The Regulation of Cryptocurrency in China

Jiye Hu*

Abstract: As a distributed ledger technology (DLT) application, cryptocurrency has impacted the current financial legal relationship, and its regulation is becoming increasingly important. Some international organizations and countries have ratified laws and regulations concerning cryptocurrency. However, the supervision and regulation of cryptocurrency in China are still encountered some problems, such as consumer protection, the opposition between the global asset flow and the supervision of a single sovereign state, and the difficulty in determining the subject of legal responsibility. To seek solutions to these problems in China, the primary task is to define the legal attribute of cryptocurrency, to balance blockchain innovation and financial risk. At the same time, the regulatory sandbox can be used to regulate blockchain-based cryptocurrency. Among others, the core regulatory measures are establishing the technical standard access system, financing audit registration system, and investor suitability management system of blockchain financial enterprises.

Keywords: blockchain; cryptocurrency; sandbox supervision; legislation; regulation

Cryptocurrency, as defined by the European Banking Authority, is not issued by the central bank or monetary authority, nor linked to legal currency, but is based on blockchain technology and accepted by the public; therefore, it can be used as a means of payment, electronic transfer, storage, or transaction, so it is a digital representation of value. With such an understanding of the characteristics and legal nature of cryptocurrency, this paper explores the challenges of cryptocurrency, and the regulatory measures taken by relevant foreign organizations and institutions, and provides suggestions for improving the supervision and regulation of cryptocurrency in China.

*Corresponding author: Jiye Hu, Professor of Law and Finance, Department of Finance, Business School, China University of Political Science and Law, Beijing, China; and Specially-appointed Professor, Krirk University, Bangkok, Thailand, E-mail: jiyeh@cupl.edu.cn. https://orcid.org/0000-0001-9486-5889

Open Access. © 2024 the author(s), published by De Gruyter on behalf of Zhejiang University. This work is licensed under the Creative Commons Attribution 4.0 International License.
1 The Technical Characteristics and Legal Challenges of Cryptocurrency

1.1 Technical Characteristics of Blockchain Distributed Ledger

Nakamoto (2008) proposed a new electronic payment system based on cryptographic principles instead of credit currencies, by which the peer-to-peer electronic cash system enables any two parties to reach an agreement. Based on a distributed ledger, Bitcoin provides a solution to the double-spending problem using a peer-to-peer network (Patgiri, Acharjamayum, and Devi 2019). The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing. The payment can be made directly without the involvement of a third-party intermediary. Bitcoin is regarded as a decentralized, peer-to-peer virtual currency. It can be exchanged for traditional currency or buy goods or services, usually through online transactions. Unlike traditional currencies, Bitcoin has neither central bank support nor any governmental authority support.

Bitcoin is the earliest and most successful application of blockchain technology in the field of digital finance (Hashemi Joo, Nishikawa, and Dandapani 2020). According to ISO 22,739 issued by the International Standard Organization, a blockchain is a distributed ledger formed by sequentially adding blocks using cryptographic technology, which is confirmed by consensus (ISO 2020). The distributed ledger technology (DLT) in the Bitcoin system is shared and synchronized in a distributed manner in recording transactions. In the construction and application of distributed ledgers, applications of smart contracts, cryptography, and consensus mechanisms are paid more attention. At the same time, the synchronization of distributed ledgers can be achieved by the decentralized or multi-centralized technical architecture. Compared with traditional technologies, distributed ledgers can prevent tampering, easy auditing, high transparency, strong reliability, and automatic execution of smart contracts. They are considered to be the technological prototype of a new generation of financial market infrastructure. Based on distributed ledgers, blockchain technology integrated with the Internet of Things, cloud computing, big data, artificial intelligence, etc., can form a completely new generation of information technology eco-system to maximize the value of data.

Before the invention of the distributed ledger, most of the economic activities were single bookkeeping, and each business was recorded in one account. After a certain period, an inventory must be carried out to sort out all the previous accounts. Due to the existence of problems such as income and expenditure and
difficulty in external verification, it was gradually replaced by double-entry bookkeeping. The important feature of double-entry bookkeeping is that two or more accounts must be recorded for each business. There is an objective cross-check relationship between accounts, and the results of account records can be balanced by trial calculations. Double-entry bookkeeping achieves the goal that external stakeholders can verify the internal accounts of the company. External investors can judge the company’s financial status, profitability, and future potential based on the financial data disclosed in the listed company’s annual report and then make investment decisions. Therefore, double-entry bookkeeping is of great significance to developing the modern capitalist market economy (Ryan 2014). However, due to the limited number of participants in double-entry bookkeeping, the possibility of fraudulent accounts still exists. In the Enron scandal in 2001, Arthur Andersen, who was among the top five accountants in the world, became notorious for assisting Enron’s accounting data falsification and finally withdrew from the accounting and auditing market, which fully illustrates the shortcomings of double-entry bookkeeping (Şenyiğit 2013). Zhu Rongji, the then-Chinese Premier at the time of the scandal, rarely wrote inscriptions openly; however, in 2002 he wrote the school motto “Make no false accounts” in his hand to the three newly established National Accounting Institutes in China to train finance and accounting personnel to put an end to false accounts.

Can the false and fraudulent activities of double-entry accounting be prohibited technically? DLT may be one of the solutions (Farahani, Firouzi, and Luecking 2021). Unlike double-entry bookkeeping, the transaction information recognized in the distributed ledger will be confirmed to form a block and be recorded in the ledgers of all participants, and each on the blockchain will be stamped with a unique “timestamp”, which can confirm that certain data exists at a certain time. In this distributed ledger technology, the accounting information of all participants is the same, and all kinds of tampering become an almost impossible task. For example, in a WeChat group of 100 people, one member sent an electronic red envelope that could only be snatched by 10 people. The record of opening the red envelope was recorded the same for each group member. Timestamp recorded the exact recipient time of these 10 lucky members. Since all group members’ terminals simultaneously record the receipt results to form a distributed accounting in every subscriber’s terminal devices, no one suspects that the record of this red envelope is a “false account”. The same is true for the record of sending Bitcoins on the blockchain. The receiver can accept Bitcoin through his private account, but everyone on the chain has recorded the transaction, thus ensuring the uniqueness of the same transaction and avoiding double payment (Crepaldi 2020). Distributed accounting ensures that if you want to modify the transaction information in a block, that is, one of the ledgers, you must modify all the content of the block and subsequent connected blocks, just like on the
mobile phones of all group members modifying the red envelope distribution record, so it is extremely difficult to tamper with.

