Front. Eng. Manag. 2020, 7(4): 471–484
https://doi.org/10.1007/s42524-020-0134-0

RESEARCH ARTICLE

Hongfeng CHAI, Quan SUN, Yu ZHOU, Tao ZHU

Design of a digital currency information system based on the UnionPay network

Abstract Digital currency can reduce the issuance and circulation costs of physical cash and improve the convenience and transparency of economic activities. Therefore, digital currency has received widespread attention from central banks in recent years. As an important financial infrastructure, the UnionPay network is expected to provide effective support for the construction and operation of a digital currency system. This study uses the UnionPay network as basis to systematically propose a digital currency information system from three aspects, namely, digital currency account opening, exchange, and use, and further expounds on the operation mechanism of a digital currency information system prototype. This study also discusses how to apply blockchain technology to digital currency, such as using distributed ledger for digital currency confirmation and registration and using blockchain-enabled smart contracts to realize the forward guidance function of the central bank digital currency. Lastly, the current research introduces the value of using the UnionPay network to support the operation of a digital currency information system and its technical challenges, aiming to provide beneficial guidance and reference for future research effort.

Keywords UnionPay network, digital currency, information system, blockchain, smart contracts

Received June 29, 2020; accepted August 1, 2020

Hongfeng CHAI, Quan SUN (✉)
Fudan University, Shanghai 200433, China; China UnionPay Co., Ltd., Shanghai 201201, China
E-mail: quansun@unionpay.com

Yu ZHOU, Tao ZHU
China UnionPay Co., Ltd., Shanghai 201201, China

1 Introduction

Currency originates from the exchange of commodities and labor services, and it has the credit deflation function of economic regulation in the modern economy. Given the progress of the economy and technology, the form and function of currency have continuously extended and evolved, which has experienced three stages, i.e., physical, credit, and electronic currencies. Physical currency in the first stage is the initial form of currency, which is the relatively primitive equivalents of cattle, sheep, grains, and shells, among others; and the general equivalents of bronzes, jade, gold, and silver. Given the low extent of portability and standardization, physical currency is difficult to popularize on a large scale. The second stage of credit currency is real currency (Qiu, 2017), which is based on private and countries' credit intermediaries, in the form of bills and banknotes and with three advantages: Convenience, standardization, and popularization. Since the 1980s, the rapid development of information and Internet technology has made currency enter the third development stage, namely, electronic currency, which is the expression of credit currency from the physical form to electronic form (Shi and Zhou, 2018). Electronic payment requires communication equipment, terminals, accounts, and related carriers to achieve, and different combinations of electronic accounts and carriers constitute different types of electronic currency.

David Chaum invented the online digital currency E-Cash system in the 1970s and published the first paper on digital currency in 1988 (Chaum et al., 1988). In 1990, he created DigiCash, a professional company specializing in operating digital currency. Accordingly, he is known as the "father of digital currency". At present, statistics indicate over 2000 types of digital currencies based on blockchain technology, including Bitcoin (Nakamoto, 2008) and Ethereum (Buterin, 2013; 2014). The rapid development of the digital currency industry has resulted in immense changes in payment methods around the world. This development has also brought new

opportunities and challenges to currency issuance, circulation, and policy implementation of central banks in various countries. Moreover, the central banks of various countries actively promote the research of legal digital currency (Bordo and Levin, 2017). The Bank of England tested the central bank digital currency (CBDC) model "RSCoin" based on blockchain. The Bank of Canada conducted the digital currency test "Jasper" based on the R3 Corda DLT (distributed ledger technology) platform (Engert and Fung, 2017). The central bank of Singapore completed the digital currency "Ubin" project (MAS, 2019). The People's Bank of China is testing DCEP (Digital Currency/Electrical Payment) in several pilot cities (Yao, 2016; Fan, 2018). The detailed information of diverse digital currencies is shown in Table 1.

This study aims to design and expound the operation mechanism of a digital currency information system based on the UnionPay network from three aspects (i.e., digital currency account opening, exchange, and use), and proposes a prototype digital currency information system. In addition, the current study analyzes a series of technical challenges faced by the UnionPay network supporting the construction of a digital currency operation system. The purpose of this study is to provide a beneficial reference for the issuance and circulation of CBDC (Qin et al., 2017; Han et al., 2019).

2 Possible roles of the UnionPay network in the digital currency era

China UnionPay, as a card scheme in China, owns and operates a global financial payment information system called UnionPay network. UnionPay connects banks, institutions, merchants, and users, and extensively unites all parties in the industry to service the standardization of electronic currency. Accordingly, UnionPay has successfully expanded payment business from bank card acceptance to the entire business services ecosystem, such as scene construction, business circle building, and member management. China UnionPay provides critical support for social and economic development and is an important financial infrastructure in China.

Judging from the progress of local and international research, countries remain in the early stage of digital currency research, mainly focusing on the analysis of currency issuance and circulation forms, as well as the impact and challenges on the financial system and infrastructure. However, few countries has investigated the construction, circulation promotion, financial supervision, and other aspects of digital currency system. The current study is guided by the structure of the People's Bank of China's digital currency (Yao, 2016), and

Table 1 Detailed information of diverse digital currencies

	Bitcoin	Ethereum	RSCoin	Jasper (CAD-Coin)	Ubin	DCEP
Start time	2008	2014	2016	2016	2017	2017
Supervision organization	/	/	Bank of England	Bank of Canada	Monetary Authority of Singapore	People's Bank of China
Participating organization	Technology geek	Technology geek	University College London	Bank of Montreal, Canadian Imperial Bank of Commerce, Royal Bank Of Canada, National Bank of Canada, and Hong Kong and Shanghai Banking Corporation (HSBC), among others	Bank of America Merrill Lynch, Development Bank of Singapore, HSBC, JPMorgan Chase, United Overseas Bank, Citibank, and Standard Chartered Bank, among others	Industrial and Commercial Bank of China, Agricultural Bank of China, Bank of China, and China Construction Bank, among others
Technical support	Open source blockchain	Open source blockchain	Two-tiered system, optimized based on Bitcoin	R3 Corda	R3 Corda, Quorum, and Hyperledger Fabric	Two-tiered system, no blockchain
Application scenarios	P2P (Peer to Peer) transfer	P2P transfer, smart contract, and Defi	Research on blockchain to support retail payments	Experimented to apply DLT in wholesale settlements, such as inter-bank settlements, delivery versus payment, and cross-border settlements	Experimented to apply DLT in wholesale settlements, such as inter-bank settlements, delivery versus payment, and cross-border settlements	Replace physical cash for retail payments
Characteristics	Decentralization, anonymity, no national boundary, and anti-regulation	Decentralization, anonymity, no national boundary, anti-regulation, and programmable	Two-tiered system, auditability, and high performance	Payment systems based on DLT technology can save costs and improve efficiency	7×24 real-time service, liquidity saving mechanism, and reduced operational risks of the trading system	Secure, stable, controllable anonymity, convenient, and efficient
Current situation	Stable operation	Stable operation	Prototype	Experiment	Experiment	Pilot in some cities

UnionPay network can support the development of digital currencies in various countries from the following aspects.

2.1 Top-level design of digital currency information system

Information system architecture is the cornerstone of the stable operation of digital currency. When designing the top layer of the information system architecture, the security, stability, and scalability of the digital currency system must be fully considered. Security indicates that a system must have a highly reliable guarantee in trusted communication, basic security, data security, transaction security, and terminal authentication, among others. Stability emphasizes that a system must consider the massive transaction scale of digital currency, involving powerful real-time throughput and concurrent processing capabilities, to ensure the stable circulation of digital currency. Scalability means that a system must consider the good connection with the information system of existing financial institutions and be compatible with blockchain application systems. As the core of the current financial infrastructure, the UnionPay network should be a key participant in digital currency research, experiment, and landing. The reason is that this network has extensive operational experience in the construction of large-scale financial systems, combined with its own relevant research and accumulation of digital currency underlying technologies, such as blockchain, cryptographic algorithms, and network security.

