

|  |
| --- |
| Central Bank Digital Currency  Summary Report  2020 |
|  |
| May 4  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, cash decline and the private cryptocurrencies issued by private parties.  **Definition** Central Bank Digital Currency, known as CBDC, is a digital payment token which is issued and fully backed by central bank and considered as legal tender. It may be exchangeable with bank notes and reserves. Also, CBDC is considered programmable money in which specific design features and attributes can be built into the token itself. Generally, CBDC has two types: ‘wholesale central bank digital currencies’ that enhances the efficiency of the central bank clearing operations between the central bank and its member banks, and ‘retail central bank digital currencies’ for public use and equivalent of a bank note but in digital form. CBDC might be exposed to the general public with high availability, anonymity and security. Each central bank could design their CBDC according to monetary policy and economic objectives central bank sees.  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.   * 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.   Most of the projects performed proof of concept to assess the use of blockchain in banking to address scalability, resilience, privacy, securities settlement and cross-border transactions. It is expected that central banks will initially issue their CBDC on a permissioned or private blockchain network. This means that access and control to the blockchain is limited to a select group of approved participants, permitting the central bank to retain control of the overall money supply. |
| **People’s Bank of China CBDC** Realizing the impact that Facebook’s Libra could have on China’s foreign exchange management and cross-border capital flows, as well as affecting the Renminbi’s (RMB’s) internationalization, the Chinese central bank accelerates its plans to launch its own digital currency.  Chinese CBDC is considered digital legal tender issued by people’s bank of china (PBoC), backed 1:1 by fiat reserves, with manageable anonymity and encryption features. PBoC didn’t release any formal document about their CBDC. However, based on details provided by the central bank related entities, the CBDC will be based on a two-tier system for issuance and redemptions. **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 features direct interaction between commercial banks and PBoC, and would include online payment service providers. Namely, the PBoC would issue and redeem China’s CBDC 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. And as this layer would be managed by financial institutions, the Chinese CBDC could potentially run on multiple different networks at the same time.     **Two-tier Prototype Operating System of PBoC’s CBDC**  Undeniably, the two-layer network supporting CBDC targets to achieve transaction performance of “at least 300000 transactions per second”. Blockchain 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 scaling improvements such as sharding or side-chains. Yet, on this second layer, the use of blockchain remains undecided as the PBoC still hasn’t drafted a clear technical roadmap for its digital currency.  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. Hence, CBDC can be stored in digital wallets in the form of digital ledgers verified by cryptography and consensus algorithms. In Mr. Yao’s (the former head of PBoC’s Digital Currency Research Institute) 2018 paper, private cryptocurrencies are criticized as displaying not enough information to express the real attributes of a currency. As a result, some of the missing elements have been added into China’s CBDC publicly-released design attributes. Specifically, the proposed model of the prototyped CBDC is expressed as:  EXPCBDC = Sign (Crypto (ATTR))  ATTR ɛ {id, value, owner, issuer, ExtSet}  *EXPCBDC: CBDC’s encrypted expression/ ATTR represents 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.

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.