As cryptocurrency's underlying technology, DLT revolutionizes the double-entry accounting that has continued for hundreds of years. By using asymmetric encryption authentication methods and peer-to-peer network architecture, it maintains a continuous ledger database that cannot be tampered with (Gourisetti et al. 2021). It is possible to enable the participating nodes in the blockchain to directly realize value transfer without mutual recognition and establishment of trust relationships, instead of relying on offline intermediaries. This mechanism greatly increases the difficulty of tampering with information, making no false account truly technically realized. The natural trust gene brought by DLT is an epoch-making change in double-entry bookkeeping technology that may falsify accounts. Its significance is no less than the transition from a single account book to double-entry bookkeeping, which will profoundly impact human economic life in the future.

### 1.2 Challenges of Cryptocurrency to the Current Legal System

As the underlying technology of encrypted cryptocurrency, blockchain technology has the characteristics of disintermediation, openness and transparency, and difficulty in tampering (Centobelli et al. 2022). It has huge potential value in the future of finance. As financial technology innovation, cryptocurrency has brought new opportunities and challenges to the financial market. Since the first batch of Bitcoin in the world came out in January 2009, cryptocurrency based on blockchain technology has continuously impacted human traditional financial thinking and has aroused widespread concern and controversy in society. Since then, many cryptocurrencies have appeared, and the price of Bitcoin increased dramatically, which has caused the general public to pursue almost all cryptocurrencies.

In June 2019, Facebook, which has nearly 2.7 billion users around the world, released its Libra project white paper, proposing that the vision of Libra is to build a simple global monetary and financial infrastructure that benefits billions of people, to become a stable cryptocurrency which is backed by physical asset reserves and built on a safe, reliable, and scalable open-source blockchain, and to be managed by a Swiss-based company which is independent of Facebook and participated by many institutions (Libra 2020). The launch of Libra was a major event in the field of cryptocurrency after the launch of Bitcoin in 2009. It is not only a cryptocurrency but also a financial infrastructure that includes core functions such as underlying, clearing, and settlement. It is equivalent to a new clearing and settlement network, where the original Facebook social network platform is used, through the deep
integration of network business and financial services, to constitute a huge challenge to the existing commercial financial system. The ultimate question is whether the public can place its trust in Facebook and its business partners to manage a global cryptocurrency, or is that trust better placed in the hands of central banks? Central banks of many countries, such as France, Germany, etc., have explicitly refused Libra to enter.

By adopting distributed ledger-based technology, which is different from traditional financial products, the financial market can strengthen investor protection and improve the efficiency of risk management. The change in the technology paradigm with the introduction of DLT systems for securities and derivatives FMI can increase investor control, and the efficiency of risk management, and, to some extent, augment the distribution of systemic risk (Avgouleas and Kiayias 2019). However, the emergence of cryptocurrency brings both challenges and risks.

Firstly, the global flow of cryptocurrency will have certain impacts on financial stability, including the risk exposure caused by financial institutions’ direct or indirect participation, the improper influence of financial regulatory agencies, and the operational risks of cryptocurrency in payment and domestic currency settlement. The wealth effect risk brought by the extremely volatile market value of digital assets may be amplified, and the traditional financial market has added the unstable factor of cryptocurrency assets.

Secondly, cryptocurrency brings enormous risks to investor protection. For example, in 2014, hackers stole $460 million worth of Bitcoin from the Bitcoin exchange Mt. Gox, and then it went bankrupt (McMillan 2014).

Thirdly, the disintermediation of cryptocurrency has brought about difficulties in supervision. On an international scale, the challenge brought by blockchain is the contradiction between the global flow of virtual digital assets and the single regulatory legal system of each sovereign country. Most securities are traded in specific institutions and centralized exchanges. However, cryptocurrency transactions can easily break through the existing regulatory system of such centralized institutions.

Fourthly, cryptocurrency brings new challenges to the fight against crime. The anonymity of cryptocurrency brings forth the problem of difficulty in determining the subject of legal responsibility, and it is easy to be used for terrorist financing, money laundering, dark web transactions, and other illegal and criminal activities.

Based on these risk factors of cryptocurrency, as early as December 2013, the People’s Bank of China and other financial regulatory commissions issued the regulation “Notice on Preventing Bitcoin Risks”, which identified cryptocurrencies as “specific virtual commodities” that did not have the same legal status as legal tender and prohibited relevant institutions from carrying out business activities related to
cryptocurrencies. On September 4, 2017, the People’s Bank of China, the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the former State Administration for Industry and Commerce, the former China Banking Regulatory Commission, the China Securities Regulatory Commission, and the former China Insurance Regulatory Commission jointly issued the “Announcement on Preventing Financing Risks of Token Issuance”, confirming that the virtual currency issued in the initial token offering (ICO) is the reality of “funds” financed in the name of “commodities”, the financing entities will be sold and circulated illegally through tokens to raise Bitcoin and Ether from investors, and virtual currency is essentially an illegal public financing behavior without approval. The announcement also points out that the act is suspected of illegally selling tokens and coupons, issuing securities, illegal fund-raising, financial fraud, pyramid schemes, and other illegal and criminal activities (PBC 2013).

The National Internet Finance Association of China (NIFA) is a national self-regulatory organization in the field of Internet finance and is initiated by the People’s Bank of China in collaboration with relevant ministries and commissions, which is one of the regulatory bodies on cryptocurrencies. The IMO model (Initial Miner Offerings) of issuing virtual digital assets represented by Xunlei’s LinkToken was criticized by NIFA for its intrinsic similarities to an ICO (NIFA 2018).

In 2018, the Notice on Carrying out Self-Inspection and Rectification Work for Providing Payment Services for Illegal Virtual Currency Transactions issued by the Business Management Department of the People’s Bank of China further strengthened the crackdown. On the surface, although China adopts a strict prohibition attitude the effect of blindly adopting a “blocking” rather than “sparse” attitude is not ideal. For example, under the circumstance of unabated demand, many platforms can still provide relevant services to domestic users through overseas registration with the same office space, putting financial activities related to cryptocurrencies under a regulatory vacuum, and eventually causing financial consumers to suffer losses.

