

|  |
| --- |
| Central Bank Digital Currency  Summary Report  2019 |
|  |
| December 13  Authored by: Hadi Jibbawi |



|  |
| --- |
| **Central Bank Digital Currency** The acceleration of technological advancement and transformative force are impacting the main role of Central Banks across the world, and reshaping the financial ecosystem toward widely accessible and digitized ecosystem. Central Bank Digital Currency is one of the challenges due to the emerging customer needs, technology revolution and the private cryptocurrencies issued by private parties.  **Definition** Central Bank Digital Currency, known as CBDC, is a digital currency issued and regulated by the Central Bank (CB), more broadly accessible than current CB deposits, and serves as a legal tender.  CBDC has two variants:   1. **Wholesale CBDC:** the case of commercial banks and clearing houses. Banks and big institutions open their own account at Central Bank. The network in this case is private with limited known members.   Wholesale CBDC focuses mainly on domestic use to enhance the efficiency in interbank payments and interbank securities and settlements.  Some of the countries that are experimenting this type are: Canada, South Africa, Japan, Thailand, Saudi Arabia.   1. **Retail CBDC:** the case of general use for peer to peer payments and payments from consumers to merchants. CBDC aims to replace cash, and exposed to the general public with high availability from everywhere at any time.   Some of the countries that are experimenting this type are: Sweden and Uruguay.  Retail CBDC has two issuing forms:   * + **Account-based CBDC:** Balances in reserve accounts and many forms of commercial banks money are account-based. Individuals and firms hold their accounts at Central Bank and use it to transfer funds.   + **Token-based: CBDC:** known as “value-based”. Cash is token-based, in which users store CBDC in their digital wallets and use these wallets to transfer value when making any payment.    In operation perspective, the structure and design of the whole ecosystem is one of the following forms regardless of the technologies used:  * Centralized System: Central Bank plays the actual CB roles plus the central role in the retail CBDC and customers network in place of the commercial banks. In other words, CB manages everything related to CBDC, i.e. issuance, circulation, liquidity control, risks mitigation, AML, transactions verification, account holder, etc. In this case, a heavy and expensive package will overload Central Bank’s work plus will add another couple of complex systems to overcome these roles including the following:   Moreover, the anonymity and direct settlement of cash is not solved in this approach, because every transaction is processed and validated from the payer to the payee through CB processes.  Single Point of Failure (SPOF) is another drawback regarding this approach. The huge work overload, the wide network, the large number of connections, and the increase of accessibility to Central Bank will increase the risk of undergoing system failures or security attacks that has direct effect on the availability of CBDC system.   * Decentralized System (Peer to Peer): CB acts as a member in the P2P network where each peer has a copy of the ledger and can update it with consensus and some further processing.   The default role of Central Bank in this approach is cancelled. CB cannot manage and control the monetary policies, exchange rate, and security policies such as AML.   * Two Tier System: Similar to the existing form of ecosystem. The first tier represents the traditional links of Central Bank with commercial banks and financial institutions. Whereas, the second holds the relations of customer-to-customer, customer-to-business, business-to-customer, and business-to-business.  However, in any CBDC design, the model has to consider the following:  1. Maintain the role of Central Bank in the financial ecosystem: issuance, liquidity management, KYC, AML, financial inclusion, etc. 2. Provide a secure, resilient, and scalable network. Meanwhile when CBDC is considered as cash, peers should be anonymous with direct settlement of transactions (i.e. transaction and settlement are one).   *Hint: security, anonymity and direct settlement could be served by Distributed Ledger Technology (DLT). Whereas, Scalability and resiliency could be served by the Big Data Technologies (Hadoop, Kafka, etc.).* |
| **People’s Bank of China CBDC****Operating Structure** People’s Bank of China (PBoC) proposed a​ two-tier operating structure​ for its CBDC, represented by two distinct layers:   1. The first layer plays the role of direct interaction between commercial banks and the People’s Bank of China. Mainly, the PBoC issues and redeems its CBDC only​ via commercial banks. 2. In the second layer, ​ CDBC would also be ​token-based. Financial institutions like commercial banks, would be responsible for distributing CBDCs to the general public as well as businesses, which would then circulate the CBDC. From the perspective of both individuals and businesses, the deposit and withdrawal processes would occur in a similar fashion as a normal interaction with their domestic commercial banks.     **Two-tier Prototype Operating System of PBoC’s CBDC**  By adopting ​the two-tier system on its digital currency​, the People’s Bank of China would achieve its goal of ​replacing paper money ​without subverting the existing monetary issuance and circulation system, which is also ​two-tier based​ (i.e., commercial banks are required to maintain capital above the required minimum reserve ratio at the PBoC).  Technical Points   1. **Manageable Anonymity Mechanism**   China’s CBDC will adopt a ​"loosely-coupled" design, allowing fund transfers without a bank account.  The end goal for the CBDC is to display a turnover rate as high as cash, while achieving “manageable anonymity”. In other words, in the first-layer network of the CBDC, real-name institutions are expected to be registered while the transfer in the second-layer network would be anonymous ​from the perspective of users. Officials from the PBoC believe that this would benefit “both the RMB’s circulation and internationalization”. |

