Blockchain: The Breakthrough Technology of the Decade and How China Is Leading the Way – An Industry White Paper

Chamber of Digital Commerce Publishes More than 80 Patent Applications Filed by the Chinese Government, Translated in English

By: Perianne Boring, Founder and President, Chamber of Digital Commerce and Marc Kaufman, Partner, Rimon Law

INTRODUCTION

The rise of digital currencies and blockchain technology will be remembered as one of the most important breakthroughs of the last decade. In just a few short years, digital currencies have captured the attention of technologists, regulators and some of the most powerful institutions and influencers around the world, including central banks, particularly the People's Bank of China (PBoC). About 80 percent of central banks are interested in or already pursuing central bank digital currency. China wants to be a leader in developing blockchain technology. Dubbed Digital Currency Electronic Payment (DC/EP), the Chinese central bank-controlled digital currency platform has been in production for a number of years and is currently being internally tested.[1]

It is important for policymakers and industry participants worldwide to understand how serious other nations are taking blockchain technology and what we can expect to see from frontrunners in the space. The PBoC has filed many patents relating to digital currency. *The purpose of this post is to leverage the disclosures of the PBoC patent applications to ascertain details of the platform that are likely to be implemented in support of the DC/EP platform.* This post does not attempt to predict the scope of protection that might be achieved through granted patents, and does not address the effect that such granted patents could have on restricting other parties from issuing digital currencies.

THE PBOC'S PATENT PORTFOLIO

Patent applications are published roughly 18 months after filing. Since this study is necessarily based on public documents, it does not include unpublished patent applications, e.g. patent applications filed in the last 18 months prior to January 22, 2019. The PBoC has filed 84 patent applications, as of January 2, 2020. All 84 published patent applications have been translated to English directly from the Chinese text of the documents for the purpose of this study. Note that none of these patent publications have yet been issued as granted patents. The patent portfolio includes patent publications teaching concepts that can be classified in the following non-exclusive categories:

- Digital Currency Management, Circulation and Interbank Settlement;
- Digital Currency Wallets;
- Processing Payments and Deposits; and
- Distributed Ledger Transactions and Technology.

1 *See, e.g.,* 21st Century Business Herald, 央行法定数字货币有望试点? 知情人士称是内部测试 [Central Bank Legal Digital Currency is Expected to be Piloted? Insider Claims Internal Testing] (December 12, 2019), https://www.cebnet.com.cn/20191212/102624015.html

OVERVIEW OF THE LIKELY DC/EP PLATFORM

Objectives and characteristics of the DC/EP platform have been described in the press based on public statements.

The Chinese Central Bank Digital Currency (CBDC) is a proposed digital legal tender centrally issued by the People's Bank of China (PBoC), backed 1:1 by fiat reserves. It aims to replace the M0 supply, through the digitization of cash and hence, would also rely on the credibility of the central bank. Some of its core features relate to manageable anonymity and encryption along with China's **CBDC not necessarily requiring a bank account (but may require KYC) to use the currency.**

Built on a two-tier system, the Chinese CBDC would be distributed through two distinct layers: (1) between the central bank and commercial banks and (2) between commercial banks and individuals & businesses.[2]

Further information on the DC/EP platform can be gleaned from discussions on August 10, 2019 at the China Finance 40 Forum where Mr. Mu Changchun, the Deputy Director of the PBoC's Payment and Settlement Department, announced that PBoC would soon be issuing the DC/EP and unveiled the overall design structure of the platform.[3]

From the perspective of the public, deposit, withdrawal, payment and circulation of the digital currency would occur in a manner analogous to a normal interaction with domestic commercial banks. The system will be designed to guarantee that transactions are anonymous from the user perspective, while also preventing money laundering, terrorist financing, and tax evasion. In other words, the PBoC will have at least enough insight into transaction information to conduct regulatory functions, such as Anti-Money Laundering (AML). The DC/EP is also designed to serve as a currency without disrupting central bank functions or competing with other financial products. However, it remains to be seen whether it's also designed to reign in WeChat and Alipay operations.

The PBoC patent portfolio gives us greater insight into likely implementations of the DC/EP. Briefly, the PBoC Patents indicate that DC/EP will be a tokenized crypto-currency (or perhaps simply a digital currency) managed by a distributed ledger and wallets that store and transact the asset in an "end-to-end" fashion. The tokens will be issued by a central bank and distributed to the public by commercial banks. Consumers and businesses would download a mobile wallet and swap yuan for the crypto-currency, which can then be used to make and receive payments. While transactions would appear anonymous to users, the DC/EP platform could track each transaction, including the value of the transaction and the identity of the transacting parties. The patents indicate, among other things, how wallets will be managed and how the DC/EP will be integrated tightly into the existing banking system.