1. Smart Contract Availability

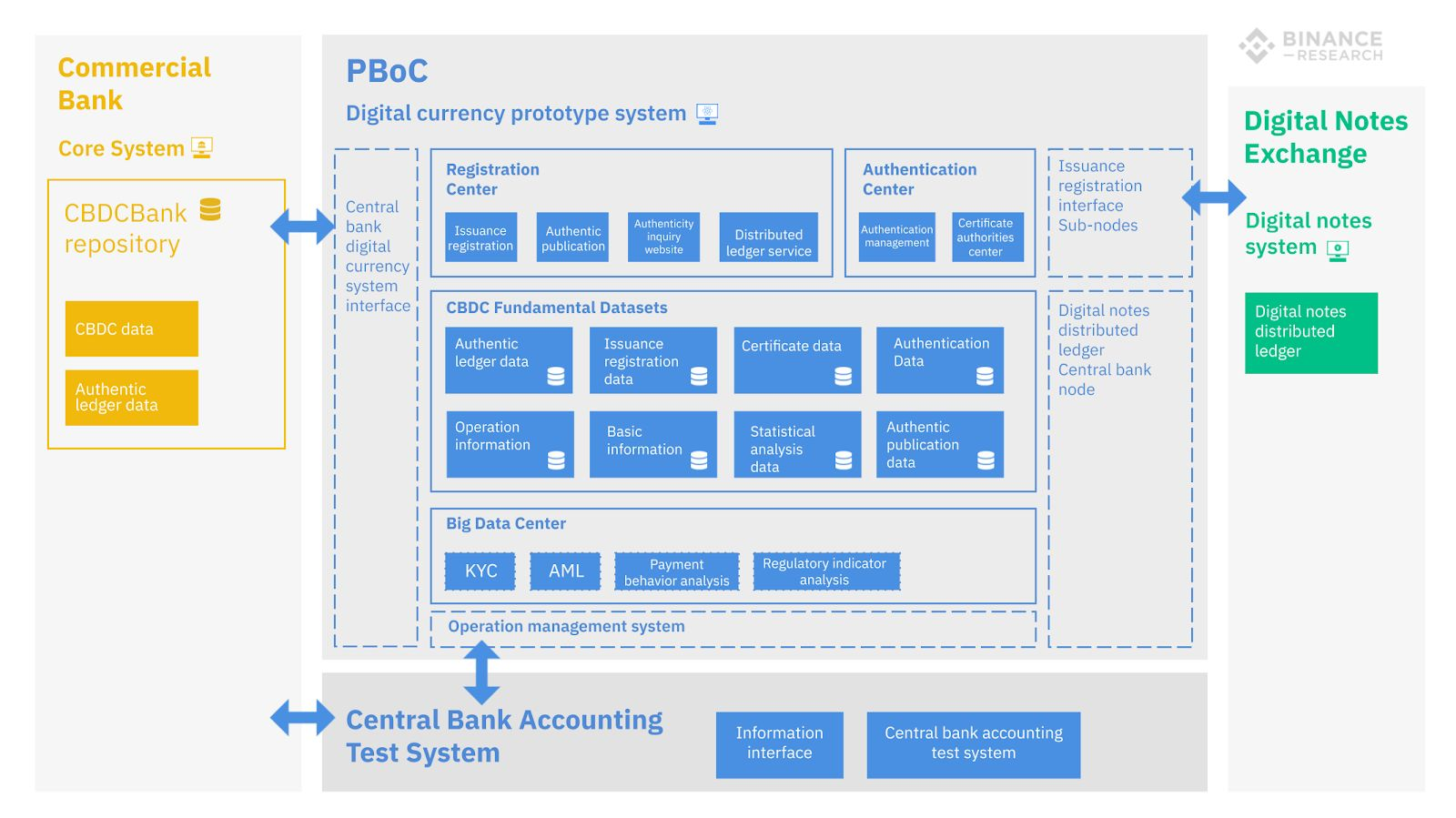
The People’s Bank of China suggested that its CBDC could function with smart contracts, but would not run on contracts that provide functionality beyond that of “basic monetary requirements”. This is due to concerns that ​it may add additional value to the CBDC and “downgrade” this CBDC into some kind 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.

China expects that CBDC would share major properties of cash such as portability and anonymity, make clearing more efficient for institutions by a distributed inter-bank ledger system, enable increased speed and lower costs for cross-border payment, lower the operating costs – in the existing cash-based system, issuance, operation and maintenance costs of paper currency and coins are relatively much higher, and improve anti-money laundering policies and reduce illicit uses – since cash remains the easiest way for such activities, the use of CBDC would lead to lower risks and threats from illicit activities.

By issuing a digital currency, it is believed by some analysts that the PBoC could use its CBDC to internationalize the RMB.

