Iberpay

Always one step ahead

SMART MONEY Initiative

Preparations for the possible
launch of a digital euro
or bank digital money
by the Spanish financial sector

Index

Executive summary

The Spanish banking sector has been working hand-in-hand with the support of Banco de España in the ongoing development of innovative initiatives to improve payment services for the sector and, ultimately, for citizens.

In a context of constant evolution where the digitization of services and the emergence of new players in payments have played a key role, collaborative work in the banking sector is essential to achieve cutting-edge technological solutions in order to meet the needs of individuals and businesses.

The following document presents the main conclusions and achievements made in digital payments, specifically within the framework of the Smart Money initiative. Led by Iberpay, this initiative has focused on experimenting with the technical aspects and design options of the digital euro, its distribution to financial institutions and practical use, under a possible public-private partnership model with the Eurosystem, through regulated and supervised market infrastructures, as is the case of Iberpay.

With this purpose, a sectoral proof of concept has been carried out, including a legal and functional analysis, as well as technical developments. The PoC has involved the analysis of the legal and technical feasibility of a double layer system through which digital money is distributed to institutions on a first level, providing its further distribution to their customers on a second level, by means of the Red-i infrastructure (interbank Blockchain network) provided by Iberpay.

Within this dual-layer system, two models of digital money representation have been tested: a token-based model and an account-based model. Both have also been tested to coexist on the same network, as well as the advantages and disadvantages associated to each case.

Among the most relevant functionalities implemented were the feasibility of making offline payments (only in a token-based model), setting limits to the amount of digital money held by an individual, and the establishment of a remuneration system to discourage the use of digital money as store of value without undermining its use as a means of payment. In addition, issues have also been addressed within the framework of the project, such as compliance with personal data protection regulations, measures aimed at preventing money laundering and other security concerns.

As a result of the above, this document is a contribution from the Spanish banking sector to the current debate on the digital euro. Through experience and the implementation of a practical project, it aims to clarify some aspects still to be defined and contribute with the most relevant conclusions reached after testing, identifying the main areas for improvement or pending further study.

Objectives and scope

The development of so-called cryptocurrencies, along with the interest of large technology companies in the field of payments and digital currencies, as in the case of Facebook with Libra, now Diem, have increased the focus of the financial sector globally on issuing retail digital money, strengthening, even more, the role of technology in finance.

The concept of digital money is not new since central banks already provide digital money to commercial banks in the form of central bank reserves. Nevertheless, the use of the term "digital money" for the purposes of this report refers to the form of money issued by central banks in digital form, available to end users and thus different from central bank reserves.

Research in digital money projects has experienced exponential growth in recent years. Cases such as Sweden, Canada or China have increased the interest of both the authorities and the financial sector in delving deeper into the benefits and challenges of digital money. Indeed, according to recent data from the Bank for International Settlements (BIS) in Basel[1], 86% of central banks are currently researching, testing or developing CBDCs, i.e. digital currencies issued by central banks. Digital money has also attracted the interest of commercial banks, which have analysed the potential that the eventual issuance of digital currencies could have on their business models. Unlike CBDCs, this money would be considered private money and would not be backed directly by central banks, although it could have some of their functionalities such as programmability or decentralisation when using advanced technologies such as DLT.

In Spain, 17 of the main banks representing around 98% of the Spanish market share have promoted the sectoral initiative called Smart Money, coordinated by Iberpay. The main goal of this project is to try and test different options of digital money as well as to evaluate the potential and suitability of its different technological alternatives, in case of a possible decision by the European Central Bank (ECB) to issue a digital euro.

The purpose of this report is to describe the main conclusions related to the developments within the Smart Money initiative, including identification and analysis of the options studied in the project from a strategic, legal and technological perspective. In Section 1, this paper examines the background and current situation of CBDCs worldwide, and in Section 2 it focuses on the European context of this phenomenon and its future prospects. The paper then focuses on the Spanish proof of concept called Smart Money, whose objective, scope, design and main conclusions are presented in Section 3. This section also includes a possible sectoral alternative different from the issuance of digital money by the ECB: the issuance of sectoral digital bank money or a synthetic CBDC by a neutral infrastructure.

Finally, Section 4 provides the Spanish banking sector's assessment of the potential impact which the issuance of a digital euro by the ECB could have on the financial sector.

