegated proof-of-stake (DPoS),” EOS, Bitshare White Paper 1.0, 2014.
- [5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2016, pp. 839–858.
- [6] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [7] J. Yli-Huomo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where is current research on blockchain technology?—A systematic review,” *PLoS ONE*, vol. 11, no. 10, Oct. 2016, Art. no. e0163477.
- [8] M. Belotti, N. Bozic, G. Pujolle, and S. Secci, “A vademecum on blockchain technologies: When, which, and how,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3796–3838, 4th Quart., 2019, doi: [10.1109/COMST.2019.2928178](https://doi.org/10.1109/COMST.2019.2928178).
- [9] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, “Security services using blockchains: A state of the art survey,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019, doi: [10.1109/COMST.2018.2863956](https://doi.org/10.1109/COMST.2018.2863956).
- [10] R. Zhang, R. Xue, and L. Liu, “Security and privacy on blockchain,” *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, 2019.
- [11] E. Zaghoul, T. Li, M. W. Mutka, and J. Ren, “Bitcoin and blockchain: Security and privacy,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 1028–10313, Oct. 2020, doi: [10.1109/IJOT.2020.3004273](https://doi.org/10.1109/IJOT.2020.3004273).
- [12] P. J. Taylor, T. Dargahi, A. Dehghantaha, R. M. Parizi, and K.-K.-R. Choo, “A systematic literature review of blockchain cyber security,” *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020.
- [13] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, “Survey on blockchain for Internet of Things,” *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.
- [14] A. Ahl, M. Yarime, K. Tanaka, and D. Sagawa, “Review of blockchain-based distributed energy: Implications for institutional development,” *Renew. Sustain. Energy Rev.*, vol. 107, pp. 200–211, Jun. 2019.
- [15] N. O. Nawari and S. Ravindran, “Blockchain and the built environment: Potentials and limitations,” *J. Building Eng.*, vol. 25, Sep. 2019, Art. no. 100832.
- [16] W. Gao, W. G. Hatcher, and W. Yu, “A survey of blockchain: Techniques, applications, and challenges,” in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Hangzhou, China, Jul. 2018, pp. 1–11, doi: [10.1109/ICCCN.2018.8487348](https://doi.org/10.1109/ICCCN.2018.8487348).
- [17] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain technology overview,” NIST, Gaithersburg, MD, USA, Tech. Rep. 8202, 2018.
- [18] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
- [19] C. Decker and R. Wattenhofer, “Information propagation in the bitcoin network,” in *Proc. IEEE P2P*, Trento, Italy, Sep. 2013, pp. 1–10.
- [20] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
- [21] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
- [22] R. C. Merkle, “Protocols for public key cryptosystems,” in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, Apr. 1980, pp. 122–133.
- [23] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.
- [24] N. Koblitz, “Elliptic curve cryptosystems,” *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
- [25] L. Lamport, “The part-time parliament,” *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, May 1998.
- [26] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, “A blockchain privacy protection scheme based on ring signature,” *IEEE Access*, vol. 8, pp. 76765–76772, 2020.
- [27] L. Xiao, W. Huang, Y. Xie, W. Xiao, and K.-C. Li, “A blockchain-based traceable IP copyright protection algorithm,” *IEEE Access*, vol. 8, pp. 49532–49542, 2020.
- [28] X. Li, F. Lv, F. Xiang, Z. Sun, and Z. Sun, “Research on key technologies of logistics information traceability model based on consortium chain,” *IEEE Access*, vol. 8, pp. 69754–69762, 2020.
- [29] M. Milutinovic, W. He, H. Wu, and M. Kanwal, “Proof of luck: An efficient blockchain consensus protocol,” in *Proc. 1st Workshop Syst. Softw. Trusted Execution (SysTEX)*, Trento, Italy, 2016, pp. 1–6.
- [30] M. C. Kus Khalilov and A. Levi, “A survey on anonymity and privacy in bitcoin-like digital cash systems,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2543–2585, 3rd Quart., 2018.