## **European System of Central Banks (ESCB)**

In fact, any digitization in the economy should take into consideration the balance between a certain degree of privacy in electronic payment and guarantees compliance with regulations aimed at tackling money laundering and the financial terrorism (AML/CFT regulations). For that, ESCB introduce a proof of concept which states that is possible to deliver a simplified payment system that gives users some degree of privacy for lower-value transactions, while still ensuring that higher-value transactions are linked to mandatory AML/CFT checks.

The proof of concept provides a digitization solution for AML/CFT compliance procedures, whereby a user’s identity and transaction history cannot be seen by the central bank or intermediaries other than that chosen by the user. The enforcement of limits on anonymous electronic transactions is automated, and additional checks are delegated to an AML authority. This anonymity automation is achieved using “anonymity vouchers” that allow users to anonymously transfer a limited amount of CBDC over defined period of time, as to be explained in the technical part.

However, ESCB built their proof of concept on four principles:

1. CBDC should have cash features. The privacy of users’ lower-value transactions is required, and balances are not remunerated.
2. The design is built around intermediaries in a two-tier model. In this case, intermediaries that have central bank accounts provide CBDC to users. Intermediaries, also, process transactions on behalf of their clients and offer them custodial services.
3. Central bank is the only entity that issue CBDC units and remove them from circulation.
4. A dedicated “AML authority” performs AML/CFT checks. This authority checks the identity of the users involved in large-value transactions and prevents CBDC from being transferred to embargoed users.

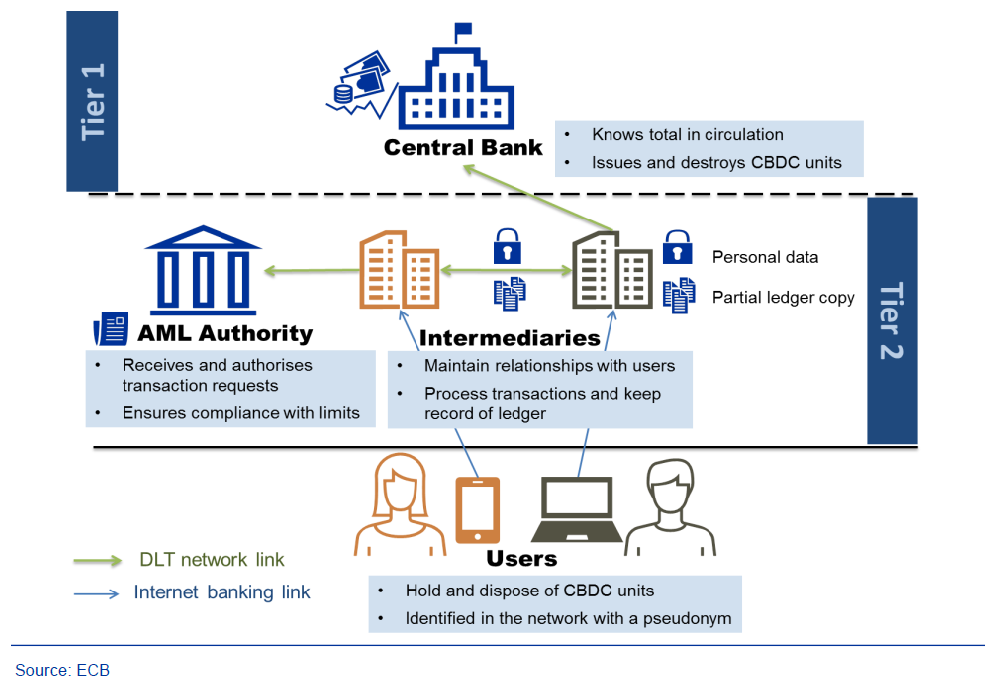


Figure 1 Two-tier model and relationship between entities

Technically, the proof of concept (PoC) has been developed using Corda. Corda is a Distributed-Ledger-Technology (DLT) platform which is designed to ensure that the information held locally by two users, which store details of their bilateral transactions, is consistent with the overall information in the system, without these information being shared with other users, thus a user for instance cannot spend the same CBDC unit in two different transactions with two different payees. The PoC sorts four entities (2 intermediaries, 1 central bank, and an AML authority) – each is represented in the network by a node that operates a CorDapp (this logic enables assets to be transferred between entities), an intuitive web application allowing interaction between users, and a set of application programming interfaces (APIs) allowing communication and interaction between parties.

