Prospects for the Development of Digital CNY

Yuan Fu *

School of King's College London, London, United Kingdom

*Corresponding author: K21160758@KCL.AC.UK

Abstract. After decades of development, digital currency has been recognized worldwide. But the current private cryptocurrencies in the market, including stable coins, don't have the potential to become a unified currency. In this context, central banks of global countries have also started research on currency digitization. The People's Bank of China started research on the digital CNY in 2014, which will help the CNY escape the control of the USD and help it dominate the world currency field. After nearly ten years of development, the feasibility and development path of digital renminbi have basically formed a definite idea. However, the development prospects of the digital CNY still face issues related to the degree and method of Block Chain integration, the impact on sovereign currencies, and decentralization. This article will give a theoretical basis and policy suggestions on the development feasibility and development prospects of the digital CNY through a brief introduction and function analysis.

Keywords: Digital currency; block chain; derivatives.

1. Introduction

A digital currency is an unregulated, digitized currency, usually issued and managed by a developer, accepted and used by members of a specific virtual community [1]. But it is different from virtual currency and electronic currency: digital currency can be exchanged and exchanged back with real currency at a certain rate, and its value is not determined by other currencies. It can be considered as a legal currency existing in the applicable community [2].

This article will gradually introduce the concept of digital CNY through a brief introduction to the history of digital currency development and Block Chain technology, and analyze the development prospects and development routes of digital CNY through functions. Secondly, it will briefly introduce derivatives and the possibility of combining digital CNY with derivatives. At the end, it summarizes the full text and gives policy recommendations.

1.1 Private Digital Currency

According to different methods of assignment, private digital currencies can be divided into two categories: one is native tokens based on the Block Chain, also known as encrypted digital currencies; the other is digital currencies that are issued and operated on the Block Chain but supported by assets outside the chain, also known as stable currency.

The development of cryptocurrencies has gone through three stages:

E-Cash stage: Invented by David Chaum in 1993, E-Cash is considered to be the prototype of digital currency, but it did not attract the attention of many new users because it did not choose a suitable partner.

E-Gold stage: In 1996, Douglas Jackson was committed to creating a digital currency independent of government control, so E-Gold came into being. E-Gold promoted the globalization of digital currency in the early 21st century. Unfortunately, due to technical loopholes that were often used by lawbreakers for money laundering and other activities, it went bankrupt under government pressure in 2009.

Bit-Coin stage: While the digital gold currency is developing, the cryptocurrency has not stopped. In 1997, Adam Back invented HashCash in order to solve the problem of spam attacks. And this is the rudimentary form of proof-of-work in Block Chain technology. In 1998, Wei Dai created B-money, which is the prototype of the distributed system in the current Block Chain technology. In the same year, Nick Szabo proposed a revolutionary new digital currency system - Bit Gold. In addition,

he wrote the pioneering work of smart contracts "Smart contracts" in 1994. So far, the core technologies of the Block Chain: public key encryption, proof of work, distributed systems, and smart contracts have all emerged.

Finally, in the context of the 2008 financial crisis, the "Bitcoin White Paper" initiated by Satoshi Nakamoto proposed a decentralized, peer-to-peer network and consensus initiative, open source code, and Block Chain as the bottom layer a brand new cryptocurrency for technology [3].

1.2 Stable Coins

Stable coins use a series of legal currency-denominated assets as reserve assets, and the value of the currency is more stable than that of cryptocurrencies [4]. On the one hand, stable coins can take advantage of the characteristics of real-time transactions, programmable, open and anonymous that distributed ledgers have. The "Triffin Dilemma" of currency existence. However, since the issuer of the stable coins is an unofficial organization and is not restricted by national borders, without the restriction of a global unified regulatory framework, there is no credibility to ensure the safety of reserve assets, the transparency of reserve asset management is not clear, and the issuance is not clear. The rights and responsibilities of holders and currency holders will lead to instability in the value of stable coins.

1.3 Central Bank Digital Currency

The initial development of digital currency exists in the form of private digital currency. Private digital currency is usually issued by a single individual or institution. In the early stage, customers are attracted to the core community through the "consensus of faith", and in the later stage, customers are tied to the community through the "consensus of the system", so as to maintain the currency circulation and sustainable and stable development [5]. From the perspective of development model, the value of private digital currency is supported by consensus and traffic. The complete decentralization of a private digital currency means that its value cannot be manipulated by humans, and not being tied to legal tender means that its value is not comparable. Therefore, private digital currency is not universal, and its development is also limited.