2.2 UnionPay network for digital currency circulation

If digital currency lacks the equipment for various application scenarios, the public will be unable to use or even contravene the digital currency for transactions and may convert digital currency into physical cash, thereby substantially affecting the promotion of digital currency. The UnionPay network relies on UnionPay cards, POS (point of sales) terminals, and ATMs (automatic teller machines), and has formed a huge acceptance network with card issuers, acquirers, and merchants. If the UnionPay network is reused for digital currency circulation, then the difficulty of promoting digital currency will be substantially reduced. In addition, many products based on the UnionPay APP, QuickPass, on mobile phone, and QR (quick response) code will also generate additional digital currency application scenarios, thereby increasing the use frequency.

2.3 Digital currency payment and application ecology construction

Payment is the most basic function of currency, but the application of digital currency is not limited to payment but likewise focuses on complex financial business processes, such as banks, securities, and insurance, thereby realizing a programmable and digital financial ecology. The UnionPay network will use cloud computing, trusted mobile payment, blockchain, smart terminal, big data, and machine learning to conduct digital currency payment ecological research. This type of research, which can provide merchants with digital currency payment, verification, and cashing solutions, explores digital currency-based clearing, settlement, acquisition, authentication, and other value-added service solutions. In addition, embarking around digital currency, a series of existing blockchain-based cryptocurrencies (Hileman and Rauchs, 2017) have not only been limited to payment services but achieved the application of digital assets, digital vouchers, and other financial fields.

3 Design of digital currency information system based on the UnionPay network

3.1 Meeting the "regulatory sandbox" requirements

The term "regulatory sandbox" originated in the UK. The Financial Conduct Authority (FCA) of the UK led in implementing the Regulatory Sandbox project on May 9, 2016 (FCA, 2016), which intended to simplify market access standards and procedures within a limited range, and enabled the rapid landing of fintech innovation companies or businesses on the premise of ensuring consumer rights and interests (Ye, 2017; Zhang, 2017; Hu and Yang, 2019). Numerous countries, including Singapore and Australia, initially imitated the concept of the British Regulatory Sandbox (MAS, 2016; ASIC, 2017). On January 14, 2020, the Business Management Department of the People's Bank of China publicly solicited opinions on six applications that will be included in the pilot supervision of fintech innovation.

Issuing digital currency is not only a significant national project but also a huge social project (Fan, 2018). Therefore, thinking deeply and planning afterwards are necessary, and the "regulatory sandbox" provides a good innovation and trial environment. Thus, the design of a digital currency information system based on the UnionPay network will be implemented in accordance with the requirements of the "regulatory sandbox" mechanism. "Regulatory sandbox" breaks through the traditional regulatory thought, which, through flexible differential regulatory design, would provide convenience to new entrants in the market and those who have attempted to provide new products, creating a mechanism that provides real innovations with the opportunity to be piloted in actual operations. Apart from observing how these innovative business models should be managed after real operations, the laboratory concept would, meanwhile, be allowed to be verified on the spot. "Regulatory sandbox" is a test

mechanism for financial product innovation, thereby attempting to effectively balance the contradiction between financial innovation and legal supervision.

3.2 Simulating digital currency operating mechanism

Digital currency is the digital form of physical cash. Analogous to the current UnionPay network that supports the flow of electronic money, the operation mechanism of the digital currency information system will be expounded from three aspects: Digital currency account opening, exchange, and use. The two scenarios of near-field and remote networking are also included.

3.2.1 Digital currency account opening

Figure 1 shows that users can open digital currency account through offline banking outlets or mobile APPs. The specific process is as follows.

1) When a user applies for a digital currency account with a commercial bank, if they go offline, then user information will be recorded and verified according to the traditional account opening process; if they apply online through a commercial bank APP, then users will need to complete identity authentication when they submit their identity documents, which are entered with biometric information, such as fingerprints or human faces.

2) After completing the verification of users' identity information, commercial banks generate a digital currency account bounding to users (a pair of public and private keys) and transmit the public key to UnionPay. Thereafter, UnionPay records the public key to facilitate subsequent routing control and transaction distribution. For the storage of private keys, if through offline branch, then commercial banks will import the private key into the users' mobile phone Secure Element (SE) and keep a backup in the cloud; if an online APP is used, then commercial banks will not transmit the private key through the network to the terminal but store in the cloud. Accordingly, users should extract the private key for transaction confirmation in the future.

3) Commercial banks send the user identity authentication information to the central bank authentication center for centralized storage.

4) After receiving the reply from UnionPay and the central bank, commercial banks inform users that the account is successfully opened.

Note that users may open digital currency accounts in many different commercial banks, resulting in difficulties in effectively account managing and using. Therefore, the UnionPay has developed the UnionPay digital currency wallet (see Fig. 2) by connecting the APIs (application programming interfaces) of various commercial banks.

3.2.2 Digital currency exchange

Figure 3(a) shows that exchange refers to the process of exchanging digital currency in and out. That is, an equivalent amount of money is exchanged between digital currency and traditional bank accounts. For example, transfer refers to the amount of digital currency account increases and the amount of traditional bank account decreases. Meanwhile, redeem refers to the amount of digital currency account decreases and the amount of traditional bank account increases. Figures 3(b) and 3(c) show the specific process of digital currency exchange transaction through the UnionPay digital currency wallet.

1) Via logging into the UnionPay digital currency wallet APP, users can submit a digital currency exchange transaction request after completing identity verification.

2) If the transaction is a transfer transaction, then this transaction will be forwarded to the commercial bank where the bank card account is located. If the transaction is a redeem transaction, then this transaction will be forwarded to the commercial bank where the digital currency account is located.

3) For transfer transaction, the commercial bank will evaluate whether the traditional bank account balance can perform the transaction. If there is no problem, then commercial bank will respond to UnionPay after account processing. If it is a redeem transaction, then commercial bank will determine whether users have the right to use the digital currency and then respond to UnionPay.

4) After the UnionPay receives the response, if it is a transfer transaction, then this transaction will be forwarded to the commercial bank where the digital currency account is located and the bank will be notified to change the owner of the digital currency; if it is a redeem transaction, then this transaction will be forwarded to the commercial bank where the bank card account is located, and the bank performs balance changes in the traditional bank account. The commercial bank will respond to UnionPay after successful transaction.