In September 2021, the Notice on Further Preventing and Resolving the Risks of Virtual Currency Trading and Speculation was issued by the People’s Bank of China, the Cyberspace Administration of China, and other ministries emphasizing that the business activities related to virtual currency are illegal financial activities. All government departments, administrative regions, and industry associations shall fully leverage various media and other communication channels to educate the public about the unlawfulness, and harmfulness, to enhance public awareness of risk prevention (PBC 2021). For the first time, overseas virtual currency exchanges providing services to Chinese residents via the Internet are also illegal financial activities.
1.3 The Confusion in Actual Judicial Trials

At present, China’s legal positioning of cryptocurrency is ambiguous, which has confused inconsistent law applications in judicial trials.

China’s central bank defined cryptocurrency as a specified virtual commodity (Huang and Mayer 2022). This legal attribute is not clear, which brings difficulties in consumer protection and criminal identification. For example, in the case of “Improper Enrichment Dispute between Gao and Liu”, the plaintiff Gao transferred his 31.659 Bitcoins to the defendant Liu because of an operating error. Then the plaintiff negotiated with the defendant about the return of the Bitcoin via text messages and phone calls. The defendant always buckled his case. To protect his legitimate rights and interests, Gao had no choice but to sue and ask the defendant to return 31.659 Bitcoins (approximately RMB 70,000 at then). However, the court’s judgment regards Bitcoin as a P2P form of cryptocurrency, a type of online virtual currency. According to the Central Bank’s definition of specific virtual commodities, Bitcoin cannot and should not be used as currency in the market, at the same time Bitcoin’s transactions are not protected by law. The plaintiff mistakenly remitted his Bitcoins to the defendant’s account through the trading platform. This type of trading behavior is not protected by law in China and the consequences caused by his behavior are at his own risk. The plaintiff lost the case.

The vague legal positioning of cryptocurrency has led to the issue of sentencing and conviction. In the case of “Chen theft”, the defendant Chen logged in to the victim Wang’s Huobi account, modified Wang’s contact number, address, and bound account information registered on the website, and sold 1.514 Bitcoins in Wang’s account, getting the sales proceeds of RMB 6583.35. The next day, Chen cashed out RMB 6500, deducting RMB 32.5 from the website handling fee, and transferred the remaining RMB 6467.5 to his banking account. The court ruled that Chen had secretly stolen RMB 6500 of the victim’s online money for illegal possession, which was a relatively large amount. In the end, the court ruled that Chen’s behavior constituted the crime of theft. However, a similar case was convicted of illegally obtaining computer information system data in another court.

It can be seen from the above three cases that the current judicial practice has not clearly defined the virtual currency of Bitcoin. How to make clearer legal qualifications to regulate the operation of China’s cryptocurrency can be learned from international experience in this regard. The in-depth application of modern technologies such as blockchain and 5G in the judicial field will strengthen the protection of new rights and interests such as digital currency, network virtual property (Song and Ma 2022), and data (Cheng and Liu 2023; Li, Cai, and Cheng 2023), and give full play to the value-leading role of judicial judgments in the protection of property rights.
2 International Experience in Cryptocurrency Supervision and Legislation

According to a research report released by the blockchain security company CipherTrace, by the end of July 2021, major crypto thefts, hacks, and frauds totaled $681 million (CipherTrace 2021). It is precisely because of the existence of these problems that supervision has become the inevitable choice of governments.

2.1 The Regulatory Concept of International Organizations on Cryptocurrencies

Under normal circumstances, only a specific subject who violates the law can bear the corresponding legal responsibility. The anonymity of cryptocurrency makes it difficult to determine the subject of legal responsibility (Reynolds and Angela 2017). In addition to the less influential blockchain applications such as private chains and consortium chains, the current special needs to control risks and regulate their behavior are mainly public chains. The public chain network node is uncertain. Anyone who has special computer equipment can access or exit at any time. Once someone uploads false information, who is packaging and recording the information cannot be determined in advance. This feature makes cryptocurrency a new choice for criminals.

Since a country’s supervision of cryptocurrency transactions or exchanges is usually only within the scope of its sovereign state, the supervision of the above behaviors is beyond reach, and the supervision and coordination of international organizations are very important. In response to the challenges and risks posed by blockchain-based cryptocurrencies, sovereign states, and international organizations have begun to develop independent or joint regulatory rules (Irina 2018). Studying the regulatory measures in various countries and regions can provide a reference for improving China’s supervision of cryptocurrencies.

The Committee of Payment and Settlement System (CPSS) of the Bank for International Settlements (BIS) and the International Organization of Securities Commissions (IOSCO) jointly issued the “Principles of Financial Market Infrastructure” in 2017, putting forward the thesis that “distributed ledger technology will fundamentally change the way assets are maintained and stored”. Under the current situation, the financial system still relies on traditional double-entry bookkeeping. Distributed ledger technology, on the other hand, is very forward-looking as reducing financial risks in the existing financial system is universal for
the virtual digital financial system. This principle requires that the future financial market infrastructure should reduce complexity, increase end-to-end processing speed, reduce coordination across multiple ledger management infrastructures, improve the transparency and non-tampering of transaction records, and improve the network through distributed data management flexibility, thereby reducing operational and financial risks (CPMI 2017). Due to the international status of these two organizations in the field of indirect financing and direct financing, the financial market infrastructure principles put forward by the two organizations have important guiding value for future digital currency supervision.

In response to the international financial crisis caused by the spread of the US subprime mortgage crisis, the 2009 G20 summit decided to establish the Financial Stability Board (FSB). The FSB (2017) report proposes that given the rapid development of financial technology, international institutions, and national authorities should consider financial technology issues in their existing risk assessment and regulatory frameworks, and this is the first time that people proposed the allocation of cryptocurrencies (FSB 2017). The FSB further confirmed in October 2018 that crypto assets are a kind of private assets with the functions and characteristics of digital transaction methods. The FSB realizes that the distributed ledger technology at the bottom of cryptocurrency is widely used in securities settlement, asset registration, transaction reporting, and inclusive finance. At the same time, it has also been noted that the anonymous nature of encrypted digital assets may lead to failure to find violations of regulatory rules. The main body of responsibility has aggravated problems such as money laundering and tax evasion. Given that many encrypted digital asset platforms are transboundary, these issues usually require international coordination and serious consideration by international standard-setting agencies (FSB 2018). In April 2019, the FSB released the “List of Crypto Assets Regulators”. The list provides information on FSB member states’ regulatory agencies and related international regulatory agencies that deal with crypto-asset issues, including regulatory agencies in 25 countries or regions and 7 international organizations. In the list, FSB specifies China’s regulatory agencies: the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Public Security, the China Banking Regulatory Commission, the China Securities Regulatory Commission, and the People’s Bank of China (FSB 2019). It can be found that the FSB, a regulatory coordination organization established to maintain international financial stability, has not been absent during the development of cryptocurrency. It is vigilantly monitoring the potential financial stability risks related to encrypted digital assets. Due to the characteristics of its global flow, it is the common responsibility
of the international community to prevent impacts on international financial stability.

