Research on Legal Regulations of Blockchain

Mohong Liu[*]

Macau University of Science and Technology
lmh_tsifira@outlook.com
*corresponding author

Keywords: blockchain, risks and challenges, legal regulations.

Abstract: Blockchain is a chained data structure that combines data blocks in sequence in chronological order. It has the advantages of decentralization, immutability, distribution and transparency. Blockchain is mainly used in economy and finance, judicial practice, social governance, public welfare and charity, and other fields in China. As a new technology, the risks and challenges brought by blockchain include but are not limited to: algorithm security, convenience for crime, difficulty in determining jurisdiction, and inability to guarantee the right to be forgotten. To prevent blockchain risks requires to establish scientific algorithm rules, improve blockchain legislation, innovate regulatory measures, and establish a blockchain global governance system.

1. Introduction

In recent years, in the context of the digital transformation of the Chinese economy, blockchain technology has developed and popularized rapidly. The research and application of blockchain technology has moved from the initial conceptual stage to the stage of large-scale practical application, and is considered to be the new generation of technological innovation revolution after steam engines, electric power, and the Internet, which will profoundly change the economic and social pattern[1].

China has gradually formed a "Chinese Consensus" in the development of blockchain technology, trying to give a "Chinese voice" to the world. However, technology is a double-edged sword. In the developing process of blockchain technology in China, it brings challenges to people's economic and social life while providing scientific and technological support for various fields. As a revolutionary technological innovation, how to prevent and evade the risks and challenges brought about by blockchain technology while guaranteeing and promoting the development of blockchain is a brand-new issue that needs to be solved by laws and regulations. The Chinese government has begun to pay close attention to blockchain technology and has formulated relevant institutional measures, but the development of related technology industries is still at an early stage. Therefore, under the background of this era, research on legal regulations in blockchain applications is carried out, which has great significance for promoting theoretical research and practical applications in China, accelerating the formation of an independent innovation system, paying close attention to the frontier trends of international industry development, improving the blockchain policy system and regulatory framework, and accelerating the improvement of public service levels and governance.

To this end, this paper analyzes current industry application status of the blockchain, future research development trends, and the upcoming social governance challenges based on sorting out

the principles and characteristics of blockchain technology, and proposes methods to improve blockchain legal regulations.

2. Connotations and characteristics of blockchain

2.1. Definition of blockchain

Blockchain technology is a special database technology based on cryptographic elliptic curve digital signature algorithm (ECDSA) to achieve decentralized, peer-to-peer system design.

According to the "China Blockchain Technology and Application Development White Paper" released by the China Blockchain Technology and Industry Development Forum in 2016 under the guidance of the Ministry of Industry and Information Technology, the concept of blockchain can be divided into broad sense and narrow sense. In a narrow sense, a blockchain is a chained data structure that combines data blocks in sequence in chronological order, and is a distributed ledger that cannot be tampered with or forged, guaranteed by cryptography. In a broad sense, blockchain is a new distributed infrastructure and computing paradigm that uses block-chain data structures to verify and store data, uses distributed node consensus algorithms to generate and update data, uses cryptography to ensure the security of data transmission and access, and uses smart contracts made of automated script codes to program and manipulate data[2].

2.2. Technical principles and main characteristics of blockchain

Typical blockchain technologies include distributed ledger, peer-to-peer networking, consensus algorithms, encryption technologies, and smart contracts. The innovative combination of these technologies makes the blockchain has its unique technical characteristics:

2.2.1. Peer-to-peer and decentralized distributed network

Peer-to-peer, namely the P2P network technology, is a decentralized network system that relies on users to directly exchange information. The whole process of blockchain network data formation is based on the distributed network structure, and the collective operation of the distributed network is realized by pure mathematical methods, and a P2P self-organizing network is constructed, in which each node has the same rights and obligations.

2.2.2. Openness, transparency and collective maintenance

The blockchain system has an open consensus mechanism, which ensures that all nodes in the system can participate in the verification of new blocks through a specific incentive mechanism. Therefore, all transaction information in the blockchain network has a high degree of openness and transparency, and all nodes on the chain are visible and collectively maintained by all nodes.