[1] BIS Working Papers no. 114 "Ready, steady, go? – Results of the third BIS survey on central bank digital currency". January 2021 https://www.bis.org/publ/bppdf/bispap114.pdf

1

International context of digital money

1.1. Background to digital money

The technological and computational development commenced in the 1970's brought advances as important as the Internet and the birth of the digital age. Against this background, the idea soon came about to digitise money and create new payment solutions to facilitate commercial relations and transactions. Some of the most important milestones in this regard are the following:

1983: David Chaum published the technical document on eCash, an anonymous electronic currency based on asymmetric encryption. Later on, in the 1990's, he was to found the company DigiCash which would use the eCash idea as a micropayment system in a US bank. This system allowed users to pay for goods and services using eCash at web portals in a simple manner online. Users could spend their digital currencies at any online store that accepted eCash without having to create an account with the seller or send their credit card number. This revolutionary step on the digital payment market is regarded as the start of the cryptocurrency life cycle.

1998: Nick Szabo designed a decentralised digital money system which he called Bit Gold. Bit Gold was regarded as a direct forerunner of Bitcoin and its architecture. It used similar cryptographic functions to guarantee security. Bit Gold was never implemented but its idea influenced other initiatives such as B-Money, as well as all the Blockchain-based technologies.

1998: B-Money was a proposal by Wei Dei to create a distributed, anonymous digital money system. Wei proposed two protocols: the first, a message distribution channel to transfer value and the second based on the application of Proof of Work for the issuing of digital currencies.

2004: Hal Finney was part of a crypto-activist network which called itself "cypherpunks" and which advocated the widespread use of encryption. Finney was one of the developers and cypherpunks with the most influence in the early days of the development of Bitcoin. In 2004 he published the work "Reusable Proof of Work", some tokens issued through the use of proof of work. These generated tokens could be used to carry out transactions between users of the network.

2008: the previous works created the bases for the white paper published in 2008 "Bitcoin: A Peer-to-Peer Electronic Cash System". This document put forward a decentralised digital currencies issuance system using a series of technologies and the possibility of carrying out transactions using a digital signature on a point-to-point network. This marked the start of cryptocurrencies as we know them today.

In this white paper the pseudonym "Satoshi Nakamoto" not only created the first successful cryptocurrency, but he established the bases for a whole technological revolution called Blockchain in the same document. The launch of Bitcoin, which Nakamoto created as an alternative to traditional means of payment, coincided with an international financial crisis and the doubts that emerged concerning the financial sector, facilitating the popularisation of this cryptocurrency. This, combined with the application of its theoretical characteristics to other projects like Ethereum, has entailed a major impact on the financial sector, both public and private. Even though Bitcoin is regarded as the mother of all cryptocurrencies, over time, and particularly as from 2017, new implementations began to emerge aimed at safeguarding privacy. Dash, Monero or Zerocoin are just a few examples.

1.2. The development of private stablecoins

The popularity of cryptocurrencies and the lack of legal and economic guarantees about the feasibility of projects have brought about great volatility and instability in their purchase prices. High volatility has harmed their usefulness as a means of payment, store of value or unit of account and has meant that their acceptance as a means of payment is still limited. Furthermore, the authorities have been warning[2] about the risks of cryptocurrencies for consumers, highlighting that they are not regarded as a means of payment, are not backed by central banks or public authorities, nor are they covered by customer protection mechanisms such as the Deposit Guarantee Fund.

[2] Banco de España (2021): "Joint press statement by the CNMV and Banco de España on cryptocurrency investment risks". Press release. https://www.cnmv.es/portal/ verDoc.axd?t=%7B52286f9f-c592-4418-9559-b75bf97115d2%7D

In response to the high volatility of cryptocurrencies, the so-called "stablecoins" have emerged, cryptoassets which seek to maintain their value stable compared with another specific asset (e.g. a fiat type currency) or a set or basket of assets, or using algorithms (algorithm-based stablecoins)[3]. In summary, there are two ways in which their price stability can be achieved: the first consists of the computerised control of the supply and volume of currency units on the market; and the second pertains to the creation of a reserve of assets backing the issuance of new units. Some examples of this type of currency are DAI or Tether, referenced to the value of the dollar.

International bodies such as BIS[4] or FSB have already warned about the possible risks of operating using this type of instruments, specifically indicating:

- The difficult integration of these cryptocurrencies into the control measures against money laundering and the financing of terrorism.
- Risks in the creation of private payment systems which are not regulated nor supervised in terms of their security, efficiency and the integrity of the operations.
- Absence of data protection control and protocol.
- Development of a parallel financial market which harms and competes under unequal conditions with the traditional companies of the sector.
- Inherent risk for financial stability and the transmission of monetary policy, particularly in countries or regions with weaker financial authorities.