CBDC units are represented in the ledger by Corda “states” (a state template provides standard definitions and patterns for the representation of assets in Corda ledger). Each state holds information on its value, details of its past and current owners, and cryptographic proof of its validity. Sates in Corda follow the unspent transaction output (UTXO) model, whereby ever transaction consumes one version of a state and triggers, in the same ledger, the creation of a new version that can be used in a subsequent transaction. At any given time, only state versions that are unspent, and whose previous versions have been spent in accordance with the rules of the system, can be accepted by payees. It is ultimately the responsibility of payee’s intermediary to ensure that the states which are received by its client are valid and can be redeemed with the central bank on demand.

Also, a special node called “non-validating notary” allows intermediaries to check the validity of states by maintaining a registry of all currently valid UTXO’s. To protect users’ privacy, the notary has no access to data such as transaction values, users’ addresses or states’ histories. Rules governing transfers of states between parties are kept to the minimum that is necessary to avoid double-spending and implement AML constraints set by system. At the same time, all entities are able to apply additional rules of their own choosing while maintaining adherence to the core rules, and can turn CBDC units into programmable money.

In order to enforce AML/CFT limits on the amount that a user can spend without the AML authority seeing transaction data, a novel new concept “anonymity vouchers” has been created. The AML authority issues these additional, time-limited sates to every CBDC user at regular intervals. If user wants to transfer CBDC without revealing information to the AML authority, he needs to spend these vouchers at the ration of one voucher per CBDC unit transfer. Thus the amount of CBDC that can be spent anonymously is limited by the number of vouchers that the AML authority provides to each user. Although vouchers are technically “spent”, they are issued free of charge and are not transferrable among users. This means that limits on anonymous CBDC transfers can be enforced without recording the amount of CBDC that a user has spent, thereby protection users’ privacy.

When an intermediary receives a CBDC issuance request from a client, it checks that the client’s post-transaction CBDC balance will remain below any wallet cap that it may have set. If that is the case, the intermediary requests CBDC units from the central bank on behalf of its client (in exchange, the intermediary will draw down its reserve balance held at the central bank by the face value of the CBDC units). This mean that issuing central bank does not limit supply of CBDC in a way that that could lead to excess demand from its users, since limits are only applied at the level of each individual wallet. Conversion to and from CBDC always occurs at a ratio one-to-one, to ensure that CBDC has the same value as alternative forms of the same currency. The central bank debits the intermediary’s reserve balance and authorizes the creation of new CBDC units by approving (thus signing) the issuance request through its node. The new units are then added to the original client’s CBDC account, and that client account with the intermediary in private money is debited by the same amount.

After that, the CBDC transfers are done without the interference of the central bank. A payer sends a CBDC transfer instruction indicating the amount, the pseudonym of the payee (account identifier and intermediary identifier) and whether or not the payment should occur anonymously. If this is the first time payee has received CBDC units from the payer’s intermediary, the transfer starts with a look-up request by the payer’s intermediary in order to obtain the payee’s address from its intermediary. The intermediary’s node then initiates the transfer by following a process that varies depending on whether the AML authority is involved in the transaction. The transfer mechanism allows for AML checks by intermediaries, but it largely safeguards confidentiality.

The transaction can be accepted by the payee’s intermediary with no need for approval from the AML authority if the payer has a sufficient number of anonymity vouchers and ask to use them. In that case, the payer’s intermediary removes the necessary vouchers from the user’s reserves and attaches them to the transfer of CBDC, to prove to the payee’s intermediary that the transaction can be validated without checks being carried out by the AML authority.