2.2.3. Trustworthy and non-tamperable

With the help of the Proof-of-Work mechanism (PoW), data exchange between nodes on the chain does not need to establish substantial trust, but conducts mutual verification through digital signature technology to form a reliable consensus credit based on cryptographic algorithms. At the same time, in accordance with the established rules of the system, nodes cannot deceive other nodes. Unless they can control more than 51% of the nodes in the entire system at the same time, a small number of nodes cannot modify the database.

3.   Development and application fields of blockchain technology in China

3.1.   Current development of blockchain in China

From the implementation of blockchain projects, at present, there are a total of 1,787 blockchain projects in China, of which there are 843 application projects in the blockchain industry, accounting for 47.2%. The financial sector is the most influenced area of blockchain technology, accounting for 56% of all application projects. There are 536 digital currency projects, accounting for 29.9%, and blockchain information services and community projects accounting for 10.6%. Blockchain application technology projects (including smart contracts, data services, information security, blockchain hardware, blockchain tools, etc.) account for about 9.1%. Blockchain social projects account for 7.3%, entertainment projects account for 6.7%, and basic technology projects (including blockchain underlying technology, identity verification, payment settlement, anonymity technology, blockchain BaaS services, etc.) account for 3.1%[3].

As more and more projects implemented, China's blockchain industry has begun to enter a cycle of accelerated applications. At present, the application scenarios of blockchain technology are expanding to a wider range and deeper level, and blockchain is more closely integrated with the real economy.

3.2.   Typical application fields of blockchain industry

3.2.1. Financial sector

In China, the blockchain technology has firstly been greatly developed in the financial field. For example, the Digital Currency Research Institute of the People's Bank of China and the Shenzhen Central Branch of the People's Bank of China promoted the establishment of a trade-finance blockchain platform in the Guangdong-Hong Kong-Macao Greater Bay Area to conduct supervision for trade and financing activities in various scenarios such as accounts receivable on the platform and realize dynamic real-time evaluation of various financial activities.

3.2.2. Digital content copyright

Block technology has also been applied in the field of copyright protection. For example, Zhigui Technology, a blockchain technology product service provider, has built a professional full-type copyright storage platform based on blockchain technology. Internet AI company Baidu and network security platform Qihoo 360 have used blockchain technology to develop digital copyright image authentication platforms "Totem" and "Tuke". Tencent also uses blockchain technology as the basis to confirm and protect virtual digital assets such as online game items.

3.2.3. Electronic Deposit

In judicial practice, there are difficulties in accessing electronic evidence and collecting evidence online, and blockchain technology is precisely used to solve the current difficulties in obtaining evidence in the judicial field. For example, China's first electronic evidence platform and judicial blockchain were officially put into operation at the Hangzhou Internet Court, providing a solution to the problem of electronic evidence storage and access. Beijing Internet Court also applied blockchain evidence access technology to its cases of copyright ownership and infringement disputes.

3.2.4. Anti-counterfeiting traceability

The traceability advantage of blockchain technology provides a more convenient and reliable tool for anti-counterfeiting traceability of food and medicine. For example, technology industry giants such as JD.com, Ant Group, and ZA Tech have increased the research and development of blockchain technology and industry integration in the anti-counterfeiting and traceability of food, medicine and other products. Taking JD.com as a typical example, it uses the high-reliability technical characteristic of the blockchain to develop blockchain traceability technology from solving the consumer trust crisis, and completely records the information of the entire process of the product from raw materials, production and transportation, promoting further development of anti-counterfeiting and traceability of the blockchain industry application.