- [31] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, “Consortium blockchain-based malware detection in mobile devices,” *IEEE Access*, vol. 6, pp. 12118–12128, 2018.
- [32] P. Daian, I. Eyal, A. Juels, and E. G. Sirer, “(Short Paper) piecework: Generalized outsourcing control for proofs of work,” in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Sliema, Malta, 2017, pp. 182–190.
- [33] A. Miller, A. Kosba, J. Katz, and E. Shi, “Nonoutsourcable scratch-off puzzles to discourage bitcoin mining coalitions,” in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Denver, CO, USA, 2015, pp. 680–691.
- [34] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoin-NG: A scalable blockchain protocol,” in *Proc. USENIX Conf. Netw. Syst. Design Implement. (NSDI)*, Santa Clara, CA, USA, 2016, pp. 45–59.
- [35] Y. Sompolinsky and A. Zohar, “Secure high-rate transaction processing in bitcoin,” in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, San Juan, Puerto Rico, 2015, pp. 507–527.
- [36] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, “Prism: Deconstructing the blockchain to approach physical limits,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, Nov. 2019, pp. 585–602.
- [37] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, 2017, pp. 357–388.
- [38] D. R. Lee, Y. Jang, and H. Kim, “Poster: A proof-of-stake (PoS) blockchain protocol using fair and dynamic sharding management,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, Nov. 2019, pp. 2553–2555.
- [39] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of activity: Extending Bitcoin’s proof of work via proof of stake,” *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.

- [40] J. Blocki and H. S. Zhou, "Designing proof of human-work puzzles for cryptocurrency and beyond," in *Proc. Theory Cryptogr. Conf.*, Berlin, Germany, 2016, pp. 517–546.
- [41] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. Annu. Cryptol. Conf.*, Santa Barbara, CA, USA, 2015, pp. 585–605.
- [42] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Trust-com/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 57–64.
- [43] P. Das, L. Eckey, T. Frassetto, D. Gens, K. Hostáková, P. Jauernig, S. Faust, and A.-R. Sadeghi, "FastKitten: Practical smart contracts on bitcoin," in *Proc. USENIX Secur. Symp.*, Berkeley, CA, USA, 2019, pp. 801–818.
- [44] S. Steffen, B. Bichsel, M. Gersbach, N. Melchior, P. Tsankov, and M. Vechev, "Zkay: Specifying and enforcing data privacy in smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, Nov. 2019, pp. 1759–1776.
- [45] C. Ganesh, C. Orlandi, and D. Tschudi, "Proof-of-stake protocols for privacy-aware blockchains," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Darmstadt, Germany, 2019, pp. 690–719.
- [46] R. Zhang and B. Preneel, "Lay down the common metrics: Evaluating proof-of-work consensus protocols' security," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2019, pp. 175–192.
- [47] M. Rodler, W. Li, G. O. Karame, and L. Davi, "Sereum: Protecting existing smart contracts against re-entrancy attacks," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2019, pp. 1–15.
- [48] S. Matetic, K. Wüst, M. Schneider, K. Kostianinen, G. Karame, and S. Capkun, "BITE: Bitcoin lightweight client privacy using trusted execution," in *Proc. USENIX Secur. Symp.*, Berkeley, CA, USA, 2019, pp. 783–900.
- [49] T. Cai, Z. Yang, W. Chen, Z. Zheng, and Y. Yu, "A blockchain-assisted trust access authentication system for solid," *IEEE Access*, vol. 8, pp. 71605–71616, 2020.
- [50] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. Bitcoin cash: Coexistence or downfall of bitcoin cash?" in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2019, pp. 935–951.
- [51] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, "Anonymous multi-hop locks for blockchain scalability and interoperability," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2019, pp. 1–30.
- [52] S. Dziembowski, L. Eckey, S. Faust, J. Hesse, and K. Hostáková, "Multi-party virtual state channels," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Darmstadt, Germany, 2019, pp. 625–656.