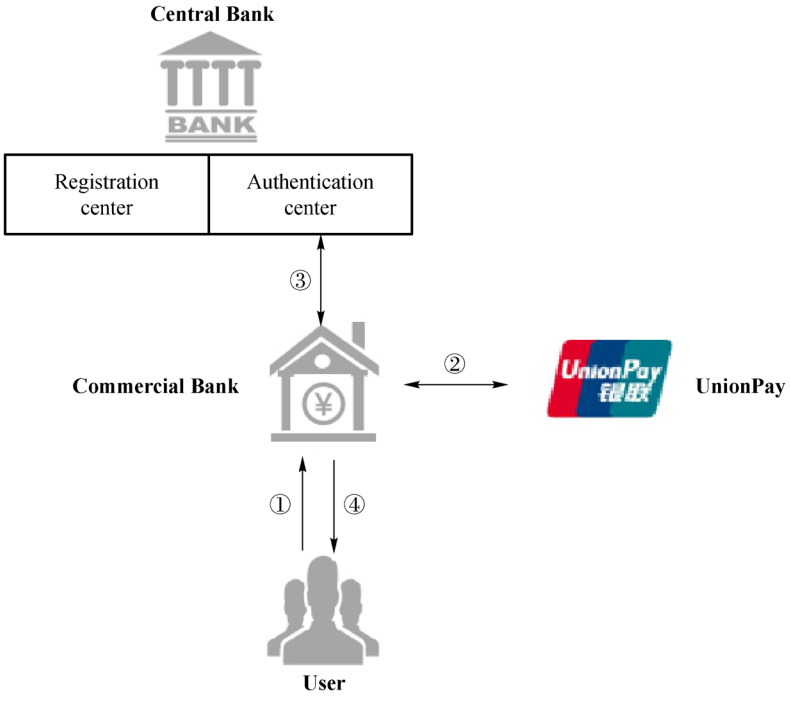
5) When receiving a successful response, the UnionPay sends the information to the smart terminal; after which, the terminal prompts that the exchange is successful.

6) UnionPay will transfer the information of digital currency owner change to the central bank registration center for centralized accounting within a certain period.

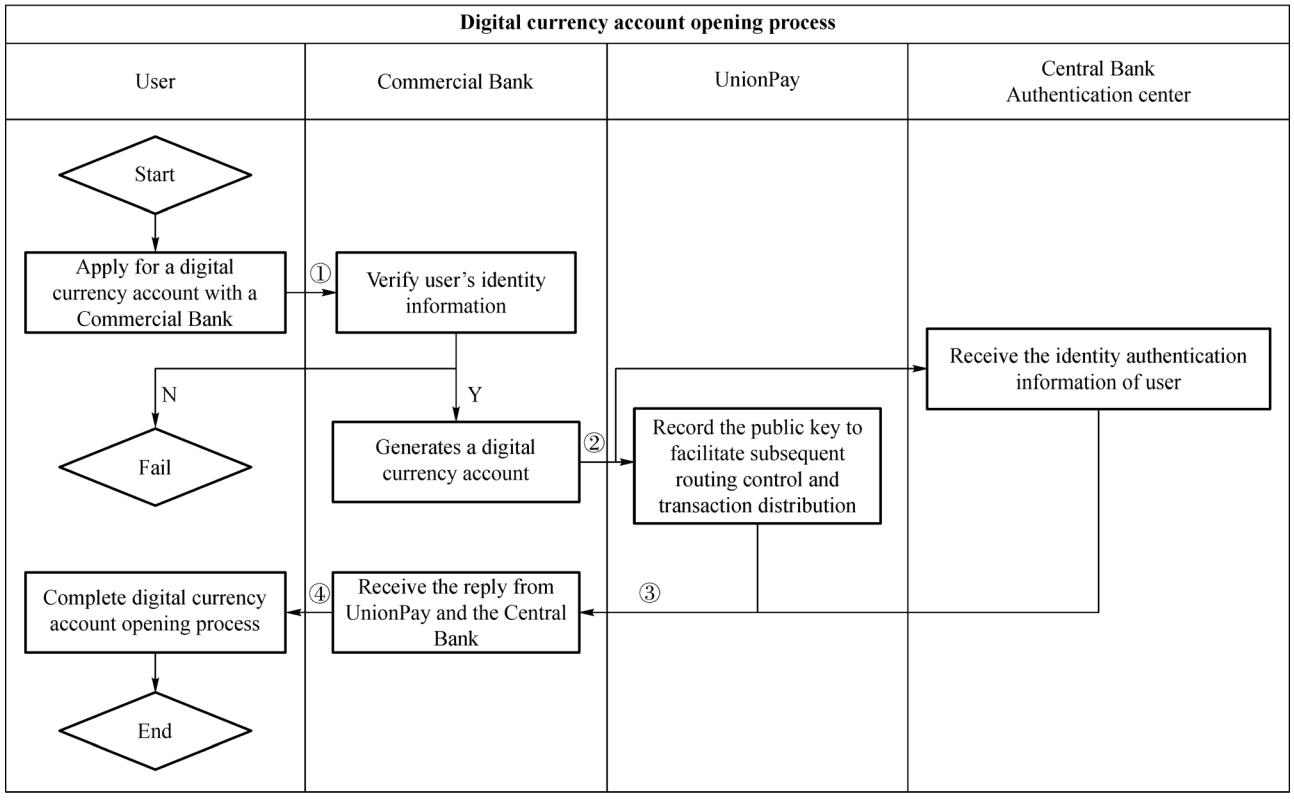
7) Commercial banks will regularly synchronize the account data of the registration center for reconciliation.

3.2.3 Digital currency use

The use of digital currency mainly includes near-field and remote networking modes, which can be grafted on existing bank card acceptance methods, such as NFC (near-field communication) and QR codes.



(a)



(b)

Fig. 1 Digital currency account opening process.

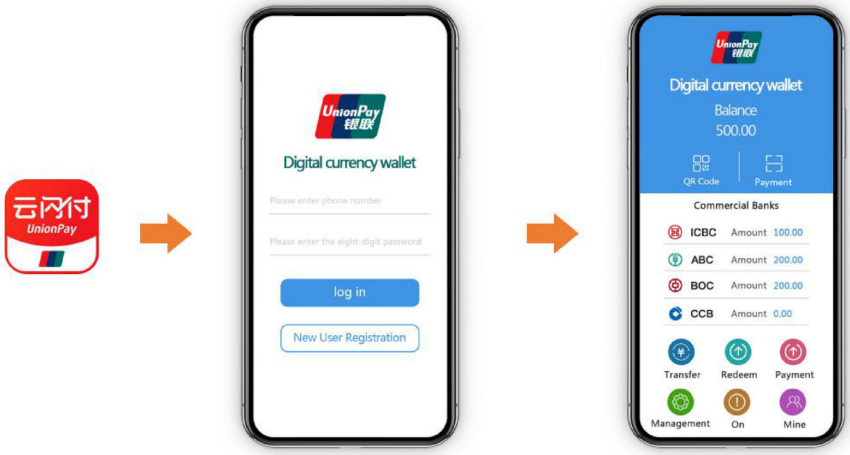


Fig. 2 Example of the UnionPay digital currency wallet managing digital currency accounts of various banks.

(1) Near-field networking mode

a. NFC transaction

As long as NFC-enabled mobile phones are near terminals, the terminal devices will automatically initiate and complete the digital currency payment. Figure 4 shows the specific NFC transaction process.

1) After users complete their purchase with the merchants, the latter uses the acceptance terminal to collect digital currency and enters the amount to prompt payment. The terminal NFC device will serve as the initiating device in passive mode.

2) Users move the payment device near to the merchants' digital currency collection device for data interaction.

3) After collecting the payment elements of both parties, the collection device sends the transaction to UnionPay.

4) After the transaction information is analyzed and verified, the transaction is transferred to commercial banks where payers are located, which will evaluate the right to use the digital currency. If there is no problem, then the digital currency will be de-owned and the information will be responded to UnionPay.

5) After UnionPay receives the response, it forwards the digital currency transaction information to commercial banks where the payees are located, which will change the owners of the digital currency and respond to UnionPay.

6) After receiving the reply, UnionPay sends the successful transaction information to the payment collection device.

7) After receiving the successful response, the receiving device prompts that the payment is successful.

8) UnionPay will transfer the change information of the digital currency owners to the central bank registration center for centralized accounting within a certain period. Commercial banks will regularly synchronize the account data of the registration center for reconciliation.

b. QR code transaction

Figure 5 shows an example of users using the UnionPay digital currency wallet to conduct a QR code transaction. This transaction is divided into two types, namely, active and passive scan modes. In the passive mode (B scan C), the digital currency wallet convert the digital currency wallet address of the payers into a dynamic QR code. After scanning the dynamic QR code, the receiving terminal obtains the information of the payers. Figure 6 shows the example of B scanning C, and the specific transaction process is as follows.