2 *See, e.g.,* Binance Research, First Look: China's Central Bank Digital Currency (August 28, 2019), https://research.binance.com/analysis/china-cbdc

3 *See, e.g.,* Bloomberg News, China's PBOC Says Its Own Cryptocurrency is 'Close' to Release (August 11, 2019), https://www.bloomberg.com/news/articles/2019-08-12/china-s-pboc-says-its-own-cryptocurrency-is-close-to-release

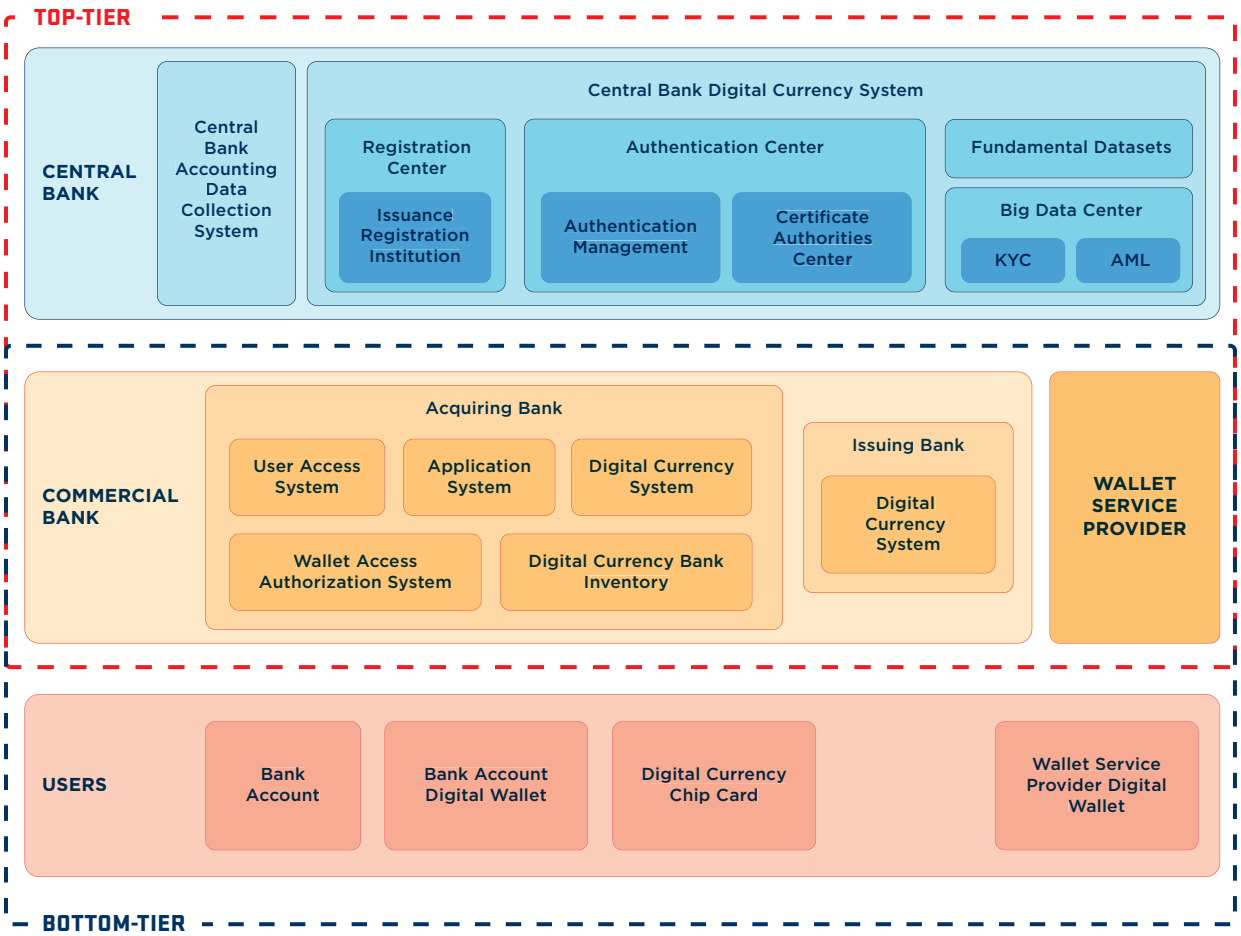

FIGURE 1 above is a block diagram, gleaned from various reports, of the expected DC/EP platform. On the top tier, the central bank issues and manages digital currency and distributes the same through commercial banks. On the bottom tier, however, commercial banks circulate digital currency amongst each other (through inter-bank transactions and settlements) and circulate digital currency between the central bank and users (individuals and business entities). An issuing bank issues digital currency to users.