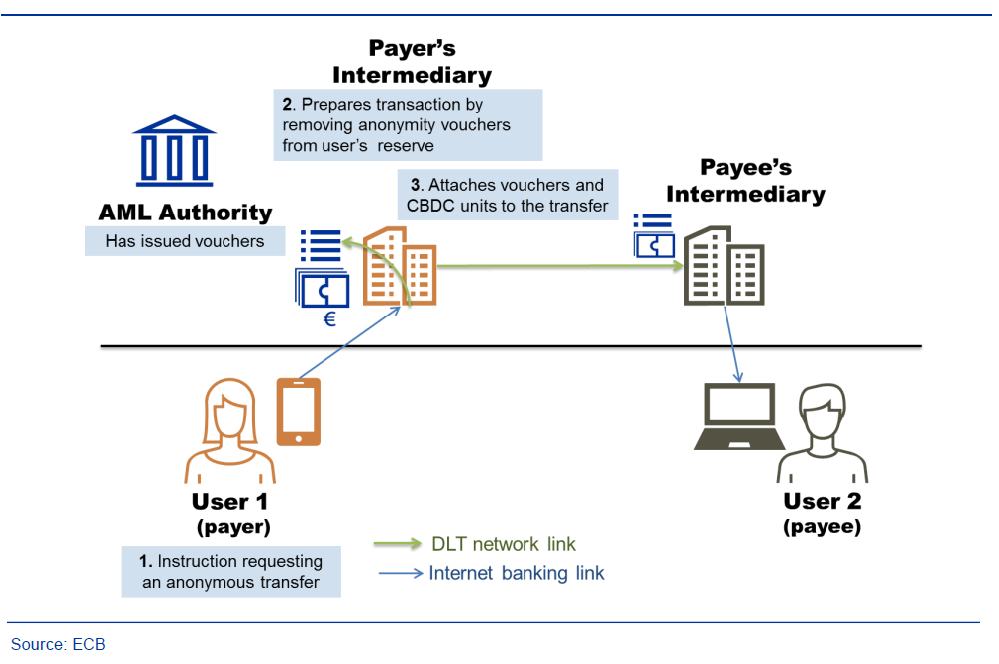


Figure 2 Transfer with anonymity vouchers

If a payer chooses not to use vouchers or does not have enough vouchers available, its intermediary will prepare the transfer and route it via the AML authority, sending additional information on the payer for the necessary AML checks. On the basis of the information provided, the AML authority will either approve or reject the transfer (rejection is automatic and based on text-matching rules). The payee’s intermediary will only accept the payment if it is approved by the AML authority.

