Whitepaper for a retail DLT-based CBDC

This document is distributed by SIA S.p.A.
All of the data which it contains are public and the information therein is the result of analyses conducted by SIA S.p.A., and may derive from a variety of sources.
Such sources are considered to be reliable and in good faith, nevertheless no representation or warranty, either expressed or implied, is made by SIA S.p.A. as to their accuracy, completeness or correctness.
The evaluations, opinions, forecasts or estimates contained in this document exclusively refer to the date of the document with the evaluations, opinions, forecasts or estimates included herein.
All the information contained in this document may, subsequent to the date of its drawing up, be subject to amendment or update by SIA S.p.A., without any obligation on its part to communicate such amendments or updates to those parties to whom this document was previously distributed.
This publication is provided for information and clarification purposes only and is purely indicative.
Furthermore, in the absence at present of a clearly defined legal/ regulatory framework on the subject, SIA S.p.A. does not guarantee the legal/regulatory aspects of the evaluations contained herein.
That being said, the contents of the document exclusively reflect the opinions of the authors and they do not imply any responsibility on the part of SIA S.p.A.
Neither SIA S.p.A. nor its directors and employees can be held responsible for any direct or indirect damages, also deriving from inaccuracies and/or errors, that may be caused to third parties when using this document.

The information contained in this document is updated in line with the data available at 31/12/2020.

Index

1. Executive Summary

Digitalization of payments is one of the various declinations of the overall process of digital transformation that is growingly affecting every aspect of economic and social life.

The advent of the so-called cryptoassets, starting from bitcoin, drew the attention of central banks and regulatory bodies alike on the threats and opportunities arising from such emerging technologies that open to completely new and uncharted scenarios.

Central Banks in particular are exploring the concept of Central Bank Digital Currency (CBDC): a digital form of central bank money that is different from other forms of money such as currency-denominated central bank money, commercial bank deposits or electronic money.

The debate on the feasibility of a CBDC and its implications, both positive and negative, is open and particularly lively. Finding an answer to the various issues that are still on the table of central banks and other relevant stakeholders is obviously out of the scope of this paper.

What follows is an attempt to outline a possible solution for a general purpose CBDC and a related payment system based on a DLT platform, analysing the topic not only from the technical point of view but also considering operational and regulatory issues.

It has not the ambition to be the ultimate answer, but a contribution to the discussion, a stimulus to further analysis and an invitation to promote experimentations.

2. Evolution of digital payments and the role of Central Banks

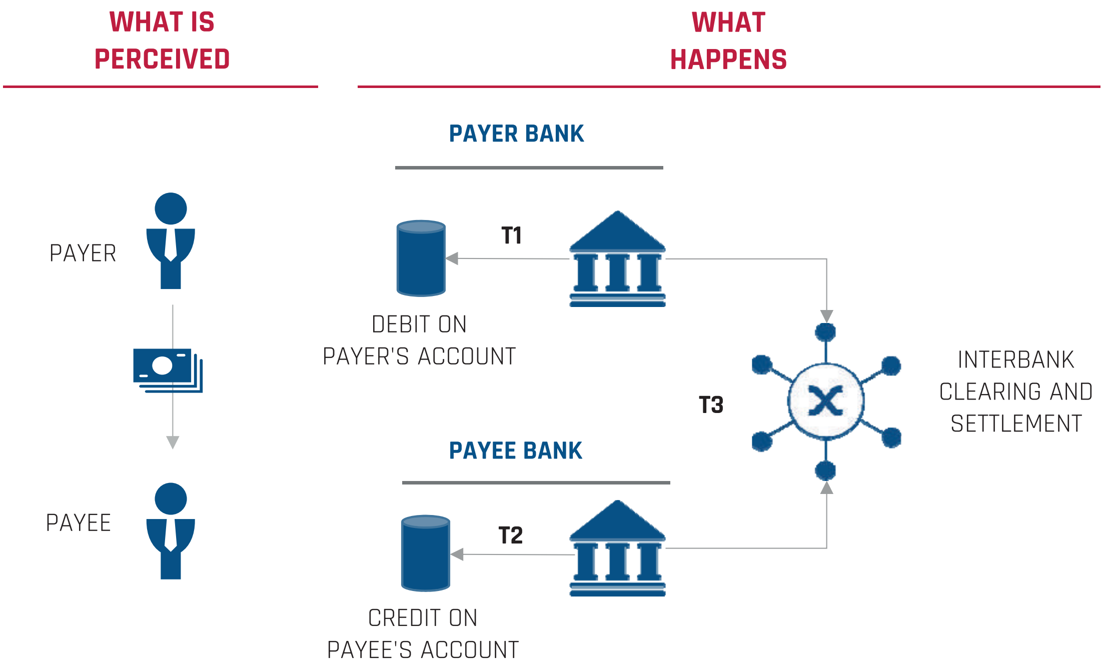
The mix of technological evolution and market expectations sets the conditions for the raise of new forms of money and for a more active role of Central Banks in retail digital payments.

2.1 Payments: from digitization to digital transformation

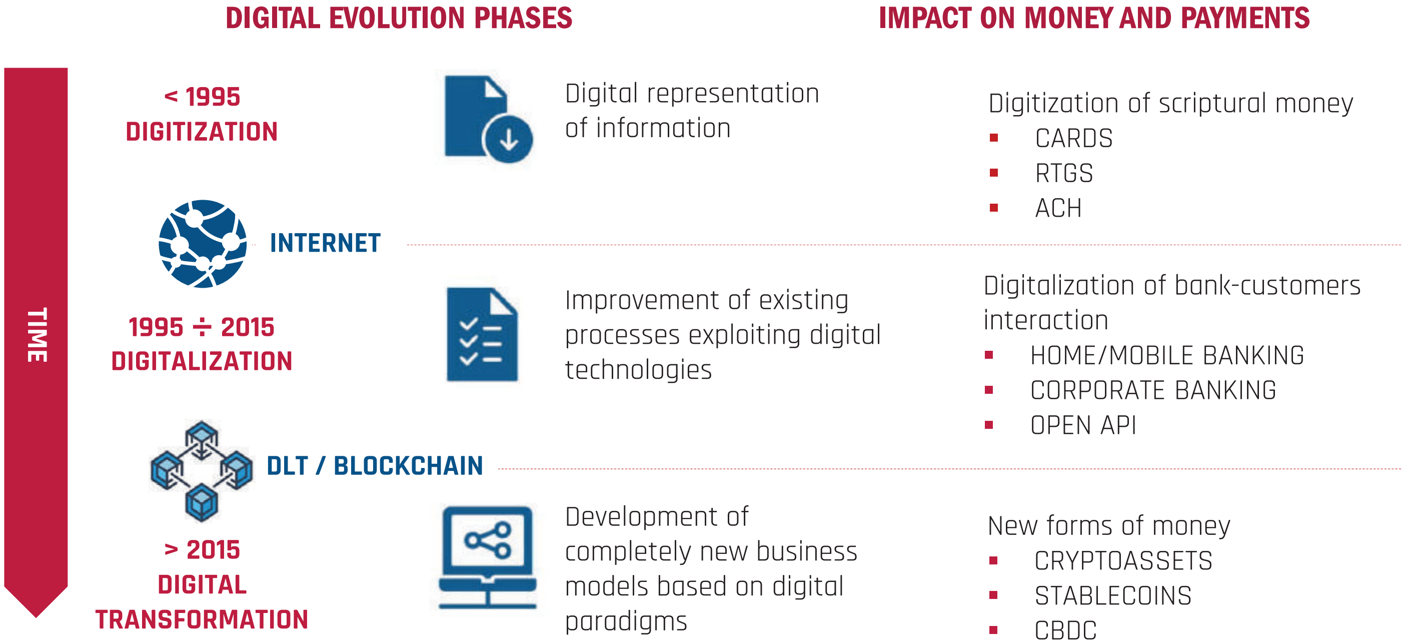
Looking back at the history of payments, we can identify several breakthroughs, among which the invention of “scriptural money”, the money available on the current accounts held by households and businesses at a financial intermediary (typically a bank, thus the term “bank money”). Unlike physical fiduciary money issued by a Central Bank (banknotes and coins), scriptural money is intangible but can be converted into liquidity at any time and can be used to perform payment operations based on the principle of the transfer of credit, relying on interbank clearing and settlement arrangements.
As an example, in the context of a payment transaction, the European regulation (Directive 2015/2366 – PSD2) recognizes bank money as “funds” along with banknotes and coins and electronic money, so that, from the user’s perspective, there is no difference among these widely accepted means of payment.

ELECTRONIC MONEY
In Directive 2009/110/EC ‘electronic money’ is defined as: electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […] and which is accepted by a natural or legal person other than the electronic money issuer.
Therefore, electronic money (e.money) is a mean of payment representing the equivalent amount of funds held by the e.money issuer.
An e.money transaction is ultimately based on the same principle of credit transfer between accounts.

PAYMENT OPERATION THROUGH BANK MONEY



In an effort to make payment operations easier and faster for the customers and the intermediaries alike, the payment industry has embraced the digital evolution, mainly looking for efficiency.
With the advent of the internet, a number of new actors entered the arena, leveraging the customer-centric attitude of the then called “new economy” paradigms to exploit the flaws of existing services, mainly focusing on customer experience.


DIGITAL EVOLUTION PHASES

IMPACT ON MONEY AND PAYMENTS

TIME

< 1995
DIGITIZATION

Digital representation of information

Digitization of scriptural money
- CARDS
- RTGS
- ACH

INTERNET

1995 ÷ 2015
DIGITALIZATION

Improvement of existing processes exploiting digital technologies

Digitalization of bank-customers interaction
- HOME/MOBILE BANKING
- CORPORATE BANKING
- OPEN API

DLT / BLOCKCHAIN

> 2015
DIGITAL
TRANSFORMATION

Development of completely new business models based on digital paradigms

New forms of money
- CRYPTOASSETS
- STABLECOINS
- CBDC

None of the innovations implemented so far have had any impact on the inner structure of digital payment transactions, that are still based on the transfer of credit among financial intermediaries.

2.2 Bitcoin and the blockchain

In 2008 the anonymous developer Satoshi Nakamoto issued the whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” proposing the creation of a payment instrument alternative to official currencies (bitcoin in fact) and a transaction registration system that guarantees the anonymity of users, the absence of an intermediary and the immunity of transactions to the “double spending” problem.
The underlying technology is the blockchain: a distributed database of transaction (distributed ledger).

DISTRIBUTED LEDGER TECHNOLOGIES

Distributed ledger technology (DLT) can be defined as digital system for recording transactions in which the transactions among the participants in a network and their details are recorded in multiple places at the same time and validated according to a consensus protocol shared among the participants themselves.
Unlike traditional databases, distributed ledgers have no central data store or administration functionality. The consensus protocol allows the two participant in a transaction to complete it in a secure way without the need of a trusted third party.

Bitcoin and similar are sometimes also defined as cryptocurrencies, with the term recalling both the technical aspect (crypto) since they rely heavily on cryptography, and the ambition (currency) to become a widely adopted mean of payment.

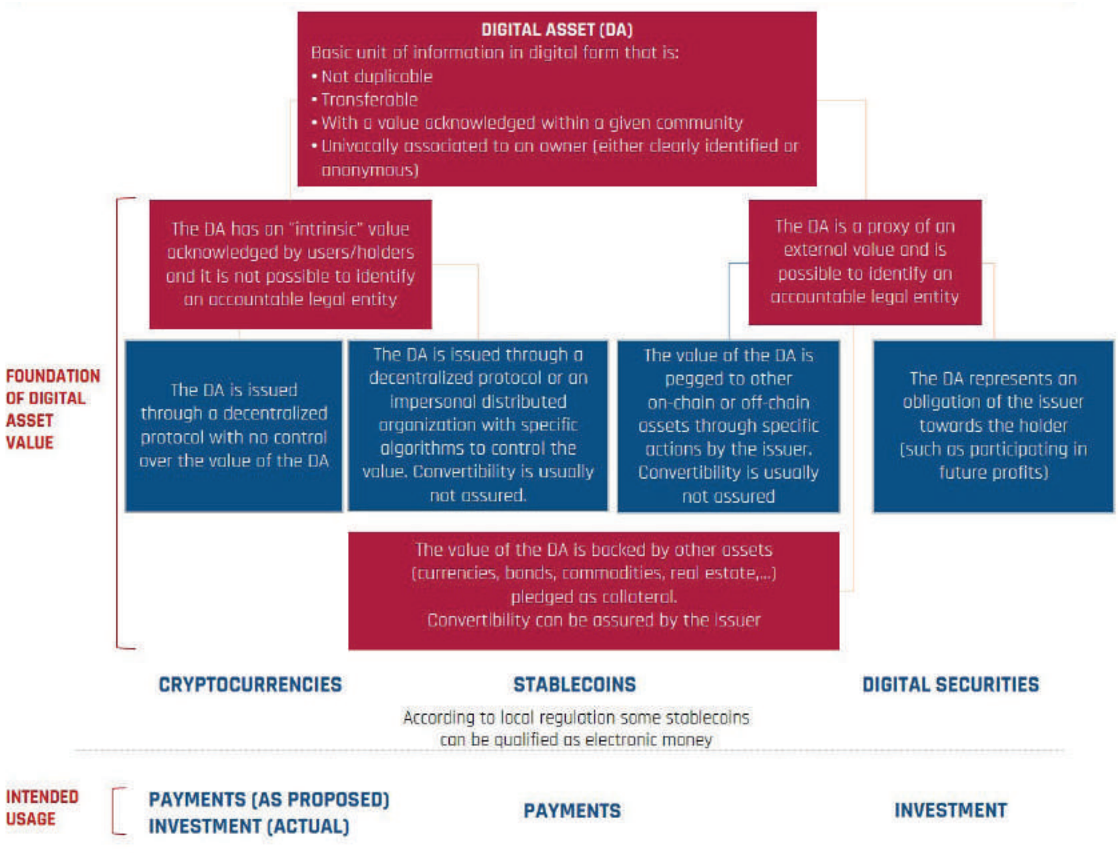
Bitcoin was the first of a number of similar solutions collectively known as cryptoassets.

Even if bitcoin and the similar do not have so far gained a relevant role in payments, addressing an estimated 1% of the overall non cash payments, they have demonstrated the technical feasibility of the secure exchange of a digital asset avoiding the double spending risk and without the need for the involvement of a trusted third party. This is a real breakthrough in the history of payments that questions the foundations of digital payments, as we know them.

2.3 The evolution: the stablecoins

Cryptoassets in their original form lack any kind of value backing (they do not represent any liability on an identifiable subject) and the acceptance is only based on the willing of the involved parties. Hence, the extreme volatility of their value, that makes them unsuitable for day-by-day payments.
The so-called stablecoins try to solve the volatility problem by adding some sort of price stabilization mechanism either by means of specific algorithms to influence the supply-demand dynamic of cryptoassets in order to flatten the value fluctuations or by linking the cryptoassets to other virtual or physical assets.

SIMPLIFIED QUALIFICATION OF DIGITAL ASSETS


DIGITAL ASSET (DA)
Basic unit of information in digital form that is:
• Not duplicable
• Transferable
• With a value acknowledged within a given community
• Univocally associated to an owner (either clearly identified or anonymous)
The DA has an "intrinsic" value acknowledged by users/holders and it is not possible to identify an accountable legal entity
The DA is a proxy of an external value and is possible to identify an accountable legal entity
FOUNDATION OF DIGITAL ASSET VALUE
The DA is issued through a decentralized protocol with no control over the value of the DA
The DA is issued through a decentralized protocol or an impersonal distributed organization with specific algorithms to control the value. Convertibility is usually not assured.
The value of the DA is pegged to other on-chain or off-chain assets through specific actions by the issuer. Convertibility is usually not assured
The DA represents an obligation of the issuer towards the holder (such as participating in future profits)
The value of the DA is backed by other assets (currencies, bonds, commodities, real estate,...) pledged as collateral. Convertibility can be assured by the issuer
CRYPTOCURRENCIES
STABLECOINS
DIGITAL SECURITIES
According to local regulation some stablecoins can be qualified as electronic money
INTENDED USAGE
PAYMENTS (AS PROPOSED)
INVESTMENT (ACTUAL)
PAYMENTS
INVESTMENT

The scheme is a simplified representation, does not cover all the possibilities.

