Legalization of Central Bank Digital Currency under Blockchain Industry

Yuting Hsu[1], Chengyong Liu[2*]

[1] *The Department of Ocean and Border Governance, National Quemoy University, Kinmen, Taiwan (R.O.C)*

[2] *School of Law, Jimei University, Xiamen, Fujian, China*

**Corresponding Author.*

Abstract

In recent years, private digital currency based on blockchain industry has caused many doubts, such as privacy infringement, money laundering tools, consumer protection and financial stability. However, as digital currency has gradually become the important issue, the central banks of various countries have already started to study the central bank digital currency (CBDC). In this paper, firstly, the concept of private digital currency and its derivative issues are explained. Secondly, based on the two chains scheme of the blockchain, a CBDC system is established to facilitate supervision, which stores and accesses transaction information and verification information separately to balance the user privacy security and the convenience of supervision. Meanwhile, the consortium blockchain is settled to the public chain to protect the reliability of the data. Moreover, although some countries have started to develop CBDC, laws and regulations which regulate various aspects of it are still deficient. Therefore, in this paper, in addition to proposing a general outline of the legal system regulating the CBDC, it also illustrates separately the monetary rights and obligations of the central bank, merchant banks and the public, which will be helpful for the future legal construction.

Keywords: *central bank digital currency (CBDC), blockchain industry, two chains scheme, legalization*

I. Introduction

Recently, there has been a growing interest in digital currency and a lot of controversy. For example, the well-known cryptocurrency exchange in July 2019 announced a suspension of services 12 days after being attacked by hackers, and its parent company claimed stolen funds of up to JPY 3.5 billion (approximately USD 32 million). For another example, Facebook's plan to issue the cryptocurrency Libra in 2019 has become a global focus, which has raised concerns about privacy, money laundering, consumer protection and financial stability. Even though digital currencies face many challenges, Central Banks have already envisaged the issuance of legal digital currencies. For instance, in 2019, the State Council of China formally carried out cooperation projects of central bank digital currencies (CBDCs), indicating that the importance of digital currencies is indubitable and that government issuance of digital currencies is more reliable than private. In this paper, to study the CBDC topic in the context of China, three levels are explored, including the concept of digital currency, the CBDC in the context of blockchain technology, and the legal architecture of China's developing CBDC.

II. Overview of Digital Currency

2.1 Definition and status

Digital Currency is a cyber currency based on node network and encryption algorithm, is issued and managed by developers, and can be used for practical goods and services transactions. According to the developers, digital currency can be separated into central bank digital currency and private digital currency. The latter usually refers to a scattered subjunctive currency which is not issued by the central bank, but generated based on Distributed Ledger

Technology (DLT) and can realize point-to-point transactions, such as Bitcoin (BTC), Ethereum (ETH), Ripple, Litecoin (LTC), etc.

Compared with other legal tender, digital currency's greatest innovation lies in the use of brand-new blockchain technology as a support, which is characterized by distributed decentralization, trust based on consensus, difficulty in tampering, traceability and high security. Therefore, the blockchain technology provides the possibility to realize digital cryptocurrency, which needs extremely complicated and sophisticated scientific and technological support. The blockchain uses various skills such as data store, agreement mechanism, encryption algorithm, point-to-point transmission, etc. to build a scattered distributed ledger database, which can calculate the value created by various participants or nodes in each stage through algorithms in a real-time, transparent and non-missing way. All participants' contributions, interactions, participation and influences in their business system will be reported in the block, their value recognition will be automatically displayed in their blockchain wallet in the form of digital cryptocurrency, and the value distribution process will be automatically realized through smart contact, thus eliminating all intermediate links such as confirmation, review and implementation, greatly reducing trust costs and improving economic efficiency [1-2].

2.2 Problems

Despite the appeal of the concept of private digital currencies such as Bitcoin, a number of risks have been exposed during the rapid development of the last decade, including the following aspects: [3].

(1) High price fluctuations: The lack of a national credit base for private digital currency issuance has led to frequent and sharp currency fluctuations in digital currency, with negative effects on financial stability. For example, Bitcoin, with a fixed limit on the number of issues and the difficulty of "mining", although it will not cause the inflation problem of the sovereign currency, it will cause large price fluctuations under the action of the market [4].

(2) Regulatory gaps: Because digital cryptocurrency is anonymous, decentralized and global, it can make cross-border barrier-free payments and transactions all over the world. Governments can't control its operation mechanism and supervise it. Hence, digital cryptocurrency has become the money laundry tool in various crimes, or the payment tool in various illegal transactions.