Wallet service providers provide digital currency wallets to users. The wallets can be linked to conventional user bank accounts. Users transact digital currency through the wallets. User Identification is provided through a secure chip card or other user terminal device.

DETAILS YIELDED BY THE PATENTS

Various aspects of the DC/EP platform are discussed below in connection with examples of PBoC patents that correspond to the functions.

DIGITAL CURRENCY MANAGEMENT, CIRCULATION AND INTERBANK SETTLEMENT

Patent Publication CN108629678A discloses a method for managing digital currency supply based on economic conditions. Digital currency return interest rates are adjusted when the state of the economy fulfils certain set conditions and the digital currency is bought back by the core system according to the newly adjusted return interest rate. This process is intended to provide adjustment of the return interest rates that financial institutions impose on digital currency issuers according to the counter-cycle to the overall state of economy at the time. This would reduce the risk characteristics of financial institutions and the pro-cyclicality of their lending behavior to thereby avoid the "liquidity trap" and realize the counter-cyclical regulation of the economy. This indicates that the PBoC intends to apply algorithmic processes to manage digital currency in accordance with conventional economic theories to avoid adverse effects of market fluctuations.

Patent Publication CN107330692A discloses a method for the circulation of digital currency, which can meet the requirements of physical currency circulation. A payment node will select a digital currency data string from a digital currency safe deposit storage (which stores digital currency data strings associated with the payment node) based on the payment amount and a matching algorithm. The digital currency data string set will then be sent from the payment node to a corresponding management node. The digital currency data string contains the payment amount field and all of the identification fields. The management node will register the data strings from the digital currency data string set originating from the payment as inactive and send the digital currency data strings a payment collection node. The amount in the payment-related digital currency data strings will become the payment amount and the identification will become the payment collection node.

Patent Publication CN 107358522A discloses a method and system for the exchange of digital currency and deposits without the need for banks to return currency through the digital currency issuing institute. Deposits are exchanged with other banks that are in need of digital currency, therefore promoting the usage of digital currency. A bank's system sends a report on the usage of digital currency to exchange for deposits to the agency bank's system, and sends a report on the digital currency payment to the agency bank to the digital currency system. The digital currency system processes the report, and sends the results to the bank and an agency bank's system. The balance of the bank's interbank deposit account in the agency bank will be increased by the amount equivalent to the digital currency amount.

Patent Publication CN107392751A discloses a method for inter-bank digital currency settlement, which integrates the traditional settlement method with digital currency to provide banks with flexibility in the choice of settlement. The bank system sends a digital currency payment message to the digital currency

core system. Also, a clearing message regarding the sending of digital currency to the receiving bank is sent to the clearing bank system. The digital currency core system processes the message, and then sends the results to the initiating bank system and the clearing bank system. The clearing bank system increases the balance in the receiving bank's interbank account deposit by the amount equivalent to the digital currency payment and returns a successful clearance message to the receiving bank and initiating bank.

The PBoC patents indicate that the DC/EP Platform will leverage characteristics of digital currency to streamline circulation by allowing banks to use various settlement mechanisms that increase efficiency. Digital currency circulation and settlement will be tightly integrated with conventional banking processes.

DIGITAL CURRENCY WALLETS

Patent Publication CN107392601A discloses a method for a user to apply for a digital currency wallet through a bank account and binds the bank account and digital currency wallet. The acquiring bank user's access system receives information on the user's digital signature and digital currency wallet application, and sends the information to the acquiring bank's digital currency system which verifies the user's digital signature, creates the digital currency wallet, assigns a digital certificate to the wallet and adds the acquiring bank's digital signature to the wallet identification and certificate before sending it to the issuing bank's digital currency system which verifies the acquiring bank's digital signature.

Patent Publication CN108229938A discloses a method for the opening of a digital currency wallet. A digital currency wallet terminal generates a private/public key pair and sends the public key to a wallet service provider. The wallet service provider sends the public key and a corresponding wallet identification to the digital currency issuance registration institution. The digital currency issuance registration institution sends the digital certificates generated from the public key and wallet identification to the wallet service provider and the wallet service provider sends the digital certificate, wallet identification and wallet contract code address to a digital currency wallet terminal to create the digital currency wallet in accordance with the digital currency wallet terminal's opening request. A registration request is sent to the digital currency issuance registration institution and the digital currency issuance registration institution proceeds with the registration in accordance with the registration request, wallet identification and wallet certificate.