4. Risks and challenges of the blockchain technology

4.1. Algorithm security

As for technology, blockchain data rely on blockchain algorithm rules, and all algorithms have security issues. Because in the consensus algorithm of PoW, there is a rule of "the minority obeys the majority", if the computing power of the node is stronger than the rest of the system, the data information can be controlled and processed arbitrarily. This is a kind of computing power attack, that is, the nodes on the blockchain system use their own strong computing power to win the competition for the computing power of the nodes in the system and perform illegal operations on the previous data records. Once a computing power attack is achieved, it can cause irreparable property losses and privacy leaks to relevant blockchain participants by stealing node account information.

More importantly, it can use super computing power to tamper with most of the node account data to control the entire blockchain system, which will challenge national network security and information security and threaten national sovereignty and social stability[4]. In 2016, attackers took advantage of the recursive invocation leak in programming language Solidity to transfer 3.06 million Ether on the Ethereum crowdfunding project "The DAO"[5], which is a good example of algorithm security.

4.2. The anonymity facilitates crimes

The anonymity of the blockchain network does help protect the privacy of its network service participants, but it also facilitates related crimes. For example, as the underlying technology of Bitcoin, the blockchain's decentralization and high anonymity make Bitcoin and other virtual currencies easier to be used by criminals, thus becoming a tool for cross-border money laundering, terrorism financing, tax evasion, illegal transactions, and other crimes.

The high degree of anonymity and global transaction of the blockchain network not only exacerbate the risk of virtual currency being used in criminal activities, but also make the investigation of related criminal activities more difficult. On the Internet, it is difficult for relevant institutions to accurately and effectively trace the crimes committed through blockchain technology. Even if illegal transactions or criminal details are traced, because of the anonymity of blockchain information service participants, the real responsible party is still difficult to be accurately locked. As early as 2012, the European Central Bank has emphasized that because Bitcoin did not have a central authority, law enforcement agencies will face severe challenges in investigating suspicious activities, identifying users and obtaining transaction information, and even shutting down Bitcoin services. These issues may attract criminals and money laundering to use Bitcoin[6].

4.3. Split accounting and decentralization make it difficult to determine jurisdiction

Decentralization is one of the core features of blockchain technology, and each block in the blockchain network does not have a specific physical address, which leads to the invalidation of traditional jurisdiction determination rules. Traditional jurisdiction determination rules use information such as residence as the connection point, but the distributed network and decentralized characteristics of the blockchain enable its data to exist in multiple locations around the world and be subject to multiple different jurisdictions. The scope of the jurisdiction is not controlled by any specific organization or individual, and its managers exist in several different jurisdictions, which creates huge difficulties for the determination of jurisdiction.

4.4. Inalterability makes it difficult to guarantee the right to be forgotten

In the Internet field, citizens have the right to be forgotten, which was confirmed by the Court of Justice of the European Union in the case of Google Spain v AEPD and Mario Costeja González, and its legal status was established in the form of legislation in the General Data Protection Regulation (GDPR) passed in 2016. The GDPR stipulates that data subjects have the right to request the data controller to modify or delete personal information under certain circumstances[7]. However, the blockchain is collectively maintained and is difficult to tamper with, which makes it difficult to exercise the rights of data subjects in the blockchain system in practice. Moreover, if criminals use blockchain technology to write some information that is clearly prohibited by law into the blockchain, it will create great obstacles for companies to fulfill their obligation to delete, for citizens to exercise their right to delete, and for the government to supervise illegal activities, which destroy the order of cyberspace governance[8].

5. Prevention and response to legal risks of blockchain

5.1. Create scientific algorithm rules

In face of the continuous innovation and iteration of blockchain technology and algorithms, through the construction of code technology and other algorithm rules that are updated in synchronization with technology, technology is used as an auxiliary supervision method to make up for the lag of laws, and the development of a new generation of computing architecture is stepped up to ensure the impartiality and correctness of mathematical algorithms, the privacy and reliability of the data, the whole process of the data, and the efficiency of the mathematical algorithm at the same time, so as to achieve technological independence and realize the innovative integration of algorithm rules and legislative regulations on this basis.

On the basis of respecting technical rules, it's important to actively implement new regulations against structural vulnerabilities in blockchain technology, and adopt multi-party cooperation and connected governance mechanisms to jointly promote the legalization of the blockchain industry.