(3) Imperfect technology: The infrastructure of traditional financial markets has failed to meet the needs of developing the digital currency, especially the infrastructure for the issuance, management and storage of digital currency. Meanwhile, so far, blockchain and smart contract are cutting-edge technologies that are not yet fully mature, inevitably with flaws and loopholes, which lead to an endless stream of theft incidents in digital currency.

(4) Possibility of market manipulation: Due to the fact that the digital cryptocurrency is heavily owned by the oligarchs and the exchange of the digital cryptocurrency does not have a fair disclosure system like the stock exchange, it is impossible to truly avoid the falsification and falsification of the account books, thus making it possible to manipulate the private digital currency market.

(5) Insufficient consumer protection: Because of the decentralized, anonymous and tamper-proof nature of the transaction, it is hard to compel the restoration of digital currency once the transaction is in question, even if there is a legitimate repayment request, without the voluntary transfer of the current holder, making it tough for consumers to make up for their losses.

2.3. Positions of governments

At present, most governments do not recognize the legal status of digital cryptocurrency. The Chinese government,

for example, has imposed a number of bans on digitally cryptocurrencies, and the People's Bank of China has introduced several regulatory measures: (1) The *Notice on Preventing Bitcoin Risks* issued in December 2013 pointed out that Bitcoin is a specific subjunctive commodity that should not be used as currency in the market. (2) In September 2017, the *Announcement on Preventing Financing Risks of Token Issuance* was issued, which characterized ICO as an illegal financing act, requiring all kinds of token issuance financing activities to stop immediately, and requiring organizations and individuals who have completed token issuance financing to make arrangements such as repaying. (3) On August 24, 2018, the *Risk Tips on Preventing Illegal Fund Raising in the Name of "Virtual Currency" and "Blockchain"* was issued, which listed the financing risks of new digital cryptocurrencies including IFO, IEO and IMO.

Despite the above-mentioned strict regulatory measures, the Chinese government does not object to the digital cryptocurrency technology itself. The People's Bank of China maintains that digital currency can only have sustainable and effective development if it is endorsed by the national credit through legal issuance, and has started relevant research and planning [5]. In 2015, the central bank began to investigate some key issues in the field of digital currency and formed a series of research reports. In 2017, the People's Bank of China officially established the Digital Money Research Institute in Shenzhen. In September 2018, the Digital Monetary Research Institute of the Central Bank set up a platform for trade and financial blockchains.

III. The Application of Blockchain in Digital Currency of the Central Bank

On the premise of the existence of the concept of "state", private digital currency cannot be circulated together with legal tender, but blockchain and other technologies are worthy of reference by the legal tender, so the central banks all over the world are actively discussing the scheme of CBDC. Central bank digital currency (CBDC) is an encrypted string of numbers issued by a central bank or a monetary authority representing a specific amount that can be used to consume and trade real goods and services [6].

3.1 Key elements

According to the CBDC concept put forward by many countries (UK, Singapore, Canada, etc.), its key elements include: issuer (central bank or others), distribution carrier (M0, M1 or M2), technology (distributed ledger or more), entry threshold (open or restricted), anonymity (completely anonymous, anonymous or not anonymous), operation availability (seven days a week, 24 hours a day), whether to pay interest, etc., whose design determines the different operation modes and completely different impacts of the CBDC in the future.

In March 2020, the People's Bank of China developed the Digital Currency Electronic Payment (DCEP) based on blockchain technology. As a new encrypted electronic currency system, DCEP uses a two-layer operation system. In other words, the People's Bank of China first exchanges DCEP to banks or other financial institutions, which then exchange DCEP to the public. In August of the same year, the Ministry of Commerce of the People's Republic of China proposed that Shenzhen, Chengdu, Suzhou, Xiong'an New Area and other places should first carry out digital currency pilot programs. At present, the key elements of the CBDC in China are conceived as follows: [7] (1) The issuer is the central bank; (2) The issue object is M0 (equivalent to an electronic wallet); (3) The core technologies are big data, distributed ledger and other technologies; (4) The entry threshold is restricted; (5) It is anonymous; (6) Operation availability is uninterrupted; (7) No interest is paid.

3.2 The application of blockchain

Distributed ledger technology and encryption technology are still the core technology of some CBDC, while consensus algorithm is the core technology of distributed ledger. At present, the main consensus algorithms include: POW (Proof of Work), POS (Proof of Stake), DPOS (Delegated Proof of Stake), PBFT (Practical Byzantine Fault Tolerance) and DBFT (Delegated Byzantine Fault Tolerance), which consumes different power cost and other costs.