1) After users complete their purchase with the merchants, the former (payer) should open the UnionPay digital currency wallet and generate a payment QR code.

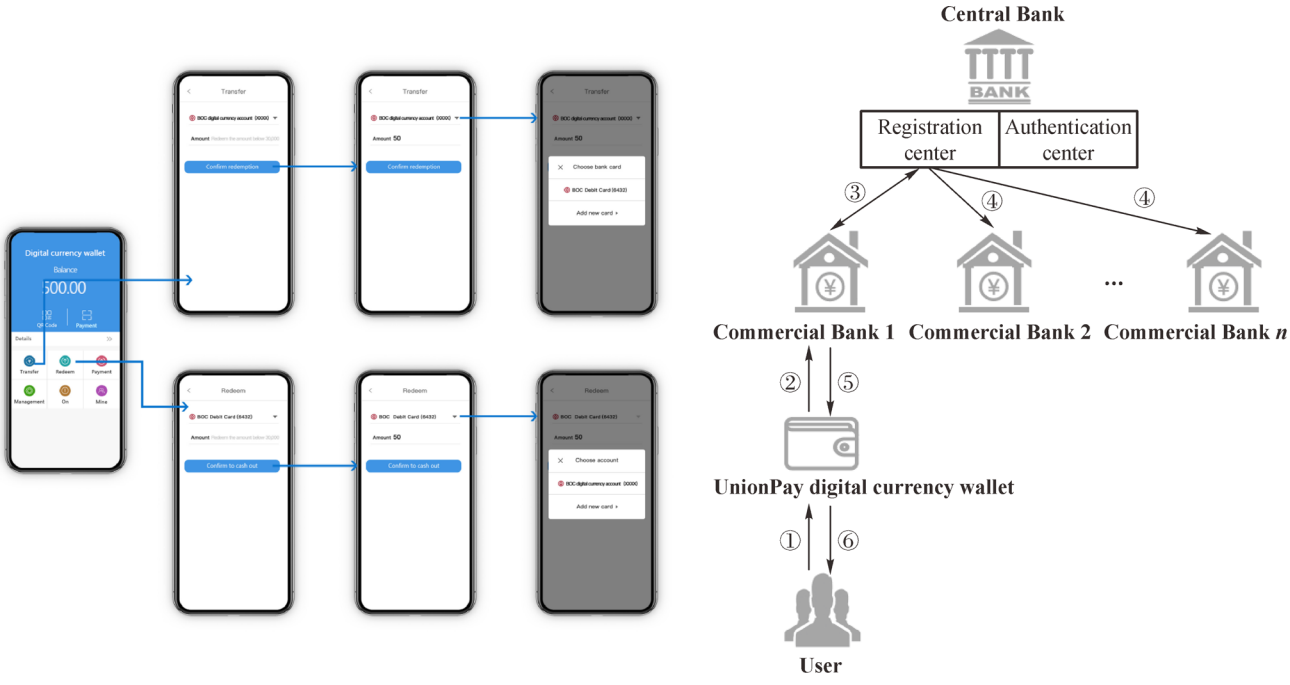
2) The merchants (payee) will scan users' QR code with a code scanner, which is equivalent to accessing the backend URL of payers' digital currency wallet. Then the payers' backend retrieves the private key based on the scanned information and signs the transaction, after which, the wallet will package both payers' signature information and payees' information to UnionPay.

3) After UnionPay authenticates the submitted information, it is forwarded to commercial banks where payers are located, which will judge the right to use digital currency. If there is no problem, then the digital currency will be de-owned and the information will be responded to UnionPay.

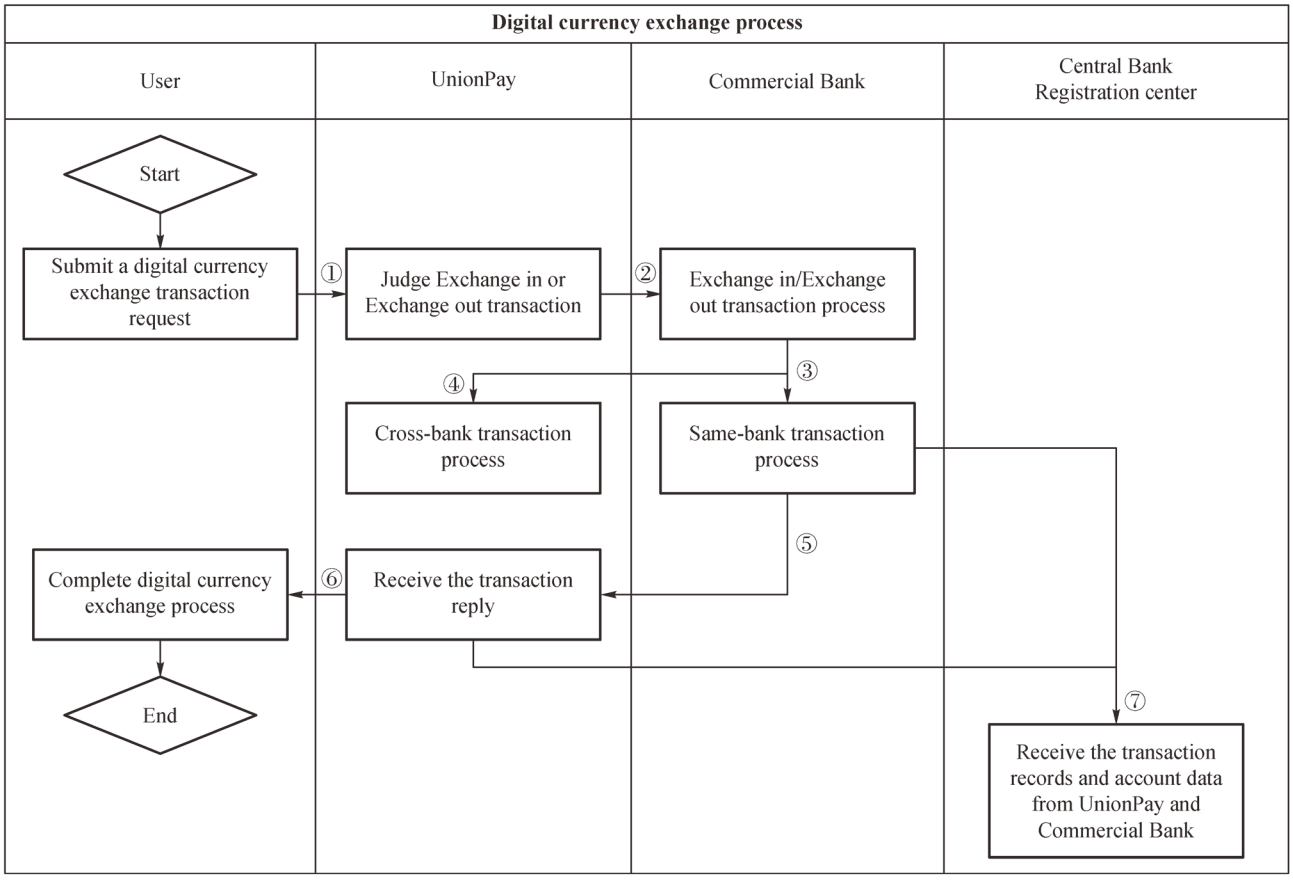
4) After receiving the response, UnionPay forwards the digital currency transaction information to the commercial banks where payees are located, which will change the owners of the digital currency and respond to UnionPay.

