# CONCEPTUAL PROTOTYPE OF CHINESE DIGITAL FIAT CURRENCY

*YAO Qian*
*General Manager of the China Securities Depository and Clearing Corporation and former Director-General of the Institute of Digital Money of the People's Bank of China*

## INTRODUCTION

**Design of Chinese digital fiat currency (DFC) follows the basic idea that it should be a PBOC-led initiative where digital currency based on encryption algorithm be issued in parallel with physical cash, and the DFC would be part of M0.**

**Governor ZHOU Xiaochuan of the People's Bank of China has made full elaboration in a series of speeches on the theoretical basis and design concepts of Chinese digital fiat currency (DFC), based on which we should draw upon international knowledge and experience and conduct in-depth analysis of the core technologies regarding digital currency. It is important, on one hand, to construct the theoretical foundation of Chinese DFC by reviewing domestic and international literature on cryptocurrency, and on the other hand, to build a basic prototype of Chinese DFC by studying various types of typical electronic and digital currency systems currently in operation.**

### Development History of Cryptocurrency

#### Relationship between digital currency and cryptographic technology

Currently in China, payment realized via electronic accounts has become very common, however it is by nature merely an informatized representation of the existing fiat currency rather than digital currency by strict definition. DFC must be issued by central bank as it is by itself a currency instead of a mere tool of payment.

A hotspot of various studies is to try to ensure digital currency security with cryptographic technologies. It is fair to say that cryptographic technology is the supporting pillar of digital currency of which issuance and circulation should be built on cryptographic principles, and that cryptographic protocols should be adopted to meet all kinds of security demands.

#### Centralized scheme for digital currency and its cryptographic solution

In 1982, David Chuam, known as the "father of digital currency", published a paper called B*lind Signatures for Untraceable Payments* at the International Cryptology Conference where he presented a new cryptographic protocol called blind signature based on which an anonymous and untraceable e-cash system could be constructed. The paper is regarded as the earliest elaboration on digital currency. The digital currency model proposed by Chaum is based on the tripartite model involving banks, individuals and merchants. In this model, the banks serve as an authoritative central institution which transactions between the other two parties have to rely on. The design of this solution adopts the RSA-based blind signature mechanism. A typical use case involves six steps as follows:

1. Consumer blinds transaction message M (i.e. to hide the information) and sends the blinded information B to the bank.
2. The bank signs on the blinded message B as a proof of the effectiveness of the involved digital currency. The bank then sends the signature to the consumer and at the same time deducts the corresponding amount from the consumer's account.
3. The consumer verifies the effectiveness of the blinded message B—if effective, the consumer will unblind B, thus getting message M and signature S which will be sent to the merchant.
4. The merchant verifies whether M and S are issued by the bank with the bank's public key. Valid M and S will be sent by the merchant to the bank for settlement.
5. The bank verifies if M and S are legally issued. If not, the transaction will be blocked. If yes, the bank will continue to examine if the message has existed in the consumption list—if not, the transaction will be validated and corresponding amount of money will be added to the merchant's account, otherwise the transaction will be blocked.
6. The bank informs the merchant that the transaction has been completed.

This process has become a classic cryptographic solution for centralized digital currency scheme. David Chaum founded DigiCash in 1990 and developed E-cash. Following studies on group bind signatures, fair transaction, offline trading and divisibility of currency are all based on Chaum's scheme.

The centralized scheme for digital currency relies heavily on the central party to ensure security and efficiency. Over the past few decades, studies on such scheme have focused on improving security and efficiency of the tripartite model.

## Decentralized scheme for digital currency and its cryptographic solution

In 2008, Satoshi Nakamoto published a paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System* which proposed to eliminate the central institution (i.e. the banks) in the transaction process. In the digital currency scheme proposed by Nakamoto's paper, the tripartite model is replaced with a peer-to-peer two-party model. Bitcoin is by far the most mature use case of decentralized digital currency scheme. Other decentralized digital currencies all share basic features similar to those of Bitcoin.

The basic unit of Bitcoin transaction is an unused transaction output called UTXO. Essentially, the existence of Bitcoin is realized by transaction orders. Similar to bank account statements, transaction orders serve as evidence of the amount of money a customer has by recording the arrival and leaving of currency instead of providing specific balance numbers. Transaction orders record detailed information of a transaction such as the payer, the payee and the payment amount.

Via P2P network, Bitcoin adds timestamp to a bunch of transaction information within certain period of time, and the information is then integrated into a block. Mutually verified blocks are connected to one another to form a blockchain. Each block keeps a record of the previous block's header which is generated by Hash function, meaning that sequence of the blocks cannot be changed once confirmed. At the same time, the digital signature in the transaction order adopts 256-bit elliptic curve digital signature algorithm (ECDSA) to ensure the integrity and undeniability of transaction data.