International organizations such as CPSS, IOSCO, and FSB have fully realized the possible impact of cryptocurrencies and derivative stable currencies on the financial system, and have put forward the ideas of full attention and prudent supervision in the future. China is the world’s second-largest economy and an important member of these three international organizations. These regulatory principles and methods for cryptocurrencies are of high reference value for China.

### 2.2 Regulatory Measures for Digital Financial Companies in Relevant Countries

In addition to the aforementioned international organizations, many countries have begun to regulate emerging cryptocurrencies through their domestic administrative, legislative, and judicial systems (Alvarez 2018).

The United States’ regulation of blockchain, virtual currency, and ICO is mainly carried out within the framework of its Securities Act. In 2017, the Securities and Exchange Commission (SEC) proposed that all ICOs must be registered unless they are exempt from the Securities Exchange Act of 1934. In 2018, the SEC issued the “Investor Announcement: Initial Token Issuance”, confirming that tokens may become securities, and any illegal activities carried out in the name of the cryptocurrency, tokens, or other names must be subject to penetrating supervision. All services involving “remittance” (fiat currency and cryptocurrency) must comply with AML (anti-money-laundering) and KYC (know-your-customer) standards (SEC 2018). While the United States has allowed corporate self-regulation of consumer privacy, California became the first state to introduce its law – the California Consumer Privacy Act (CCPA). It was officially implemented on January 1, 2020. CCPA covers the operationalization of opt-out, non-discrimination rules, economic ramifications, consumer literacy, and a comparison with other privacy frameworks. The act aims to change the way data is processed, requiring all technology company platforms to strictly protect the privacy of their customers. For consumers who explicitly require the platform not to sell personal information, the platform must not sell the consumer’s personal information it collects (Baik 2020). Since many digital platform giants are registered in the State of California, this bill is of great significance to the privacy protection of digital financial consumers in the United States and the healthy development of encrypted virtual digital assets (Cheng and Wang 2019).

On May 25, 2018, the EU’s normative legal document on the protection of personal data information, the General Data Protection Regulation (GDPR), was fully
implemented. The regulation clarifies the rights of data subjects such as the “right to portability”, “right to know”, and “right to forget”, and how to protect data privacy and technical cooperation for companies that collect and use personal data in controlling and processing data. Regulations and other aspects have put forward higher requirements and challenges, that is, personal data must not be processed in a way that is harmful, discriminatory, accidental, or misleading to the data subject. The data subject should obtain the highest degree of autonomy in controlling their data; the data subject must be able to communicate with the data controller and exercise their rights; the expected processing should meet the data subject’s expectations, etc. This is a milestone for the EU in the field of data governance. Under the background of the pervasive information system and the profound change in human life in the digital economy, GDPR, like other EU-level directives, applies to all member states, establishes a unified personal data protection framework (Li and Kit 2021), clearly defines the direction of personal data circulation, and becomes the consensus of EU countries in data governance. The promulgation and implementation of the regulations have had a broad impact on global data governance. At the same time, it will also have a profound impact on the launch of cryptocurrencies.

In December 2019, the European Central Bank (ECB) released a EUROchain project based on Proof-of-Concept. The project is based on the General Data Protection Regulation and hopes to balance the relationship between data application and privacy protection, that is, to strike a balance between allowing a certain degree of privacy in electronic payments and ensuring compliance with regulations aimed at combating money laundering and terrorist financing. Under the coordination of the EU, the European Central Banking System (ESCB) has established an anonymous proof of concept in digital cash called “Central Bank Digital Currency, CBDC” (Forbes 2019). On July 14, 2021, the ECB announced that the digital euro would officially enter a 24 month trial phase, which aims to solve key issues in the digital euro’s design, circulation, and distribution, paving the way for its official launch. The Eurosystem is establishing a market practitioner group that takes account of the views of prospective users and distributors of a digital euro during the investigation phase of the project (ECB 2021). It is expected that CBDC will work with China’s upcoming sovereign virtual currency. Digital currency (e-CNY) is similar, which will help optimize the payment function of traditional legal currency, further, alleviate the dependence on payment services of the commercial sector, reduce the burden and pressure of central bank supervision, and thereby improve the status of legal tender. The reason the People’s Bank of China and the European Central Bank have introduced sovereign cryptocurrencies in unison is that they hope the central bank will play a leading role in the financial system in the competition in the field of cryptocurrencies and compete directly with non-sovereign cryptocurrencies such as Bitcoin and Ripple.
On April 1, 2017, Japan began to formally implement the amendment to the “Fund Settlement Algorithm” passed by the National Assembly. By way of background, Japan has been a leading nation in its approach to the regulation of certain virtual currencies under the amended Payment Services Act, which introduces the registration requirement for operators of “Virtual Currency Exchange Businesses”, defined as businesses engaging in the exchange of virtual currency for legal currency or another virtual currency or brokerage of such exchange (Day 2017). Since then, the Japanese Cabinet meeting passed the “Cabinet Office Order Regarding Virtual Currency Exchange Operators” and amended the “Payment Services Act” to include the payment business involved in cryptocurrencies into the scope of supervision. Due to the legal protection of virtual currency in Japan, in addition to the application of Bitcoin, there is also a large number of cases in industrial application fields, such as real estate certificates, identity authentication, supply chain finance, liquidation, settlement, etc. Considering the hacking incidents and social problems with crypto assets in Japan, the Financial Services Agency established the Research Group on virtual currency Exchange in March 2018 (Ren 2020). On May 1, 2020, the amendments to Japan’s “Fund Settlement Algorithm” and “Financial Instruments and Transaction Law” came into effect to strengthen the supervision of user funds of virtual currency exchanges and prevent fraud, theft, and money laundering (Wisenbaker 2010).