5) After receiving a successful response, UnionPay sends the information to the collection device, which then prompts that the payment is successful.

6) UnionPay encrypts and transmits the transaction owners change information to the central bank registration



(a) (b)



(c)

Fig. 3 Digital currency exchange process through the UnionPay digital currency wallet.

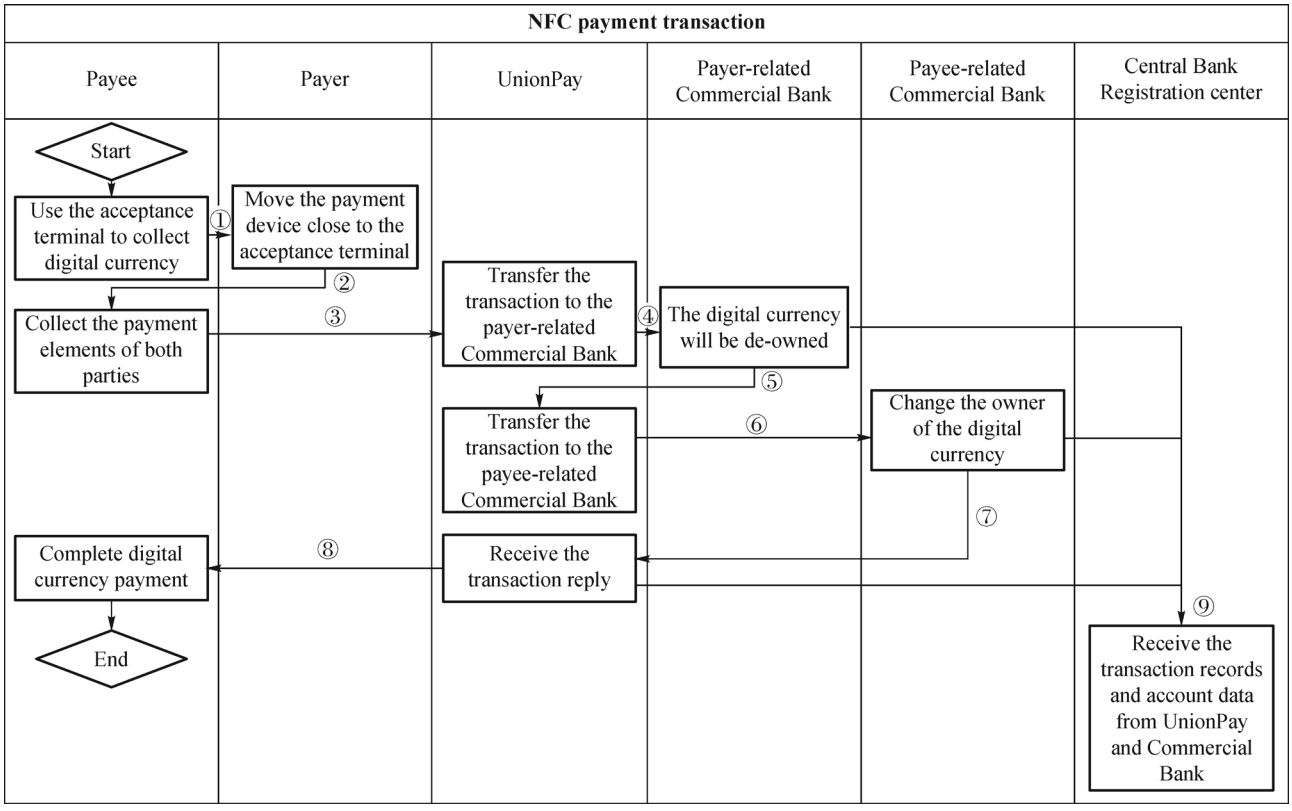


Fig. 4 NFC transaction process.

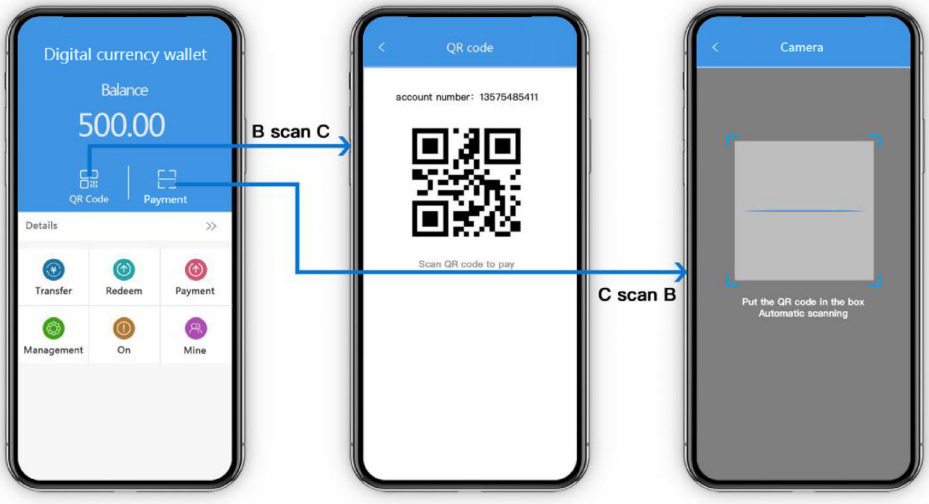


Fig. 5 Use of digital currency through the UnionPay digital currency wallet.

center for centralized accounting within a certain period. Commercial banks will regularly synchronize the account data of the registration center for reconciliation.

In contrast, in the active mode (C scan B), the merchant side can convert the UnionPay digital currency wallet address into a QR code, then print it, and post it at the cashier. When paying, payers can use the digital currency wallet to scan the code to complete the payment. However, this process has limited security, and it is easy to produce a risk event for the static QR code.