- [53] K. Wüst, K. Kostianinen, V. Čapkun, and S. Čapkun, "PRCash: Fast, private and regulated transactions for digital currencies," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Saint Kitts, Nevis, vol. 11598, 2019, pp. 158–178.
- [54] L. Cocco, A. Pinna, and M. Marchesi, "Banking on blockchain: Costs savings thanks to the blockchain technology," *Future Internet*, vol. 9, no. 3, p. 25, Jun. 2017.
- [55] E. Avgouleas and A. Kiayias, "The promise of blockchain technology for global securities and derivatives markets: The new financial ecosystem and the 'holy grail' of systemic risk containment," *Eur. Bus. Org. Law Rev.*, vol. 20, no. 1, pp. 81–110, 2019.
- [56] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.
- [57] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.
- [58] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proc. Cloud Comput. Secur. Workshop (CCSW)*, New York, NY, USA, 2017, pp. 45–50.
- [59] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, Jun. 2018.
- [60] M. Li, S. P. Guan, and R. R. Du, "Research on the application of customs supervision on cross-border import e-commerce retail business from the perspective of blockchain," in *Proc. 6th Int. Conf. Manage. Sci. Manage. Innov. (MSMI)*, 2019, pp. 1–5.
- [61] Q. Tao, X. Cui, X. Huang, A. M. Leigh, and H. Gu, "Food safety supervision system based on hierarchical multi-domain blockchain network," *IEEE Access*, vol. 7, pp. 51817–51826, 2019.
- [62] M. Montecchi, K. Plangger, and M. Etter, "It's real, trust me! Establishing supply chain provenance using blockchain," *Bus. Horizons*, vol. 62, no. 3, pp. 283–293, May 2019.
- [63] C. G. Schmidt and S. M. Wagner, "Blockchain and supply chain relations: A transaction cost theory perspective," *J. Purchasing Supply Manage.*, vol. 25, no. 4, Oct. 2019, Art. no. 100552.
- [64] J. Li, F. Qu, X. Tu, T. Fu, J. Guo, and J. Zhu, "Public philanthropy logistics platform based on blockchain technology for social welfare maximization," in *Proc. 8th Int. Conf. Logistics, Informat. Service Sci. (LISS)*, Aug. 2018, pp. 1–9.
- [65] D. Sun, W. Ying, X. Zhang, and L. Feng, "Developing a blockchain-based loyalty programs system to hybridize business and charity: An action design research," in *Proc. 40th Int. Conf. Inf. Syst. (ICIS)*, Munich, Germany, 2019.
- [66] B. Reinsberg, "Blockchain technology and the governance of foreign aid," *J. Institutional Econ.*, vol. 15, no. 3, pp. 413–429, Jun. 2019.
- [67] S. Jain and R. Simha, "Blockchain for the common good: A digital currency for citizen philanthropy and social entrepreneurship," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1387–1394.
- [68] A. Alammery, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic review," *Appl. Sci.*, vol. 9, no. 12, p. 2400, Jun. 2019.
- [69] M. Han, Z. Li, J. He, D. Wu, Y. Xie, and A. Baba, "A novel blockchain-based education records verification solution," in *Proc. 19th Annu. SIG Conf. Inf. Technol. Edu.*, New York, NY, USA, Sep. 2018, pp. 178–183.
- [70] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash, and R. Pradhan, "A distributed credit transfer educational framework based on blockchain," in *Proc. 2nd Int. Conf. Adv. Comput., Control Commun. Technol. (IAC3T)*, Allahabad, India, Sep. 2018, pp. 54–59.
- [71] R. Chaudhari, R. Deshmukh, V. Bari, S. Rajput, and K. Rode, "Medicine traceability system using blockchain," *Int. J. Trend Sci. Res. Develop.*, vol. 3, no. 4, pp. 346–349, 2019.
- [72] X. Xia, X. Lin, W. Dong, and Z. He, "Design of traceability system for medical devices based on blockchain," *J. Phys., Conf. Ser.*, vol. 1314, Oct. 2019, Art. no. 012067.