The emergence of digital currency has subverted the existence, circulation and payment methods of traditional currency. Although the threat of private digital currency to the legal currency market has prompted the central bank to actively participate in the research of legal digital currency, the development of private digital currency proves its essence. There is a contradiction in this aspect: the contradiction between completely relying on the degree of consensus to form a value scale and not being universal. This means that the development of digital currency should be decentralized, but not completely decentralized. Therefore, in this context, the emergence of central bank digital currency provides new feasibility for the development of digital currency.

About CBDC, this article mainly focus on the digital CNY. There are two reasons for the proposal of the digital CNY: First is to conform to the current international financial development trend and the second is to get rid of the financial control of the dollar.

Although the financial order led by the US dollar has caused dissatisfaction around the world, the BIS survey report shows that the influence of the US dollar is still growing. China has already started research on digital CNY in 2014, and the development of digital CNY may bring a new turning point to Sino-US relations. Before the hegemony of the US dollar, the development of digital CNY can provide strategic advantages in three aspects.

First, the central bank's digital currency provides a new solution for the global settlement system. The digital CNY’s separation from the U.S. dollar for payment can effectively weaken the hegemony of the U.S. dollar.

Second, China's cooperation with its major currency partners can increase the scope of application of the digital CNY and reduce the share of the US dollar in the international market.

Third, the leading position in the research of digital CNY may give China the opportunity to formulate new rules for the international financial system.

2. Block Chain

Block Chain is a trusted technology derived from but surpassed Bitcoin. The innovation of Block Chain technology not only gave birth to various private digital currencies, but also aroused extensive interest and exploration of central banks in various countries. At present, most central bank digital currency experiments are carried out based on Block Chain technology, but whether CBDC adopts Block Chain technology is still controversial. A typical view is that there is a conflict between the decentralization of the Block Chain and the centralized management of the central bank, so many scholars believe that CBDC should not adopt this technology [6].

2.1 Differences between CBDC and Block Chain

Combining the central bank's digital currency demand and the basic situation of Block Chain technology, the differences between the two can be roughly divided into three points. Now this paper will study these three differences in detail. The details are as follows.

2.1.1 Differences between decentralization and the top-level structure of the CBDC

The central bank's digital currency requires that while optimizing transactions through new technologies, it’s essential attributes as national legal tender cannot be shaken in the slightest. Therefore, the central bank, as the continuation basis of the country's legal currency - the direct agent and actual execution department of the endorsement of national power, must also insist on its core position in the key links of currency stock and flow management, monetary policy formulation and transmission, etc. in the Block Chain system. The highest authority and macro-control ability over other nodes. This runs counter to the design philosophy of Block Chain decentralization [7].

2.1.2 Differences between private key dependence and CBDC audience universality

Asymmetric encryption system is the cryptographic basis of Block Chain technology. We can use the non-linear correlation between the independent variable of the HASH function and the increment of the dependent variable, and cooperate with the important fact that the public key and the private key of encryption problems such as RSA, D-H, and elliptic curves cannot be interpreted mutually, to realize the security in the non-trusted public network environment’s trade safety.

Block Chain technology has a deep-rooted dependence on private keys. The holders of the central bank's digital currency are ordinary people with different ability to accept new things. They need to use legal tender with low threshold, especially legal tender that can tolerate their various negligence and can quickly respond and recover damages. The unique location of private keys in the Block Chain would be a heavy burden on their convenient and safe use.

2.1.3 Differences between the visibility of the transaction information and the confidentiality requirements of CBDC

Block Chain technology uses the unique transaction records of the main chain instead of the respective balance records of the nodes to judge the feasibility of the transaction.

Further considering that the central bank's digital currency will inevitably require the real-name authentication of the user's address, then this part of the information is not only a micro-account of national economic activities over a period of time, but also a detailed account of the currency holder's personal receipt and payment behavior. It has very important political, economic and social significance. Once leaked, it will not only mean that the key data of the national economic operation dynamics will be exposed to the outside world, but will also arouse the sensitivity and concern of the majority of currency holders to the exposure of personal privacy. The central bank must ensure that members of the consensus circle including itself store it safely, use it reasonably, and keep it strictly confidential.