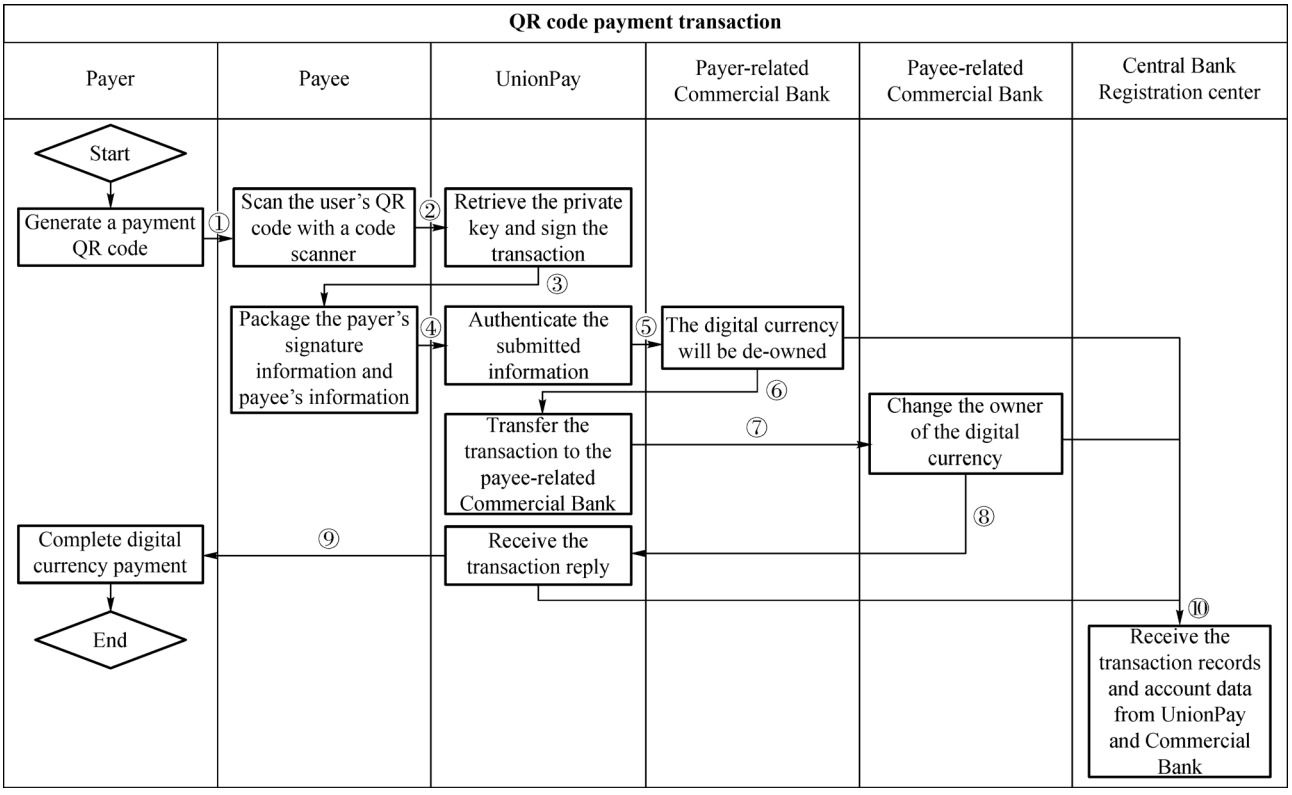


Fig. 6 QR code transaction process.

(2) Remote networking mode

The remote networking mode in-APP means that users place an order directly through a third-party APP, then the APP calls up the payment plug-in and selects the UnionPay digital currency wallet to initiate and complete the payment. Figure 7 shows the specific process of in-APP payment as follows.

1) When purchasing products, users place an order in merchants' APP. In the payment process, the merchants' APP calls the UnionPay digital currency wallet SDK (Software Development Kit), and users choose to use the wallet for payment on the pop-up payment selection interface. After verifying the users, the wallet sends a payment request to the backend, which collects payment elements from both parties, then packages and sends them to UnionPay.

2) UnionPay authenticates the submitted information and forwards it to the commercial banks where the payers are located, which will judge the right to use the digital currency. If there is no problem, then the owners of digital currency will be changed and the information will be responded to UnionPay.

3) After receiving the response, UnionPay forwards the digital currency transaction information to the commercial banks where the payees are located, which will change the owners of the digital currency and respond to UnionPay.

4) After receiving a successful response, UnionPay sends the information to the collection device, which then prompts that the payment is successful.

5) UnionPay encrypts and transfers the transaction owner change information to the central bank registration center for centralized accounting within a certain period. Commercial banks will regularly synchronize the account data of the registration center for reconciliation.

3.2.4 Applying blockchain technology to digital currency

Blockchain is also known as DLT, which has the characteristics of decentralization, collective maintenance, tamper-resistant, traceability, and auditability (Yuan and Wang, 2018; Melanie, 2015). Blockchain can be applied to digital currency in the following two ways (Radziwill, 2018).

(1) Using distributed ledger for digital currency confirmation and registration

By maximizing the non-tamperable and non-forgeable characteristics of a distributed ledger (Wang et al., 2018), an "online digital currency detector" (i.e., digital currency confirmation account book) can be constructed in the CBDC registration center to provide CBDC online query services.

The issuance registration subsystem of central banks performs ownership registration on the confirmation account book, which notifies the confirmation issuance

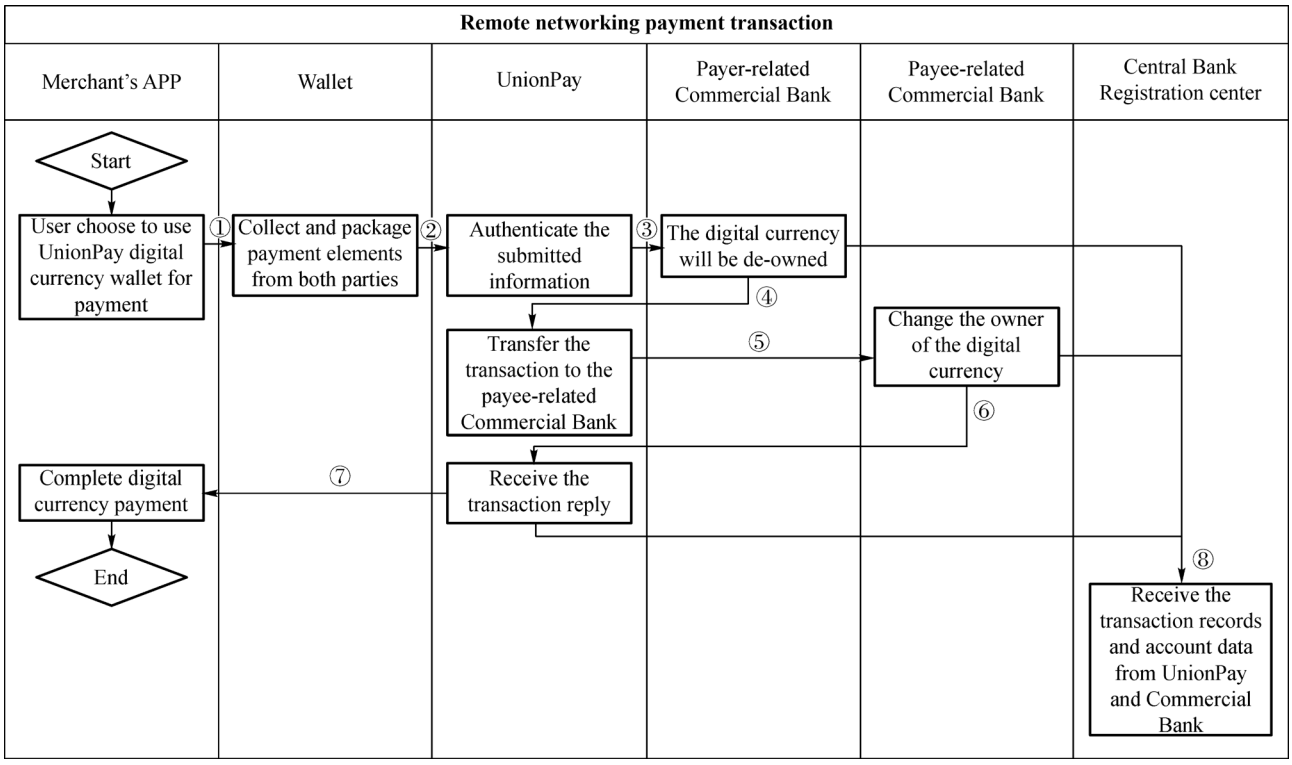


Fig. 7 Remote networking transaction process.

subsystem of ownership information for the issued CBDC. Thereafter, the confirmation issuance subsystem desensitizes the registered ownership information and releases them asynchronously to the CBDC confirmation ledger. The confirmation query website provides online CBDC ownership query services for the public. The blockchain distributed ledger guarantees the consistency of CBDC ownership information between central banks and commercial banks.

On the one hand, this design isolates the core issuance registration subsystem from the outside world and simultaneously uses the advantages of distributed ledger to improve the security and credibility of the CBDC confirmation data. On the other hand, given that the distributed ledger is only used to provide query services for the public, the transaction processing is still carried out by the issuance registration subsystem, thereby effectively avoiding the performance bottleneck of the existing blockchain technology (Yao, 2018a).