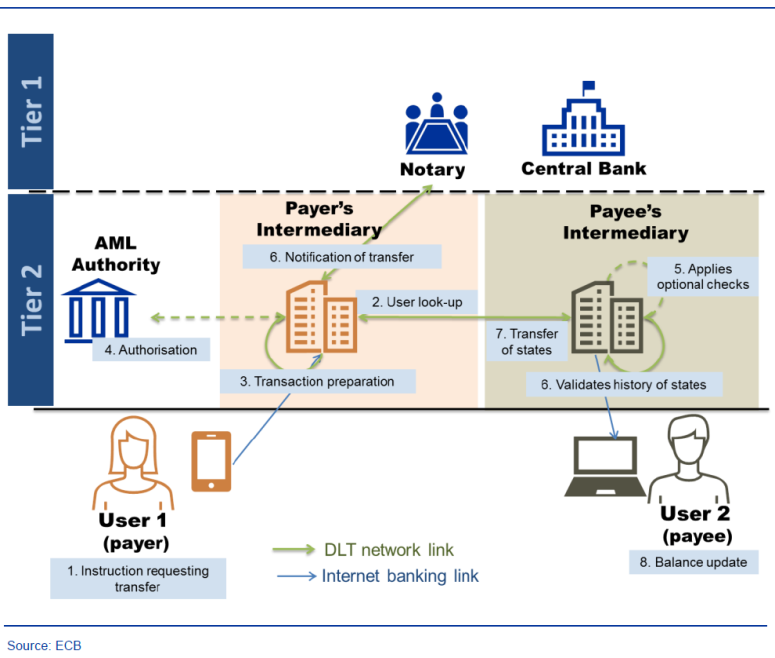


Figure 3 Transfer with AML checks

Limits on the amount of CBDC that can be transferred in a given period of time and caps on the CBDC holdings of individual users are enforced at the level of individual intermediaries, which will be driven to reject transactions that infringe AML/CFT requirements by (i) respect for the rule law and (ii) financial incentive (since they will not be able to redeem CBDC units at the central bank if those units have been transferred illicitly at any point of time). It should in this context be noted that limiting the amount of CBDC at the level of individual wallets would indirectly allow the overall CBDC volume to be controlled if for example the number of wallets per citizen and the usage by non-citizens were restricted.

Moreover, users are able to convert their CBDC units back into other forms of currency by initiating a process through their respective intermediaries. When an intermediary receives such a request, it takes the requested amount of CBDC units from the client’s wallet and marks them as spent. The intermediary then sends a request to central bank to reclaim funds in the RTGS system and updates the balance of its user’s account in private money.

Finally, ESCB proved that it is possible to build a simplified CBDC payment system that protects the users’ privacy in lower-value transactions, while still ensuring the higher-value transactions are subject to a mandatory AML/CFT checks. However, the proof of concept also highlights number of areas where there is a room for improvement. Upcoming improvements could work on reducing the amount of information visible to parties not involved in the transaction, adding user’s ability to access or spend CBDC balances when the intermediary is unavailable, adding privacy-enhancing techniques, Interoperability with an RTGS system, and practical functioning of the prototype since the PoC focuses on concept and design rather than functioning of the prototype and efficiency of it (for example the scalability of the prototype was not analyzed).

## **E-Krona – Central Bank of Sweden (Riskbank)**

Sweden states the decline in cash payments as the most important reason for its e-krona pilot program to test their official new digital currency, where the pilot is set to run until the end of February 2021.

So the Riskbank’s goal is to provide the public with a digital equivalent cash and thus offer a complementary (“risk-free”) solution to digital money from private market parties (i.e., commercial banks). This pilot should be considered as a technical outline of possibilities, not as a likely implementation. Sweden’s e-krona pilot project is assessed in a case study: the Riskbank is consulted by Accenture and uses R3’s Corda platform. The proposed outcome is a value-based, closed system with a two-tiered architecture with a global notary (i.e., consensus) node.

The general architecture of Sweden’s CBDC pilot is two-tiered:

1. 1st tier: consists of three different node types. The Riskbank node that issues kronor (the token) to Participant (i.e., banks) and a Notary Node confirming transactions.
2. 2nd tier: describes the distribution of kronor to end-users.