The possibility for stablecoins to get a widespread adoption depends on the specific conditions of each jurisdiction. In advanced economies, we can consider as driving factors (incomplete list for illustrative purposes only):

- **Growing customer expectations.** Consumers are used to "social media-like experience" in every digital interaction: ease of use and real-time results (considering payments, that turns into instant availability of funds).

- **Robust digital infrastructure.** Relatively low cost devices with high computation power are widely available, along with pervasive network access through mobile broadband (5G coming) and growing diffusion of standard-based digital identity and e-signature solutions. At platform level, we observe that enterprise grade DLT platforms are rapidly approaching performance and reliability levels suitable for mission-critical applications.

- **Emerging use cases.** Apart from the financial inclusion of unbanked/underbanked people, a wide area of possible applications arise from the programmable money paradigm.

Stablecoins have the potential to revolutionize the payments landscape, enabling innovative use cases and business models with positive effects on efficiency and inclusion.
On the other hand, as everything in the digital realm, they are prone to concentration phenomena with the possibility for a stablecoin issuer to get a global footprint with potential impact on financial stability and the risk to significantly challenge the comprehensiveness and effectiveness of existing regulatory, supervisory and oversight approaches.

Work is under way at national and international level by institutions and organizations to find the best way to manage this kind of complexity.

THE PROGRAMMABLE MONEY

The concept of "programmable money" has nothing to do with the possibility, for example, to automate the execution of a payment on the basis of the occurrence of a given event, that is what payment service providers do every day. A possible interpretation is: "a payment instrument whose performance are determined by a program code, which aim to facilitate the transfer of value according to carefully vetted conditions and rules". Programmable money features can enable novel forms of contractual relationships. Some examples are provided in par. 4.5.

2.4 The role of Central Banks in retail digital payments

Apparently, a possible forward looking scenario sees the digital payment world split between two forms of private solutions respectively based on bank money and stablecoins.

Nowadays, Central Banks have an indirect role in retail digital payments by providing payment assets (settlement accounts) and infrastructures (Real Time Gross Settlement systems – RTGS) for payment settlement among commercial banks. Access to settlement accounts is limited to qualified financial institutions; therefore, citizens and business alike do not have any possibility to access a risk-free payment instrument to be used in digital payments.

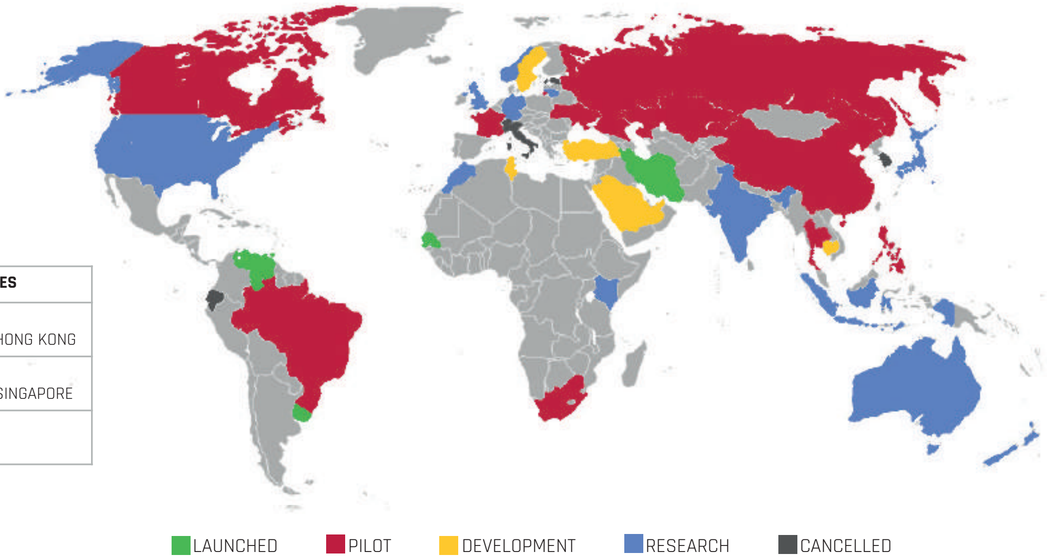
Furthermore, in advanced economies, the use of cash is declining and some merchants now openly refuse to accept cash. This leads to the paradoxical situation that the legal tender is potentially driven out by private money.

Central Banks around the world are therefore evaluating the opportunity to issue a new form of fiduciary money, which is in digital form like central bank deposits and settlement accounts but is widely accessible like cash: the **Central Bank Digital Currency**.

THE CONCEPT OF RISK-FREE PAYMENT INSTRUMENT

Payment transactions are subject to a series of risks for the involved parties, the financial intermediaries that actually perform the transaction and the central bank providing interbank settlement like credit risk (a participant not being paid for an outstanding claim) and liquidity risk (a counterparty not being able to meet its payment obligations). Cash, because of its "instant settlement" features and the central bank guarantee is considered "risk free" from this point of view, even if it is subject to, for example, risk of losing, stealing etc.
A digital payment instrument bearing the same features of cash (instant settlement and central bank guarantee) could have the same "risk-free" connotation. Obviously, the underlying payment system would be subject to operational risks that must be properly managed.

SELECTED CBDC INITIATIVES



CROSS-BORDER PROJECTS

PROJECT NAME	INVOLVED AUTHORITIES
ITAHON-LIONROCK	• BANK OF THAILAND • MONETARY AUTHORITY OF HONG KONG
JASPER-URBIN	• BANK OF CANADA • MONETARY AUTHORITY OF SINGAPORE
STELLA	• EUROPEAN CENTRAL BANK • BANK OF JAPAN

Source: elaboration on cbdctracker.org (Oct. '20); internet (press release, papers etc.)

According the Bank of International Settlement survey (January 2020), some 80% out of the 66 central banks participating in the survey are actively working on CBDC and 10% have developed pilot projects.

3. CBDC at a glance

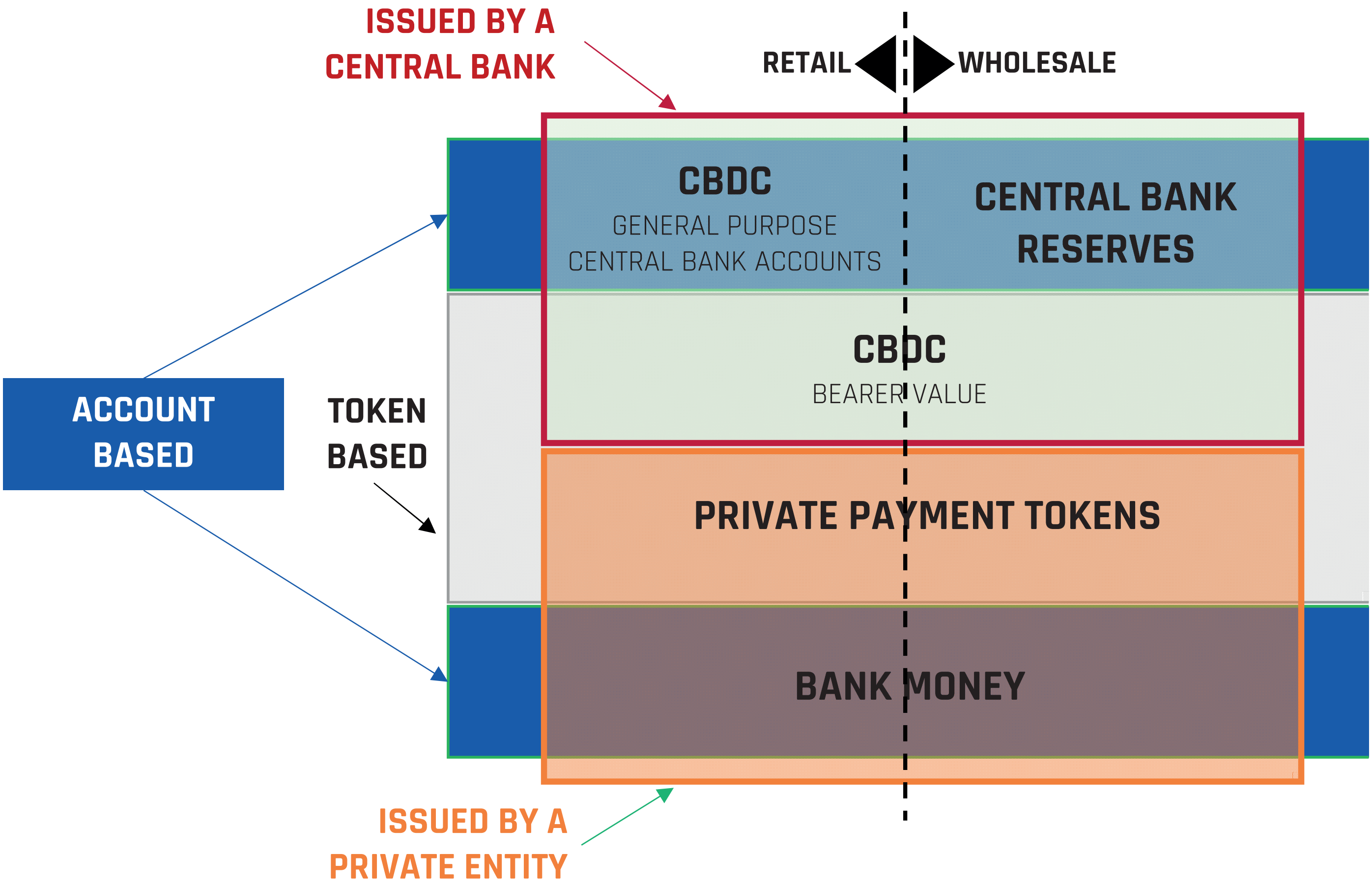
A new digital form of Central Bank issued money complementing existing payment instruments

3.1 Definitions

The accepted definition of Central Bank Digital Currency is:
"A digital form of central bank money that is different from balances in traditional reserve or settlement accounts. Hence, a digital payment instrument that is a direct liability of the central bank."

It is worth noting the use of the term "currency" which denotes the official means of payment of a given jurisdiction, denominated in its official monetary unit. It is therefore understood that CBDC should get "legal tender" status: it entitles a debtor to discharge monetary obligations by tendering CBDC to the creditor.

DIGITAL PAYMENT INSTRUMENTS



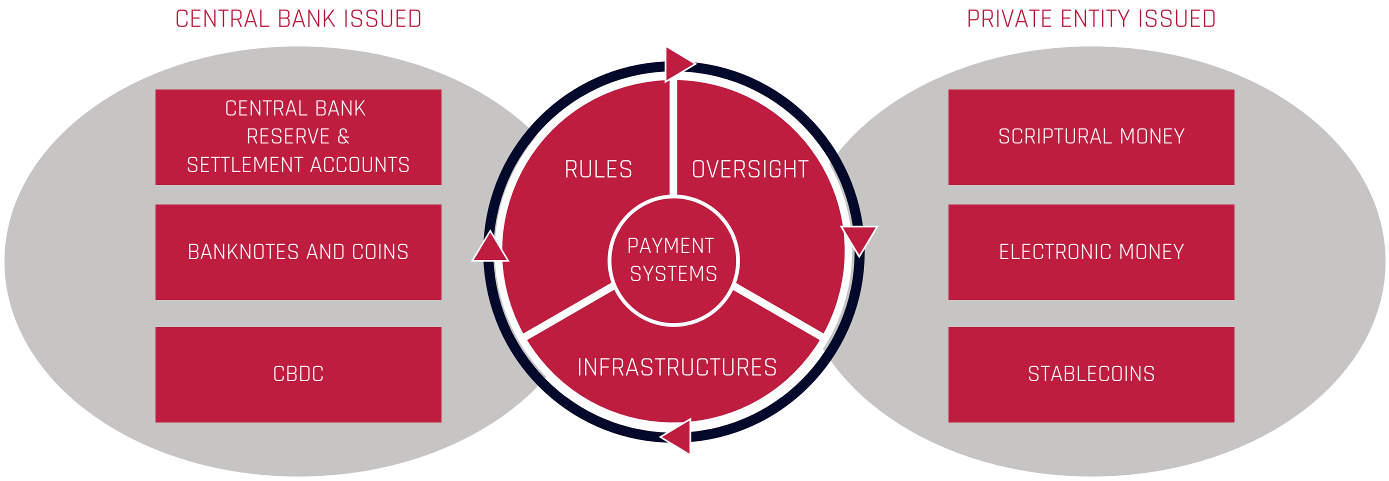
We can place a CBDC in the universe of the digital payment instruments on the basis of three main drivers:

- value transfer mechanism: **account based** (the value is somehow certified by a third party, the account servicing provider, like in payment accounts) versus **token based** (the payment instrument bears the value: the transfer of ownership finalizes the transfer of value, like banknotes and coins)
- issuer: **Central Bank** versus **Private Entity**
- accessibility: the payment instrument is available to the generality of users (**retail**) versus availability limited to selected entities (**wholesale**).

3.2 Scope

There is a wide acceptance among central banks that a CBDC is to be intended as a form of money complementary to existing and prospected ones and not a substitute. The CBDC as a means of payment can therefore constitute the foundation for a new payment system addressing the specific needs of users and the objective of the Central Bank that not only co-exists, but interoperates with other payment systems. We can therefore envision a "money ecosystem" where central bank-issued and private entity-issued payment instruments co-exist and interact through payment systems that rely on dedicated infrastructures and subject to the same rules and oversight duties.

MONEY ECOSYSTEM



That is why in this document we tend to distinguish between a CBDC, intended as the new digital medium of exchange issued by the Central Bank, and a CBDC-based payment system, that is the combination of actors, technologies and rules that make possible the issuance, distribution, storage and transfer of CBDC among users.

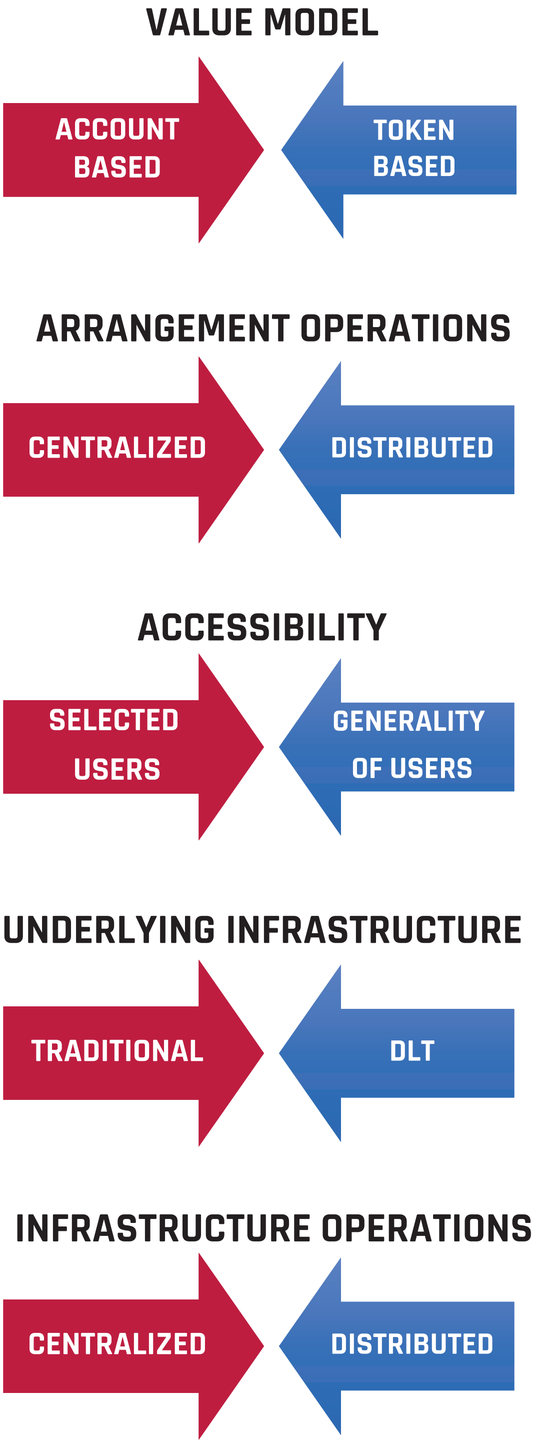
3.3 CBDC implementation models

The different CBDC models proposed so far are a combination of several variables as synthetized in the scheme on the right.