On August 1, 2017, the Monetary Authority of Singapore issued “Clarifies the Regulatory Position of Digital Tokens in Singapore”. It defines a digital token as a cryptographically-secured representation of token-holders rights to receive a benefit or to perform specified functions, while a virtual currency is a particular type of digital token, which typically functions as a medium of exchange, a unit of account, or a store of value. MAS divides digital tokens into payment, utility, and securities tokens. The issuance of payment tokens needs to comply with the relevant provisions of the Payment Services Act (Tan 2021). The issuance of utility tokens is not subject to supervision as long as there is no risk of money laundering and terrorist financing. The issuance of securities tokens needs to follow the relevant provisions of the Securities Law unless exemptions can be obtained. MAS also supervises the intermediary agencies that provide services for the issuance of digital tokens, requires them to operate under a license, and emphasizes the importance of anti-money laundering and anti-terrorism supervision. Singapore supervises ICOs by the country’s current laws and regulations. Its regulatory policies have cleverly achieved a balance between encouraging technological innovation and controlling risks, but there is also the problem of transplanting related risks overseas.

It can be found that the regulations governing cryptocurrencies in various countries set thresholds by the current financial legal systems such as banks and
securities, rather than laissez-faire. The purpose is to encourage the development and growth of high-quality blockchain and digital financial companies and to shut out companies with poor qualifications.

### 2.3 International Experience in Virtual Digital Asset Supervision Legislation and Investor Protection

In April 2012, US President Barack Obama signed the “Jumpstart Our Business Startups Act” (JOBS Act), which has strict requirements to protect small crowdfunding investors. The so-called CROWDFUND Act enables entrepreneurs and small business owners to sell limited amounts of equity in their companies to a large number of investors via social networks and various Internet platforms. If the annual income or personal net worth of the investors does not exceed US$100,000, the highest fundraising amount in a year is US$2000, or 5% of the net income (Stemler 2013). This small crowdfunding model makes small and medium investors have limited losses even if they make investment mistakes, which is a good reference for cryptocurrency investors. If small investors invest in cryptocurrencies, they can learn from the JOBS Act for investor suitability management, thereby better-protecting investors.

In April 2019, the US Securities Regulatory body SEC issued the “Digital Assets Investment Analysis Framework” on how digital encrypted assets can pass the Howe test to apply to securities laws. The Howe test allows ICOs to be identified as securities in most cases, including information disclosure and investor protection. Since ICO is regarded as a securities IPO by the SEC, the SEC has severely cracked down on cryptocurrency financing activities that do not comply with the Securities Act. Here is a typical case: the SEC issued Announcement No. 212 of 2019, accusing two entities of raising US$1.7 billion from the development of a blockchain application called the “Telegram Open Network” in January 2018, which is a typical ICO. These two entities did not register the issuance of “Grams” in line with the attributes of securities by the securities registration provisions of the “Securities Act of 1933”. They cannot simply label their products as “encrypted currency” or “digital token” to circumvent the supervision of securities laws. The SEC filed an urgent action in the Manhattan Federal District Court, accusing the two defendants of violating Sections 5(A) and 5(C) of the Securities Act, imposing emergency relief and permanent injunctions, property with pre-judgment benefits, and civil penalties (SEC 2019). It can be seen that the practice of ICO in the United States is not banned in name, but is broadcasted through public punishment and public precedents. In this way, those cryptocurrency issuers who do not comply with the Securities Law are deterred, while the interests of investors are protected.
In April 2019, the U.S. Congress passed the Token Classification Act of 2019, which excluded encrypted digital currencies from securities by amending the Securities Act of 1933, the Securities Exchange Act of 1934, and the Investment Company Act of 1940. After that, Congress began to discuss the draft of the “Cryptocurrency Act of 2020”, which divided digital assets into three categories: encrypted commodities, encrypted securities, and encrypted currencies. It is recommended that the Commodity Futures Trading Commission mainly supervises encrypted commodities and securities. The Securities Exchange Commission mainly regulates encrypted securities, and the Financial Crime Enforcement Network (FinCEN) under the Ministry of Finance regulates encrypted currencies. It can be found that the U.S. Congress has begun the legislative process on virtual digital assets. With the rapid development of the digital economy today, it is believed that the passage of the bill can lay the judicial foundation for cryptocurrencies at the federal level. The leading position of legislation also provides a legal basis for law enforcement and administrative punishment.

The well-known digital currency in the United States is Libra which Facebook launched in its white paper in June 2019. Due to its huge number of 2.7 billion users of Facebook, Libra wants to become a systemically important payment tool in the world, making Libra a stored value tool in some countries with unstable currency values, and even an independent accounting unit. The white paper has aroused great attention and vigilance from financial regulatory agencies in various countries. In April 2020, the second edition of the Libra white paper made major changes, including improving the security of the Libra payment system with a complete compliance framework and establishing a strong protection system for the Libra asset reserve in response to the country’s concerns about regulators (Libra 2020). Central banks and regulators are right to be concerned about Facebook’s stablecoin because it creates new risks for consumers and savers, as well as the global financial stability. Libra shifted its focus from an anchoring basket to an anchor currency in April 2020 after losing major backers including Visa and Mastercard following a backlash from global regulators. Libra officially changed its name to Diem in December 2020, in what was seen in the industry as Facebook’s concession to regulators. The Diem Network will operate using the Diem Blockchain, a new blockchain designed to be highly scalable, secure, and flexible. To meet the regulatory requirement, Diem has worked with regulators, central bankers, elected officials, and various stakeholders around the world to determine the best way to marry blockchain technology with accepted regulatory frameworks. Unfortunately, despite giving Diem positive substantive feedback on the design of the network, it nevertheless became clear from Diem’s dialogue with federal regulators that the project could not move ahead. On January 31, 2022, the
Diem Association announced the sale of its intellectual property and other assets related to the running of the Diem Payment Network to Silvergate Capital Corporation (Diem 2022). Diem’s announcement means that cryptocurrency has a long way to go to get approval from the regulatory authority.

It can be found that the international regulatory framework for data and cryptocurrency has been established, mainly based on the current securities law, anti-money laundering law (Al-Tawil 2023), and personal data privacy protection rules, and committed to adopting amendments to current laws and based on the digital economy, legislation regulatory rules are set. Under the current legal framework of the securities laws of various countries, there is no exemption for cryptocurrency issuers, which is equivalent to setting up a public company threshold similar to listed companies, and compulsory information disclosure and investor protection by the requirements of securities laws have important reference value for the future supervision and legislation of China’s cryptocurrency.