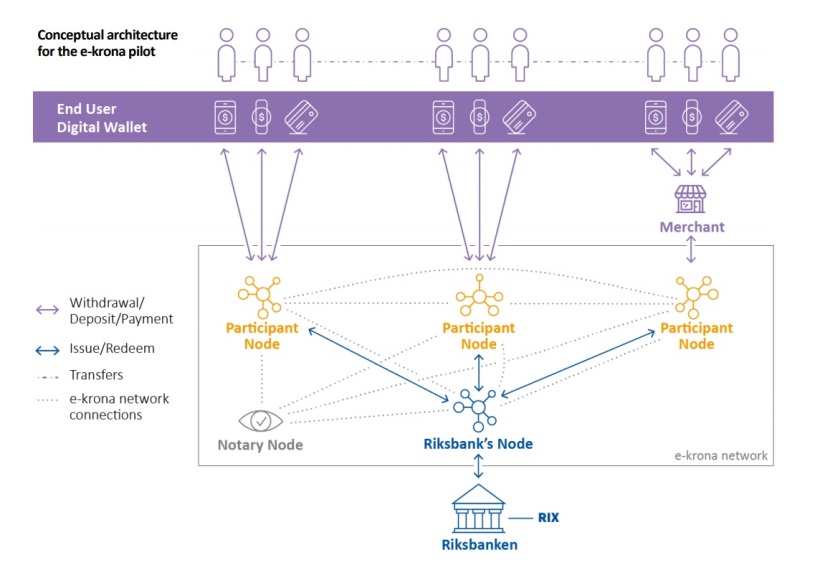


Figure 4 Conceptual architecture for the e-krona pilot

To become a node in the network, the operating entity must have indirect access to the central bank operated settlement system, RIX. As such access would be restricted to existing banks. These banks are expected to provide liquidity by reacting to consumer demand and exchanging their RIX balances (i.e., central bank money A) into Kronor-token (i.e., central bank money B). This consumer demand will have to outweigh the commercial banks’ costs of increasing their central bank money balances.

After activating a user wallet with a Network Participant, end-users shall be able to use kronor for P2P and P2C transactions in an inclusive, 24/7 available manner with offline functionality.

Notary nodes fulfill the role of miners in Nakatomo consensus-based blockchains. Notaries thus avoid double-spending and create finality for transactions. While Corda’s original whitepaper states that notaries “are expected to be composed of multiple, mutually distrusting parties”, there are simpler options – such as having only one notary node i.e., which is the case in this prototype.

The case study shines light on the role and relevance of technology providers and consultants. Certain technology providers, R3 in particular, appear to be dominating the provision of distributed ledger technology frameworks for CBDCs. Sweden’s e-krona seems to be the “generic R3 package”. The role of consultancies such as Accenture can be understood as “translating” between the functional expectations and the technical implementation.

Generally, the design elements displayed in the below table are considered in the typical “CBDC wishlist”.

When assessing the e-krona within this framework, it becomes evident that various design specifications have not yet been made. As such, the current e-krona prototype is exciting, potentially even representative of the most common development status, but most likely neither pioneering, nor the most advanced CBDC set-up.

## **Republic of the Marshall Islands**

Marshall Islands launches its central bank digital currency – Marshallese sovereign (SOV) – on Algorand blockchain protocol, while SFB Technologies is the company that develops SOV’s blockchain infrastructure. Algorand is an open-source blockchain protocol provider, permissionless and with proof-of-stake protocol. It also allows the development of scalable blockchain solutions for real use cases. So, the Algorand protocol will be implemented to provide the SOV initiative with speed, scalability, and security. The protocol also provides the required compliance controls such as identity management and the compliance platform.

“Marshall Island’s vision is for global participation and inclusion in an open financial system by harnessing the benefits of blockchain technology. It is consistent with a truly global and decentralized society. We also believe it made possible with our technology. We are proud to support the country on its revolutionary journey towards the adoption of digital currency, “said Silvio Micali, founder of Algorand.

The island nation aims to reduce its dependence on the US dollar, which is currently the national currency. Algorand clarified that the SOV would circulate alongside the US dollar. The SOV supply will algorithmically fix at 4% growth per year to prevent inflation.

## **National Bank of Cambodia (NBC)**

NBC will launch a blockchain-based, peer-to-peer payment and money transfer platform in the next few months, it is called “Project Bakong”. It is now in the final stage of the deployment. By comparison to conventional payment and transfer methods, NBC claimed that Bakong is cheaper and more convenient.

NBC partnered with Japanese blockchain firm Soramitsu which built a real-time gross payment system (RTGPS) based on Hyperledger Iroha distributed ledger technology. The primary application of the Bakong project is for payments, and its mobile payment app is integrated with eleven banks. The digital wallets are linked to bank accounts, but only 20-30% of the population currently has accounts. Users will be able to set up a Bakong wallet that will be automatically linked to their bank accounts, allowing easy fiat currency exchange into the new CBDC in real time. NBC claims that it will store all transaction data from the platform, suggesting payments may be fully traceable.

Makoto Takemiya, the CEO of Soramitsu, said that the CBDC “is simply a tokenized version of the USD and Riel fiat money in NBC’s reserves”.

## **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.