At present, it is not possible to define a single solution, as it depends on the combination of several variables that are specific of each jurisdiction, such as:

- political goals and priorities
- efficiency of local banking sector and payment systems
- cultural and social conditions
- status of local digital infrastructure.

All are elements that central banks have to factor in when considering the opportunity to introduce a CBDC.



3.4 Reasons why and why not

According to the outcomes of various researches, some reasons can sustain the introduction of a CBDC.

We can highlight (incomplete list):

- **Financial inclusion.** Considering the term in a very broad sense, the possibility for every citizen to receive and make payments is the possibility to produce value for the benefit of the community, so it is a declination of a wider concept of social inclusion. Because of the growing digitalization of economy, financial inclusion has to be intended also as digital financial inclusion.
  A CBDC-based payment system may be therefore associated to the concept of "universal service", where the term identifies a low-cost service, available for all the population that fulfils a basic need. Furthermore, some population segments that do not need or want full banking services, could benefit from a CBDC-based payment system as an "entry level" financial education instrument.

- **Payment systems differentiation.** The availability of an alternative digital payment instrument can set the conditions for the development of novel payment services by actors other than traditional payment service providers. This can foster positive competition and contribute to the resilience of the whole payment ecosystem through differentiation.

- **Additional tool for monetary policy.** Theoretically, a remunerated CBDC accessible to all citizens could pass on policy rate changes immediately to CBDC holders. However, beyond the theory, there are challenges and risks such as to foster disintermediation. Multi-tier remuneration schemes are under discussion.

- **Simplification.** Real benefits are in terms of efficiency and cost cutting: payments finality is instant and independent from any clearing/settlement process, with a frictionless and near-free backend processing.

- **Monetary sovereignty.** A CBDC strengthens the position of the national currency in the digital realm and can also counterbalance privately issued digital money. On the other hand, a CBDC denominated in a strong currency that is available for use in another jurisdiction could jeopardize the local currency with an effect of "digital dollarization".

Besides, the introduction of CBDC poses complex question:

- **Integrity of the financial system.** An easily accessible risk-free digital money could facilitate a sort of "digital bank-run" in turbulent periods, posing a significant threat to the banking system.

- **Disintermediation.** In case of a significant shift from bank accounts to CBDC, banks could face hard time in performing their traditional role of deposit taking and lending, limiting access to credit for both companies and families negatively affecting the whole economy.

- **Integration with the existing financial infrastructure.** It is very important for a CBDC-based payment system to be easily integrated with existing payment systems at Central Bank level (e.g. integration with T2 / T2S in the case of Eurozone) as well as Payment Service Providers level in order to preserve investments and ensure interoperability.

Central Banks and other regulatory and political bodies are still in the process of pros and cons analysis of a CBDC and to provide an answer is far beyond the scope of this paper.

The aim is to propose a feasIble solution for a retail-oriented CBDC as a contribution to the debate and as a stimulus for further analysis and experimentations.

4. Context considerations and guiding principles for a possible CBDC solution

A proposal for a retail-oriented CBDC based on distributed ledger technology in an advanced economy scenario, focused on interoperability and compliance.

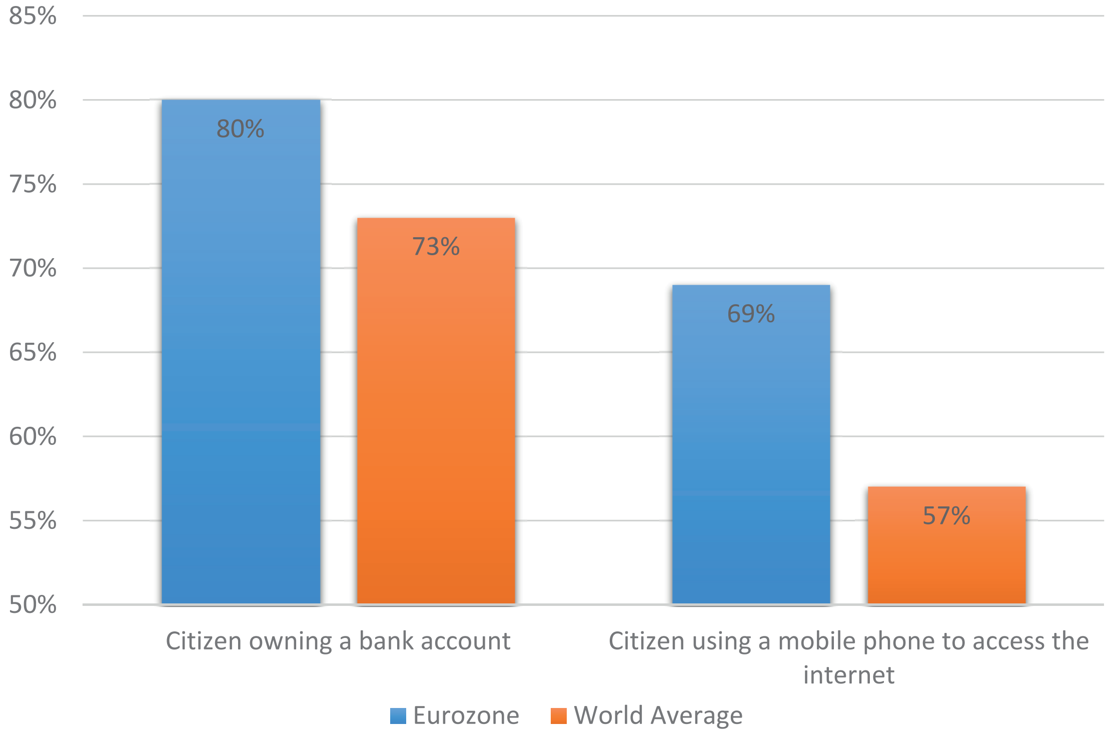
4.1 General considerations

The selection of a CBDC implementation model is heavily conditioned by the peculiarities of a given jurisdiction. For the purpose of this paper, we are considering an advanced economy, such as that of the Euro Zone.

For the citizen's attitude, we can consider as a proxy two simple indicators:

- percentage of citizens owning a bank account (proxy of financial inclusion)
- percentage of citizens using a mobile phone to access the internet (proxy of digital literacy).

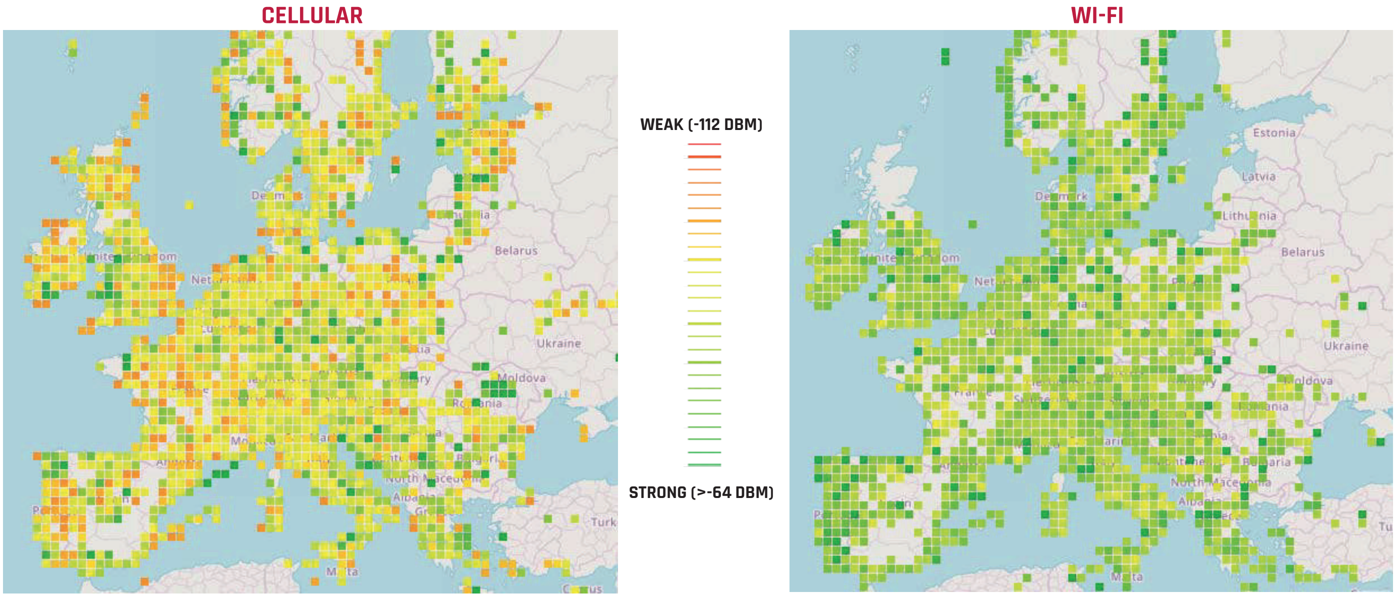
PROXY OF FINANCIAL INCLUSION AND DIGITAL LITERACY IN EUROPE - 2019



Source: elaboration on data from Worldbank, Eurostat, Statista

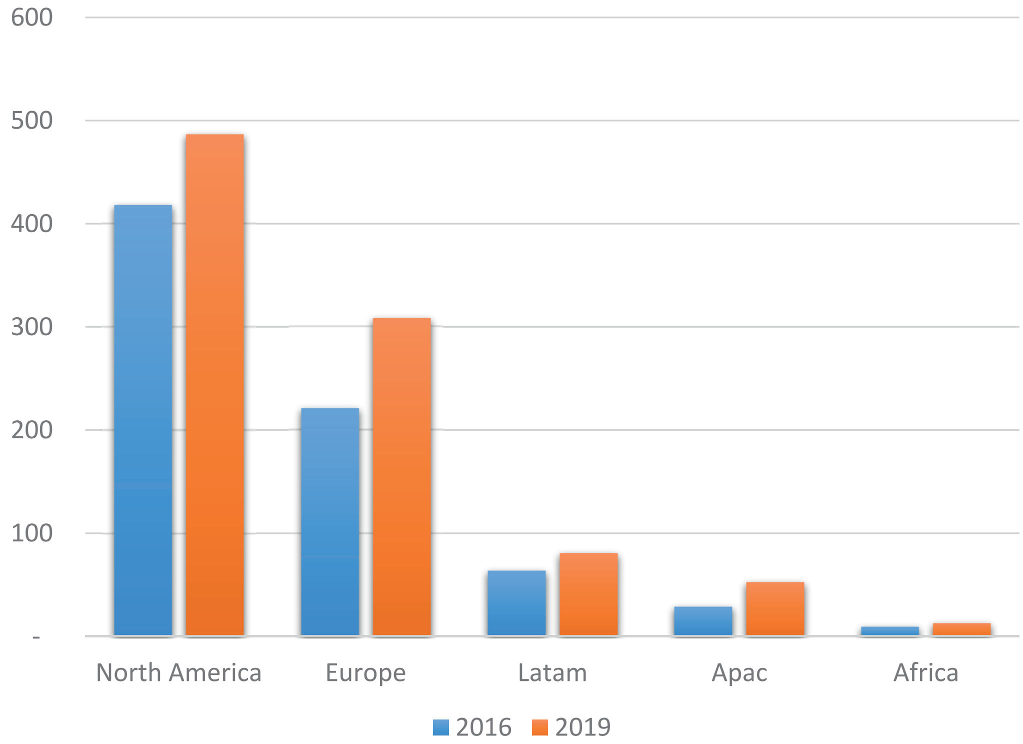
From the digital infrastructure point of view, we consider the availability of mobile broadband services.

MOBILE BROADBAND COVERAGE



We can also consider Europe as a favourable area for cashless payments, counting not only the number of pro-capita transactions (even if there are differences among the various countries), but also the growth in the last five years (effects of COVID-19 are not considered).

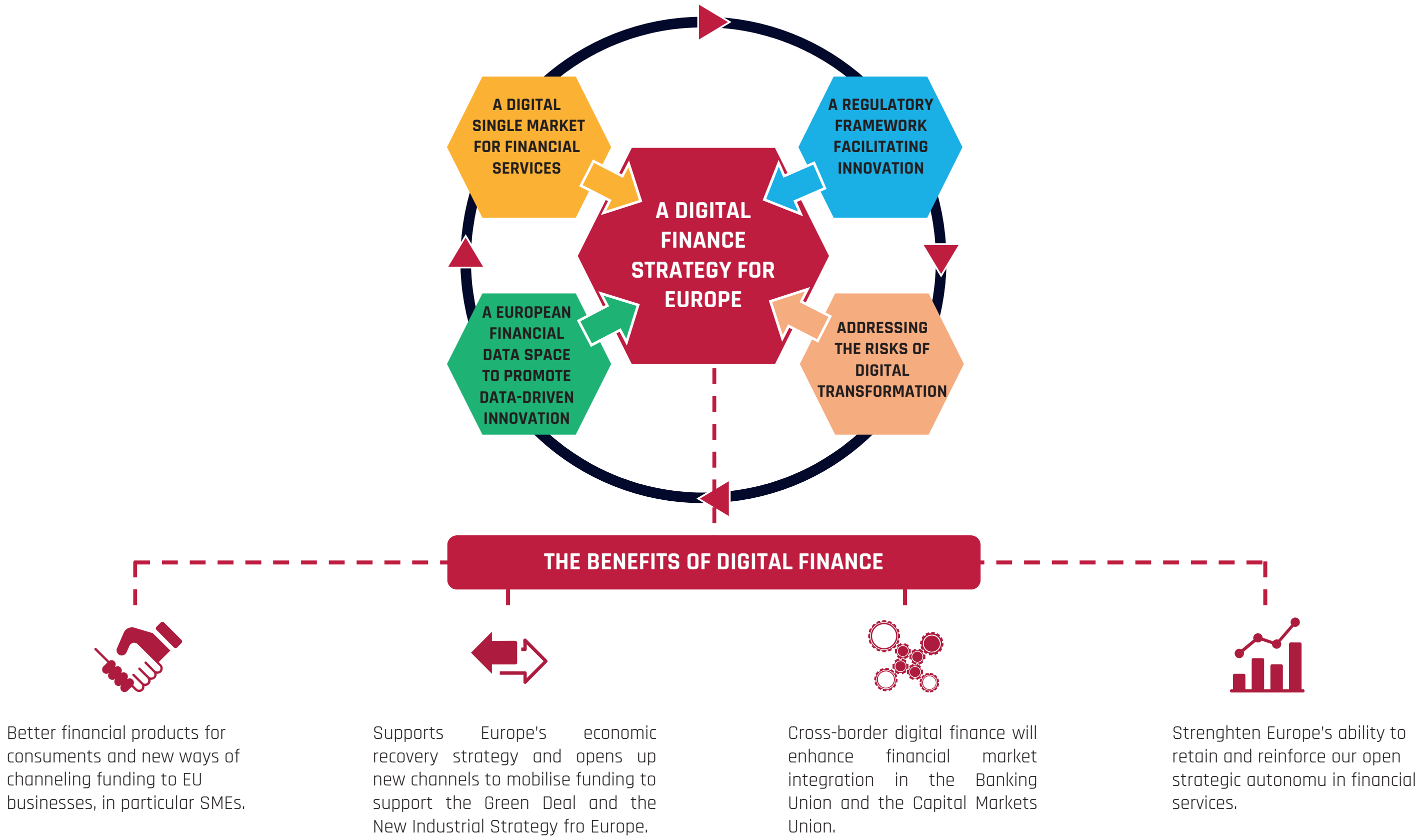
PRO CAPITA CASHLESS TRANSACTIONS



Source: elaboration on data from Population Reference Bureau, Cap Gemini World Payments Report 2020

To complete the environment analysis, we also have to consider the regulatory and political attitude.
From this point of view, we can refer to two events.

