# Introduction

Dozens of central banks are exploring the possibility to issue Central Bank Digital Currency (CBDC) as a new bank money format and central bank liability part of the monetary base, and some started implementing it. Technology advances and cash usage decline are behind this digital shift.

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’ which 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. Each central bank could design their CBDC according to monetary policy and economic objectives central bank sees.

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 mean 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.

# CBDC Projects

## 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.

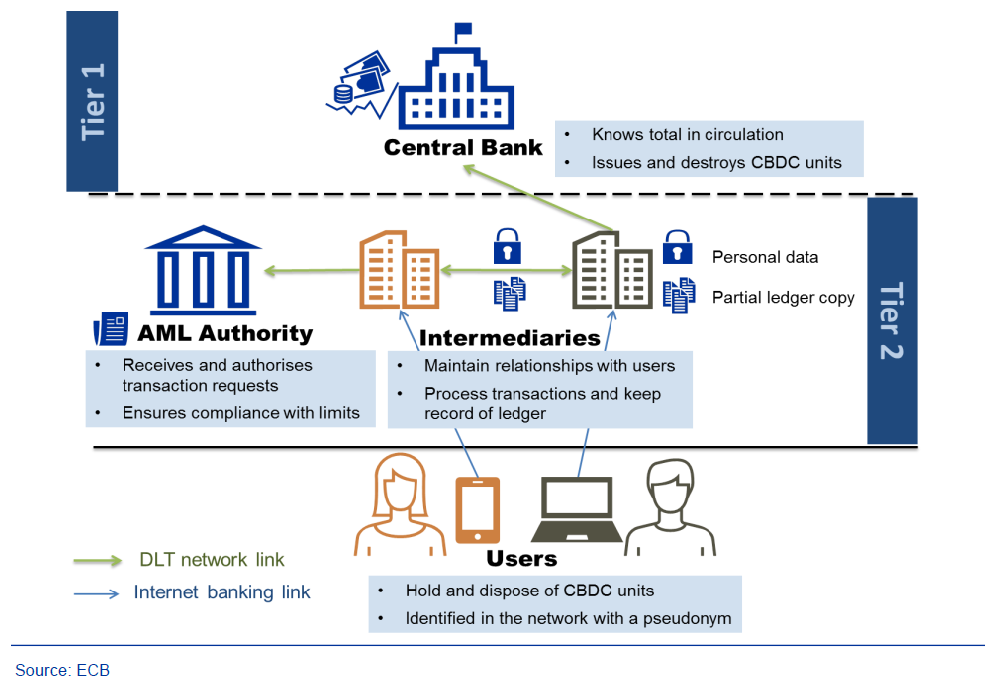


Figure Two-tier model and relationship between entities

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.

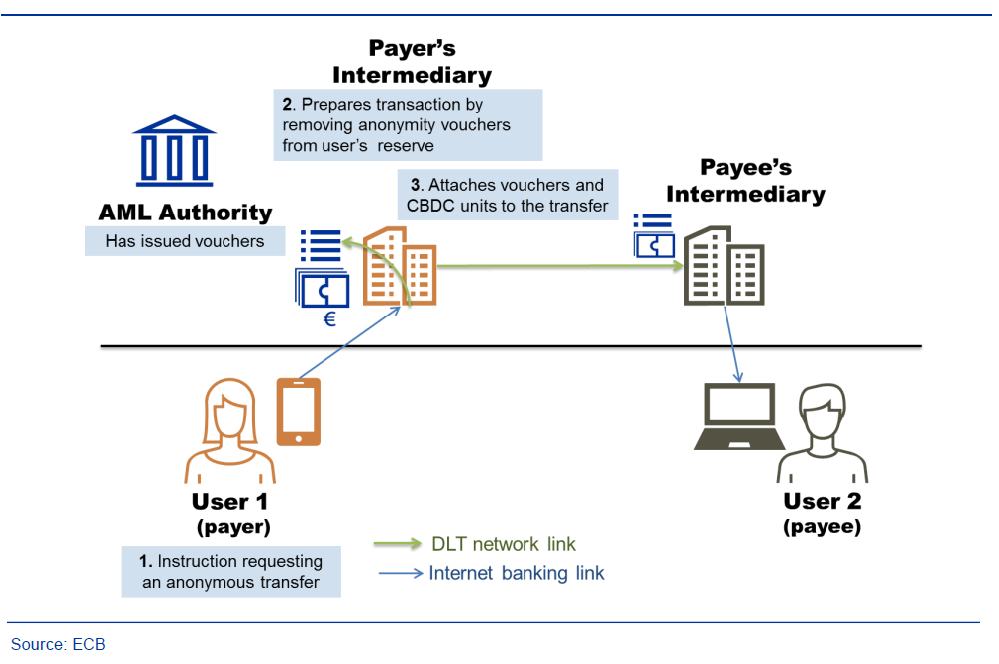


Figure Transfer with anonymity vouchers

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.

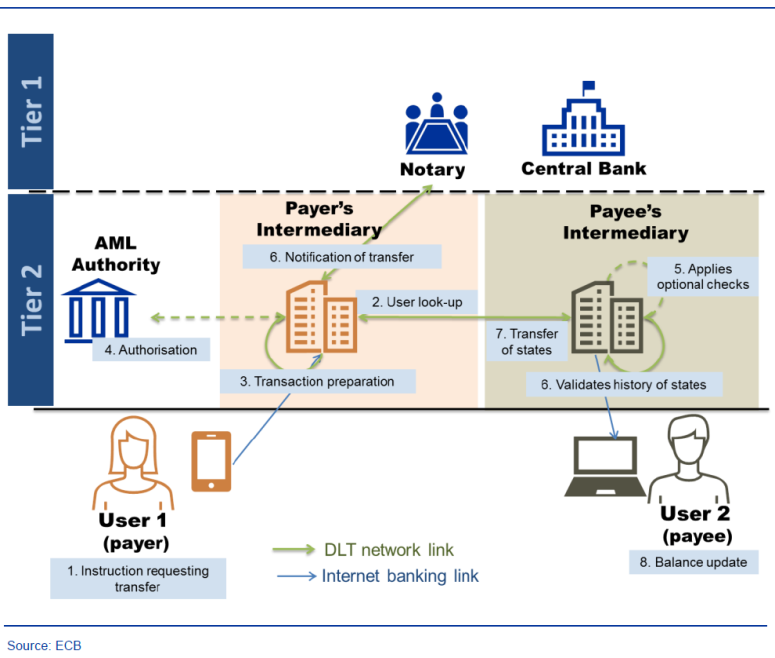


Figure Transfer with AML checks

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 analysed).

1. E-Krona – Central Bank of Sweden

An earlier E-Krona project in 2018 concluded that E-Krona is compatible with the Central Bank of Sweden’s (RiskBank’s) task to promote a safe and efficient payment system.

1. Stella – Bank of Japan, European Central Bank

The Stella project in phase 3 attested that improvements can be obtained in cross-border payments in terms of safety by using distributed ledger technology.

1. People’s Bank of China (PBoC)

PBoC aims to release CBDC at the retail sector only without institutional and wholesale payments. It plans to enable commercial banks and certain institutions to distribute the CBDC to the general public instead of distributing it directly to the public. However, users will need to open a digital wallet to send, receive, and hold coins without any linkage to a bank account. No interest will be paid for holding CBDC, and also there should be no implications for inflation and no impact on central bank monetary policy.

1. Republic of the Marshall Islands

In February 2018, it issued the Sovereign Currency Act of 2018, which introduces a new Blockchain based currency called the Sovereign (‘SOV’).