5.2. Scientifically formulate blockchain legislation

First is to update the legislative concept and reconstruct the principle of blockchain supervision. First, introduce the concept of inclusive governance, including diversification of legislative bodies, democratization of legislative procedures, and let legal rules, principles, and technical regulations work together. Also, technologies such as data codes and smart contracts could be used to improve the scientificity of blockchain legislation and enhance the guidance and operability of laws and regulations to achieve an effective combination of technical governance and legal governance.

Second is to formulate supporting laws to fill gaps and loopholes in the blockchain law. To start with, legislation is used to clarify issues such as the attributes of data rights, the legal status of tokens, and the effectiveness of smart contracts[9]. Then, from the comprehensive environment at this stage, blockchain technology and related industries cover a large area and are in continuous development and change. The cognition to both the technology itself and the industry application is not mature enough. Therefore, the legislative condition is not mature. From the perspective of feasibility, it is possible to formulate a temporary system for mature issues in the practice of blockchain development, or to absorb through the interpretation of existing laws. For issues that need to be further developed or are more controversial, we can further expand research and consider legislation when it's appropriate. On this basis, comprehensive consideration is given to formulating a relatively independent blockchain legal system.

Third is to establish a blockchain application governance system. As an innovative technology, the value of blockchain is not inherently positive, and its application risks are highly uncertain. In addition to traditional specific administrative actions, such as blockchain business approval, administrative penalties for violations of laws and regulations, blockchain administrative information disclosure, and blockchain violation data seizures, the governance system can also provide recommendations, advice, and other non-mandatory measures for blockchain application risks to require administrative guidance for each node of the blockchain to act or not.

Finally, local laws and regulations, on the premise of not contravening the constitution, laws and regulations, adhere to the principles of local characteristics and the spirit of the times, formulate local blockchain standards in accordance with local conditions, and enhance operability[9].

5.3. Innovate regulatory methods and strengthen industry self-discipline

First is to innovate regulatory methods to improve regulation efficiency. Giving full play to the advantages of the decentralized characteristics of the blockchain, putting the regulator in the blockchain network, and clarifying the "regulatory node" in the blockchain network will not only help the regulatory authority to monitor and control the real-time information of the blockchain more efficiently, but also enable the supervisory department to discover and deal with the problems on the chain in time. Moreover, in related industries that require stricter supervision, "super-computing power nodes" can be set on the chain. The supervisory nodes can be given enough computing power through technological development to master the right of speech and the dominance of governance on the chain, coding the on-chain protocols and becoming part of the operation of the blockchain network, and finally establish an innovative supervision mechanism that integrates technology and system. In addition, it is also possible to implement differentiated information provision standards for each node. When a node initially joins the blockchain, only minimum information is required. If the node's behavior remains normal, the information provided maintains a minimum standard. Once the node has abnormal behavior, it is forced to provide the corresponding personal information according to the degree of abnormality and the level of computing power, which provides direction and tools for supervision and helps maintain information security[10].

Second, the government should strengthen guidance and improve industry self-discipline. The government guides blockchain-related industries through policy guidance to actively establish industry associations and other effective third-party regulatory agencies to achieve effective supervision. Industry self-discipline, as an aid to legal supervision, can jointly establish an on-chain multi-center governance model with relevant national regulatory agencies. The third-party regulatory agencies can also join the on-chain network system as a sub-central node to monitor the entire operation of the industry's blockchain network. Industry associations and other third-party regulatory agencies can formulate unified blockchain technology industry standards, establish a multilateral blockchain governance system that adapts to multinational businesses through strengthening

international exchanges and consultations, promote the standardized development of on-chain businesses through the formulation of on-chain industry conventions, and have regular credit evaluation and publicity of all nodes and publicity. At the same time, an off-chain appeal and complaint system should be established, an appeal and complaint agency should be set, and corresponding processing procedures should be established to ensure the legitimate rights and interests of the participants in the blockchain service in the physical space.