International authorities have highlighted that although these cryptoassets do not represent today any material risk to the world financial stability, depending on how its usage evolves, they may entail a risk and have implications for financial stability in the future, amongst other reasons if their use for payments becomes widespread. In this regard, the emphasis has been placed on the so-called "global stablecoins", those private initiatives that have the potential for attaining a substantial adoption in multiple jurisdictions.

As the FSB[5] mentions, stablecoins have the potential to lend efficiency to payments and promote financial inclusion. However, in view of the systemic nature that global stablecoins may attain as a means of payment, it highlights the need to promote the coordinated, effective regulation, supervision and surveillance of these initiatives to face up to the risks of financial stability that they raise and at the same time support responsible innovation in this regard. With this in mind, the FSB has issued 10 recommendations for the regulation, supervision and surveillance of global stablecoins, proportional to their risks and according to the principle of the same activity, the same risk and the same rules.

As far as Europe is concerned, in late 2020 the European Commission launched what is known as the "Digital Finance Package"[6] which includes a proposal aimed at regulating the cryptoassets' markets (MiCA). This proposal sets out to harmonise the legal framework for cryptoassets (among others, stablecoins), defining concepts and establishing requirements for the issuers of these instruments, as well as for the various players involved in these markets in Europe.

In turn, the US federal regulator also recently issued a communication in which it authorises federal banking entities and savings' associations to use stablecoins and to deploy nodes on public Blockchain networks to carry out payments[7]. It is too soon to predict the impact of this type of measures, but everything would suggest a successive integration or conciliation of the official financial system and the innovations developed in the Fintech sector.

Finally, special mention should be made of Libra -currently, Diem-, a project launched in mid-2019 and led by Facebook in which, in their early days, highly relevant companies from the payments services sector took part together through an association.

[3] Financial Stability Board (2020): "Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements". FSB, Final Report and High-Level Recommendations. https://www.fsb.org/wp-content/uploads/P131020-3.pdf

[4] G7 Working Group on Stablecoins (2019): "Investigating the impact of global stablecoins", BIS. https://www.bis.org/cpmi/publ/d187.pdf

[5] Op. Cit (3)

[6] Directorate-General for Financial Stability, Financial Services and Capital Markets Union (2020): "Digital finance package". European Commission. https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

[7] Hubbard, B. (2021): "Federally Chartered Banks and Thrifts May Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities". OCC. https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2.html

In theory, Libra was designed as a currency issued by this company association backed by a basket of several currencies. The distribution of the currency would be carried out through the intermediation of so-called resellers, responsible for directly interacting with the reserve. From a technical perspective, it uses instruments such us smart contracts for their management and a Blockchain network like the one developed by Ethereum 2.0[8].

However, the publication of the Libra white paper brought along with it major reactions in the financial sector, particularly by the supervisory authorities. Many bodies warned about the potential systemic risk of the project and about the concentration of information in the hands of the operators of this currency. The subsequent abandonment of some of the initial participants like Visa, MasterCard or PayPal[9] has lowered the project's expectations, however, this has not stopped it from commencing the licensing acquisition process in Switzerland[10].

At the very outset of this process, Libra's conception changed considerably, and it is now intended to be issued as a stablecoin referenced to the dollar called Diem. If the experience proves positive, the association could also launch other currencies which, instead of being fixed to the dollar, would be referenced to the euro or other currencies, depending on the markets on which the company wishes to launch its payment services through its platforms.

On the other hand, some social media platforms or communications' systems, such as WeChat, already value integration with this type of currency in order to offer their clients a payment method which, if it occurs, would undoubtedly speed up the adoption of these instruments.

1.3. Central bank digital currencies and the role of central banks

The digitalisation of the economy and the rise of digital currencies, such as the one driven forward by Facebook, has led financial authorities and central banks all over the world to start analysing the possibility of issuing digital currency.

Central banks are studying whether CBDC can help them achieve their aim to safeguard the public's trust in cash, maintaining price stability and ensuring security and resilience of payment infrastructures and systems.