In September 2020, the European Commission published the Digital Finance strategy along with a series of documents covering a retail payments strategy, a proposal for a regulation for a pilot regime for market infrastructures based on distributed ledger technology, a proposal for a regulation on Markets in Crypto-assets.
The European Commission demonstrates to have a strong and clear commitment to create conditions as favourable as possible to promote innovation in the European financial industry, exploiting all the opportunities arising from new technologies.


A DIGITAL FINANCE STRATEGY FOR EUROPE
A DIGITAL SINGLE MARKET FOR FINANCIAL SERVICES
A REGULATORY FRAMEWORK FACILITATING INNOVATION
A EUROPEAN FINANCIAL DATA SPACE TO PROMOTE DATA-DRIVEN INNOVATION
ADDRESSING THE RISKS OF DIGITAL TRANSFORMATION
THE BENEFITS OF DIGITAL FINANCE

Better financial products for consuments and new ways of channeling funding to EU businesses, in particular SMEs.

Supports Europe's economic recovery strategy and opens up new channels to mobilise funding to support the Green Deal and the New Industrial Strategy fro Europe.

Cross-border digital finance will enhance financial market integration in the Banking Union and the Capital Markets Union.

Strenghten Europe's ability to retain and reinforce our open strategic autonomu in financial services.

Source: European Commission – Digital Finance Factsheet, September 2020

In October 2020, the European Central Bank published the Report on a digital euro. The report does not take an ultimate position on the matter, but some considerations are noteworthy:

- a digital euro can provide benefits: support digitalisation in the European economy, respond to the declining use of cash, and tackle sovereignty concerns related to foreign CBDC or private digital means of payment in the Euro area
- a legal basis for the European Central Bank to be enabled to issue a digital euro treated as banknotes with the status of legal tender can be found in existing primary law.

With the accepted risk to oversimplify, we can therefore describe the environment of the proposed CBDC solution as follows:

- financial inclusion and digital literacy significantly higher compared to world average (even considering local differences)

- regulatory framework favourable to competition in financial services within a specific global strategy about retail payments evolution based on the following pillars:

  1) increasingly digital and instant payment solutions with pan-European reach
  2) innovative and competitive retail payments markets
  3) efficient and interoperable retail payment systems and other support infrastructures
  4) efficient international payments, including remittances.

- high attention to limit the possibility that the payments ecosystem is used for illicit purpose such as money laundering and terrorism financing.

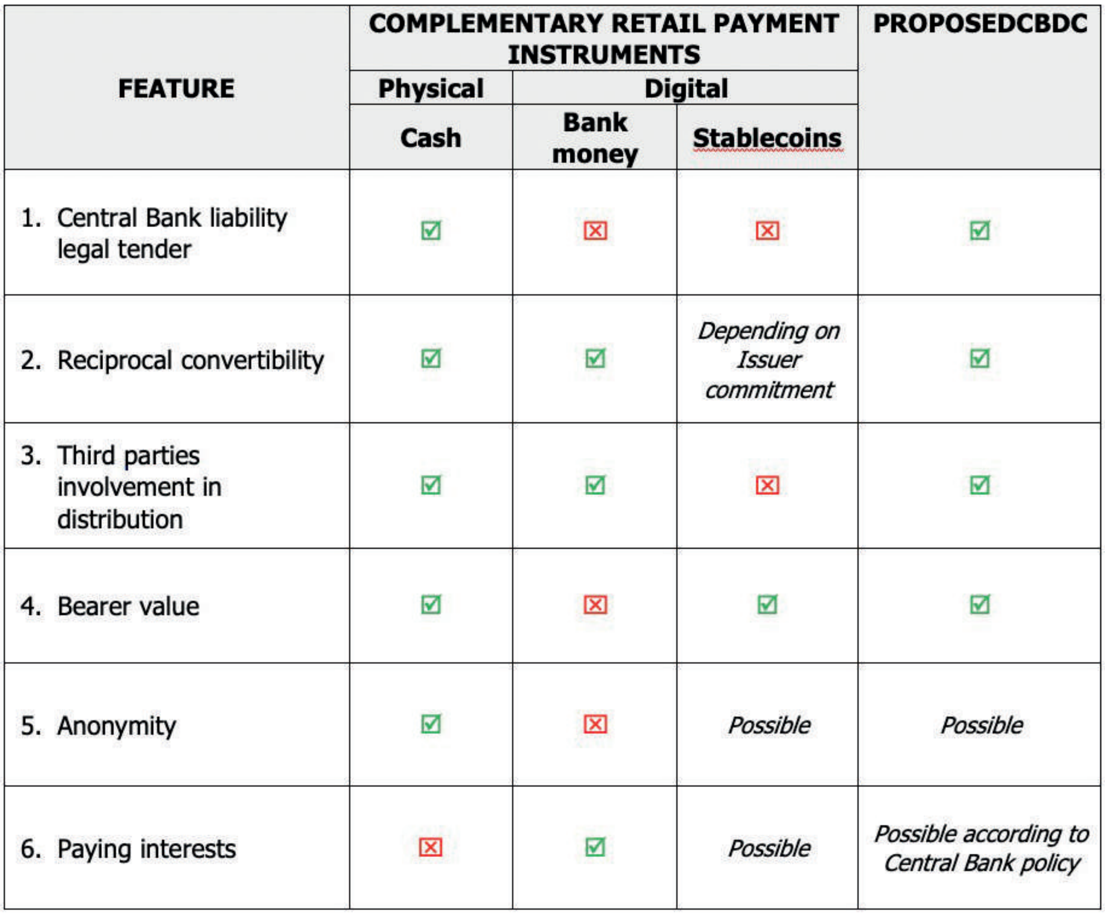
- strong sensitivity about citizen protection starting from privacy concerns.

Taking into account such a landscape, we assume that in defining a proposal for a CBDC solution, considerations regarding efficiency, resilience and compliance should prevail against considerations regarding digital divide (both technical and cultural).

4.2 A possible portrait of a general purpose CBDC

We can outline a model for a CBDC that merges the functional characteristics of cash, bank money and stablecoins.

It does not have the ambition to be the "perfect" solution, but a practical proposal to drive the subsequent analysis.



FEATURE	COMPLEMENTARY RETAIL PAYMENT INSTRUMENTS			PROPOSEDCBDC
	Physical	Digital		
	Cash	Bank money	Stablecoins	
1. Central Bank liability legal tender	☑	☒	☒	☑
2. Reciprocal convertibility	☑	☑	*Depending on Issuer commitment*	☑
3. Third parties involvement in distribution	☑	☑	☒	☑
4. Bearer value	☑	☒	☑	☑
5. Anonymity	☑	☒	*Possible*	*Possible*
6. Paying interests	☒	☑	*Possible*	*Possible according to Central Bank policy*

Starting from the underlying conditions and this high-level picture, we can formulate a list of general principles to guide the design.

4.3 Guiding principles

It is important that the design phase rests on a solid set of guidelines meeting the needs of all the stakeholders involved.

GP1. *CBDCs are direct liability in the balance sheet of a Central Bank. CBDC is considered a legal tender convertible at par with the other types of funds. The Central Bank does not have any active role in users payment operations that do not impact its own balance sheet.*

GP2. *The CBDC "lifecycle" (issuing/burning, distribution, storage, transfer – the first reserved to central banks) should be managed through a distributed model within a sound arrangement framework and accountability model.*

GP3. *CBDC-based payment services shall comply with all relevant rules and obligations concerning, for example, AML/ATF prevention, consumer protection, privacy, taxation compliance etc.*

GP4. *A CBDC could bring benefits related to financial inclusion. A CBDC shall be available to all the natural persons legally resident in the relevant jurisdiction, including natural persons with no fixed address and asylum seekers, and natural persons who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons. Consumers shall be able to perform CBDC-based payments irrespective of their location. A CBDC shall also be accessible to people temporary living in the relevant jurisdiction for work, study or tourism purpose. The access shall not be limited by the individuals' culture and technical skills.*

We have identified the following Guiding Principles:

GP5. *The infrastructure underlying a CBDC should be distributed and as much independent as possible from other financial infrastructures. It should also maximize benefits related to the monetary policy transmission, programmability of payments and efficiency of the overall monetary system.*

GP6. *The underlying technical platform shall be able to sustain all the potential users in the relevant jurisdiction, with scalability and performance levels suitable for high volumes of transactions without affecting user experience. The technical solution shall adopt a security-by-design approach with the highest cyber security standards. The system should be able to run at acceptable energy usage levels limiting negative environmental impact.*

GP7. *A CBDC architecture should enable the establishing of a competitive arena for private companies to develop value added services based on the "programmable money" paradigms. This implies the adoption of a platform approach for the CBDC ecosystem. The Central Bank defines technical and operational requirements for all the participants in the CBDC ecosystem and provides governance and oversight.*

The guiding principles drive the selection of a reference model.

4.4 The selected reference model

Considering the guiding principles, we can identify a reference model by selecting the variables identified in par. 3.2.

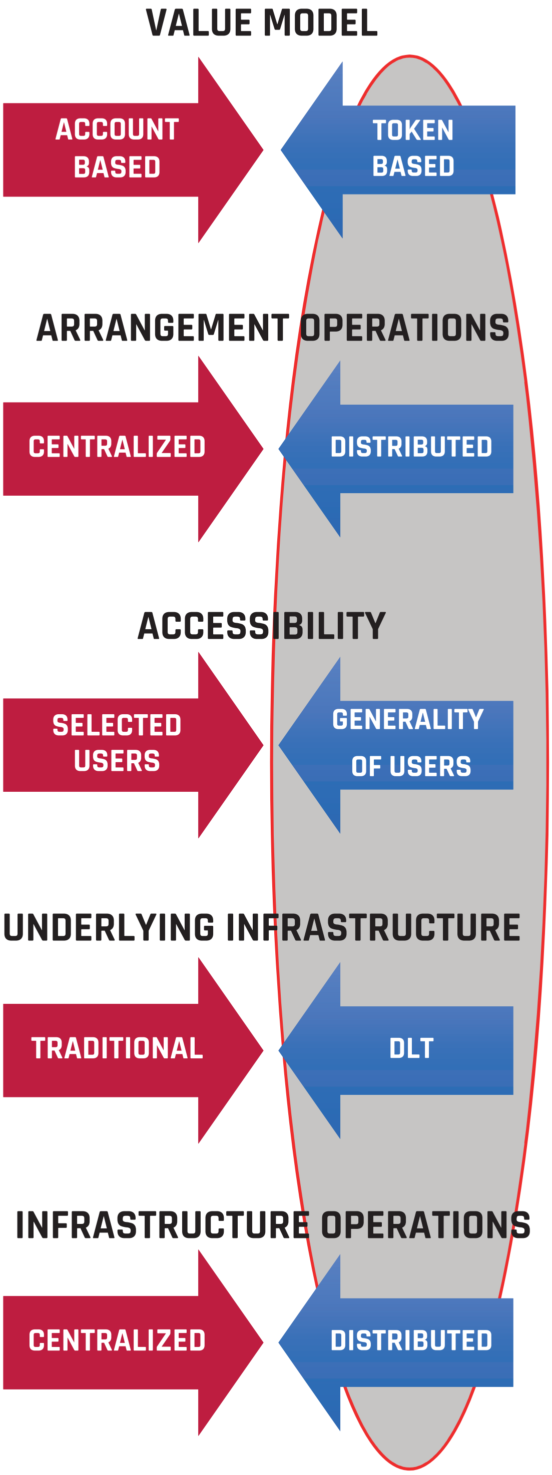
The main reasons for the choice are:

Token based value model. As described in par. 2.1, current digital payment services are based on bank money, hence on an account based model. We consider an opportunity to adopt the token-based approach to increase diversification.

Distributed model for financial roles. The effort for Central Banks to change their organization and behaviour could be very high in order to support the management of counterparties in the number of thousands or millions, while Financial Intermediaries are generally used and organized to do so in their daily business. A critical aspect is the fulfilment of KYC duties in order to comply with AML/ATF obligations (GP3). Financial Intermediaries can also manage the exchange between the various forms of funds (GP1 in relation to CBDC convertibility, GP2 in relation to management by third parties of distribution, exchange and transfer of CBDC). The roles and responsibilities are described in chapter 4.

DLT Based underlying infrastructure. Considering the CBDC portrait outlined in par. 3.2, all the defined features can be implemented independently from the adopted technology but the fourth one, bearer value. This means that the CBDC must be univocally associated to an owner, either identified or anonymous, and not duplicable: that is the description of a digital asset as defined in par. 1.3. As today, we consider DLT as the best choice to effectively manage digital assets. Detailed considerations are in par. 4.5. A DLT platform supporting a CBDC-based payment system requires a clear accountability model and continuity of service guarantees, only possible with a **permissioned solution.**

A DLT network is qualified as "permissionless" if it lacks access control mechanisms, hence everyone can participate in the network (bitcoin is the typical example of a permissionless network). On the other hand, "permissioned" networks have an access-control layer built into the architecture, so that it is possible to allow only authorized and authenticated entities to participate in the network. A permissioned network is usually preferred when security and accountability requirements are prevailing.



Distributed model for infrastructure operations. Direct consequence of the choice of a DLT based infrastructure is that is "by design" a distributed infrastructure; it would be an oxymoron to have a distributed structure centrally operated.

4.5 Focus on the choice of DLT as the preferred infrastructure

EXAMPLE OF DEFI USE CASES OVER DLT-BASED CBDC

DvP. *It is possible for a pool of qualified market operators to implement a distributed application interoperable with CBDC platform in order to perform Delivery Vs Payment exchanges of Digital Assets Vs CBDC. Such Digital Assets can represent securities, right of ownership, access to a service etc. The benefit is to share the responsibility of the arrangement over different actors, limiting the compliance requirements.*

COMPLEMENTARY MONEY. *Payment tokens fully backed by CBDC that can be issued by an entity to a user and can be spent by the users only at a selected merchant category and once received trigger a CBDC transfer from the issuer to the receiver.*

MULTI-SOURCE PROJECT FINANCING. *A pool of investors can agree to provide financial resources to fund a specific project. Through a smart contract, the resources are gathered and delivered to the beneficiary.*

SPLIT PAYMENTS. *It is possible for a merchant to define that a certain amount of the payments made with a CBDC is devoted to a given charity. The split is done immediately when the payment occurs.*

Even if the concept of CBDC is technology-agnostic, we consider DLT to have some advantages over the possible alternatives.
The first key point to be considered is the potential of DLT as a shared and easily accessible **medium of record** and the flexibility enabled by smart contracts. It is the application of the concept of “programmable money” as anticipated in par. 2.3.
These are the underlying factors enabling the so-called DeFi – Decentralized Finance – paradigm: the building of cryptoasset-based financial services among individuals accessing a public blockchain, without any intermediary and only based on distributed applications. As of August 2020, DeFI applications have moved over $ 3.7 bn in cryptoassets. Obviously, this happens outside any regulatory framework, posing issues in terms of AML compliance, consumer protection and so on.

A DLT-Based CBDC payment system can offer to the market a platform with the same potential, but within a clear and solid regulatory framework and operational robustness, upon which market operators can implement innovative services. In particular, the possibility to exchange Digital Assets and currency on the same recording medium is something very difficult to do with legacy technologies.

Such innovative services, each in the form of one or more smart contracts, can interact with each other with exponential effects in creating new opportunities in what is called **“composability”**: the possibility to consider every application as a building block of a more complex solution in an incremental model.
Several Financial Market Infrastructures have been developed by private entities using central bank money as a settlement instrument; in the future, we can envision new forms of distributed FMIs relying on a distributed CBDC platform.

Another factor is the intrinsic resilience of a distributed architecture. Under specific given conditions (e.g. level of decentralization) DLT provides limited room for arbitrary actions, translating into the impossibility for a single entity to alter the ledger bypassing the consensus mechanism. The possibility of a continuous audit trail fosters the reliability of the ledger, while the distributed architectural model reduces single points of failures. The overall risk reduction potential lowers the regulatory burden on single participants, allowing a wider participation (GP7).
It is important to clarify that the mere adoption of a DLT infrastructure to support a CBDC, does not imply the qualification of the CBDC as a cryptoasset.