1. The Use of Encryption Algorithm

The proposed model of the prototyped CBDC is expressed as:

EXPCBDC = Sign(Crypto(ATTR))

ATTR є {id, value, owner, issuer, ExtSet}  
  
​*EXPCBDC: the CBDC’s encrypted expression;  
ATTR: the attribute set contained in the expression;  
Crypto: the encryption process of the attribute set;*  
*Sign: stands for signature computations for the expression.*

This attribute set includes the following information:

​id ​= the user id, ​value ​= amount of the money, ​owner ​= owner’s information, ​issuer ​= the issuer’s information, ​ExtSet ​= extendable, scalable attribute set.

The basic process would be encrypting the information metadata, then perform a signature operation, and then receive the output of the encrypted string for the CBDC output.

Regarding wallets, there is very little information about how digital wallets would operate.  
However, China’s CBDC is likely to be accessible on mobile devices, personal computers or physical IC cards, depending on what specific currency networks the Chinese CBDC would run on.

1. No Preset Technical Roadmap, Blockchain is an option

As mentioned above, the operational system of China's CDBC is a two-tier system, with the first layer of the network being a centralized distributed ledger.  
However, it remains​ uncertain whether the second layer would also be based on a blockchain network​. As the second layer management would be delegated to financial institutions, the ​Chinese CBDC could potentially run on multiple different networks at the same time. Undeniably, the two-layer network supporting the CBDC targets to achieve transaction performance of "​at least 300,000 transactions per second​". As of today, blockchains do not achieve performances as high as the target requirement. However, this transaction speed could potentially be achieved with the "off-chain relay, on-chain settlement" mechanism or through other scaling improvements such as sharding or side-chains.