Before delving further into the concept and definition of CBDC, some of the most important grounds that have driven forward the studying of this instrument have been set out below[11]:

- **Protecting monetary sovereignty.** The authorities highlight that a significant adoption of non-denominated cash in a sovereign currency could limit the impact of monetary policy or the ability to support financial stability, impacting financial intermediation and cross-border mobility of capital. The provision of electronic payments by foreign central banks or suppliers of private services outside the Eurozone would entail the mass adoption of private or foreign initiatives without proper supervision and control by European financial authorities, which would entail new challenges, for instance, the replacement of international capital flows, control of inflation, prevention of money laundering and financing of terrorism or tax evasion.

- **Promoting digitalisation and innovation.** Some of the most innovative designs of CBDCs could even allow the automation of commercial or contractual relations, (through the programmability of money) and the incorporation of payments in business processes. In other words, the progressive digitalisation of the economy through this type of means would allow an increase in the efficiency of processes, reducing errors and promoting commercial relations by cutting costs.

- **Ensuring the risk-free access of the general public to central bank money.** In many countries a progressive fall in the use of cash has been observed, with an increase of almost 8%[12] in the use of replacement means of payment in the Eurozone. However, it should

[8] Brennan, C. (2020): "Libra: Understanding Facebook's Digital Currency", Consensys. https://pages.consensys.net/understanding-libra

[9] Álvarez, R. (2019): "Visa, MasterCard, eBay, Stripe and Mercado Pago announce their departure from the Libra Association: the Facebook cryptocurrency loses supporters. Xataka. https:// www.xataka.com/empresas-y-economia/visa-mastercard-ebay-stripe-mercado-pago-anuncian-su-salida-libra-association-criptomoneda-facebook-pierde-adeptos

[10] Lux, T and Mathys, V (2020): "Libra Association: FINMA licensing process initiated", FINMA. Press release. https://www.finma.ch/en/news/2020/04/20200416- mm-libra

[11] Bank for International Settlements (2020): "Central bank digital currencies: foundational principles and core features". Report no. 1. Series of collaborations of central banks. https://www.bis.org/publ/othp33.pdf

[12] European Commission (2020): "Communication from the Commission to the European Parliament, to the Council, to the European Economic and Social Committee and the Committee of the Regions". https:// eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=C0M:2020:0592:FIN:ES:PDF

be stressed that cash is still the most common means used in 78% of transactions[13]. The already widespread use of payment cards has given way to innovative means of payment using electronic devices such as smart phones and smart watches. The security of these new forms, their convenience and expansion in all kinds of businesses and establishments has allowed them to gain a foothold over payment by notes and coins. In addition, in recent months, the use of cash has diminished increasingly as a result of the pandemic caused by COVID-19: the limitation of movements and the fear of transmission of the virus through physical means has promoted the use of other instruments of payment such as instant credit transfers, particularly those related with mobile payment solutions like Swish in Sweden, Paym in the UK or Bizum in Spain[14].

Central banks thus think it is appropriate to cover the user's needs by introducing forms of money and payment solutions which adapt to the lifestyles and habits of the citizen[15].

- **Financial inclusion.** Some authorities see the development of CBDCs as an instrument to facilitate the inclusion in the financial system of a part of the general public which, for various reasons, does not have access to banks (or which receives financial services under insufficient conditions). In view of the reality in which part of the world[16] population does not have access to this type of financial services, this instrument would allow digital means of payment to be accessed and other services to be opted for such as credit, particularly in developing countries.

- **Improvement in cross-border payments.** The issue of CBDCs in different countries could involve a potential improvement in cross-border payments. Bodies such as the BIS are committed to improving the speed, transparency and accessibility, as well as cutting costs, with regard to international payments[17]. The possibility of making the various CBDCs from different monetary areas interoperable, being based on international standards (similar to ISO 20022 for payments), could be one of the ways to help achieve this aim.

1.3.1. An approach to the CBDC concept

Despite the fact the CBDC is becoming increasingly better known, this acronym still requires a clear definition of its nature and legal and financial implications. Some of the approaches made by the most relevant financial institutions are:

- **Committee on Payments and Market Infrastructure (CPMI):** "CBDC is not a well-defined term. It is used to refer to various concepts. However, it is envisioned as a new form of central bank money. That is, a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and as a store of value"[18].

- **International Monetary Fund:** "A new form of money, issued digitally by the central bank and intended to serve as legal tender"[19].