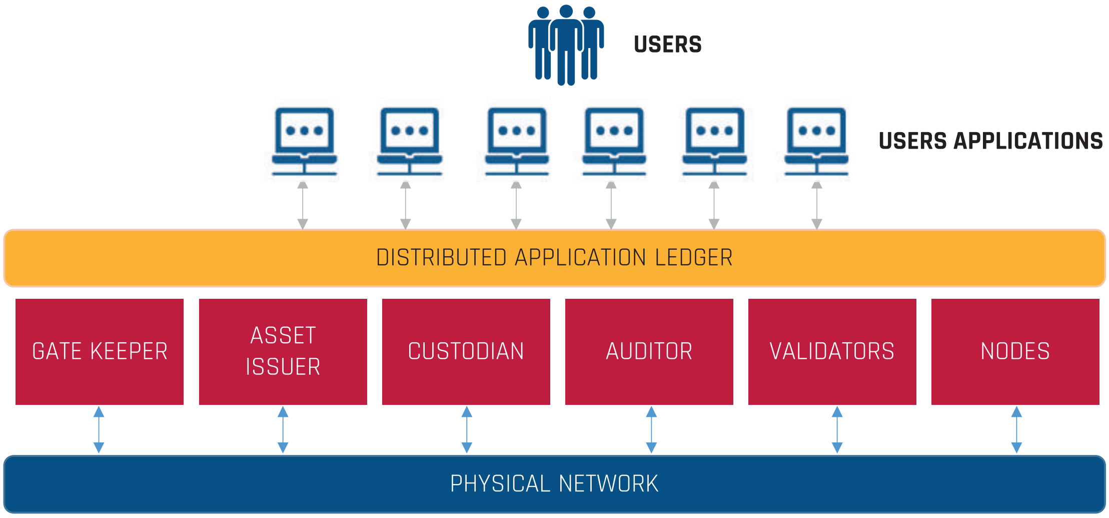
5. The high level model of DLT network

A distributed platform requires a proper governance structure and accountability model.

5.1 The logical structure

As defined in ch 1.2 DLTs are based on the concept of “nodes” for which we can refer to the following scheme.

LOGICAL ELEMENTS OF A DLT NETWORK



Nodes. The logical elements through which changes of status to the ledger are proposed.

Validator. According to the specific DLT protocol adopted, the function of participating in the consensus process that brings transactions validation.

Users Applications. Front-end applications allowing users to access the platform.

Gatekeeper. The logical function managing permissioning logics and other administrative tasks over the network.

Asset Issuer. The logical function devoted to issuing and burning of digital assets.

Custodian. The logical function managing cryptographic keys on behalf of the users.

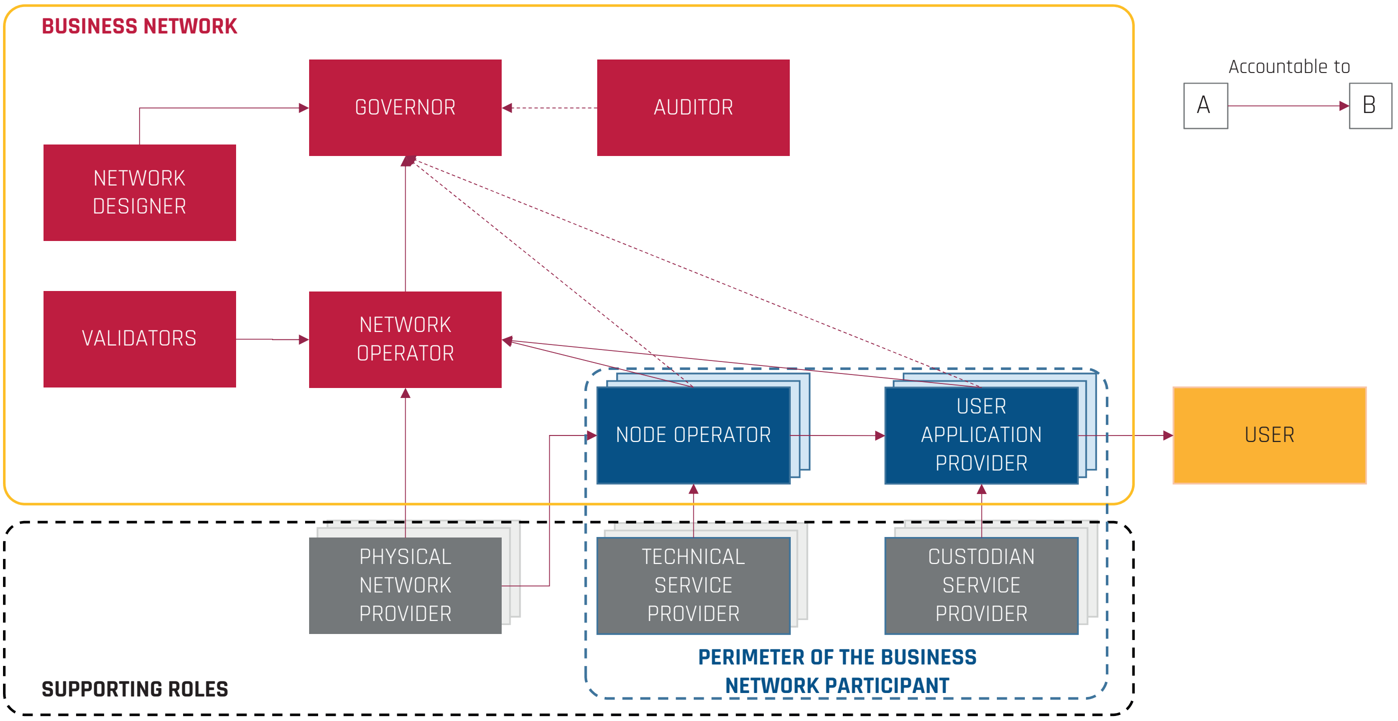
Auditor. The logical features allowing read-only activities within the network.

5.2 Operating a DLT platform: the Business Network

From the above-described logical model of a DLT platform, in order to tackle the operational model, we introduce the concept of Business Network, defined as:
"A set of members who form a community that shares one or more specific distributed applications that contribute to updating a portion of a ledger of data distributed across network nodes according to functional specifications, defined in accordance with the needs of the stakeholders and the rules of a governance model for which a single network governor is responsible."

We can refer to the following scheme:

OPERATIONAL STRUCTURE OF A DLT PLATFORM


BUSINESS NETWORK
GOVERNOR
AUDITOR
NETWORK DESIGNER
VALIDATORS
NETWORK OPERATOR
NODE OPERATOR
USER APPLICATION PROVIDER
USER
Accountable to
A
B
PHYSICAL NETWORK PROVIDER
TECHNICAL SERVICE PROVIDER
CUSTODIAN SERVICE PROVIDER
PERIMETER OF THE BUSINESS NETWORK PARTICIPANT
SUPPORTING ROLES

Within the operational structure, we can identify the core roles constituting the real Business Network and technical supporting roles.

Core roles

ROLE	Responsibilities	Accountability
Business Network Governor (BNG)	It is the entity in charge of the proper functioning of the whole system and provides the guidelines to candidate Business Network Operator (BNO) and Business Network Developer (BND) and BND. The BNG appoints the Business Network Operator in charge of managing the infrastructure and the Business Network Designer in charge of developing the distributed application. Defines technical requirements that Node Operators (NOs) Validators and User Application Providers (UAPs) have to comply to.	It is the highest level of accountability
Business Network Operator (BNO)	Implements the governance of the infrastructure and manage centralized shared ancillary services, including gatekeeping functions (management of permissioning logics), centralised oracles, monitoring, etc. Interacts with the BND for application maintenance duties. Performs the qualification of other subjects on behalf of the BNG.	Accountable towards the BNG
Business Network Developer (BND)	Develops the shared software elements according to the requirements defined by the BNG and the technical guidelines provided by the BNO.	Accountable towards the BNG
Node Operator (NO)	Entities in charge of operating validators logical elements of the DLT network on the basis of an agreement with the BNO (according to the specific DLT protocol).	Accountable towards the BNO and the BNG Accountable towards the UAP
Validators	Defines technical requirements that NOs, Validators and UAPs have to comply to.	Accountable towards the BNO
User Application Provider (UAP)	Develops and provides front-end applications.	Accountable towards the User

Supporting Roles

ROLE	Responsibilities	Accountability
Technical Service Provider (TSP)	Provides infrastructural services to the NO, according to the technical and operational requirements provided by the BNO and agreed with the BNG.	Accountable towards the NO
Validators	Provides custodian services to the UAP.	Accountable towards the BNO
Custodian Service Provider (CSP)	Provides custodian services to UAP.	Accountable towards the UAP
Physical Network Proivder	Provides connectivity services to the Node Operators. The BNO sets the specifications for connectivity services to be provided by the Physical Network Provider.	Accountable towards NO and BNO

The identified supporting roles are subject to a qualification by the BNO on behalf of the BNG. For the sake of clarity, a provider of professional services to which a NO entrusts node maintenance is not qualified as a TSP. The accountability model implies the right of audit by the entity that every role is accountable to.

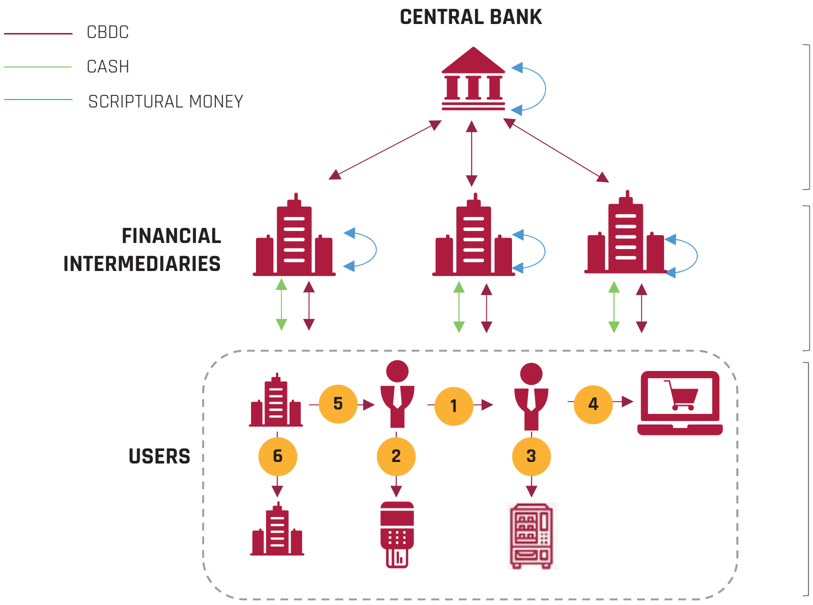
In a given Business Network there is only one Governor and one Operator, while it is possible to have many subjects performing the other roles, with possible overlaps (e.g. a Node Operator can also be a User Application Provided and the Business Network Operator can also act as a Technical Service Provider).

6. A proposal for a DLT-based CBDC payment system

The general governance structure and accountability model of a DLT platform can be adapted to a CBDC payment system. Financial Intermediaries can take on new roles.

6.1 CBDC use cases

As mentioned, the CBDC is intended as a complementary form of money along with cash and bank money, so that it should address all the most common payment scenarios.



CBDC issuing upon request by Financial Intermediaries

CBDC distribution to end users in exchange of cash or bank money

CBDC transfer among users:

1. Person-to-person
2. Payment at an attended POS (e.g. in-store purchasing)
3. Payment at an unattended POS (e.g. vending machine)
4. eCommerce
5. Business-to-Person (e.g. salary payment)
6. Business-to-Business (e.g. DvP)

The arrangement and underlying technical platform should therefore be able to satisfy the needs of the various users (natural persons, legal entities or even machines).

We therefore need to define the proper operational model and the general requirements of the instruments available to end users to access the platform.

6.2 The actors and roles

A payment system is defined as:

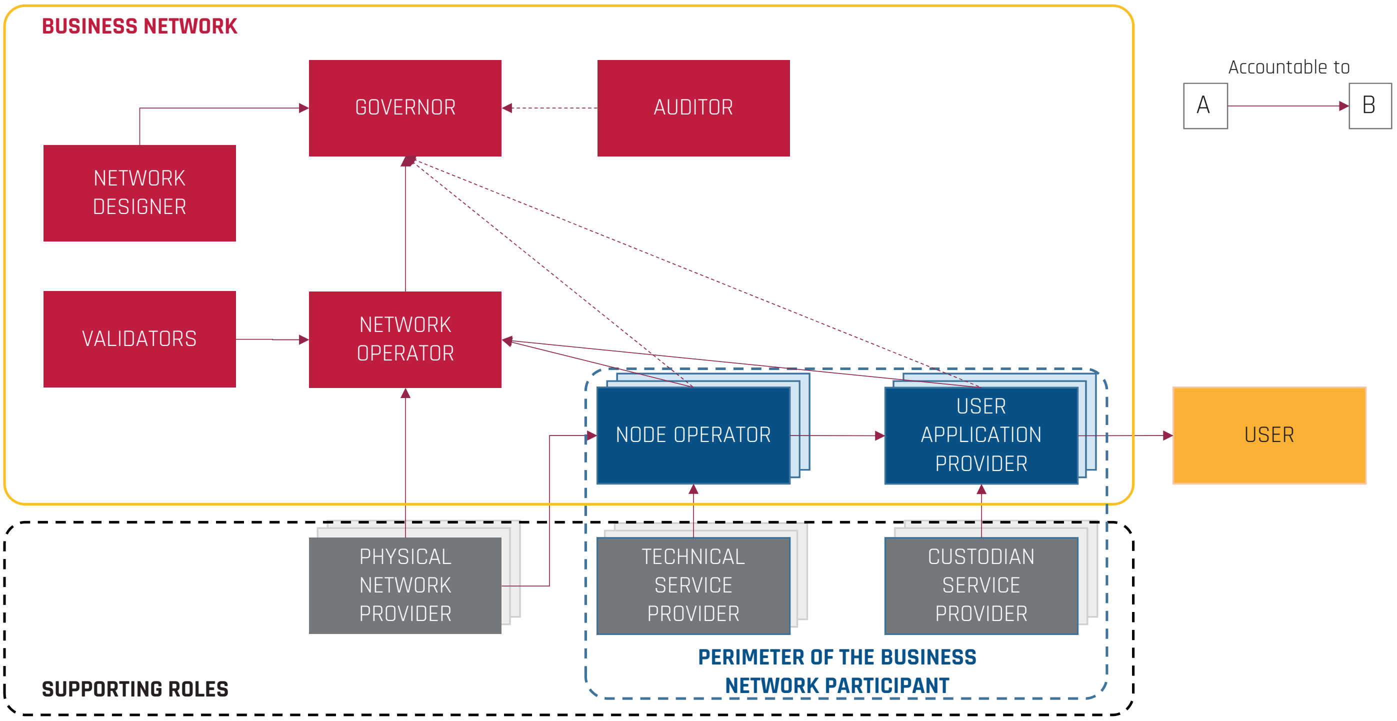
"A set of instruments, procedures, and rules for the transfer of funds between or among participants; the system includes the participants and the entity operating the arrangement. Payment systems are typically based on an agreement between or among participants and the operator of the arrangement, and the transfer of funds is effected using an agreed-upon operational infrastructure."
(Bank for International Settlements, April 2012 - Principles for financial market infrastructures).

We have to take in consideration the specificity and the distributed nature of a DLT platform in order to apply the above definition to a CBDC based payment system as proposed in this paper.
We therefore have to identify the single entities involved and the roles they cover both as participants in the payment system arrangement and as operators of the underlying infrastructure.
Financial Intermediaries, where this term do not only refer to banks but also to other qualified entities to be identified according to local regulation, play a key role.