- [73] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in *Proc. 11th Int. Conf. Commun. Syst. Netw.*, Jan. 2019, pp. 568–570.
- [74] S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery, and R. Deters, "MediChainTM: A secure decentralized medical data asset management system," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul. 2018, pp. 1533–1538.
- [75] A. A. Alomar, M. Z. A. Bhuiyan, and A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.
- [76] A. E. Nemade, S. S. Kadam, R. N. Choudhary, S. S. Fegade, and K. Agarwal, "Blockchain technology used in taxation," in *Proc. Int. Conf. Vis. Towards Emerg. Trends Commun. Netw. (ViTECoN)*, Vellore, India, Mar. 2019, pp. 1–4.
- [77] S. Xiao, X. A. Wang, W. Wang, and H. Wang, "Survey on blockchain-based electronic voting," in *Proc. Int. Conf. Intell. Netw. Collaborative Syst.*, Oita, Japan, vol. 1035, 2019, pp. 559–567.
- [78] T. Nadar, M. Rawal, J. Patel, A. Shah, and A. S. Revathi, "A novel approach to implement decentralized voting system using blockchain," in *Proc. Int. Conf. Wireless Commun.*, vol. 36, 2020, pp. 471–479.
- [79] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019.
- [80] M. Kuperberg, S. Kemper, and C. Durak, "Blockchain usage for government-issued electronic IDs: A survey," in *Proc. Int. Conf. Adv. Inf. Syst. Eng.*, Rome, Italy, vol. 349, 2019, pp. 155–167.
- [81] V. Odelu, "IMBUA: Identity management on blockchain for biometrics-based user authentication," in *Proc. Int. Congr. Blockchain Appl.*, Ávila, Spain, vol. 1010, 2019, pp. 1–10.
- [82] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, Feb. 2018.

- [83] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.
- [84] K. Wu, B. Peng, H. Xie, and Z. Huang, "An information entropy method to quantify the degrees of decentralization for blockchain systems," in *Proc. IEEE 9th Int. Conf. Electron. Inf. Emergency Commun. (ICEIEC)*, Beijing, China, Jul. 2019, pp. 1–6.
- [85] F. Wessling, C. Ehmke, O. Meyer, and V. Gruhn, "Towards blockchain tactics: Building hybrid decentralized software architectures," in *Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C)*, Hamburg, Germany, Mar. 2019, pp. 234–237.
- [86] F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," *Electron. Commerce Res. Appl.*, vol. 29, pp. 50–63, May 2018.
- [87] W. Hong, Y. Cai, Z. Yu, and X. Yu, "An agri-product traceability system based on IoT and blockchain technology," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Shenzhen, China, Aug. 2018, pp. 254–255.
- [88] J. Li and X. Wang, "Research on the application of blockchain in the traceability system of agricultural products," in *Proc. 2nd IEEE Adv. Inf. Manage., Communicates, Electron. Autom. Control Conf. (IMCEC)*, Xi'an, China, May 2018, pp. 2637–2640.
- [89] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019.
- [90] S. V. Bojja, G. Fanti, and P. Viswanath, "Dandelion: Redesigning the bitcoin network for anonymity," *ACM Meas. Anal. Comput. Syst.*, vol. 1, no. 1, pp. 1–34, 2017.
- [91] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.
- [92] A. Singh, T.-W. Ngan, P. Druschel, and D. S. Wallach, "Eclipse attacks on overlay networks: Threats and defenses," in *Proc. IEEE INFOCOM. 25TH IEEE Int. Conf. Comput. Commun.*, Barcelona, Spain, Apr. 2006, pp. 1–12.
- [93] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer-Peer Syst.*, Cambridge, MA, USA, 2002, pp. 251–260.
- [94] G. Karame, E. Androulaki, and S. Capkun, "Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin," *IACR Cryptol. ePrint Arch.*, vol. 2012, no. 248, 2012.
- [95] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, Apr. 2019.
- [96] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, Sep. 2019.
- [97] A. A. Monrat, O. Schelen, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.
- [98] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, 2019.