- **Banco de España (Bank of Spain or Spanish Central bank, henceforth BdE):** "There are two essential aspects that define a CBDC: its digital nature (...) and the possibility that the range of agents who have access to the central bank liabilities is broader. CBDC would constitute a third form of central bank money, alongside cash (physical, not digital) and reserves (digital, but with access only for credit institutions)"[20].

- **Eurosystem:** "A central bank liability offered in digital form for use by citizens and businesses for their retail payments. It would complement the current offering of cash and wholesale central bank deposits"[21].

[13] Esselink, H and Hernández, L (2017): "The use of cash by households in the euro area". ECB, Occasional Paper Series. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op201.en.pdf.
[14] Bank for International Settlements (2020): "BIS encourages central banks to continue adapting to the challenge of digital payments". Press release. https://www.bis.org/ pressZp200624_es.pdf
[15] Op. cit (1)
[16] Bank for International Settlements - World Bank - Committee on Payments and Market Infrastructure (2020): "Payment aspects of financial inclusion in the fintech era". https:// www.bis.org/cpmi/publ/d191.pdf
[17] Bank for International Settlements - Committee on Payments and Market Infrastructure (2020): "Enhancing cross-border payments: building blocks of a global roadmap". Stage 2 report to the G20. https://www.bis.org/cpmi/publ/d193.pdf
[18] Op. cit (1)
[19] Bossu, W; Itatani, M; Margulis, C; Rossi, A; Weenink, H Y Yoshinaga, A (2020): "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations", International Monetary Fund. https://www.imf.org/en/Publications/WP/ Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827
[20] Ayuso, J and Conesa, C (2020): "An introduction to the current debate on the central bank digital currency (CBDC)", Banco de España. https://repositorio.bde.es/ handle/123456789/10443
[21] ECB (2020): "Report on a digital euro". https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

As the acronym of the concept suggests, a CBDC is a digital currency issued by the central bank. This means, first and foremost, that it will be fully backed and, where applicable, it could even have legal considerations similar to the other forms of money, such as cash (notes and coins) and reserves, solely issued digitally for certain special parties.

Secondly, the digital nature is rife with a multitude of technical issues which will be analised later on regarding the infrastructure, centralised or decentralised, the form of representation, such as tokens or special accounts, access to this means by economic agents, or their possible uses as a means of payment, unit of account or store of value.

1.3.2. CBDC design options

In various reports published by official bodies[22] in the financial sector there are multitude of forms and methods for constructing a CBDC. This diversity of options may be summarised by the points below:

- **Wholesale or retail distribution:** One of the first issues to be tackled is the definition of who the recipients and users of the CBDC are. The wholesale model would be associated with the current reserves issuance system by central banks and hence geared towards a specific group of operators. The retail form would be more similar to the distribution of cash and thus aimed at the general public. The connotations of choosing one model or another have a major impact on design and architecture issues.

  In this regard, it is worth knowing that the vast majority of central banks have shown an interest in issuing a retail type CBDC (retail banking), as shown in the graphic beside.

- **As regards the architecture,** we need to define the role that the central bank would adopt and that of the remaining operators such as commercial banks, setting out the following models:

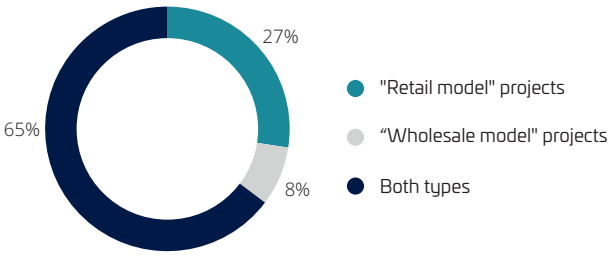
  - Direct: system operated by the central bank, in charge of keeping the registration of transactions and managing payments in the network autonomously.

  - Hybrid: retail-type payments are carried out by intermediaries, though the central bank keeps a register of the transactions, allowing intervention in the system if the accounting or security of the intermediaries fails.

  - Intermediated: this is different from the previous model insofar as the central bank only keeps a record of any wholesale transactions in the system.

- Due consideration must be given to the **digital infrastructure used**. In this regard, a discussion arises about the possibility of using decentralised networks (DLT) or whether, on the contrary, it is better to trust traditional systems with a more technical background.