(2) Using smart contracts to realize the forward guidance function of digital currency

Smart contracts are program codes deployed on the blockchain (Christidis and Devetsikiotis, 2016). Once the terms in the contracts are triggered, the codes can be automatically enforced. Smart contracts are characterized by decentralization, enforceability, and programmability (Wang et al., 2019). Smart contracts can be designed with "forward contingent" to allow fiat digital currency to solve traditional monetary policy dilemmas, such as poor conduction mechanism and counter-cyclic adjustment of the central bank monetary policy.

Smart contracts can be applied to digital currency in the following aspects. The first is to adopt the "time contingent" currency taking effect design to reduce the time lag of monetary policy transmission and avoid currency idling. The second is through the "sector contingent" currency taking effect design to implement the accurate and qualitative currency placement and structural monetary policy, thereby improving the ability of financial services for the real economy. The third is through the "loan rate contingent" currency taking effect design to realize the real-time transmission of the benchmark interest rate to the loan interest rate. Lastly, through the "economic state contingent" design and based on the macroeconomic state, counter-cyclically adjust the capital return interest rate of commercial banks to the central bank, and reduce the risk level of commercial banks and the procyclicality of their loan behavior to achieve counter-cyclical economic regulation.

Given that the fiat digital currency is built-in with the preceding condition settings and can be publicly known by commercial banks, the monetary policy of central banks (i.e., forward guidance) can be better realized (Yao, 2018b).

4 Values and technical challenges of the UnionPay network in supporting digital currency information system

4.1 Values

Digital currency will definitely change the business model of the domestic financial payment industry and promote the further improvement of financial infrastructure. The value of reusing the UnionPay network in supporting the construction of digital currency information system is mainly reflected as follows.

4.1.1 Reducing the construction costs of digital currency system

In the future development, pilot, and implementation of a digital currency system, two costs cannot be avoided theoretically: Construction costs of the digital currency operation management platform and the digital currency payment acceptance environment (Dwyer, 2015). As a financial payment infrastructure, China UnionPay can expand the core system and cooperate with financial institutions to build a new payment network based on DLT to effectively support the reduction of the construction costs of the digital currency system.

In addition, UnionPay's existing national networked merchants, POS devices, ATM acceptance network, financial IC card, mobile payment, QR code payment, and other product systems can be relied on to support comprehensive digital currency payment solutions, thereby reducing the use threshold of digital currency technology. Moreover, users' habit of using digital currency is cultivated to avoid the cost of establishing new terminal acceptance environment and related application supporting scenarios.

4.1.2 Supporting the operation of digital currency system

Information system architecture is the core of the digital currency operating system. An information system that is secure, stable, and scalable is indispensable. At present, the UnionPay network has realized stable and robust interconnection between commercial bank accounts. In the future, the UnionPay networks can serve as a bridge to interconnect traditional bank accounts and digital currency wallets. The unified payment, owner change registration of digital currency, clearing and settlement management, and other processes could avoid frequent interaction among different systems, thereby effectively improving the flow of funds and efficiency of liquidation.

UnionPay and commercial banks implement multi-active business processing networks based on a distributed technology architecture. Accordingly, they will continue to promote system expansion and improve system operation efficiency. With meeting the development requirements of Internet payment and mobile payment, they can also support high-frequency and massive digital currency transactions.

4.1.3 Promoting the large-scale application of digital currency

Digital currency applications should use electronic wallets as carriers. It may be considered to introduce the attributes of digital currency wallets on the traditional account system of commercial banks to enable one account to manage the existing electronic and digital currencies. UnionPay connects the APIs of various commercial banks, develops the UnionPay digital currency wallet, and relies on the UnionPay network to realize the unified management of digital currency accounts of multiple banks. Moreover, UnionPay combines NFC and QR codes to fully promote the large-scale application of digital currency.

4.1.4 Promoting digital currency internationalization

At present, UnionPay's international business is booming. The acceptance network has been extended to over 178 countries and regions and its brand influence and international image have been continuously improved. In the future, based on the UnionPay network, UnionPay will accelerate the development of internationalization in depth and promote the establishment of a cross-border settlement system as the technical support of digital currency. Eventually, UnionPay will become an important force in implementing the national "going out" strategy and the Belt and Road Initiative (namely, the Silk Road Economic Belt and the 21st Century Maritime Silk Road Initiative).

In summary, multiplexing the UnionPay network can be used as one of the digital currency system construction options, which would play a vital role in maintaining the stability of the financial system and promoting the development of China's social digital economy.

4.2 Technical challenges

In the future, digital currency will not be a simple electronic form of legal currency but a fixed-length encrypted string generated through anti-counterfeiting technologies, such as national encryption algorithm and digital signature system. Digital currency will surpass the existing electronic money system in terms of convenience, security, and credit. However, in the design and construction of the digital currency system, the secure, stable, and scalable information system architecture will continue to be the core. Therefore, this system must clarify a series of technical challenges that the UnionPay network currently faces.

4.2.1 Format of the data transmission message should be modified

Data transmission message refers to the information transmitted among users' digital currency clients, acceptance equipment, and acceptance system. To eliminate the heterogeneity of the core systems of various commercial banks, compatibility and convenience must be ensured.

The message between users' digital currency clients and acceptance system can choose a light-weight data exchange format JSON (JavaScript Object Notation) with good readability and fast writing characteristics. This format is convenient for automatic analysis and generation, and data exchange can be conducted among different systems.

The transaction message between the accepting terminal and accepting system can refer to China's mobile payment system and bank card system's networked universal data message format (ISO 8583). However, it is not completely reusing, and certain reforms are required on this basis. For example, the field of the original card number in the message is 19 bits, while the public key address of the digital currency generally exceeds 19 bits. Accordingly, the message must be expanded to add some blockchain information.

4.2.2 Data transmission protocol should ensure data transmission security

Digital currency should rely on stable and secure data transmission protocols during the issuance process, including message verification, transmission guarantee, and secure channel. At present, the mainstream data transmission protocols for transactions include the hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS). The latter is based on HTTP by adding security socket layer (SSL) or transport layer security (TLS) to ensure the identity authentication of the transaction subjects and data transmission encryption.

Digital currency issuance mainly involves the exchange of information between participating parties, such as central banks and commercial banks. It is recommended to reuse the existing dedicated line connection and adopt the traditional symmetric key system (session encryption key) for transmission security and data integrity protection.

Digital currency circulation primarily involves information exchange between users and commercial banks. Based on Internet transmission, a special asymmetric key system is needed for transmission security and data integrity protection.

4.2.3 Information network should be safe and reliable

A digital currency system will be different from the existing centralized electronic currency system. It is a multi-central network, jointly constructed by central bank and several commercial banks. The issuance and circulation of digital currencies will put forward strict requirements for network security. Security research on encryption, key storage, and privacy protection, among others, should be strengthened.

Controllable anonymity is a basic feature of digital currency, as well as a considered technical difficulty. Given that the UnionPay network connects various banks, transaction data with higher privacy protection capabilities than existing database technologies should be provided. The existing blind signature, ring signature, zero-knowledge proof, homomorphic encryption, and other solutions are not mature, and complex encryption operations often have a huge impact on system performance (Reid and Harrigan, 2011; Sasson et al., 2014). To effectively ensure the stable operation of a system, the transaction data should only be visible to the strong related transaction parties. That is, the strong related transaction parties share the same key to encrypt and store the transaction, while other institutions only make consensus on the transaction ciphertext and storage.