- [99] Q. Wang, S. Wang, P. Zhang, L. He, X. Li, S. Cheng, and S. Zhou, "An achieving data exchange cross-chain alliance protocol," *J. Phys., Conf. Ser.*, vol. 1213, Jun. 2019, Art. no. 042037.
- [100] J. Y. Zie, J. C. Deneuville, J. Briffaut, and B. Nguyen, "Extending atomic cross-chain swaps," in *Proc. DPM, Int. Workshop Data Privacy Manage. CBT, Int. Workshop Cryptocurrencies Blockchain Technol.*, Luxembourg City, Luxembourg, vol. 11737, 2019, pp. 219–229.
- [101] D. Fakhri and K. Mutijarsa, "Secure IoT communication using blockchain technology," in *Proc. Int. Symp. Electron. Smart Devices (ISESD)*, Bandung, Indonesia, Oct. 2018, pp. 1–6.
- [102] H. Cui, Z. Chen, Y. Xi, H. Chen, and J. Hao, "IoT data management and lineage traceability: A blockchain-based solution," in *Proc. IEEE/CIC Int. Conf. Commun. Workshops China (ICCC Workshops)*, Changchun, China, Aug. 2019, pp. 239–244.
- [103] M. S. Devi, R. Suguna, and P. M. Abhinaya, "Integration of blockchain and IoT in satellite monitoring process," in *Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT)*, Coimbatore, India, Feb. 2019, pp. 1–6.
- [104] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.
- [105] D. Di Francesco Maesa, A. Marino, and L. Ricci, "Data-driven analysis of bitcoin properties: Exploiting the users graph," *Int. J. Data Sci. Analytics*, vol. 6, no. 1, pp. 63–80, Aug. 2018.
- [106] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," in *Proc. 40th Int. Conf. Softw. Eng. Pract. (ICSE-SEIP)*, Gothenburg, Sweden, 2018, pp. 134–143.
- [107] P. Tasca, A. Hayes, and S. Liu, "The evolution of the bitcoin economy: Extracting and analyzing the network of payment relationships," *J. Risk Finance*, vol. 19, no. 2, pp. 94–126, 2018.



YIJUN ZOU was born in Jiangsu Province, China. He received the M.Sc. degree in management from the University of International Business and Economics. He is currently pursuing the Ph.D. degree in management science and engineering with the Beijing University of Posts and Telecommunications. He is also the Vice Director of the Department of Finance, BUPT. He is also the Accounting Leader of the Chinese Central Government Department. His research interests include big data, blockchain, data assets, and financial management.



TING MENG received the B.S. degree in software engineering from Yanshan University, China, in 2018. She is currently pursuing the M.S. degree with the School of Software Engineering, Beijing University of Posts and Telecommunications. Her research interests include blockchain privacy protection, blockchain transaction data analysis, and network security.



PENG ZHANG received the B.S. degree in software engineering from Shanxi University, China, in 2018. He is currently pursuing the M.S. degree with the School of Software Engineering, Beijing University of Posts and Telecommunications. His research interests include blockchain privacy protection, blockchain consensus algorithm, and network security.



WENZHEN ZHANG received the B.S. degree in software engineering from the Beijing University of Posts and Telecommunications, in 2019, where she is currently pursuing the M.S. degree with the School of Software Engineering. Her research interests include blockchain privacy protection, blockchain, traction data analysis, and network security.



HUIYANG LI was born in Taiyuan, Shanxi, China, in 1992. She received the B.S. degree in electronic information engineering from the Tianjin College, University of Science & Technology Beijing, Tianjin, China, in 2014, and the M.S. degree in software engineering from The University of Texas at Arlington, Arlington, TX, USA, in 2017, where she is currently pursuing the Ph.D. degree in computer science. Since 2018, she has been a Research Assistant with the ACES Laboratory, The University of Texas at Arlington. Her research interests include the SLO Tail latency guaranteed data center job scheduling, blockchain, resource management in cloud, and edge computing.

...