3 Legal Attributes of Cryptocurrency

To discuss the supervision of cryptocurrency, firstly the legal attributes of cryptocurrency must be clarified, that is, what kind of object is it in nature. Is it the object of creditor’s rights, the object of intellectual property, or the object of ownership? The characterization of legal attributes can help the accurate application of laws on the one hand, and provide clear guidance for subsequent legislation and amendments on the other.

3.1 The Object Positioning of Cryptocurrency

Firstly, should be discussed the creditor’s object of cryptocurrency. Does cryptocurrency have the nature of creditor’s rights, that is, can holders of cryptocurrency enjoy creditor rights because they hold cryptocurrency? Ordinary network virtual currency such as QQ coin is a centralized commodity, which is issued by network operators of central institutions such as Tencent company. Therefore, network virtual currency has the dual attributes of property rights and creditor’s rights. Network virtual currency holders have real rights to the human body other than the network operator, and they can exclusively control the network virtual currency. However, a cryptocurrency such as Bitcoin is a decentralized specific virtual commodity, and the holder of the cryptocurrency does not have the right to claim the central issuing agency. Therefore, cryptocurrency cannot be an object of creditor’s rights because it does not have the nature of creditor’s rights.
Secondly, whether cryptocurrency is an intellectual property object, intellectual property rights can be divided into creative intellectual property rights and commercial mark rights. Among them, creative intellectual achievement rights refer to copyright and patent rights, while commercial mark rights mainly refer to trademark rights. Whether it is the “ingenuity” required by the object of copyright or the “creativeness” required by the object of the patent right, the object of the right of creative intellectual achievement requires that its generation comes from the creative activities of the human brain. However, cryptocurrencies such as Bitcoin are produced by miners through “mining” and are “products” of computers, rather than specific products of human brain intelligence creation activities. Therefore, cryptocurrency cannot become the object of copyright and patent rights. To become the object of trademark rights, it is required to have an identification function, so that consumers can distinguish the source of goods or service providers. The holder of cryptocurrency holds a key, which is equivalent to a bank card password, and does not have the function of identifying the source of goods or services. Therefore, it cannot be the object of trademark rights.

The third is the ownership object of cryptocurrency. The main reason why some scholars oppose Bitcoin as an object of ownership stems from Article 2(2) of China’s Property Law. Zhao (2017) believes that to become an object of the property law, it needs to comply with the “things” and “rights stipulated by law”, and the “things” stipulated therein are limited to tangible things. Therefore, Bitcoin is not a legal right; at the same time, because Bitcoin is completely virtual, people cannot find the real carrier of Bitcoin and then think that it is not a physical thing. From this, it is finally concluded that Bitcoin cannot be an object of ownership (Zhao 2017). However, this reason is debatable. From the aspect of material manifestation, the distinction between “thing” is an understanding of the mechanical surface of “thing”. Tangible objects include real estate, movable properties, and objects that do not occupy a certain space or have a certain shape but can be controlled by human power, such as electricity, gas, light waves, and magnetic waves. It can be seen that the key to judging whether a property can become a thing stipulated by the “Property Law” lies in whether it can be controlled by people, rather than being judged from its physical manifestation.

The above viewpoint can also be confirmed by the difference between the object of intellectual property and the object of ownership. The reason why the object of intellectual property cannot be a “thing”, and juxtaposed with the object of ownership, is that people must rely on the law to control the object of intellectual property. The object of intellectual property rights, whether it is a technical solution or a work, the essence is a kind of information… Information is free, and the nature of information determines that it can flow freely… Since information is ‘free’, once the person who provides this information disseminates
the information, he cannot rely on his power to exercise exclusive control over the information. In contrast, people do not need to rely on the law for the object of ownership. As long as the object “thing” is physically possessed, it can be exclusively dominated and controlled. Cryptocurrencies such as Bitcoin conform to the definition of exclusive control of ownership and therefore have the nature of ownership object.

Whether a property can become the object of ownership is not a key factor in how it behaves physically, but whether it can be controlled exclusively by its power without relying on external forces. The money displayed in the current credit card, WeChat, and Alipay accounts is just a symbol, and even the stock in the stock account does not have a specific paper form. If none of these can be regarded as the object of ownership, the act of stealing money from another’s credit card account and stealing stocks cannot be regarded as a crime of theft. This does not conform to the increasingly virtual and digital form (Hu, Hu, and Cheng 2021) of financial assets. In the same way, it is absurd to deny the object of ownership if the tangible carrier of Bitcoin cannot be found.

Based on the above analysis, a cryptocurrency like Bitcoin is a decentralized specific virtual commodity, which does not have the nature of the creditor’s rights and cannot become the object of the creditor’s rights. At the same time, its production is based on the operation of mathematical rules, namely “mining”, which does not have the nature of intellectual property objects. However, in terms of control methods, there is no difference between cryptocurrency and the “things” of the ownership object, that is, to control them without relying on the law. Holders of cryptocurrencies can control them by holding and transferring funds themselves. Therefore, cryptocurrencies like Bitcoin should belong to the object of ownership.

3.2 Civil Law Protection of Cryptocurrency

After preliminarily determining the legal attributes of cryptocurrency as the object of ownership, it can be found that the court’s decision in the dispute case of unjust enrichment between Gao and Liu is questionable. First of all, from the perspective of fairness, the plaintiff’s property worth RMB 70,000 was possessed by the defendant, but the court ruled that the plaintiff lost the case, resulting in a loss of RMB 70,000 for the plaintiff, but the defendant gained gains for no reason. This is clearly against the principle of fairness. Secondly, on the one hand, the court recognized that Bitcoin was a virtual commodity, but on the other hand, because it was not a real currency, it inferred that Bitcoin was not protected by law in China, and even concluded that Bitcoin was illegal. This logic is wrong and contradicts the principle that “freedom is what the law does not forbid”.

The notice of the central bank only stipulates that Bitcoin does not have the same status as currency and should not be used as currency in the market. Still, it does not mean that the law does not protect Bitcoin, and it should even be deemed illegal by the negative evaluation of the law. The notice of the central bank recognizes Bitcoin as a commodity, which means that it is recognized as a legal property that should be protected by law, while the court’s approach is a misinterpretation of the notice of the central bank. Since Bitcoin is a kind of ownership object, it should be protected by property law. The central bank’s notice recognizes that Bitcoin is a specific virtual commodity. Even if the court believes that Article 92 of the General Principles of Civil Law should not be used to return illegitimate profits to protect Bitcoin holders, Bitcoin should at least be a commodity because it is the subject of the dispute. However, article 34 of the “Property Law” is applied to require the defendant to return the property claimed, to protect the interests of specific commodity owners. Therefore, at the current stage, when it comes to the protection of investors and consumers, cryptocurrency can be regarded as an object of ownership for protection.