2.2 Block Chain Technology Helps the Development of Digital CNY

Central institutions, governments, and enterprises have never dominated the market alone. In all economic research, the topic of discussion is always which side can better guide the market under any condition [8].

Although the core of Block Chain technology is decentralization, the central bank's digital currency may not be able to learn from and combine with Block Chain technology. On the contrary, it turns out that the central bank's digital currency should be combined with Block Chain technology to better stabilize the market and replace physical currency. This paper can discuss the feasibility from the following three points.

2.2.1 Construct a two-circle system of alliance chain with separation and coop

The alliance chain double-circle system is built based on the BFT consensus. It is a Block Chain form with a small number of top-level nodes but strict hierarchical control of permissions.

The consensus circle in the dual-circle system is composed of the central bank and commercial banks. All Block Chain transactions need to be confirmed by relevant authorized members of this layer, broadcast and written into the main chain.

The central bank is at the core of the consensus circle, performing the functions of member control, data maintenance, and process management. Maintain the stable and orderly operation of the main chain, participate in the consensus of each transaction data, and independently have the highest read and write permissions for all blocks of the main chain.

Commercial banks are responsible for the transactions within their authority and jointly maintain the valid data of the main chain with the central bank. In addition to the functions in the Block Chain system, the original currency-related functions of the central bank and commercial banks are still maintained.

In the trading circle of the double-circle system, holders of central bank digital currency who do not have any data writing authority fully participate in the transaction at the address-to-address level by initiating or responding to transaction information, receiving transaction results, and executing actual delivery. Other transaction links are completed and fed back by the consensus circle.

The two-circle system of the alliance chain adopts the double-layer design of the consensus circle and the transaction circle to realize the separation and cooperation of transaction response and confirmation. The consensus circle with strong control has defended the core position of the central bank's currency, while the transaction circle that fully embodies the advantages of Block Chain technology has realized the convenience, speed and low cost of the central bank's digital currency for retail transactions.

2.2.2 The commercial bank accepts the entrustment to become the actual executor of the transaction

On the basis of the double-circle system, further consideration can be given to separating transaction willingness and actual operation.

The transaction initiator entrusts the transaction information including input, output and amount to the commercial bank, and the entrusted bank needs to complete the management of customer identity, address and private key, and back it up with the central bank in real time. Afterwards, the transaction information is converted into a Block Chain format, and then encrypted and packaged with the corresponding private key of the transaction initiator and sent to the central bank. The central bank performs address mapping according to the content of the information and distributes the transaction information to the entrusted bank of the counterparty. The entrusted bank of the counterparty compares the plaintext processed by HASH with the digital signature processed by the public key. Finally, after the central bank confirms that it is correct, it will broadcast the result to the members of the consensus circle and cooperate with the corresponding authority members to carry out distributed bookkeeping, and the transaction process is completed.

2.2.3 Multi-pronged technical means to prevent core data leakage

In order to ensure the security of data, first of all, this paper should strengthen the concurrent processing to cope with extremely high pressure peaks, as well as the technical reserves in queue strategy, data stack, and deep search and delay suspension. Consolidate the foundation of the technical framework of the system. Secondly, for members of the consensus circle who have the necessary access to historical transaction information, multi-dimensional and rigorous technical means should be further adopted to limit their additional exploration and recording of core data. Including but not limited to serious rights management. Ensure that commercial banks can only process transaction data, perform transaction operations, manage transaction content, and maintain transaction networks within the scope of their own node authority settings.

Strengthen backtracking control to ensure that commercial banks automatically backtrack and temporarily store transaction records only in the necessary verification links of transactions. Moreover, the results are automatically and forcibly cleared after the process ends, and any form of manual backtracking is absolutely prohibited. Restrict consensus operations to ensure that commercial banks only add valid transaction blocks at the end of the main chain when reaching a consensus, and cannot use the open transaction exposure at this time to explore the content of the main chain against the direction of data flow.