1. Smart Contract Availability

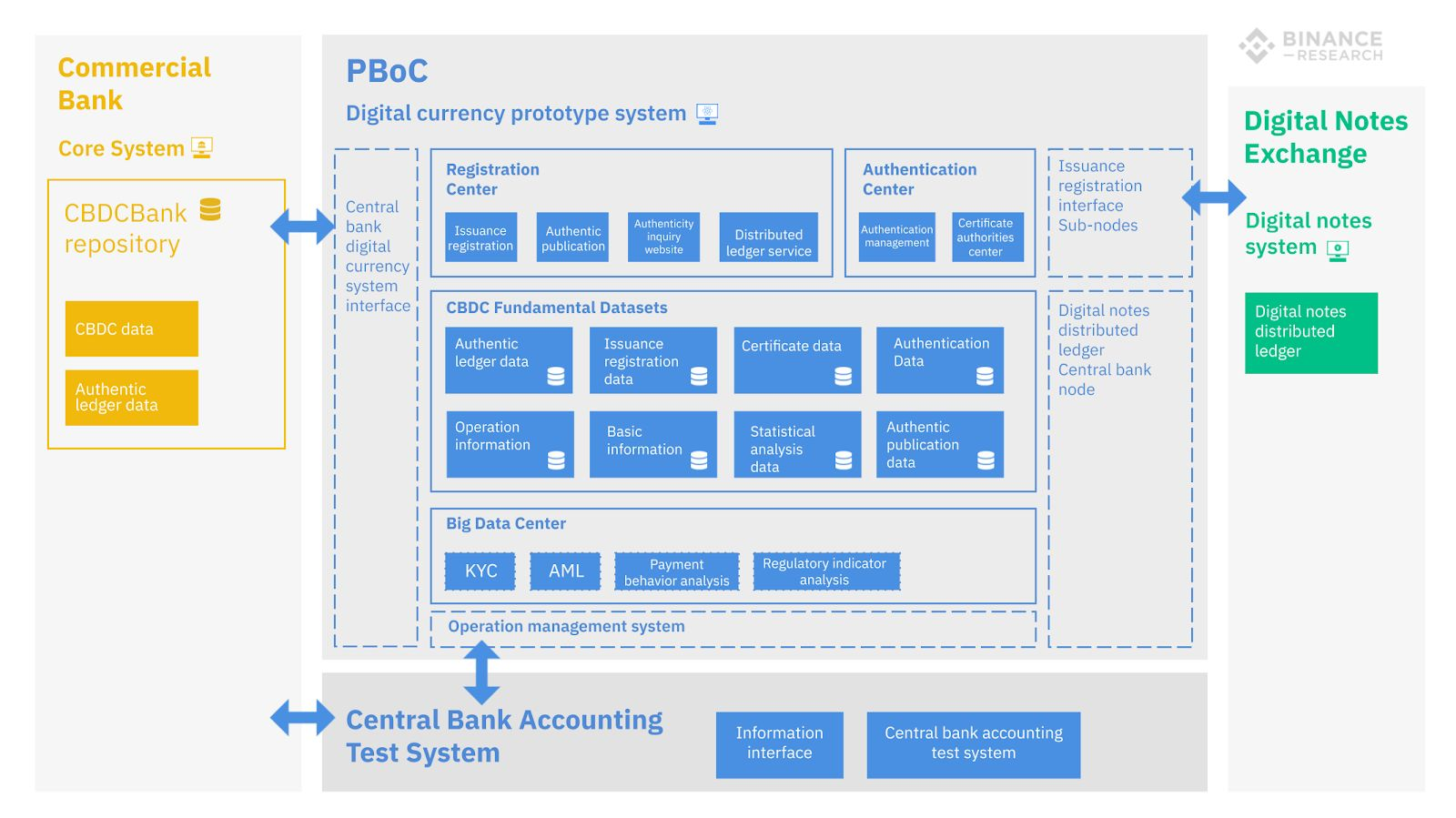
The People’s Bank of China suggested that its CBDC could function with smart contracts, but would not run on contracts that provide functionality beyond that of “basic monetary requirements”. This is due to concerns that ​it may add additional value to the CBDC and “downgrade” this CBDC into some kind of security​, consequently reducing its stability and usability, and adversely affecting the internationalization of the renminbi (RMB). However, the definition of "basic monetary requirements” has not been disclosed yet, and little information has been provided by the central bank so far. Yao Qian, former head of PBoC's Digital Currency Research Department, in his 2017 paper25, emphasized that the central bank's digital currency should be programmable and extensible. In addition, if the digital currency also included automated and reliable execution thanks to smart contracts, which could pave “a new direction for the development of the legal digital currency”.

Yao Qian also mentioned that in a simulation test of a trading platform with blockchain based digital notes, the introduction of smart contracts for liquidity management “greatly improved” trading efficiency.

1. “One Coin, Two Repositories, and Three Centers”

CBDC would be built on the following "​one coin, two repositories, and three centers​"approach. Specifically, there are several elements that need to be considered:

* "One coin" ​refers to the Chinese CBDC itself: an encrypted digital string representing a specific amount guaranteed and signed by the PBoC.
* “​Two repositories"​ refer to the central bank's issuance database and the commercial bank's database, as well as the digital currency wallets used by individuals or organizations.
* “​Three centers"​ refer to authentication, registration, and big data analysis centers. An overview of these centers are as follows:
  + Authentication center: PBoC would implement centralized management of financial institutions and end-user identity information, which is the basic component of system security and an important module of the controllable anonymity design. However, in the early stages of the system, the PBoC may  
    only authenticate and manage the identity of financial institutions. In the future, authentication support for end-users may be built based on technologies such as IBC (identification-based ​cryptography​).
  + Registration center: ​Record the identity of each unit of China’s CBDC and corresponding users, and complete the registration of China’s CBDC for the following functions: issuance, transfer and redemption.
  + Big data analysis center: ​Serve​ ​several functions such as preventing  
    anti-money laundering, analyzing payment behavior analysis, monitoring real-time regulatory indicators, etc.