In addition, according to practical experience, POW is suitable for public blockchains (non-licensed), while PBFT is relatively suitable for private blockchains and consortium blockchains (licensed), but PBFT is more suitable for public blockchains when it breaks through the computing power limit. [8] At present, many central banks choose PBFT algorithm instead of POW algorithm when designing CBDC, or based on resource-consuming cost and non-disclosure.

Block chain technology provides a foundation of trust between participants for a decentralized system, but makes private digital currency no longer have centralized credit entities, which leads to regulatory difficulties. However, the CBDC based on block chain technology must be based on a regulatory basis [9]. In this paper, it is believed that the CBDC blockchain system should comply with the following requirements: (1) National supervision should be integrated into the system so that the regulatory authorities can supervise and trace the transaction information, and directly manage the account behavior; (2) As the blockchain technology is a distributed ledger technology in nature, the publicity of the account history transaction information is not conducive to the protection of privacy, so the equilibriums between both parties' privacy to the transaction and "openness and security of ledgers" needs to be considered on the basis that users accept supervision; (3) On the basis of meeting the above two conditions, users are allowed to participate in the consensus of the system as much as possible, and the credit decentralization of the block chain is fully utilized to establish the credibility of the system.

In order to achieve the above objectives, a CBDC system that is easy to supervise can be established through the two chains scheme: (1) Consortium blockchain is the core part of the system, with the internal members including banks, financial institutions and regulators, etc. These members are responsible for transaction confirmation and encryption and storage of complete transaction data, which can not only protect user privacy, but also serve as credentials in transaction traceability, and the central bank and other regulatory agencies can join the system operation and maintenance as participants therein. (2) In the public blockchain, each participant can be ordinary users, so that each user can take part in and demonstrate the system conservation, and the archieves can be utilized to confirm the account status, so that users have the ability to verify the effectiveness of the transaction after the transaction was initiated. The consortium blockchain reserve the data abstract in the public chain to prevent the alliance chain members from tampering with the message.

Therefore, the CBDC system that can be supervised under the two chains scheme should include three modules [8]: (1) User wallet: it is the originator of transactions in such system, and helps users direct their private and public keys and transactions, to provide convenience for users to query and use; (2) Alliance chain node (including supervision): it mainly undertakes the functions of transaction receiving, confirmation, confusion and packing into blocks; (3) Public chain node: it stores the transfer-in and transfer-out transaction records, which can be used as the credentials to verify the transactions and the user wallet's obtaining the account status.

Figure 1 shows the flowchart of the transaction of the CBDC system that can be supervised. In the system, there is an peer to peer relationship between the public chain node and the alliance chain node, but they process messages differently. These two parts can be regarded as servers, and the user wallet is the client that sends operation requests to the servers.

ISSN: 0010-8189

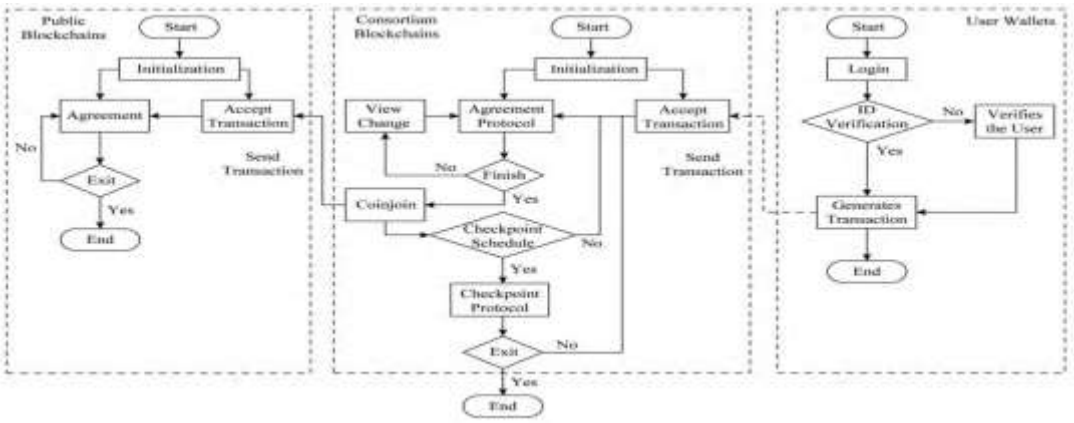

Fig. 1 The flowchart of the transaction

Figure 2 demonstrates a flowchart of the system's tracing back. The whole process merely exists between the alliance chain nodes. The Traceback Request node sends the traceback request to other alliance chain nodes including the supervision nodes. The other alliance chain nodes in Figure 2 include more than one node, which judge the request respectively, and the supervision node acquires the user identity after recovering the key.