3. A New Generation of Legal Currency

The technological innovation brought about by private digital currency will be the trend of building digital currency in the future. However, if private digital currency participates in circulation as currency, it will inevitably conflict with sovereign currency. It can be seen that under the premise of the existence of the national concept, private digital currency cannot be circulated together with sovereign currency, but technologies such as Block Chain are worthy of reference by sovereign currency.

3.1 Feasibility

The practical feasibility that the central bank must have for issuing digital currency is as follows:

3.1.1 The issuance and circulation costs of physical currency are high

From the perspective of issuance, the manufacturing process of my country's currency is complicated and consumes manpower and material resources, and the manufacturing cost of circulating coins even exceeds its own face value.

From the perspective of circulation, banknotes of different denominations have different degrees of wear and tear due to different frequency of use, so the service life of banknotes is limited, and the central bank has to recycle old banknotes and issue new ones.

In contrast, the issuance cost and circulation cost of digital currency are negligible.

3.1.2 The whereabouts of the current currency is difficult to control

Our country mostly uses monetary policy to adjust the money supply, thereby driving the economy back to the normal track. However, when the economy is in a downturn, the market sentiment is pessimistic. The additional currency issued by the central bank is often not flowed into the real economy, but is invested in the financial market, which reduces the effectiveness of monetary policy. The unknown whereabouts of funds will affect the monetary authority's control over my country's economy. At the same time, there are many problems caused by cash, such as money laundering and other illegal transactions, because cash is not easy to be tracked and monitored, criminals will use this feature of cash to disrupt social order. The distributed ledger technology applied in the digital currency can transparently record each transaction, and at the same time openly back it up at each node. The central bank can use this technology to monitor the flow of funds in real time, which can not only cut off illegal and suspicious transactions, but also control the currency. The real destination

of the currency issued by the policy, while realizing macro-control, maintains the stability of the country.

3.1.3 Government credit is a powerful guarantee of currency value

Currency has gone through a long development stage: from general equivalents to metal currency, and then to today's credit currency. Its intrinsic value has actually been separated from itself, but attached to the credit of the issuer. For the residents of a country, the most trustworthy issuer is the monetary authority. Monetary authorities issue digital currency with government credit as a guarantee, which can not only consolidate the status of sovereign currency, but also create a better payment environment with the times.

3.1.4 The driving force of the Internet+ era

As the development direction of my country's new era, "Internet +" advocates the combination of traditional industries and the Internet, so as to promote the progress and innovation of traditional industries. In this context, currency is the carrier of finance. If Internet technology is used to change its form of existence and form a new payment system, it will bring convenience to various transaction activities.

3.2 Function Analysis

From a mathematical point of view, this paper can also construct a functional relationship to prove that the digital CNY has the conditions to get rid of physical currency and become legal tender.

First of all, it is clear that the premise that currency can circulate is that there is demand, and the condition that currency can exist is that currency has intrinsic value. It is assumed that the digital CNY (hereinafter referred to as DCNY) and the CNY (hereinafter referred to as CNY) have a 1:1 exchange rate (1DCNY=1CNY) to determine the value of the initial DCNY. Logically, as the value of DCNY increases, the degree of exchange between DCNY and CNY will increase infinitely, and will eventually reach 1DCNY=∞CNY. In terms of functional relationship, the value of DCNY has a power function relationship with the degree of credit.

This paper assumed that, the initial value of DCNY is determined entirely by the value of the RMB without a premium. Secondly, we know that the development of digital currency depends on circulation and stock. Here this paper can use the number of customers to express it simply, and the number of customers can be expressed as the degree of currency credit. Because the number of customers is limited and the decreasing trend increases, the growth of credit degree also shows a decreasing trend. This shows that with the infinite increase of the credit degree, the growth trend of DCNY tends to be stable, and the logical relationship between the value of DCNY and the credit degree is a logarithmic function relationship.

Let the value of DCNY be Y, the degree of credit be x, the degree of exchange of DCNY be μ, the coefficients a, b are greater than 0 and Y, x, μ are all greater than 0. The following functional relations can be obtained from the analysis:

$$Y = [\log_a(X + 1)] + 1 \tag{1}$$

$$\mu = b^Y \tag{2}$$

The functional relationship between DCNY exchange degree and credit degree can be obtained by combining the formulas (1) and (2):

$$\mu = \frac{b}{\log_b a}(x+1) \tag{3}$$

It can be seen from formula (3) that the degree of exchange is completely linearly correlated with the degree of credit, but whether there is a positive correlation or a negative correlation is determined

by the coefficients a and b. According to the above functional relationship, this paper can preliminarily judge:

The a and b coefficients require human intervention, that is, complete decentralization is not advisable, and there should be appropriate policy regulation.