Patent Publication CN108197214A discloses a method of querying information on a digital currency transaction. A digital currency wallet terminal receives a user transaction information query command and uses the private keys corresponding to a wallet to attach a digital signature to the transaction query before sending the query to a wallet service provider. The wallet service provider verifies the digital signature before sending the query to the digital currency issuance registration institution. The digital currency issuance registration institution verifies that the signed command fulfills the query based on conditions in the query to obtain the transaction information as a query result. This allows the digital currency wallet to query the digital currency issuance registration institution and interact with the digital wallet issuance registration institution to thereby accomplish a user query of digital currency transaction information.

Patent Publication CN108229142A discloses a method for upgrading digital currency wallets. In response to a request to upgrade a wallet, a digital currency wallet terminal send the request to a wallet service provider

for verification. The wallet service provider returns upgrade installation information to the digital currency wallet terminal. Upon confirmation of the upgrade installation information by the user, the digital currency wallet terminal will send the upgrade approval command to the wallet service provider and will complete the upgrade through the wallet service provider. This allows a wallet terminal to undergo self-upgrade and achieves secure and flexible wallet upgrades.

Patent Publication CN108038678A discloses a method and system for cancelling digital currency wallets. A digital currency wallet terminal will confirm that the amount in the wallet pending cancellation is equal to zero in accordance with a wallet cancellation request submitted by the user. A digitally signed cancellation command is then sent to the wallet service provider for legal confirmation before cancelling the pending wallet's certificates and wallet identification. Thereafter, the wallet service provider sends the signed cancellation command to the digital currency issuance registration institution for confirmation that the signed cancellation command is indeed legal, before cancelling the pending wallet's certificates and wallet identification.

Patent Publication CN107392579A discloses a method for unbinding digital currency wallets with bank wallets. After receiving an unbinding request submitted by a user, a bank account access authorization request is sent to the user, and verification of the user's identity is performed. If the user is authorized, a binding between the stated user's digital currency wallet and user's bank account is cancelled. Accordingly, the functions of the digital currency wallet are effectively expanded and integrated into the user's bank account.

The PBoC patents indicate that the DC/EP will tightly integrate the creation, use and management of digital currency wallets with the existing banking system. For example, conventional bank account information will be used for identification and authorization.

PROCESSING PAYMENTS AND DEPOSITS

Patent Publication CN107369009A discloses a method and system for automated digital currency payments that addresses the problem of seller and third-party credit risk. The payee is notified after the receipt of a payment processing request sent by a payer. The payment is then processed in accordance with a payment contract between the payer and payee. The payment process request includes the payee's identification and the payment contract's matching information. Payment verification information is generated when the payer and/or the payee and/or the third party undergoes the business process in accordance with the payment contract. The payment verification information is verified in accordance with the payment contract and the payment process is carried out upon successful verification.

Patent Publication CN107392578A discloses a method for the indirect payment of digital currency. A payment request is sent by the payee account. The payment request specifies the digital currency to be used in the payment, the payment amount, and payee client agent information. The stated digital currency payment amount will be paid to the agent and at least a portion of the stated payment amount will be transferred to the final payee client in accordance with a pre-selected contract. This is intended to decrease risk in the transfer between the payer and the final payee across one or more agents.

Patent Publication CN107392580A discloses a method for exchanging digital currency for deposits. A user's identity is verified in accordance with the user's bank account information. A digital currency exchange deposit request is provided by the user to generate a digital currency transfer request toward the issuing bank's digital currency system. The digital currency exchange deposit request specifies information on the exchange amount, while the digital currency transfer request specifies all of the digital currency information pertaining to the user. A transfer confirmation is returned by the issuing bank's digital currency system. The transfer confirmation includes information pertaining to the generation of destination currency from the original currency. The destination currency is transferred to the acquiring bank's digital currency bank inventory, thereafter increasing the exchange amount of the stated user's verified bank account. This method allows for the controllable and traceable exchange of digital currency to deposit and thus allows the digital currency to be integrated into the banking system.

Patent Publication CN107392600A discloses a method for digital currency transaction payment registration. A digital currency transaction payment registration request is received, the existing digital currency registration status is deleted, and the new digital currency is registered in accordance with the stated transaction payment registration request. A confirmation is returned upon the successful registration to the requester of the digital currency transaction payment registration.