ENTITY	ROLE CBDC PAYMENT SYSTEM ARRANGEMENT	ROLE WITHIN THE DLT-BASED CBDC BUSINESS NETWORK
Central Bank	Is the orchestrator of the arrangement and provides the rules and guidelines to be followed by all the involved parties.	The Central Bank is primarily the Governor of the Business Network. Being the sole entity in charge of issuing and burning CBDC, it also operates as the **Asset Issuer**. The Central Bank is a **Node Operator**. According to the regulations applied in every single jurisdiction, the Central Bank can also operate as the **Auditor.** The Central Bank can also take directly the roles of **Business Network Operator** and **Business Network Developer**.
Financial Intermediary	Is the main participant in the Payment System managing three core functions: - KYC processes for the on-boarding of users - Distribution of CBDC and exchange into other forms of funds (cash and bank money) and vice-versa - User-relationship management.	The Financial Intermediary can cover different roles: - **Users Application Providers** providing the CBDC wallet to Users (see par. 6.3) - **User** of CBDC - **Node Operator.** When acting as a UAP the Financial Intermediary is not required to operate a node, but can access the ledger through another Financial Intermediary it has an agreement with - **Custodian Service Provider-**
Users	Access the Payment System to receive, store and transfer CBDCs.	N/A
Business Network Operator	Infrastructure operations	As defined in par. 4.2., the BNO can also operate as a TSP to provide outsourcing services for the Node Operators.
Business Network Designer	Infrastructure operations	The BND is in charge of the development of the application protocol logic that constitutes the foundation of a CBDC payment system (including smart contracts). It develops the dashboards needed for system management and governance. It develops the instruments required for oversight and supervision duties. It provides the technical documentation for the use of these systems by the UAPs. According to the Central Bank's choice, the BND could be asked to develop a specific SDK to facilitate for the UAPs to develop front end applications.
Validators	Infrastructure operations	As defined in par. 4.2.
Custodian Service Provider	Infrastructure operations	As defined in par. 4.2.

The operational structure is therefore adapted as follows:

OPERATIONAL STRUCTURE OF A DLT PLATFORM


BUSINESS NETWORK
GOVERNOR
AUDITOR
Accountable to
A
B
NETWORK DESIGNER
VALIDATORS
NETWORK OPERATOR
NODE OPERATOR
USER APPLICATION PROVIDER
USER
PHYSICAL NETWORK PROVIDER
TECHNICAL SERVICE PROVIDER
CUSTODIAN SERVICE PROVIDER
PERIMETER OF THE BUSINESS NETWORK PARTICIPANT
SUPPORTING ROLES

A note about the role of the Auditor: in a complex arrangement, as could be a CBDC payment system in the Eurozone, the National Central Banks part of the Eurosystem could act as Auditors as part of their supervision activities.

6.3 Participating in the CBDC Business Network

While the roles of BNO and BND are assigned by the Central Bank, if the Central Bank itself does not cover these roles, other actors have to follow a specific process according to the role they intend to cover.
We envision that Financial Intermediaries will have to apply to the Central Bank in order to be part of the CBDC payment system. The Central Bank will set the detailed requirements about corporate structure and the like regarding the CBDC arrangement's point of view. From the infrastructure operations' point of view, a Financial Intermediary should be required to:

- describe the features of the different kinds of wallets provided to customers
- describe if it also wants to be a Node Operator within the Business Network, either directly operating a node or adopting a service form a TSP, or access the ledger through another Node Operator
- describe how the custodian services (if included) are provided, if directly or through a CSP.

We consider three possible different classes of Financial Intermediaries on the basis of the services provided to users, for example:

Services	Class A	Class B	Class C
CBDC store and transfer	✔	✔	✔
CBDC distribution	✔	✔	
Custodian services	✔		
Comparable to	Account Servicing Payment Service Provider	Currency Exchange	Cryptocurrency Wallet Provider

Acting as the BNG, the Central Bank verifies the application and, if accepted, instructs the BNO to manage the inclusion of the new member into the Business Network, also by providing the instructions to deploy the distributed application (if the new member is a Node Operator).

Considering such a structure, it is evident that the role of Financial Intermediary is open, not only to existing payment service providers operating in the financial arena, but also to new kinds of operators that can leverage the opportunity to build completely new business models. The Central Bank retains its roles of supervision and oversight.

For the **Technical Service Provider,** it is possible to imagine a process where the Business Network Operator publishes the technical and operational guidelines (agreed with the Central Bank) for the entity aiming at cover this role.

The Central Bank, possibly with the operational support of the BNO, performs the initial certification and subsequent audits.

For **Custodian Service Providers**, the related regulations regarding crypto assets custodian services will apply.

6.4 Cyber security concerns

As for every financial market infrastructure, the highest attention must be posed to cyber security and cyber resilience at every level, also considering that a CBDC based payment system will be an obvious high-level target for large scale cyber attacks.

ISO 27000: 2018 defines “information security” as safeguarding the confidentiality, integrity and availability of the information itself that is considered an asset to which a value is associated.

The fundamental information of a DLT system can ultimately be identified in the managed “ledger” and in the “transactions” contained therein.

Considering the above, the safety objectives of a DLT can be defined as the need to ensure the following requirements:

- availability of the ledger and, more generally, availability of the functions made available by the DLT platform
- integrity of the ledger and of the information contained therein
- confidentiality of the information contained in the ledger (where required at business level)
- non-repudiation of transactions
- uniqueness of transactions
- authenticity of transactions.

Best practices shall be adopted according to the relevant regulations and guidelines starting from (considering the European environment) the Cyber Resilience Oversight Expectations for financial market infrastructures, to be adopted by every entity involved into CBDC operations. Just to name a few:

- secure and encrypted connections between all participants
- segregation of duties for operations on technical components
- architecture based on decoupled layers
- management of both network and users' cryptographic keys according to consolidated procedures and through secure devices (HSM, TEE, etc.)
- control methods, 24-hour monitoring and timely interventions with red switch and multifactor authentication
- definition of a risk model, preventive and corrective actions, possible impacts and probability of occurrence
- definition of a CSO (Chief Security Officer) for each accountable role previously identified
- application of systematic risk assessment practices
- performance of situational awareness activities as threat intelligence and info-sharing, as adaptive risk management practices
- selection, design and implementation of measures to mitigate security risks
- provisioning of assurance and verification of security controls effectiveness.

Each of the cybersecurity topics to be addressed will be covered and enforced by the operative roles included in the governance model according to the relevant accountability scheme.
The Business Network Operator, in particular, will be in charge of providing specific guidelines and audit activities.

6.5 Users Applications: the CBDC wallet

The digital wallet is the application through which the user accesses the CBDC payment system and can be managed according to two different models on the basis of the possibility to certainly associate a cryptographic key (hence the ownership over the digital asset) to the owner:

- **key-based**: no record is kept about the association between the user identity and crypto keys
- **identity-based**: a full KYC process is performed, so it is possible to track the ownership of CBDCs to the identity of the user.

To maximize the flexibility (GP4 and GP7) while ensuring a proper attention to regulation compliance (GP3) it shall be possible for the two models to coexist and for a user to adopt the solution that best fits their needs (or adopt both for different uses).
The two kinds of wallets are subject to a different on-boarding process performed by the Financial Intermediary.
The on-boarding process can be managed either on-site or on-line according to the relevant regulations.

The following description focuses on the use of smartphones as user devices.

	KEY-BASED	IDENTITY-BASED
User enrolment	The User downloads the wallet provided by a Financial Intermediary and generates the couple private key/public key. In order to generate the couple of keys, the Financial Intermediary needs first to gather a minimum set of the User's data in order to verify the existence of a wallet associated to the same person (e.g. checking a public register of hashed personal data associated to public keys). The user receives the API key to be used to access the platform. The Financial Intermediary keeps copy of the user's data strictly needed for compliance requirements. A natural person can have only **one key-based wallet**. The possibility for a legal entity to own a key-based wallet is not considered.	The user downloads the wallet provided by a Financial Intermediary. The Financial Intermediary performs full KYC according to the specific kind of User (natural person, legal person etc.) and if everything works, the wallet is enabled. It is possible for a User to have **more than one identity- based wallet.**
Key management	The user is responsible for key management, with the risk for the user to lose the crypto keys and consequently to lose money. **No custodian service is considered** for token-based wallets. The FI is not responsible for the proper execution of a payment (apart from a technical point of view as a Node Operator) and cannot deny a transaction.	The Financial Intermediary is **required to provide custodian services** (directly or through a CSP), managing keys on behalf of the users. The FI is accountable towards the user for the proper execution of payments. It is also liable in case of any technical inconvenient resulting in the loss of the user's cryptographic keys. The FI, if the need occurs, has the possibility to deny a single transaction (for example upon a suspect of illicit operation) or inhibit the access (for example upon the order of a relevant authority).

Key-based managed wallets open the theme of how to manage, for example, the accidental loss of the private key. Since it is not acceptable that losing the private key prevent a citizen from using this service, a proper solution shall be designed. A possible alternative is to implement some sort of "proof of ownership" in the enrolment phase to be used by the citizen to attest the loss and get another private key.

To address the needs of different kinds of users, different "tiers" of wallets should be considered.

As an example:

TIER	FEATURES	COMPARABLE TO
0	General purpose key-based	Cash and anonymous eMoney
1	Identity-based wallet for natural person users EU resident	Pre-paid payment cards
2	Identity-based wallet for natural person users EU resident	Payment accounts
3	Identity-based wallet for natural person users not EU resident	Payment accounts
4	Identity-based wallet for legal person users different from Financial Intermediaries	Payment accounts
5	Identity-based wallet for Public Administration	Payment accounts
6	Identity-based wallet for Financial Intermediaries (treasury account)	n/a

The Tier 0 wallet will be subject to limits on single operations value and maximum amount of CBDC stored, according to the relevant AML/ATF regulations applicable to anonymous eMoney payment instruments and/or cash payments.

Users can switch their Tier 0 wallet from a wallet provider to another by simply associating their private keys.

On the other hand, the owner of an identity-based wallet willing to change providers shall go through the KYC process of the new provider unless a proper process for data sharing among Financial Intermediaries is put in place.

Held CBDCs must be transferred from the old wallet to the new one. If the Central Bank intends to adopt the leverage of remunerating CBDCs as a monetary policy instrument (GP5), the "tiering" of CBDC wallets allows to apply different remuneration rate to the different wallets. For example, the Central Bank could apply rate 0 to key-based wallet, positive remuneration rate to resident users (issuing new CBDC directly to the Users' wallets), negative remuneration rate to Financial Intermediaries (burning of CBDC) and so on.

Furthermore, the possibility for the Central Bank to issue CBDC directly to users could also support the implementation of the so-called "helicopter money" actions if needed.

6.6 Users Devices

The User device is the instrument allowing Users to receive, store and transfer CBDC. We have to consider the requirements of several classes of Users: natural persons, legal person different from in-store and on-line merchants, in-store merchants, on-line merchants.

USER CLASS	DEVICE
Natural Person	a) Dedicated software in the form of: - Mobile app - Browser extension - Desktop Software - Web application. The dedicated software solution can implement both the identity-based and key-based approach. In order to simplify the diffusion, the Central Bank could make available specific SDKs. b) Smartcard. Key-based approach only.
Legal person different from in-store and on-line merchants	Mainly desktop based dedicated software. Identity based approach only. According to the dimensions and complexities of the companies, the need will emerge to implement adequate treasury management processes (authorization levels, multi signature etc.), opening a space for market operators to develop specific solutions to be implemented on top of the basic payment functions made available over the CBDC based payment system.
In-store merchant	Dedicated software running on smartphone, tablet or android-based pos. We expect that UAPs will develop specific applications compliant to technical guidelines.
On-line merchant	We expect that CBDC payments will be integrated into existing solutions through dedicated applications on top of the basic payment functions made available over the CBDC based payment system.

All the market solutions will be analysed by the Central Bank before their commercialization to assess security and reliability. Once a common standard is consolidated, such kind of certification will be simplified.
User applications should exploit tamper-resistant hardware (e.g. secure elements, physically un-cloneable functions or the equivalent) to foster security as well as all the widely adopted solutions to increase the Users' protection like biometric authentication.
It is possible for a key-based solution to perform off-line transaction provided the counterpart is online as in the case of a card payment at a POS.

The possibility to manage transactions where both the users' devices are off-line is a necessity in order to foster financial inclusion and provide a use experience as similar as possible to cash payments. On the other hand, it poses challenging issues.
The first topic to be considered is related to the very nature of a DLT-based CBDC. The "money" is issued in the form of a digital asset and the payment is finalized when it is recorded on the ledger the transaction between the payer and the payee. Hence, an off-line operation cannot in any way be considered a "payment" intended as a transfer of funds. What is possible is to gather a kind of pre-authorization from the payer that the payee can execute when online. This situation induce a potential liquidity risk in a payment system that should be free of such a risk, so that need to implement a technical solution that limits the risk.

Among the possible solutions currently under evaluation, we highlight:

- the CBDC balance is stored in the User device after each payment. A specific application can be developed allowing the device to process an off-line transaction up to the value of the last recorded balance amount. It requires that both the device can communicate via contactless solutions (NFC, UWB, Bluetooth etc.). The transaction is broadcasted on the ledger when the payee device is online. Such a feature should be implemented in a tamper proof way. Further limits can be included (e.g. number of transactions)

- develop an ancillary service where users can allocate part of the CBDC balance on the ledger and store the equivalent in a form of eMoney on users' device. Such CBDC-backed eMoney can be transferred among users through contactless solutions. The receiving party can "redeem" the eMoney when on-line. The risk is to create a parallel CBDC-backed eMoney circuit introducing some inefficiency.

Specific research activities are currently ongoing at both academicals and industrials level; no consolidated solutions are so far available.
We consider the smartcard solution applicable to the key-based approach in an initial phase, because an identity-based approach requires the receiving terminal to be able to identify the custodian and send a request to pay. This needs the development of a specific protocol and operational model not to be considered as a core feature of the envisioned CBDC payment system. It should be an advanced solution to be developed by market operators or a consortium of Financial Intermediaries.

Some considerations about smartcards: considering that the security requirements are the same of existing payment cards, it is advisable to refer to the same standards, like EMV. The smartcard manufacturers authorized to produce CBDC-enabled cards shall be subject to surveillance and audit processes to avoid misconduct. Best practices from PCI-DSS (Payment Cards Industry – Data Security Standards) can be adopted.

CBDC IN REAL LIFE

Sarah is a 16 year old "new European" since she was born in Europe from immigrant parents. She is happy to live in Europe even if in a small town in the south. She likes fashion, music, hanging out with friends and, if any time is left, study. Nevertheless she managed to get very good grades during the last school year, so good in fact that it made her eligible for a prize funded by a local bank. The prize is a sounding 50€ allowance to be spent for cultural purposes. Sarah is a digital native and owns a smartphone (a low-cost one). Some months ago, she heard about a new digital money and decided to try the service from a new company with a fancy name. After a very simple procedure, she got a new app to make payments using digital money. It was so easy that even when her cousin came from abroad to spend some weeks for a cultural exchange, she convinced him to download the app and change the cash he took with him into digital money through an automatic exchange kiosk.

Sarah choose to get the grant in the form of digital money. Now she stops at a local book shop, and once at the cash register the app presents the option to choose between using the grant or not. The merchant uses a service from their bank and can accept the new payments with the same device used to accept card payments. The bank automatically moves the digital money to the merchant's bank account.

It is very simple for Sarah to pay: just framing a QR code on the terminal display. The merchant thanks Sarah with a smile and starts talking about when "back in the days we used cash, and we had to carefully check for change and bring the money to the bank". Sarah uses another part of the grant to buy on-line two tickets for a classical music concert. Her friend Frances is a very good girl but with strange tastes. Frances insists to pay for her part and sends the money to Sarah using her own digital money app. Frances uses another provider that allows to send money starting from a Whatsapp chat.

Sarah is also very fond of animals and, before going home, stops at a local dog shelter where she volunteers sometimes. Mike, the shelter manager is quite happy. He has just signed an agreement with a large pet-products franchise: for the next two months 0.5% of all the sales paid with digital money will be devoted to the shelter. What is thrilling is that Mike can check every donation in real time.

There is also Joan, another volunteer. She is retired, but still very active. She also likes to use the new payment system. It was her son who took her to the local post office where a very kind clerk helped her fill in the required documents and also taught her how to use the app. Joan chose to have her monthly pension sent partly to her bank account and partly in digital money, that is so handy to make small payments.