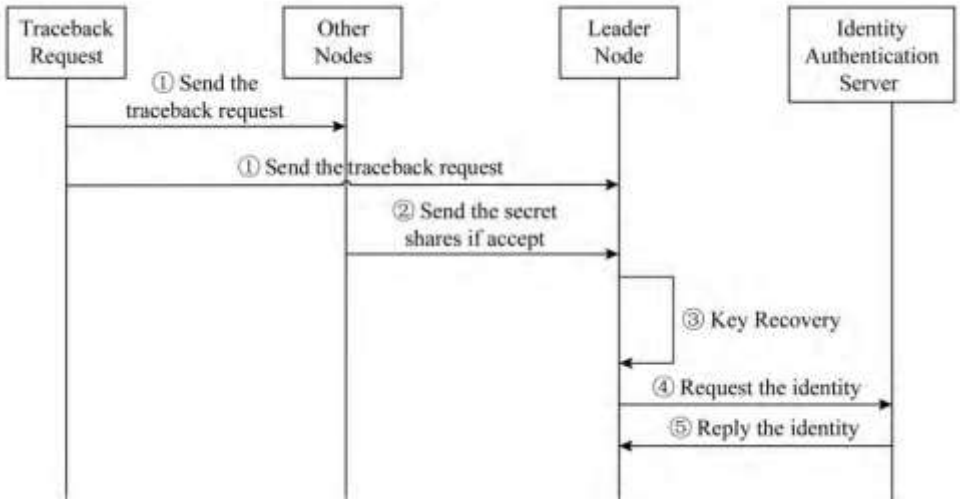

Fig. 2 The flowchart of the tracing back

IV. The Legalization of CBDC

Although countries all over the world have begun to develop CBDC, laws and regulations which regulate various aspects of it are still deficient. Therefore, in this paper, the following ideas are put forward focusing on the legalization of CBDC in China.

4.1 Overview of systems

The CBDC is a legal tender in the form of digital currency, as an alternative to the current legal cash or coins, with the same legal attributes as them. As the current electronic network skills cannot satisfy the demand that the central bank can pay in digital currency under any circumstances, the issuing and circulating CBDC cannot replace the legal cash and coins, but should coexist.

In terms of the issuance system, in the CBDC system with a double chains structure, the central bank issues digital currency directly to the unit or individual account in which it opens an account, and the CDBC transfers directly between the unit and individual account. Neither the central bank nor the third party entrusted by it directly manages the currency account, but only confirms the transaction in person or entrusts the third party to sustain the normal manipulation of the balance and payment system.

In terms of the circulation mechanism, in the "decentralized" monetary circulation mode, the currency transfer between different accounts is automatically realized by blockchain technology without the assistance of the Central Bank, merchant banks or paying agent institutions. Since the CBDC represents the credit of the central bank or the state, that in the customer account will not become bankruptcy property when it encounters bankruptcy of merchant banks or paying agent institutions, but only when the central bank or the state is "bankrupt", and it will not get interest income because of its legal tender nature, which has no value-added attribute.

The nature of an account should be interpreted as an instrument supplied by the central bank to the users for the custody, storage and payment of digital currency. The ultimate management of the account should be vested in the central bank, regardless of the direct management entity. However, the property rights of the CBDC stored in the account belong to the users of the account and it has independent property ownership rights, indirect control rights, absolute payment rights and payment priority over the digital currency.

In terms of regulatory relationship, the content of the supervision of the CBDC is not much different from that of the traditional monetary behavior supervision, including currency forgery, alteration, money laundering, tax evasion and other monetary violations. However, the paper assumes that CBDC is more effective in terms of supervision, because firstly, every monetary circulation has a shared complete record on the strength of the use of blockchain, which will make it very difficult to forge or alter legal tender, and even make many illegal and criminal acts committed by using the independence of legal tender impossible to realize; secondly, under the digital currency system of the central bank with a double-chain structure, the regulators, as participants in the alliance chain, will advance monetary circulation supervision and prevent illegal and criminal acts without violating the system and regulations of monetary circulation.