4.2.4 Information network should be able to handle massive concurrent transactions

Digital currency is issued by central banks and belongs to the category of physical cash. Therefore, the information network supporting digital currency transactions will inevitably require strong concurrent processing capability and efficiency. Referring to the actual peak business volume of the current bank card cross-bank exchange system in China (exceeding 10000 transactions per second), the actual processing capacity of a digital currency system should not be below this level, in order to effectively support the stability of future massive transactions. At this stage, blockchain and DLT remain immature. The relatively widely used Bitcoin and Ethereum can only support an average volume of 7 and 20 transactions per second, respectively, while some mainstream consortium blockchain platforms can support hundreds or even thousands of transactions, which are still difficult to meet the future digital currency online payment processing requirements. Although such technical solutions as "lightning network" and sharding solutions exist, the specific implementation effects have yet to be tested (Eyal et al., 2015; Barger et al., 2017).

4.2.5 "Delayed online" supports offline transactions of digital currencies

In the traditional mobile payment and bank card transaction processes, offline transactions only exist in the electronic cash transaction, and have not been widely used and promoted. However, digital currency transactions should be mainly used online. To realize offline transaction, the readers can learn from the UnionPay ODA (offline

data authentication) technical solution (Luo and Xie, 2019), which uses the "delayed online" core technology: 1) Offline consumption: The near-field payment completed by users when the receiving and mobile terminals are offline, in which the receiving terminal directly reject or accept and provide the data to the backend system; 2) Request at a fixed time: The backend system calculates each transaction and initiates a transaction request online for a single user's payment fee at a fixed time; and 3) Transfer and clearing processing: Transaction is transferred from the UnionPay network to the corresponding commercial bank for clearing processing.

5 Conclusions

The emergence of digital currency is regarded as a significant change in the form of currency, which is expected to become the main circulation currency in the era of digital economy. The UnionPay network is one of the most important financial infrastructures in the field of payment and settlement in China, and is expected to provide effective support for the construction and operation of the digital currency system. This study systematically proposes the design scheme of digital currency information system based on the UnionPay network. First, we introduce the operation mechanism of a digital currency information system model from three stages: Digital currency account opening, exchange, and use. In particular, we explain how the proposed system can be grafted on the existing bank card acceptance environments in near-field and remote networking modes. Second, we discuss how to apply the emerging blockchain technology to digital currency from the academic aspect, including using the tamper-resistant and non-forgeable characteristics of distributed ledger to carry out digital currency registration and confirmation, and smart contracts to realize the "forward guidance" function of digital currency. Third, we introduce the significance of using the UnionPay network for digital currency system, such as reducing the construction costs of digital currency information system, effectively facilitating the operation of digital currency system, promoting the large-scale application and circulation of digital currency, and accelerating the internationalization of CBDC. Lastly, we analyze the technical challenges and related solutions of the UnionPay network supporting the construction of digital currency information system in terms of message format and transmission protocol, among others.

References

Australian Securities & Investments Commission (ASIC) (2017). RG 257 Testing fintech products and services without holding an AFS or credit licence. Available at: asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/

Barger A, Manevich Y, Mandler B, Bortnikov V, Laventman G, Chockler G (2017). Scalable communication middleware for permissioned distributed ledgers. In: Proceedings of the 10th ACM International Systems and Storage Conference, 23

Bordo M D, Levin A T (2017). Central bank digital currency and the future of monetary policy. National Bureau of Economic Research Working Paper No. 23711

Buterin V (2013). A next generation smart contract & decentralized application platform. Ethereum White Paper

Buterin V (2014). Slasher: A punitive proof of stake algorithm. Available at: blog.ethereum.org/2014/01/15/

Chaum D, Fiat A, Naor M (1988). Untraceable electronic cash. In: Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology. New York, NY: Springer, 319–327

Christidis K, Devetsikiotis M (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4: 2292–2303

Dwyer G P (2015). The economics of Bitcoin and similar private digital currencies. Journal of Financial Stability, 17: 81–91

Engert W, Fung B S C (2017). Central bank digital currency: Motivations and implications. Bank of Canada Staff Discussion Paper 2017-16

Eyal I, Gencer A E, Sirer E G, van Renesse R (2015). Bitcoin-NG: A scalable blockchain protocol. In: Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI'16). Santa Clara, CA, 45–59

Fan Y F (2018). Some considerations about central bank digital currency. China Business News, 2018–01–26(A05) (in Chinese)

Financial Conduct Authority (FCA) (2016). Regulatory Sandbox. Available at: fca.org.uk/firms/innovation/regulatory-sandbox

Han X, Yuan Y, Fang F Y (2019). A Blockchain-based framework for central bank digital currency. In: IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). Zhengzhou, 263–268

Hileman G, Rauchs M (2017). Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance Report

Hu B, Yang H (2019). The reference of British fintech regulatory sandbox and China's realistic choice. Economic Review Journal, (11): 103–116 (in Chinese)

Luo H, Xie C X (2019). Discussion on the application of financial IC cards based on ODA technology at Guangzhou Metro. Urban Rapid Rail Transit, 32(1): 93–97 (in Chinese)

Melanie S (2015). Blockchain: Blueprint for a New Economy. Sebastopol, CA: O'Reilly Media

Monetary Authority of Singapore (MAS) (2016). Fintech Regulatory Sandbox Guidelines. Available at: mas.gov.sg/development/fintech/sandbox

Monetary Authority of Singapore (MAS) (2019). Project Ubin: Central bank digital money using distributed ledger technology. Available at: mas.gov.sg/schemes-and-initiatives/Project-Ubin

Nakamoto S (2008). Bitcoin: A peer-to-peer electronic cash system. Available at: bitcoin.org/bitcoin.pdf

Qin B, Chen L C H, Wu Q H, Zhang Y F, Zhong L, Zheng H B (2017). Bitcoin and digital fiat currency. Journal of Cryptologic Research, 4 (2): 176–186 (in Chinese)

Qiu X (2017). Issuing digital currency by the People's Bank of China:

Path, problems and countermeasures. Southwest Finance, (3): 14–20 (in Chinese)

Radziwill N (2018). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Quality Management Journal, 25(1): 64–65

Reid F, Harrigan M (2011). An analysis of anonymity in the Bitcoin system. In: IEEE 3rd International Conference on Privacy, Security, Risk and Trust and IEEE 3rd International Conference on Social Computing. Boston, MA, 1318–1326

Sasson E B, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In: IEEE Symposium on Security and Privacy. San Jose, CA, 459–474

Shi X L, Zhou Z N (2018). Electronic payment, currency substitution, and money supply. Financial Economics Research, 33(4): 24–34 (in Chinese)

Wang S, Ouyang L W, Yuan Y, Ni X C, Han X, Wang F Y (2019). Blockchain-enabled smart contracts: Architecture, applications and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11): 2266–2277

Wang S, Wang J, Wang X, Qiu T Y, Yuan Y, Ouyang L W, Guo Y Y, Wang F Y (2018). Blockchain-powered parallel healthcare systems based on ACP approach. IEEE Transactions on Computational Social Systems, 5(4): 942–950

Yao Q (2016). Prototype of China's fiat digital currency. China Finance, (17): 13–15 (in Chinese)

Yao Q (2018a). Experimental study on prototype system of central bank digital currency. Journal of Software, 29(9): 2716–2732 (in Chinese)

Yao Q (2018b). The optimization of fiat digital currency to the current currency system and its issuance design. Studies of International Finance, (4): 3–11 (in Chinese)

Ye W H (2017). The operating mechanism of the British regulatory sandbox and its enlightenment to Chinese Internet finance regulation. Financial Development Review, (4): 46–53 (in Chinese)

Yuan Y, Wang F Y (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48(9): 1421–1428

Zhang J Z (2017). Regulatory sandbox: International models and development path in China. Financial Regulation Research, (5): 22–35 (in Chinese)