Article 127 of China’s General Principles of the Civil Law stipulates that “where the law has provisions on the protection of data and network virtual property, the provisions shall be followed.” As a principled provision for the protection of data and network virtual property, this law establishes the principle of protecting data and network virtual property by the law. Especially when data becomes the fifth element after land, labor, capital, science, and technology, the protection for it will be unprecedentedly increased. At the same time, given the current disputes over the nature of the rights of data and network virtual property (Cheng and Liu 2022), it is necessary to conduct further in-depth research on the right attributes of data and network virtual property to summarize the experience of theory and judicial practice and provide a basis for future legislation.

### 3.3 Protection of Cryptocurrency in Criminal Law

Regarding the aforementioned phenomenon of “different judgments in the same case” for the theft of cryptocurrency, the reason is also whether cryptocurrency is a property protected by criminal law. The reason for determining that the theft of Bitcoin is the crime of illegally obtaining computer information system data is mainly because it is believed that Bitcoin is not property, and therefore it cannot be classified as the crime of property infringement in Chapter 5 of China’s Criminal Law. However, this conclusion is also debatable. On the one hand, the object of the crime of illegally obtaining computer information system data is public order,
but the act of simply stealing someone else’s private Bitcoin does not necessarily violate public order; On the other hand, the objective aspect of the constitutional elements of the crime requires that the data in the computer system be obtained by way of intrusion into the computer system or other technical means. The way to steal cryptocurrency is not necessarily reflected in the above-mentioned way. As long as the perpetrator has the key to other people’s cryptocurrency, he can take it as his own. From the above analysis, it can be seen that since cryptocurrency is the object of ownership in civil law, it can be regarded as property in criminal law, and the act of stealing cryptocurrency can constitute a crime of theft of property.

The prerequisite for the theft of other people’s cryptocurrency as the crime of theft is that it belongs to the crime of theft. Regarding whether the object of the crime of theft is limited to physical objects, China’s criminal law does not make specific requirements. Therefore, the criminal law of our country stipulates that the object of the crime of theft can be broadly understood. Professor Zhang Mingkai of Tsinghua University, an expert in criminal law, believes that the object of the crime of theft includes both narrowly defined property and property interests. The object of the crime of theft must have three characteristics: first, it has the possibility of management; second, it has the possibility of transfer; and third, it has value (Zhang 2016). Bitcoin as a cryptocurrency has the above three characteristics. First of all, Bitcoin holders can control and manage the Bitcoin they hold based on their private keys; secondly, Bitcoin can be traded, of course, with the possibility of transfer; third, the value of cryptocurrency is an indisputable fact. Although the volatility is huge (Liu and Serletis 2019), the value of each Bitcoin in recent years has been tens of thousands of dollars. Therefore, cryptocurrency belongs to the crime of theft, and the act of stealing other people’s Bitcoin can be regarded as the crime of theft. In the same way, in property crimes, the criminal objects of acquisition-type property crimes, such as illegal embezzlement and fraud, are the same as the crimes of theft, so they can be the objects of crimes such as illegal embezzlement and fraud. The behaviors regulated by other acquisition-type property crimes of illegally occupying other people’s cryptocurrency can also be regarded as corresponding acquisition-type property crimes.

The above discussion on the legal attributes of cryptocurrency hopes that the current civil law and criminal law can be applied to treat cryptocurrency as property. In the future, my country’s legislation should issue further detailed rules for virtual digital assets. It should be noted here that the law is not a panacea. The anonymity of cryptocurrency and other issues need to be resolved through technical measures such as regulatory technology. To balance innovation and risk and ensure global financial stability, it is necessary to establish basic cryptocurrency regulatory rules.
4 Establishing Cryptocurrency Regulation Rules

To meet the network security needs, China speeds up the legislation process in the cyber area. On January 1, 2020, the “Cryptography Law of the People’s Republic of China” came into effect. “Data Security Law” was adopted on June 10, 2021, and “Personal Information Protection Law” was adopted on August 20, 2021. The Chinese government hopes to regulate blockchain-based information services, and how implementing the rule of law into blockchain management is the key. On March 30, 2019, the Office of the Cyberspace Administration of China issued the “Announcement of the National Internet Information Office on Issuing the First Batch of Domestic Blockchain Information Service Record Numbers”. The first batch of 197 domestic blockchain information services received the record number. The second batch of 309 was filed. Although the filing is only the registration of the main body’s blockchain information services, it does not mean that the Cyberspace Administration of China recognizes its institutions, products, and services, but after all, it has taken the first step in the country’s supervision of blockchain.

It is very important to implement the rule of law in blockchain supervision to achieve a balance between innovation and risk. In recent years, a large number of P2P thunderstorms in the name of “Technology Finance” have sounded the alarm for the rule of law in blockchain finance. Industrial development must be synchronized with supervision, otherwise, it will cause huge losses to the public and government credibility. To achieve the goal of the rule of law of the blockchain, it is necessary to provide a completely legal basis for the supervision of the blockchain (De Filippi and Wright 2018). In the Securities Law supporting regulations and regulatory document legislation, an investor suitability management system for virtual digital assets can be established so that those who can take risks and those who dare to take risks to become the subjects of innovation.

As a novelty, the global flow of cryptocurrency will have a certain impact on financial stability, including risk exposure caused by the direct or indirect participation of financial institutions, the reputational impact of impropriety or inaction of financial regulators, and operational risks of encrypted digital assets brought by the application in payment and local currency settlement, wealth effects, and risks brought by the extremely volatile market value of cryptocurrencies. To maintain the stability of the financial market and prevent the impact of digital financial assets on the existing financial system, the regulatory measures adopted should be said to be timely and appropriate. However, the development of digital finance is not based on people’s will. The characteristics of cryptocurrency flow make it difficult for traditional financial firewalls to work. It is necessary to ensure that the constraints and implementation of financial regulatory laws can
keep up with the pace of digital financial development, and blockchain and
distributed ledger technologies can contribute to financial stability and can learn
from the Regulatory Sandbox system.