6.7 Some considerations about privacy in a CBDC payment system

Privacy is a key success factor in order to gain acceptance from citizens. From this point of view, some considerations can be shared. We can consider cash as the maximum level of privacy protection, as it ensures the full anonymity of transactions: it is not possible to track the change of ownership of a banknote. On the other hand, in several jurisdictions the use of cash is subject to various degrees of limitations to reduce the risk of tax evasion, money laundering and terrorism financing.

In a CBDC-based payment system, the challenge is to get a proper balance between privacy and control to limit such risks.

Anonymity, privacy and confidentiality

Talking about data there is the risk to consider the terms as synonymous, even if they have very different meanings.

Anonymity refers to data that are never linked to an individual.

Privacy refers to a person's right to control and protect their private information, and to decide what information is deemed private.

Confidentiality is about the practice of managing information to protect an individual's privacy and avoid any misuse of data.

Within a CBDC-based payment system, as in any other payment system, the highest level of attention must be devoted to ensure confidentiality in order to protect individuals privacy rights.

We consider the following principles as a reference framework to define privacy protection requirements:

- CBDC-based transactions will be subject to the same reporting obligations as bank money transactions

- above a defined threshold, for law enforcement duties it should be possible to determine the personal identity of users involved in a transaction

- if not otherwise required by relevant law, in a commercial transaction the payer's identity shall be hidden from the payee.

The key-based approach allows a high level of protection, since the association with the natural person is not recorded anywhere, hence the need to set adequate limits to reduce misconduct risks.

The identity-based approach is, on the other hand, comparable to a bank account since it is based on a contractual relation between the user and the Financial Institution.

At platform level, the adoption of a permissioned approach limits the access to the ledger to qualified entities in a context of a proper arrangement and accountability model.

We are aware that some work still has to be done at technical level to foster data protection.

At operational level, all the provisions of the privacy protection regulation (e.g. GDPR in the European Union) can be satisfied, leveraging the experience of Financial Institutions in providing privacy protection to their customers. Once again, the accountability model helps in identifying the entities in charge of data protection duties. We consider as guiding principles for addressing the confidentiality requirements the Financial Market Infrastructure and Privacy Enhancement Technology (PET) principles described in the document "Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies" (cfr. https://www.enisa.europa.eu/publications/pets)."

7. CBDC lifecycle

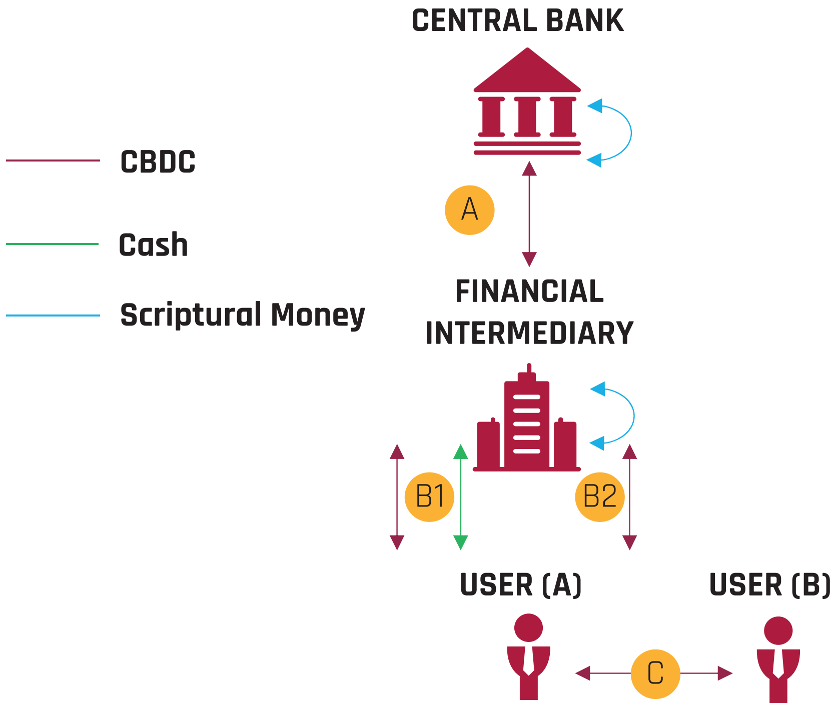
Financial Intermediaries ensure the interoperability across the different forms of money.

7.1 Overview

We consider four step in CBDC lifecycle:
A. Issuing
B. Exchange
C. Transfer
D. Burning

According to GP2, several entities are involved in the lifecycle management.

CBDC LIFECYCLE



A) Issuing / Burning

B) Distribution

B1) Exchange against cash

B2) Exchange against scriptural money

C) Transfer

7.2 CBDC issuing and burning

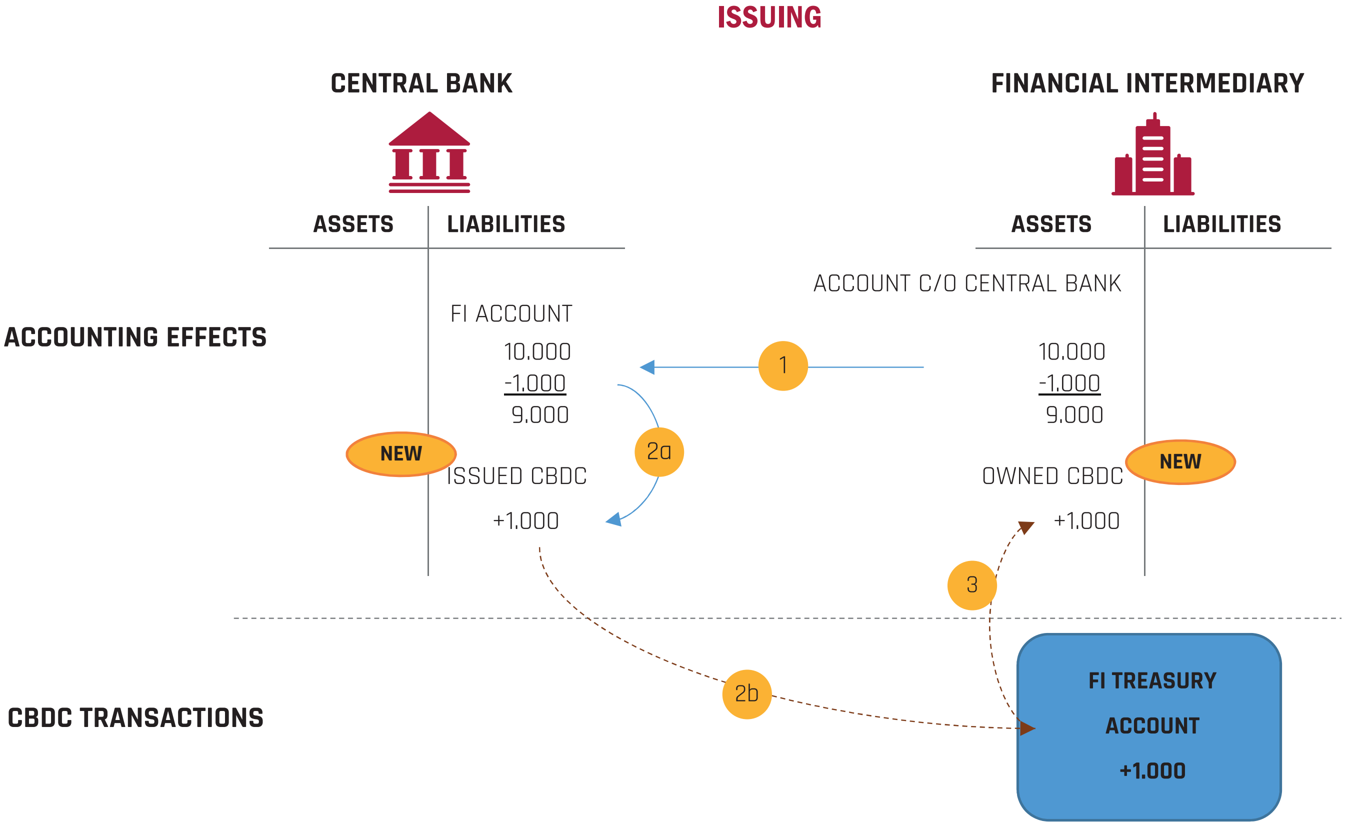
The issuing and burning of CBDC must have as low an impact as possible on existing processes and legacy systems and applications. Therefore, we consider that the issuance of a CBDC is done by the Central Bank upon the request of a Financial Intermediary that has access to Central Bank settlement accounts.

Linking issuing and burning of CBDCs to settlement accounts, greatly simplifies the implementation since the process rests on existing procedures and systems (RTGS on behalf of the Central Bank).

The messages between involved parties can make use of the industry-wide ISO 20022 standard.

The **Issuing** process starts with the Financial Intermediary sending a request to the Central Bank. The Central Bank issues over the DLT an amount of CBDCs equivalent to the value debited on the Financial Intermediary settlement account.

The value of issued CBDCs is registered in a specific new section of the Central Bank balance sheet (as a liability). On the other side, the Financial Intermediary registers the value of owned CBDCs in a specific account of its balance sheet (as an asset).



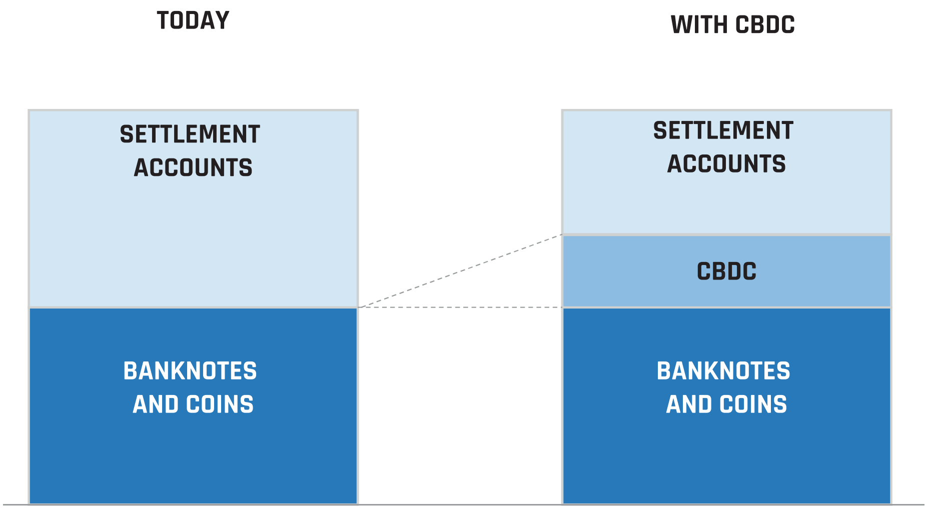
1. The FI sends a request to the Central Bank

2. The Central Bank debits the FI settlement account and (2a) creates new CBDC assigned to the FI and (2b) registers the value in the Issued CBDC account

3. Once the issuance of CBDCs is confirmed, the FI registers the value in the Owned CBDCs account

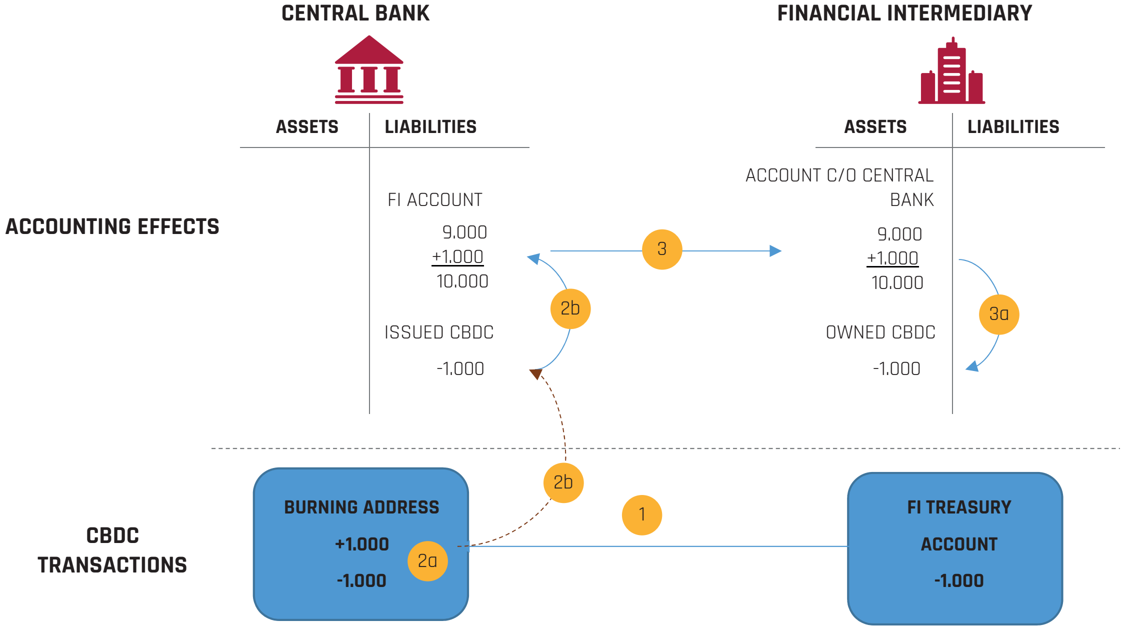
In this model, the issuing of CBDC does not alter the amount of money supply at a given time, since it is a shift from one form (settlement account) to another (CBDC).

CBDC ISSUING IMPACT ON M1 MONETARY AGGREGATION



In the **Burning** process, the Financial Intermediary transfers CBDCs to a "Burning Address" of the Central Bank. The Central Bank removes the CBDCs and credits the equivalent amount to the Financial Intermediary settlement account, debiting the CBDC Issued account in its own balance sheet.

BURNING



1. The FI CBDCs to a specific "burning address" of the Central Bank
2. The Central Bank (2a) burns the CBDCS, (2b) debits the Issued CBDCs account and (2c) credits the FI account
3. Once the credit of FI account is confirmed, the FI updates its balance sheet

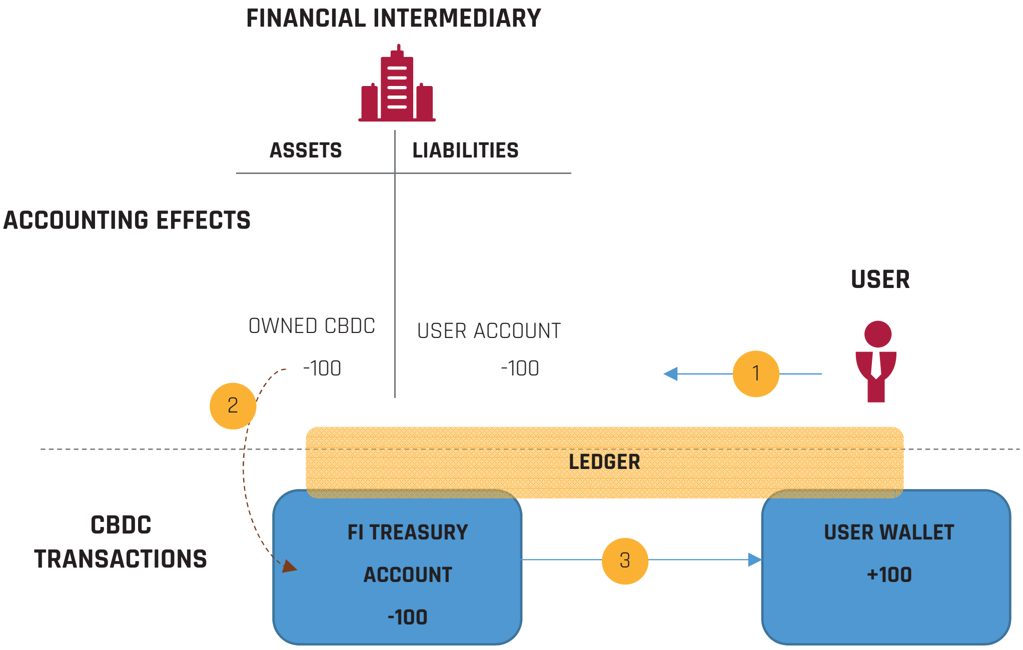
As for issuing, the burning process does not alter the money supply.
Both processes are mainly based on automatisms, with the possibility for a human operator to intervene on single transactions if needed.