5.4. Promote international regulatory consensus and realize global governance of blockchain

The openness, decentralization and autonomy of blockchain technology itself implies globality.

For a revolutionary technology with distinctive globalization characteristics such as blockchain, its subversive decentralized governance value concept will also have a negative effect on the society, inspiring human society to construct a corresponding global governance mechanism for a global technology.

Current challenges faced by blockchain in global cross-border governance are largely due to the difficulty in the definition of jurisdiction and the lack of relatively unified regulatory systems and technological awareness in different jurisdictions. In order to solve the geographical risks that may be caused by global technology, the construction of a unified blockchain global governance mechanism will establish a global trust bond in this innovative technology field, and treat blockchain governance as a global issue related to the ups and downs of the whole human society.

Through experience exchange, institutional negotiation and technology sharing to promote the reaching of international regulatory consensus, a unified international industry regulatory standard for blockchain-related industries could be established, and a global unified algorithm rule could be built to assist international regulation, which is conducive to the realization of global democratic decision-making and promote an open, transparent, and efficient global governance, as well as further promote the realization of a community with a shared future for mankind.

6. Conclusion

Blockchain is a revolutionary technological output in the 21st century. With its unconventional distributed thinking and high credibility, it is regarded as a potential underlying technology in many fields such as finance, law, government affairs, and social governance.

At present, the underlying technology of the blockchain is not yet mature, and the technical bottleneck for large-scale and reliable applications needs to be broken. The real implementation and application effect is still far from the society's expectation. There are also a series of risks and problems in the technological development and practice in the blockchain-related industries that need to be solved urgently in China, which means that we are in a period of great opportunities for blockchain technology and industrial innovation and development.

In order to create a good development environment for blockchain technology, it is necessary not only to further improve legislative policies and innovative regulatory methods, but also to encourage technological innovation and provide research and development support. How to formulate targeted legal governance for the unique endogenous mechanism of blockchain mainly lies in how to balance the relationship between technological innovation and legal regulation. Under this background, all fields of society are working hard to promote this trend of innovative technology.

Research on the legal regulations related to blockchain will provide theoretical and decision-making reference for China's legislation, law enforcement, and judicial response and grasping the opportunities brought by the blockchain technology.

References

[1] *Pan Jian, Zhao Yahui, Duan Xinyi, Si Erxun. The Developing Blockchain in China, ANNUAL REPORT ON CHINA'S BLOCKCHAIN APPLICATION AND DEVELOPMENT (2019), edited by Ye Zhenzhen & Luo Hua. Social Sciences Academic Press (2019), pp-3*

[2] *China Blockchain Technology and Industry Development Forum, "China Blockchain Technology and Application Development White Paper (2016)", Oct. 18, 2016. pp-5*

[3] *ANNUAL REPORT ON CHINA'S BLOCKCHAIN APPLICATION AND DEVELOPMENT (2019), edited by Ye Zhenzhen & Luo Hua. pp-13*

[4] *Jin Lu. Between Rules and Technology: Risk Analysis and Legal Regulation of Block Chain Technology Application. Law Science Magazine. 2020(7)*

[5] *Zhu Yan, Wang Qiaoshi, Qin Bohan, Wang Zhonghao. Survey of blockchain technology and its advances, Chinese Journal of Engineering. 2019(11)*

[6] *See European Central Bank: Virtual Currency Schemes. (2012) :42 - 45. https: //www.ecb.europa.eu/pub/pdf /other/virtualcurrencyschemes201210en. pdf (last visted mar29,2021).*

[7] *GDPR, arts. 16-17.*

[8] *He Bo. Blockchain Technology and Its Legal Problems. Professional Perspective. 2018(209)*

[9] *Qi Xuexiang. Beyond Risk: Application Risk and Governance of Blockchain Technology. Social Sciences in Nanjing. 2020(1)*

[10] *Chen Qiwei, Nie Linfeng. Technology + Legislation: Legal Protection of Personal Information Rights in the Era of Block Chain. Jiangxi Social Sciences. 2020(6)*