The blockchain ledger is the one and only definite ledger in the P2P network of Bitcoin. Every node in the network keeps the same ledger copy and any node can join or leave the blockchain network at any time. Any update of the blockchain would be broadcast to all nodes within the network and be recognized and stored to their own databases after consensus has been reached among all the nodes based on consensus algorithm, so as to ensure the consistency of data across the entire network.

Blockchain manages to eliminate the guarantee provided by the central intermediary with sophisticated algorithm and enables a peer-to-peer payment scenario where money in an online payment initiated by one party gets to be paid directly to the other party without the involvement of any financial institution or intermediary, thus realizing the online transfer of value. Therefore, the features of Bitcoin as a classic demonstration of decentralized digital currency are made possible due to a combination of "blockchain+cryptography".

## Inspiration of Typical Systems

Drawing on the experience of typical electronic and digital currency systems such as E-Cash, M-PESA, GDM, game coin, third-party payment, Bitcoin and BitMint (some of them are just experimental systems but still have academic value), the design and construction of Chinese DFC should give careful thoughts on the following core issues.

*Online and offline.* Currently operating electronic currency systems are mostly online. The issuance and circulation of Chinese DFC should be able to support both online and offline operation, and the two should have different rules and processes to make the design concise.

*Convenience and security.* Convenience is important for DFC to achieve market recognition, and security is the foundation for the healthy operation of the entire system. A balance between the two is of critical importance. To enhance efficiency and convenience, high-value and small-value payments might be treated differently in terms of security mechanisms.

*Real name and anonymity.* Digital currency scheme can adopt either real-name system or anonymous system, or a combination of both. Chinese DFC might be designed to allow "anonymity at frontend and real-name at backend".

*Transaction and data analysis.* In the environment of big data and cloud computing, identification is no longer the sole measure to ensure transaction security. The role of client behavior analysis in assuring transaction security and risk prevention deserves great attention. Enhancing client behavior analysis is an important factor to consider for central banks that may issue DFC. Digital currency can be used to support big data analysis on a macro level, but on micro lever, privacy of legitimate users should not be violated.

*Relevance to bank accounts.* Current electronic currency systems are mostly based on bank accounts, which is not necessarily the case for pure digital currency systems.

*Ecosystem construction.* For the design of Chinese DFC, it is important to involve the financial and technological community and to conduct in-depth study on and reasonable application of all kinds of creative new technologies, so as to optimize the technical framework of digital currency issuance and circulation, hold sufficient expectation of technological advance and bring in a constantly evolving and improving development idea.

*Expectation of blockchain technology.* Blockchain technology has received great attention as a rudiment of the next generation of cloud computing, but cases of mature application by enterprises are rare. The ideas of "private cloud+high-performance database+mobile terminal" and "private cloud+blockchain+mobile terminal" might be two related but differentiated models. It will always be the goal of central bank-issued digital currency to make the center stronger, the data more secure, the terminal smarter and the payment action of individuals more independent. If blockchain is to be applied to the development of central bank-issued digital currency, is it okay to do some necessary modification to the technology? How should blockchain make substantial breakthrough to improve the speed and efficiency of large-denomination transactions?

In a word, it is the intention of digital currency issuers to make transactions more secure and convenient, to reduce clearing steps and to lower transaction costs.

## Conceptual Prototype of Chinese Digital Currency

Chinese digital currency, as a DFC, must be assured by Chinese sovereignty and its design should comply with the preliminary idea that it should be a PBOC-led initiative where digital currency based on encryption algorithm be issued in parallel with physical cash, and the DFC would be part of M0. The issuer may use security chip to make secret key and algorithm process secure, so as to ensure the security of digital currency.

The master framework for the issuance of Chinese DFC can be described as follows—the PBOC digital currency is, in accordance with the current RMB administration principles, issued and withdrawn from circulation based on the "central bank-commercial bank" system where the central bank is responsible for the issuance, verification and monitoring of digital currency and commercial banks, having obtained digital currency from the central bank, provide circulation services directly to the public and build application ecosystem.

### Core components of central bank digital currency system

The core components of central bank digital currency include the following: one type of currency, two currency repositories and three operation centers. More specifically, the system contains the following main components.

*Private cloud of central bank digital currency,* to support the fundamental infrastructures on which central bank digital currency operate.

*Digital currency,* an encrypted numerical string representing specific amounts that is guaranteed, signed and issued by central bank.