The British government proposed the concept of a regulatory sandbox in March
2015. As a safe space, the regulatory sandbox is a framework established by regu-
latory agencies to enable relevant companies to conduct small-scale field tests on
innovations in a supervised and controlled environment within a certain period,
enjoying special exemptions, acquiescence, and other limited exceptions. Fintech
companies can test their innovative financial products, services, business models,
and marketing methods in this safe space without being immediately bound by
regulatory rules when related activities encounter problems (Deloitte 2018). The
regulatory sandbox can enable more openness and dialogue between regulators and
digital financial service providers, and it can also enable regulators to quickly modify
and develop regulatory frameworks. Legislative and law enforcement agencies need
to take the lead in formulating relevant blockchain guidelines based on existing legal
rules. At the same time, they must also consider how to combine traditional legal
rules with current technical rules to give full play to their respective advantages and
better combine execution and flexibility.

China can refer to the UK’s regulatory sandbox system to supervise blockchain
financial companies, help these companies form a clearer corporate development
strategy, reduce the adverse impact of regulatory uncertainty on companies, and
provide better financing channels for the innovative development of the blockchain
field. China’s third-party payment, represented by Alipay and WeChat Pay, has
grown into a global benchmark for inclusive finance under a relatively loose regu-
latory environment. As of the end of 2018, the proportion of adults using electronic
payments was 82.39% (PBC 2019), which is far ahead in the world. The outstanding
practice of China’s digital economy and electronic payment provides a good refer-
ence for China’s next digital currency supervision.

In the current wave of global digital finance development, the establishment of
a national-level digital financial supervision sandbox and a timely summary of
successful experiences and failures can accumulate experience for future legislation
and amendments. The blockchain testing and supervision sandbox can be assem-
bled. The industrial sandbox is a virtual testing environment formed by many
companies in the industry. It can provide services for technology finance, customers,
entrepreneurial incubation, education and scientific research, and fund investment.
At the same time, sandbox technology also needs online monitoring to cope with real-
time changes in the blockchain system, because digital legal currency and digital
asset transactions are settled in real-time, and transactions are conducted 24 h a day,
a week, and a day (Leinonen 2023). If there is no real-time supervision, the
transaction is very easy to go wrong in progress. This requires the use of a “traditional supervision sandbox + industrial sandbox” for real-time supervision.

At present, China’s regulatory sandbox has been officially launched. On January 14, 2020, the Business Management Department of the People’s Bank of China (Beijing) announced the first batch of 6 pilots. The participants included commercial banks, clearing organizations, payment institutions, technology companies, and other institutions. The business involves the application of cutting-edge technologies in the financial field such as the Internet of Things, big data, artificial intelligence, blockchain, application programming interfaces, etc. The implementation of the first batch of pilot applications is an important measure to alleviate the dilemma of “loose supervision causes risks, and strict supervision stifles innovation”. As the blockchain will become a cross-border and cross-regional chain network, financial blockchains must learn from the principles of financial market infrastructure advocated by international organizations such as CPSS and IOSCO. Regulatory testing technology must keep pace with the times and be constantly updated (Cheng, Qiu, and Yang 2023). Regulatory sandbox technology needs to be continuously optimized with the development of blockchain technology. In the future, we can strengthen the development of regulatory technology (RegTech), adjust the intensity of supervision, and do good jobs in regulatory coordination, to protect financial consumers, help financial technology companies shorten the innovation cycle, and help regulators find potential risks early, and finally achieve the aim of promoting high-quality economic growth.

5 Conclusions

China should actively participate in the formulation of international standards related to blockchain and digital finance, connect with open-source organizations and organizations of international standards, strengthen exchanges between national and international standards, and continuously improve China’s international voice of blockchain and digital currency standards system. At the same time, in the supervision of blockchain-based cryptocurrencies, for blockchain technicians, we can learn from the “registered structural engineer” model of the national construction authority, and the technical architecture designed by them must stand the test of time. Just like the design of the bridge must be responsible for life, we strengthen their sense of responsibility, screen out those who are indiscriminate among the good and bad practitioners, and ensure that the blockchain products designed by the blockchain engineers have the basic technical standards and safety standards. For corporate managers involving cryptocurrencies, using for reference the financial industry qualification certificate system issued by financial regulatory
agencies can keep away from illegal fund-raising and other activities, establishing a blockchain and digital financial access standard system. It can carry a substantive review of blockchain financial companies, not just filing with the National Cyberspace Administration of China, and it can eliminate those companies that use the name of blockchain but do not have blockchain technology. For investors in blockchain finance, it can be learned from the Securities and Futures Investor Suitability Management Measures issued by the China Securities Regulatory Commission and the division of investors in the U.S. Equity Crowdfunding Act. It can make blockchain financial companies truly “Know your customers (KYC)”, and sell appropriate products to investors with equivalent investment ability and investment level to prevent financial risks. The blockchain financial supervision regulations which are established based on these rules will truly bring about the healthy development of blockchain finance in the new era and avoid repeating the mistakes of the blind development of P2P and insufficient supervision in previous years.

Acknowledgments: This paper is the phased achievement of “Key Project of Social Science Research of the Ministry of Education (21JZD035)”. I appreciate Hu Junze, Wan Jieru, Du Muzhen, Yu Zehui, and Liu Ziyue for their excellent research assistant work, and thank anonymous reviewers for their valuable comments. None of the above should be held responsible for any errors or omissions.

Research funding: This work was supported by Key Project of Social Science Research of the Ministry of Education, PRC (21JZD035).

Research ethics: Not applicable.

Author contributions: The author has accepted responsibility for the entire content of this manuscript and approved its submission.

Competing interests: The author states no conflict of interest.

Data availability: Not applicable.

References


**Bionote**

**Jiye Hu**

Department of Finance, Business School, China University of Political Science and Law, Beijing, China

Specially-appointed Professor, Krirk University, Bangkok, Thailand

jiyeh@cupl.edu.cn

https://orcid.org/0000-0001-9486-5889

Jiye Hu is a professor of law and finance, at the China University of Political Science and Law, and a visiting scholar at Oxford University, Duke University, and Erasmus University. He received bachelor’s and master’s degrees from Tsinghua University, and a Ph.D. in economics from the Graduate School of the Chinese Academy of Social Sciences. Before his appointment in 2006, he worked for the Beijing local municipal government and held various posts in the policy-oriented economic research field. In 2009, 2010, and 2017 he was appointed as a local senior expert at the EU-China Social Security Reform Cooperation Project. In 2011 he was appointed as a local expert on a joint project by the World Bank and