7.3 CBDC distribution

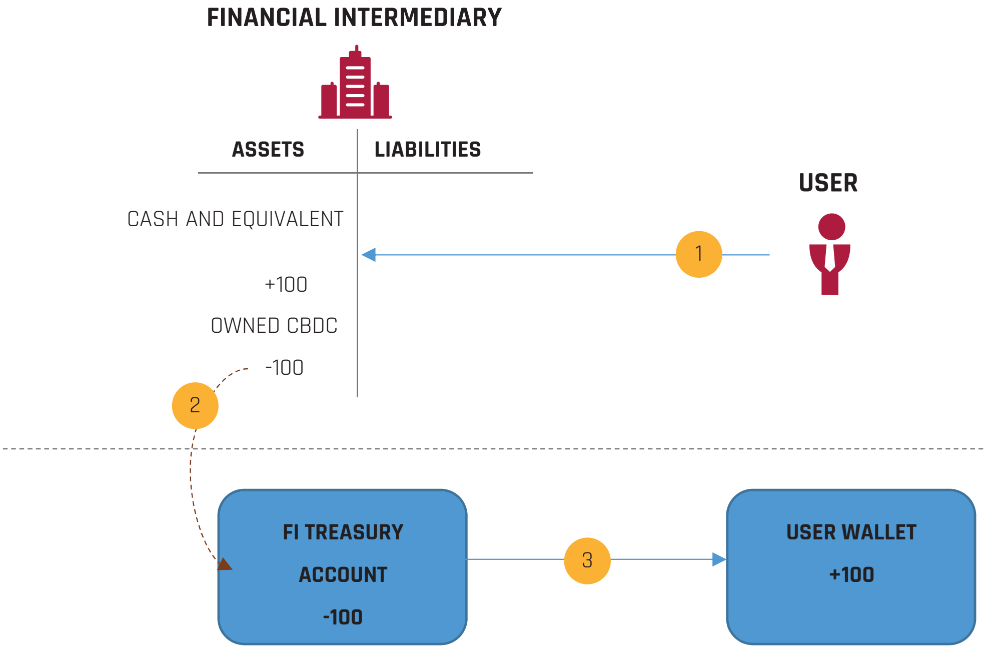
The exchange of CBDC into other forms of money is the core role of Financial Intermediaries.

A User can obtain CBDC from a Financial Intermediary either by depositing cash or debiting their bank account. Obviously, the process works both ways.

CBDC EXCHANGE AGAINST SCRIPTURAL MONEY



CBDC EXCHANGE AGAINST CASH



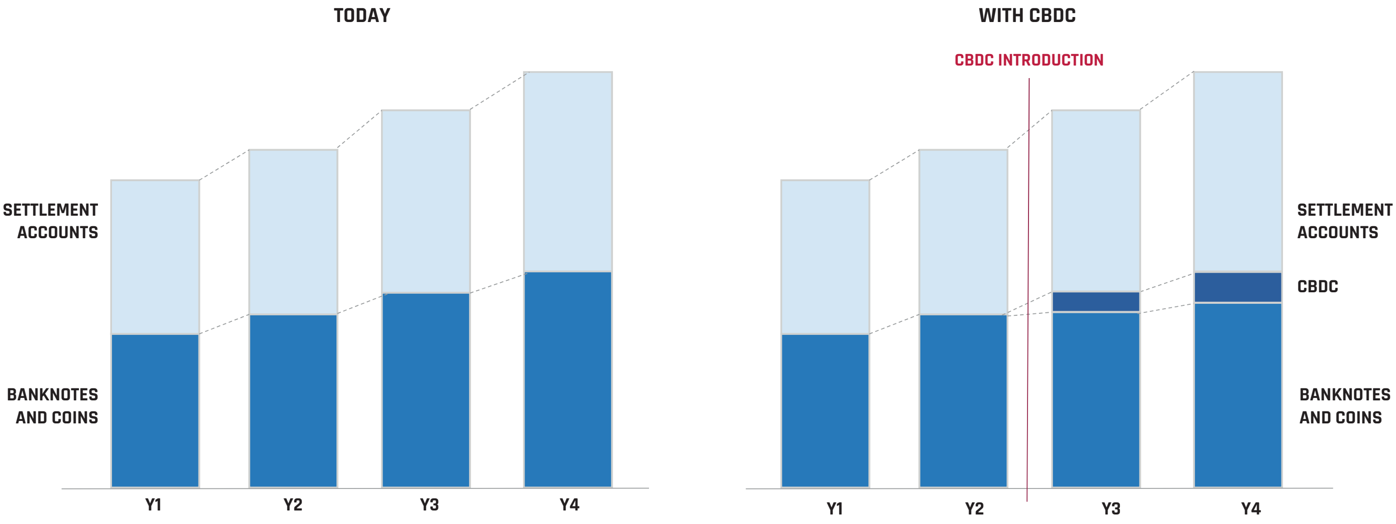
1. *The User sends an order to the FI he has an account to*
2. *The FI debits the User account and contextually debit its “owned CBDC” account*
3. *The FI transfers the equivalent amount of CBDC form its treasury account on the ledger to the User’s wallet*

1. *The User deposits cash to a FI*
2. *The FI credits its “cash account” and contextually debit its “owned CBDC” account*
3. *The FI transfers the equivalent amount of CBDC form its treasury account on the ledger to the User’s wallet*

Considering the exchange between CBDC and scriptural money, it is not mandatory for the User to have an account at the Financial Intermediary performing the exchange, but he can get CBDC through a credit transfer from another Financial Intermediary.
The same is valid for the reverse process, where the User can provide a destination account for the funds.
For the sake of clarity, once the CBDCs are transferred to the Users wallet they are no more accounted for in Financial Intermediary balance sheet.

On a medium term outlook, it is expected that CBDC will mostly affect cash growth.

MEDIUM TERM IMPACT OF CBDC ON M1 MONETARY AGGREGATION

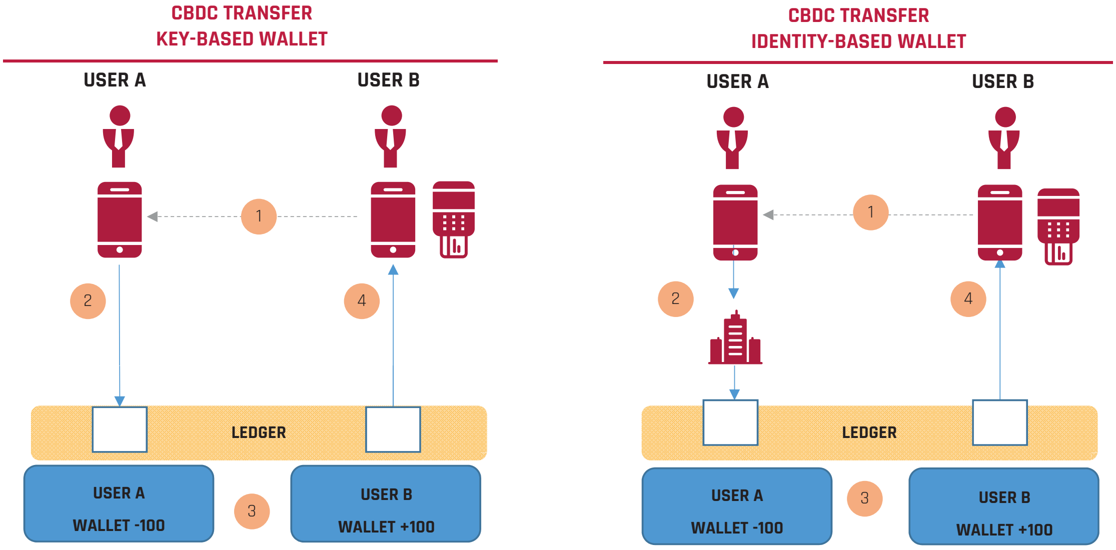


For illustrative purpose only. The graph does not represent reciprocal proportions

7.4 CBDC transfer

In the following example, User A is the payer and User B is the payee (either a natural person or an unattended device).

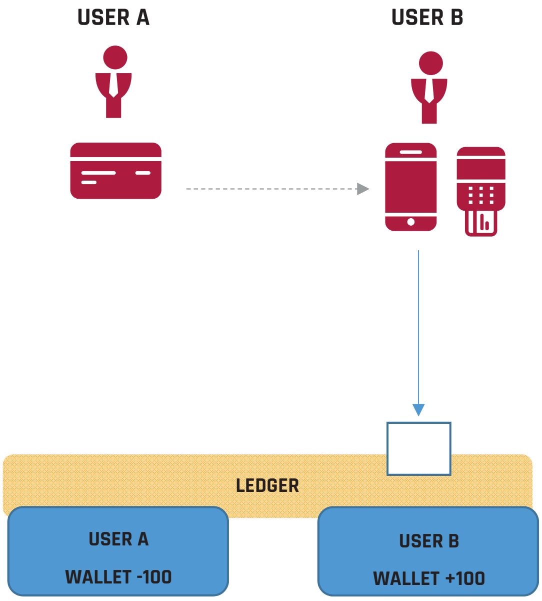
SEND MONEY



The transaction starts with User A obtaining User B's public key.
In case of User A owning a key-based wallet, the transaction is completed. In case of an identity-based wallet, User A sends a payment instruction to their Financial Intermediary operating as Custodian that completes the transaction on behalf of the User.

The same process applies if either User B is a natural person accepting the payment with a smartphone (or another device) or it is an unattended appliance.
In case of a card payment, User B's terminal processes the transaction.

In a card-based payment the acceptance terminal (dedicated device or dedicated software solution on a smartphone or tablet, either attended or unattended) interacts with the card to create and sign the transaction that is subsequently broadcasted to the network.
In the CBDC transfer process, the Financial Intermediary performs a service somehow comparable to what is described in Art. 3 point j) of PSD2, related to operations not subject to the Directive itself:
"Services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services, with the exclusion of payment initiation services and account information services."



8. Challenges and impacts

Notwithstanding several issues to be overcome before the implementation of a CBDC payment system, the potential is overwhelming.

We can envision some obstacles on the CBDC path.

The first one is cultural. It is important for citizens to be fully aware about what a CBDC is, why it is different from bank accounts and from cryptoassets, with related advantages and risks. What is at stake is trust, so an education effort on this topic is required. This must be carefully considered, because as any digital innovation it is reasonable to expect that the first users will be the younger generations, less used to the precautions required to manage digital finance instruments.

Another is what could be called a "go to market" strategy for CBDC. The involvement of the public sector in this area is fundamental in order to boost the adoption of CBDC, for example favouring the use of CBDC to pay tributes and taxes.

8.1 Impacts

Evaluating the social and economic impact of a CBDC is out of scope of this paper.

In particular, the effects on the integrity of the whole financial system is one of the core topic at the attention of Central Banks and relevant authorities.

Nevertheless, some considerations can be done.

The availability of risk-free, easily available digital payment instruments will boost the digitalization of the whole society with the establishment of new ecosystems based on novel business models. From this point of view, it is a challenging exercise to try to imagine all the possible applications.

As in every aspect of the digital transformation, the creative energies of the market will be unleashed, leading to unexpected results. At the dawn of the internet era, noone figured out social media, app stores or the concept of CBDC itself. Once the proper conditions are set, the innovation process will take care of itself.

9. Conclusions

The analysis provides the foundations for a target scenario that shall be validated through in-depth analysis and pilot projects.

The outcome of our analysis provides a scenario for a CBDC payment system based on a DLT solution with a strong involvement of Financial Intermediaries aimed at ensuring interoperability with existing payment systems and facing compliance issues and consumer protection.
It is neither proposed as the unique possible solution, nor as the perfect one.

Furthermore, not all the implications on both technical and operational point of view have been analysed in full details, and there are many other topics that should be carefully evaluated.

The next step is to test this vision in a series of pilot projects for which a feasibility study and a prototype are under development.

Bibliography

- ABI (Italian Bank Association), July 2020 – Media release: 10 considerations for a central bank digital currency
- Association of German Banks, October 2019 – Position paper
- Bank for International Settlements, April 2012 - Principles for financial market infrastructures
- Bank for International Settlements, February 2017 – Distributed ledger technology in payment, clearing and settlement
- Bank for International Settlements, March 2018 – Central Bank Digital Currencies
- Bank for International Settlements Working papers n. 107, January 2020 - Impending arrival, a sequel to the survey on central bank digital currency
- Bank for International Settlements Quarterly Review, March 2020 - The technology of retail central bank digital currency
- Bank for International Settlements Working papers n. 800, August 2020 - Rise of the central bank digital currencies: drivers, approaches and technologies
- Bank for International Settlements, October 2020 - Central bank digital currencies: foundational principles and core features
- Bank of England, March 2020 - Central Bank Digital Currency. Opportunities, challenges and design
- Bocconi University, June 2018 -21st century cash: Central banking, technological innovation and digital currencies. Keynote address by the Deputy Governor of the Bank of Italy Fabio Panetta
- European Central Bank, August 2019 - In search for stability in crypto-assets: are stablecoins the solution?
- European Central Bank, December 2019 - Innovation and its impact on the European retail payment landscape
- European Central Bank, January 2020 - Tiered CBDC and the financial system
- European Central Bank, October 2020 - Report on a digital euro
- European Commission, September 2020 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU
- European Commission, September 2020 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payment Strategy for the EU
- Financial Stability Board, October 2020 - Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements
- Frankfurt School of Finance and Management, July 2020 - The Digital Programmable Euro, Libra and Implications for European Banks
- G7 Working Group on Stablecoins, October 2019 - Investigating the impact of global stablecoins
- International Monetary Fund, November 2018 - Designing Central Bank Digital Currencies
- International Monetary Fund, June 2020 - Distributed Ledger Technology Experiments in Payments and Settlements
- International Monetary Fund, October 2020 – Digital money across borders: macrofinancial implications.
- Lietuvos Bankas, December 2019 - CBDC in a whirlpool of discussion
- OMFIF, February 2020 – Digital Currencies, a question of trust
- Satoshi Nakamoto, 2008 - Bitcoin: A Peer-to-Peer Electronic Cash System
- World Economic Forum, January 2020 - Central Bank Digital Currency Policy Maker Toolkit

SIA - a subsidiary of CDP Equity - is European leader in the design, creation and management of technology infrastructures and services for Financial Institutions, Central Banks, Corporates and the Public Sector, in the areas of Card & Merchant Solutions, Digital Payment Solutions and Capital Market & Network Solutions. SIA Group provides its services in 50 countries, and also operates through its subsidiaries and branches in Austria, Belgium, Croatia, Czech Republic, Germany, Greece, Hungary, the Netherlands, Romania, Serbia, Slovakia, and South Africa. The company also has representation offices in the UK and Poland.

SIA Group operates in three distinct business sectors:

Card & Merchant Solutions, comprising services of issuing and acceptance of card payments based on domestic (PagoBANCOMAT) and international (Visa, MasterCard, etc.) schemes. It also includes new digital systems (Apple Pay, Samsung Pay, Alipay, WeChat Pay, etc.) plus a wide range of services dedicated to physical payments and e-commerce, such as processing of value-added transactions and services.

Digital Payment Solutions, comprising the activities related to account-to-account payments, from solutions for acceptance and processing of retail and corporate payments (SEPA, Instant Payments, domestic payments) to clearing and settlement systems for central institutions (RTGS, Automated Clearing House, etc.). It also includes digital bank services, corporate remote banking platforms, PSD2, Open Banking and collection instruments for Public Administration.

Capital Market & Network Solutions, comprising network and access services for the Eurosystem's payments, securities and collateral infrastructures systems (ESMIG), innovative solutions based on blockchain technology, and services and solutions dedicated to capital markets.

Contacts:
mario.delorenzo@sia.eu
luigi.paris@sia.eu
francesco.lanza@sia.eu

With the contribution of:
Vittorio Baroni
Christian Governatori
Daniele Ianni
Mattia Ozzello
Alessandro Roveda
Giancarlo Sfolcini

Follow us

SIA S.p.A.
Via Francesco Gonin 36
20147 Milan

+39 02.6084.1
info@sia.eu
www.sia.eu