One, Two, Three approach schema

1. Privacy and Anonymity

The "three centers" are designed to guarantee that Chinese CBDC's transactions are anonymous from the user perspective​, while also preventing money laundering, terrorist financing, and tax evasion. Mu Changchu, the deputy director of the PBOC’s Payment and Settlement Department, in his speech on August 10th, stated that China’s CBDC aims to "strike a balance" between anonymity and the AML/CFT/ATA work”. China’s CBDC is less likely to be an instrument of illegal activities even if it were anonymous like cash, as both the PBoC and financial institutions on the second layer would have the ability to immediately freeze any CBDC or accounts if they were involved in suspicious transactions, helping deter illicit activity on the network. According to Yao Qian's 2018 version of the prototype system, China's CBDC expression contains a user id and the owner information, and according to his description, every time a CBDC is transacted, it will generate a new CBDC string which includes the new owner’s  
identity.  
Even if transactions would be anonymous at the user level, it would still remain possible to retrieve the entire history of transfers of each individual CBDC unit, hence providing it a variable ​fungibility​ status. It would be more fungible than most cryptocurrencies, like Ethereum and Bitcoin, at the user level as transaction history would not be retrievable.

However, unlike privacy coins, central authorities would be able to gather information.  
Eventually, identities would likely be tied to respective individual wallets, hence making it fully non-anonymous, unlike Bitcoin.

## **Facebook Libra**

Facebook is considered a major motive of Central Banks to investigate and research in Central Bank Digital Currency. It released a white paper about its own cryptocurrency, known by Libra, and its testnet for its blockchain system before a public launch in the first half of 2020.

Libra is not CBDC. However, it would mitigate the Central Bank roles through providing essential digitized financial services.

Libra is a cryptocurrency which will allow purchases and money transfers with nearly zero fees. Anyone will be able to purchase Libra online or at local exchange points, and spend it via interoperable third-party wallet apps or Facebook’s own Calibra wallet that will be integrated with Whatsapp, Messenger and its own application.

Once anyone purchases Libra through dollars or his respective currency, Libra is minted and doled out to that person, while the paid currency goes into the Libra Reserve. And when this person aims to go out the Libra Association, his owned Libra are destroyed and he will receive back an equivalent value in his local currency. This guarantees that 100% of the Libra is in circulation, collateralized with real-world assets in the Libra Reserve.

## **The Libra Blockchain**

Libra Blockchain is a cryptographically authenticated database that acts as public online ledger designed to handle 1000 transactions per second. The blockchain is operated and constantly verified by founding members of the Libra Association, in which each member invested $10 million or more for a say in cryptocurrency’s governance and the ability to operate a validator node.

Every payment is recorded permanently to this blockchain. When a transaction is submitted, each of the participating nodes runs a calculation based on the existing ledger of all transactions. Also, the blockchain’s system is Byzantine Fault Tolerant, so only two-thirds of the nodes must come to consensus the legitimation of the transaction before it is executed and recorded to the blockchain.

A technical drawback in Libra is that if an attack compromises over one-third of the validator nodes causing a fork in the blockchain, Libra Association temporarily halt transactions, figure out the extent of the damage and recommend software updates to resolve the fork.

The current Libra Blockchain is permissioned, where only entities that fulfill certain requirements are admitted to a special in-group that defines consensus and controls governance of the blockchain. This structure is not truly decentralized, so it is more vulnerable to attacks.

The dilemma is that till now Facebook failed to find a permissionless structure that is reliable and code scale securely to the number of transactions Libra will need to handle. Also adding more nodes will slow the overall work efficiency.

Libra Association’s target is to move toward permissionless system based on proof-of-stake that will protect against attacks by distributing control, encourage competition and lower the barrier to entry.