The value of the digital CNY can be completely independent of the physical CNY.

4. Derivatives Market

Before the popularity of digital currency, derivatives have become widely used financial instruments in the traditional financial industry. Derivative products determine the value of the general underlying assets, and sign a contract between two or more parties to settle at the agreed price before the maturity date. Typical derivatives include forwards, futures, options and swaps, etc[9].

In the cryptocurrency market, the two most common types of derivatives are futures and options contracts. Digital currency derivatives can be officially traded on traditional exchanges and regulated digital currency exchange.

Major digital currency exchanges are also actively participating in digital currency derivatives transactions. The current digital currency derivatives market is mainly divided into two categories: one is bitcoin and mainstream currency derivatives transactions, and the other is altcoin derivatives transactions. Headquartered in Malta, OKEX focuses on Bitcoin and mainstream currency derivatives transactions, providing futures and perpetual swap transactions, which is a contract with no expiration date and a leverage ratio of 100 times, and through an optimized, scalable the engine trades these contracts. Supports a range of popular encrypted assets such as Bitcoin, Ethereum and EOS, and also newly launched stable coin USDK [10].

In the early stage of digital CNY development, it is entirely possible to learn from the development path of the private digital currency derivatives market. The issuance of digital CNY will inevitably challenge the exchange of traditional currencies in the future, but through derivatives transactions, this paper can intervene in advance to control the future exchange range within the range we want. Secondly, through the derivatives market, this paper can build more ecological chains of digital CNY. While bundling and comparing with other currencies, it can also be integrated and annexed at the right time, so as to expand and consolidate the market share of digital CNY.

5. Conclusion

To sum up, the development of digital CNY is necessary and fully feasible, and during the development of digital CNY, this paper discussed that its centralization can be preserved, and we must respect the market However, the market regulation principle cannot be allowed to maximize the development freedom and market freedom of the digital CNY. In the development process of digital RMB, we can and must use Block Chain technology, which will ensure a high degree of freedom for digital RMB. However, while introducing Block Chain technology, it is necessary to complete the construction of a separate and collaborative alliance chain double-circle system to ensure commercial banks are entrusted to become the actual executors of the transaction, and implement multi-pronged technical means to prevent core data leakage. From a mathematical point of view, it can also conclude that the development of digital CNY is not necessarily a confrontation with mainstream currencies. The existence and development of digital CNY is feasible and theoretically based. The most important thing is that the prospect of digital CNY becoming a new generation of legal currency is huge, and its strategic significance is also huge. It is an area where we must strive for the right to speak in the next financial era.

References

[1] Zhou YongLin. The Nature and Future of Cryptocurrencies. China Finance, 2018.

[2] Ba ShuSong. The Development Status and Trend of Global Digital Currency. Expert Perspective, 2020.

[3] Satoshi Nakamoto. Bitcoin White Paper: A Peer-to-Peer Electronic Cash System: satoshinakamoto.me/bitcoin.PDF. 2008.

[4] Lyle Brainard, LiPeng, HeLe. Digital Currency, Stable Currency and Future Challenges. China Finance, 2020(4):2.

[5] Sheng SongCheng, Jiang YiLe. Central Bank Digital Currency Is The Real Currency. China Finance, 2016(14):3.

[6] Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptocurrencies and Privacy-Preserving Smart Contract. IEEE, 2016.

[7] People's Bank of China E-CNY Research and Development Working Group. Progress of Research and Development of E-CNY in China. 2021.

[8] Xiao Feng. Block Chain and Cryptoeconomics. National Economics Foundation. 2018.

[9] Krishnan R, Schlegel H B, Pople J A. Derivative Study on Configuration-Interaction Theory. Journal of Chemical Physics, 1980, 72(8):4654-4655.

[10] Wu XueYing. The Current Situation and Prospect of Encrypted Digital Currency and Its Derivatives - Discussion on Bitcoin. Data, 2020(007):000.