CBDC studies and projects



Source: BIS database. April 2021[23]

[22] OMFIF, IBM (2019): "Retail CBDCs the next payments frontier". European Central Bank: "What are retail payments?". https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf

[23] Auer, R; Cornelli, G and Frost, J (2020): "Rise of the central bank digital currencies: drivers, approaches and technologies". BIS Monetary and Economic Department, no. 880. https://www.bis.org/publ/work880.htm

In general, the majority of experts seem to be inclined towards a dual issuance which takes advantage of the soundest benefits of DLT systems, without neglecting other traditional forms of storage and processing of transactions for greater security.

- As regards the **form of access**, two main alternatives have been defined. On the one hand, a bearer instrument which, in the majority of cases, is identified by a token; and, on the other hand, by an account entry, similar to deposits in commercial banks.

- **Possible cross-border use of the CBDC.** Another element in the discussion is the preparation of this instrument to be used by different users in different monetary regions. In this regard, the most frequent proposal is the limitation to amounts that cover certain use cases, such as tourism travel or, on the contrary, configuration for cross-border development, in other words, to allow foreign currency exchange.

Despite the above summary, there are still issues and questions surrounding CBDC design. These include:

- The inclusion of a possible **financial remuneration**, positive or negative, with a view to incentivising or disincentivising the use of the CBDC. This remuneration could be defined in tiers to disincentivise the use of the CBDC as a store of value without reducing its use as a means of payment. In addition, the application of a financial interest in this context could be used for a monetary policy purpose.

- The **limitations** to the balance or amount that each user may have. In this regard, various solutions are proposed: from setting thresholds in line with the type of party involved, to determining limits not only to the amount of digital currency available but also to the number of transactions.

- A possible **programmability** of the CBDC through the use of smart contracts, allowing the automation of transactions when the programmed conditions are met. An example could be an automatic division of payments to make tax collection more efficient, for instance, in the case of the payment of fuels, direct consumer payments or the payment of taxes in foreign countries.

- In the same way, **privacy** is key when managing accounts and carrying out transactions[24]. In line with the design chosen, different degrees of privacy can be defined for the transactions carried out, ensuring, in any case, compliance with obligations pertaining to the prevention of money laundering and the financing of terrorism and data protection regulations with regard to intermediaries.

1.3.3. Legal considerations

CBDC also constitutes a significant challenge for a wide range of legal issues. Some of them, such as tax law, private contract law, payment systems and means of payment, insolvency, international law, data protection and regulations regarding the prevention of money laundering and the financing of terrorism, require a specific study on the impact that a CBDC would have on each of these areas.

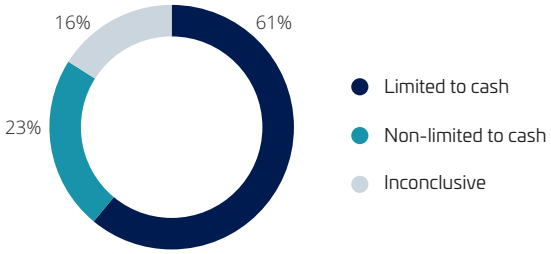
[24] World Economic Forum (2020): "Central Bank Digital Currency Policy Maker Tool-kit". http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf

Some of the legal considerations most discussed about the legislation of central banks and personal data protection have been summarised below.

As regards the capacity to issue CBDCs by the central bank[25], each jurisdiction needs to review the powers assigned to this body. The IMF itself determines that 61% of a total of 171 central banks would be limited to issuing money in the form of notes and coins, meaning that only 23% would allow potential digital issues.

Specifically, and in line with the form of digital currency chosen for issue, whether account-based, token-based (see section 3.3.) or both, the legislation about how to adapt these instruments in the system would need to be revised. For example, the case of account-based in a direct model could require the modification of access by private individuals and companies to allow the opening of accounts at the central bank. As regards token-based, there would need to be a specific definition of the nature of this means and its management in the system. From a legal perspective, the CBDC would be deemed to have been integrated in the existing monetary system, however, there are issues yet to be analysed such as the expansion of the definition with regard to what the official means of payment used in a country or region are. For example, in a European context, it is worth referring to article 11 of EC Regulation 974/98 which sets out the need to issue currency (an issue which could require modifications in view of the arrival of a digital euro) pursuant to the technical specifications issued by the EU Council. On the other hand, if a token-based model is used, it would be necessary to adapt the legal system to the new payment system in which concepts like "wallet"[26] or "address"[27] used in this type of transactions would be defined.