Patent Publication CN107230072A discloses a method for using a digital currency chip card for online transactions. A user terminal device sends payment information to an acceptance terminal device. The payment information includes the digital currency chip card information and the digital currency equivalent to the payment amount. The acceptance terminal sends the payment information to a commercial bank's digital currency system and the commercial bank's digital currency system sends a change-in-owner request to the central bank's digital currency system after receiving the payment information. The central bank's digital currency system changes the owner of the digital currency to the commercial account's merchant bank code and the commercial bank's digital currency system changes the commercial bank's account balance.

Patent Publication CN107230050A discloses a method for digital currency payment with a physical digital currency chip card, which is appropriate for offline payment. The payer's digital currency chip card sends a payment request to the payee's terminal device in the event there is no internet connection with the commercial bank's digital currency system. The payee's terminal device initiates the network connection after receiving the request and sends the payment request to the commercial bank's digital currency system once a network connection is available. The commercial bank's digital currency system sends the payment confirmation request to the central bank digital currency system to change the digital currency's owner and the central bank's digital currency system proceeds with the preset process in accordance to the request, and then sends the results to the payee's terminal device.

Patent Publication CN107230054A discloses a method for the depositing of digital currency into a deposit account. A terminal device receives the deposit amount and deposit account and determines the total digital currency amount in the digital currency wallet equivalent to the deposit amount. The terminal device sends the digital currency and deposit account to the merchant bank's digital currency system and the commercial bank's digital currency system sends the digital currency and deposit account to the central bank's digital

currency system. The central bank's digital currency system changes the digital currency owner from the user to the commercial bank and sends the successful results of the transaction to the commercial bank. The commercial bank's digital currency system increases the deposit amount in accordance to the results, thereafter sending the results to the terminal device. Therefore, the DC/EP will integrate digital currency deposits into the existing banking infrastructure in a manner that is analogous to fiat currency.

The PBoC patents indicate that payments and exchange of digital currency will be traceable and tightly integrated into existing banking system mechanisms.

DISTRIBUTED LEDGER TRANSACTIONS AND TECHNOLOGY

Patent Publication CN106850200B discloses a method for using blockchain for the security of digital currency. A digital currency client terminal sends a digital certificate registration request to the blockchain and receives the client information returned by the blockchain after verification of the identity and request. In accordance with the client information, the digital certificate registration is sent to a security chip through a trusted processing environment and the security chip generates a private key pair and digital currency wallet address in accordance with the client information, and outputs the digital currency wallet address from the digital currency client through the trusted processing environment. The digital currency client sends the digital currency wallet address to the blockchain, causing the blockchain to obtain the digital certificate from a verification center in accordance with the digital currency wallet address. The digital currency client receives the digital certificate sent by the blockchain and sends the digital certificate installation request to the security chip through a trusted processing environment, which causes the security chip to install the digital certificate.

Patent Publication CN109118363A discloses a method for the management of blockchain-based digital currency wallet addresses. Transaction requests initiated by the transaction parties' wallet addresses are verified by a smart contract. If verification is successful, the wallet addresses are updated, and the updated addresses are saved in the smart contract. This allows the transaction parties to use the new wallet addresses to initiate another round of transactions. The updating of the original wallet addresses eliminates the bind between the original wallet addresses and the transacting parties' real identity information to make tracing of the party's real identity through the original wallet addresses difficult.

Patent Publication CN106779707A discloses a regulatory method for digital currency transaction information. The initial public key of the supervising user, the initial public key of each participating user, digital currency transaction information of each participating user, and the first participant's user information are stored on the blockchain. The initial public key of the first participating user is obtained from the blockchain, and according to the initialization of the first participating user and the initialization private key of the supervising user, the first shared private key of the first participating user is generated using a shared key algorithm. Through the use of the first participant's shared private key, the plaintext data of the transaction can be obtained by the supervising user while preventing others from obtaining the data in clear form. The PBoC patents thus confirm that, from a user perspective, transaction data is confidential. However, transaction data is readily available to selected regulators.

SUMMARY

The PBoC patents indicate that the DC/EP platform will be tightly integrated into existing banking systems. Digital currency wallets can be bound to conventional bank accounts in a dynamic manner. Digital currency circulation will be managed by the central bank system and payments and deposits will be processed through commercial banks. Users will be pseudonymous. However, regulators will be able to track all transaction information, including the identity of the transacting parties, and process the transaction data in various ways to achieve regulatory oversight.

Blockchain technology offers immense possibilities for business, government, and consumers. These include the opportunity for extraordinary economic growth and a safer and more secure financial system. With the imminent release of the DC/EP platform, China and other major industrialized nations are making significant advances in promoting and adopting this technology, making a hard run to surpass the United States and to obtain the economic value blockchain technology offers.

Special thanks to Natasha Ann Lum and Jonathan LeMaire for their contributions to this report.