*Digital currency issuance repository*, the database on the private cloud of central bank digital currency that deposits digital currency issuance funds of PBOC.

*Digital currency commercial bank repositories,* the databases for commercial banks to deposit central bank digital currency, which can be stored either at local or on the central bank digital currency private cloud.

*DFC digital wallet,* the terminal APP for individuals or institutional clients to use central bank digital currency at the circulation market, and the wallet can be based on either hardware or software.

*Certification center,* to allow the central bank to manage the identity information of digital currency institutions and users in a centralized manner. It is not only the basic component to ensure system security but also an important step in controllable anonymous design.

*Registration center,* to record central bank digital currency and identities of corresponding users and conduct ownership registration; and to register the entire lifecycle of central bank digital currency from its creation and circulation to settlement and annulment.

*Big data analysis center,* to support anti money laundering, to analyze payment behavior and regulatory and policy indicators, etc.

### Encrypted creation of digital currency

To explore the representation method of Chinese DFC is definitely necessary for further studies on the basic mathematic model of digital currency (including properties, issuer, owner, user permission, scope of use, digital signature, encryption, anti-counterfeit, etc.) and for the construction of recognition and description models.

In the central bank digital currency system, D-coin can be created based on either denomination unit or the amount of physical currency in circulation. The method to be applied can be configured in the initial process by adjusting the system parameter.

An encrypted text representing certain amount of central bank digital currency is shown as:

| $D_{\#}$ | From | To | Value | Time | E | TVM | ... |
|---|---|---|---|---|---|---|---|

Its structure can be designed to meet specific demands, and therefore generates different kinds of coins with different features such as account balance method, UTXO-like method, etc.

### Issuance and circulation of digital currency

In the central bank digital currency system, there are central bank's digital currency issuance repository, commercial banks' digital currency repositories and users' digital wallets (e.g. those on mobile phones). The relationships among the three are as follows:

According to the total issuance amount the central bank generates digital currency (i.e. digital currency issuance fund) which is deposited in the central bank's digital currency issuance repository. Upon the application of commercial bank for digital currency, the central bank sends the needed amount of currency to the corresponding database of the applying commercial bank, thus completing the process of transferring digital currency from the issuance repository to the banking repository. Upon the application of user to withdraw digital currency, the currency is moved from the banking repository, enters into circulation and is put into the storage media of the user terminal (e.g. mobile phone). At the circulation stage, payment is realized by the transfer of digital currency between digital wallets of two users, and payment is categorized into online payment and offline payment.

## Key design factors

First, compliance with the idea of traditional currency management ensures that digital currency is issued and withdrawn from circulation based on the current "central bank-commercial bank" system.

Second, cryptography is adopted in the design of DFC to ensure security.

Third, the creation, circulation, settlement and annulment of DFC are entirely registered. Experience can be drawn from blockchain technology for the establishment of a ledger registration center that keeps a balance between centralization and distribution.

Fourth, trusted computing and security chip technologies are fully used to ensure end-to-end security during digital currency transaction.

Fifth, big data analysis is applied to its fullest, which not only enhances transaction security but also meets needs of AML.

Sixth, the identity authentication of digital currency user follows the principle of "anonymity at frontend and real-name at backend", which manages to protect user privacy and at the same time prevents risks of illegal transactions.

Seventh, the design of digital currency should be as concise and efficient as possible while the commercial application based on digital currency should be left to the market as much as possible, and it is important to develop sound technology standards and application rules.

Eighth, it is important to build an integrated digital currency ecosystem involving various participants including the central bank, commercial banks, third party organizations and consumers, so as to ensure that the life cycle of digital currency (i.e. its issuance, circulation and recycle) is a closed-loop with high controllability. ■

YAO Qian

Dr. YAO Qian is the Chief Executive Officer of China Securities Depository and Clearing Corporation Limited (CSDC). He is also serving as the Research Fellow at the Financial Research Centre of the Counselors' Office of the State Council of the People's Republic of China and the Secretary General of China Financial Standardization Technical Committee.

Before joining CSDC, he served consecutive positions as the Deputy Director General and Counsel of the Technology Department of the People's Bank of China (PBoC), Director General of Institute of Digital Money of PBoC, and Deputy Director General of PBoC Credit Reference Centre.

He has published around 150 papers and 7 books and holds more than 100 patents. He has been awarded provincial and ministerial first prizes for his outstanding contribution in promoting new technology development and application in the banking sector.

YAO Qian holds a Doctor of Engineering degree. He is a professorate senior engineer and a Ph.D. supervisor.