4.2 Monetary rights and obligations of the central bank

As far as the monetary power of the central bank is concerned, since the CBDC is a new type of legal tender, whose core monetary power should belong to the central bank, or else it will inevitably lead to the confusion of the whole monetary issuance and circulation system, including: the right to issue money, the right to issue proceeds, the right to manage the system, the right to authorize management, the right to make regulations and the right to supervise management. Therefore, China should build up the existing laws and regulations by: (1) amending the *Law of the People's Bank of China* and the *Regulations of the People's Republic of China on the Administration of Renminbi* and other legal documents to clearly stipulate the central bank's right to issue digital currency; (2) amending the current *Law of the People's Bank of China*, the *Basic Accounting System of the People's Bank of China* and other relevant legal documents to uniformly account for the statutory cash, coins and the issuance proceeds of the CBDC as the issuance proceeds of the statutory currency; (3) amending the existing laws and regulations such as the *Law of the People's Bank of China*, the *Law of Merchant banks*, and the *Measures for Payment and Settlement*, so as to clearly stipulate the central bank's right to manage the central bank's circulation system in digital currency; (4) amending the existing laws and regulations, such as the *Law of the People's Bank of China*, *Regulations on the Administration of Renminbi* and the *Law of Merchant banks*, to give the central bank the power to authorize merchant banks or paying agent institutions to operate and manage the digital currency system specifically, so as to prevent the complexity of the central bank; and (5) allowing the central bank to have the power to promulgate the "Digital Currency Rules of the Central Bank" according to the needs, so as to regulate the payment and settlement and system management behavior of the CBDC.

As far as monetary obligations of the central bank are concerned, the central bank should not only enjoy the necessary digital currency power, but also undertake the following monetary obligations clearly stipulated in relevant laws and regulations: (1) System maintenance: The central bank must perform the final maintenance obligation for the CBDC issuance and circulation system whether the central bank independently operates or entrusts other financial institutions to operate and manage; (2) Payment: The issuance and circulation expenses of the CBDC, mainly including system construction and maintenance expenses, right authentication expenses, network resources expenses, etc., should be paid by the central bank in principle. Only the CBDC circulation fee that is directly related to the interests of the merchant banks or paying agent institutions and is beneficial to their operation in the operation and management of the relevant business can be considered to be jointly borne by the central bank and the merchant banks or paying agent institutions, or fully borne by them. (3) Loss compensation: The obligee of the CBDC may incur losses because of various system-related factors. Once the monetary obligee claims that his/her monetary property has suffered losses, the central bank or the operating institution must bear the burden of persuasion, and as long as it and as long as it cannot prove that the obligee's claim is not valid, it must bear the liability of compensation, which is not only the obligation of the central bank to the monetary obligee, but also the obligation of the digital currency operator. (4) Privacy protection: The CBDC must be circulated in the specific network system set up by the central bank or merchant banks, and its circulation records have obvious problems in protecting the privacy rights of users in digital currency. Therefore, the right to privacy protection obligation of the central bank must be clearly stipulated in the law, which should be the basic obligation of the central bank even under the condition that other financial institutions operate as agents.

4.3 Monetary rights and obligations of merchant banks

As far as the rights of merchant banks are concerned, merchant banks should have the following the rights under the CBDC system, and the current legislation should be amended accordingly. (1)Agency operation: For the purpose of realizing the connection of monetary circulation system between central banks and merchant banks or paying agent institutions, the central bank shall endow merchant banks or paying agent institutions with the right to act as agents for digital currency issuance and circulation business of some central banks. (2)Identity examination: For the purpose of effectively preventing crime and keeping circulation records in the system for any transaction, it is necessary to give merchant banks or paying agent institutions the right to check the identity of customers in the process of operating and managing the digital currency system as agents of merchant banks or paying agent institutions, which is also their obligation. (3)One-way charging: Merchant banks or paying agent institutions should have the right to charge the central bank the agency operation and management fees, because they cannot charge the people who use the central bank digital currency with legal tender attributes.

As far as the obligations of merchant banks are concerned, since merchant banks or paying agent institutions enjoy the agency right of the CBDC system, they should undertake the following obligations in the CBDC system, and the existing laws and regulations should be amended accordingly. (1) Agent maintenance: As the operator of the CBDC system, they should also undertake the obligation of maintaining the system; (2) Audit and certification: because the central bank does not actually operate the system, it lacks the ability to deal with the central bank's digital monetary circulation system. In this case, merchant banks or paying agent institutions should accept the obligation of audit and certification of circulation behavior and payment settlement; (3) Review of illegal acts: As the main body of the first line operation, merchant banks or paying agent institutions are more able to accept the obligations of tracing tax evasion, money laundering, terrorist acts or other illegal acts of users.

4.4 Monetary rights and obligations of the public

The monetary rights of the public are different from the common legal monetary rights in the following aspects, and the current legislation should be amended accordingly: (1) Currency exchange: In order to avoid affecting the completeness of the legal monetary system and the orderliness of monetary circulation, unconditional exchange

between the CBDC and the legal cash or coins must be conducted freely without limitation by the different attributes and different financial needs; (2) Absolute payment: As long as it is a true CBDC that satisfies the statutory demands, the holder shall have the absolute right to payment. No matter whether the means used by the public to obtain the digital currency is legal or not, it will not affect the enjoyment of its monetary property rights. It must guarantee its absolute right to payment, and the payee shall not refuse to accept it. (3) Confirmation of payment: Under the condition of deposit currency payment by the CBDC, the confirmation right of currency payment shall belong to the monetary property owner, and the payment shall have legal effect as long as the statutory payment confirmation conditions are satisfied. (4) Claim for compensation: The loss of money and property in the CBDC account due to factors not attributable to the public shall be borne by the network operation and maintenance organization. As long as the public put forward the claim of property compensation, network operation and maintenance organizations should assume the responsibility of compensation in advance, for the purpose of ensuring the normal operation of the network monetary circulation system.

As far as the monetary obligations of the public are concerned, except as the general obligations of legal tender, the public also needs to undertake the following special obligations, and the current legislation should be amended accordingly: Rule compliance: The public should abide by the legal network payment rules of digital currency, and receive and pay money in accordance with the rules; (2) Pay in good faith: The payers shall pay in legal currency in accordance with the principle of good faith, and shall not cheat the payee; (3) Reasonable care: It requires the obligee to properly keep his own digital currency storage equipment, as well as the electronic signature or "private key" on behalf of his own identity in the currency payment network, to fulfil his reasonable duty of attention and to prevent others from performing monetary acts in a manner that infringes the interests of the obligee by impersonating the identity of the obligee. Otherwise, the obligee shall bear the responsibility for the loss caused therefrom and claim the right to the infringer by himself other then the digital currency payment and settlement system.

V. Conclusions

The progress of private digital currency has faced many challenges and risks. Thus, countries around the world have started conducting research and experiment on the CDBC. However, on the premise that all technologies are sufficient to support the CBDC, the central bank must be granted relevant legal power by law to issue. Therefore, it is urgent to discuss the legal structure of the CBDC, and the Chinese government must gradually clarify the rights and obligations among the people involved in the CBDC relationship in the legal system.

Acknowledgements

This research was supported by National Social Sciences Fund of China (Grant No. 20CFX006).

References

[1] Wang Hao, Song Xiangfu, Ke Junming, et al: Blockchain in Digital Currency and Privacy Protection Mechanism [J]. Netinfo Security, 2017, (7): 34-35.
[2] Sasson E B, Chiesa A, Garman C, et al. Zerocash: decentralized anonymous payments from Bitcoin. In: Proceedings of IEEE Symposium on Security and Privacy, 2014. 459–474.
[3] Chen Jian and Zhao Xue: International Experience and Enlightenment on the Development Status and Supervision of Digital Currency, China Price, November 2018, P. 45.
[4] Yang Yang, Jing Chunyu: Prospects for Digital Money of the Central Bank of China Based on Blockchain Technology, China Market, No. 14, 2017 (No. 933 in total), P.14-15.
[5] Fan Yifei: Theoretical Basis and Structure Selection of Digital Currency of the People's Bank of China [J]. China Finance, 2016, (17): 11-12.

[6] Wang Sheng: Statutory Currency Control Based on Blockchain Technology. Shanghai Finance, 2017, (1): 24-25.
[7] Zhou Li et al.: Understanding and Suggestions on Digital Money Related Issues of the Central Bank, Bankers, 2018, (10), 131-134.
[8] Zhang Jianyi et al.: Regulatable Digital Money Model Based on Blockchain, Computer Research and Development, 2018,55(10): 2219-2232.
[9] Li Nanyu: Opportunities and Legal Issues for the Central Bank's DCEP, Special Zone Economy, 2020, (381): 18-22.

ISSN: 0010-8189