Central banks' capability of issuing new types of currency



Source: BIS working paper, November 2020

Finally, as regards personal data protection[28], the analysis of the impact entailed by this initiative on users' rights to privacy shall largely depend on the final characteristics and design that this instrument has, paying particular attention to retail distribution models. In general terms, it is worth highlighting the dichotomy that exists between the development of an instrument with a certain degree of privacy for the user and, on the other hand, the need for the competent authorities to control and supervise the operation[29].

There are thus many question marks over this issue such as, for example, which personal data would be associated with a potential CBDC, what the storage time and system will be like and who would be assigned the roles of data processor and controller (where applicable) set out in the legislation, among others. Furthermore, in the event that the design includes the possibility of cross-border use, it would be necessary to harmonise or envisage the control of this aspect in foreign jurisdictions.

[25] Op. Cit (19)

[26] Digital wallet which stores the public and private keys that allow transactions to be carried out on Blockchain.

[27] Alphanumeric string which constitutes the identification of a wallet (wallet ID) and which, accordingly, allows digital currency transfers to be carried out to a specific person.

[28] We are referring to data protection in European jurisdiction: (EU) Regulation 2016/679 issued by the European Parliament and Council on 27 April 2016.

[29] Darbha, S and Arora, R (2020): "Privacy in CBDC technology", Bank of Canada. https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/

Blockchain technology and, to be precise, cryptographic advances, afford a wide range of possibilities about how to design instruments which comply with the legal data protection requirements and the regulatory obligations of money laundering, the terrorism financing and due diligence regarding knowledge of the customer.

1.3.4. Impact of CBDCs on cross-border payments

Cross-border payments have grown notably in recent years and some aspects, such as international tourism becoming widespread, the sending of remittances by migrant population and the participation in marketplace type platforms on a worldwide scale, have been conducive to a boom in this type of transactions. However, the increase in the volume of these operations contrasts with the conciliation and management methods of these payments. To be precise, current operating systems suffer from major obsolescence which results in slow, inefficient payment processing. Moreover, carrying out of this type of transactions is usually accompanied by excessive fees and entails particular issues in terms of harmonisation, compliance and management of personal data between jurisdictions.

The traditional approaches to resolving these issues have involved the study and creation of standards which allow interoperability between involved actors. On the other hand, the needs of the consumer should be considered in terms of the security and speed required when seeking to equate this type of payments to those carried out in the same system.

CBDCs appear as an instrument capable of making their use compatible in different regions as they have similar design points with each other.

In this regard, the BIS[30] is already exploring the interoperability dimensions of CBDCs and their associated benefits, particularly important for emerging market economies which are not well provided for by the current correspondent banking arrangements. However, history has shown that these benefits are difficult to achieve unless the central banks coordinate internationally and incorporate from the outset cross-border considerations in the development of their CBDCs. In this context, the BIS is already considering three possible interoperability models:

- Compatible CBDC systems (model 1): through compatible standards (message formats, cryptographic techniques, data requirements and user interfaces) which allow a reduction in frictions and barriers.

- Interconnected CBDC systems (model 2): which may be materialised through (i) a shared technical interface or (ii) a common compensation mechanism.

- Integrating multiple CBDCs into a single system based on multi-CBDC arrangements (model 3): this deeper integration allows greater operating efficiency and functionality, but it increases governance and control obstacles.

[30] Auer, R; Haene, P and Holden, H (2021): "Multi-CBDC arrangements and the future of cross border payments", BIS Monetary and Economic Department, no. 115. https:// www.bis.org/publ/bppdf/bispap115.htm

In turn, Eurosystem has warned of the possible financial and social risks that could be entailed by a cross-border use of CBDCs, in particular, in the event of the issuance of a potential digital euro. To be precise, it indicates the predictable increase in international capital flows with this currency and its impact on the exchange rate and ratios adopted by the institutions.

Furthermore, the availability of a digital euro could give rise to the replacement of the currency in third-party countries, particularly in those with weak currencies and fragile economic environments, facilitating their total or partial substitution by the euro and significantly affecting monetary sovereignty policy of the economies concerned.

For this reason, it is necessary for the CBDC design to include the setting of limits for non-residents with a view to controlling the financial stability of the system.

However, the cross-border CBDC design would allow for cost cutting and potential improvements in the efficiency of commercial dealings between different countries. Although there are still major challenges such as common legislative compliance, the management and eradication of criminal activities, as well as the application of conversion and rates of the monetary units, there is still time to design models capable of achieving significant improvements in these areas.

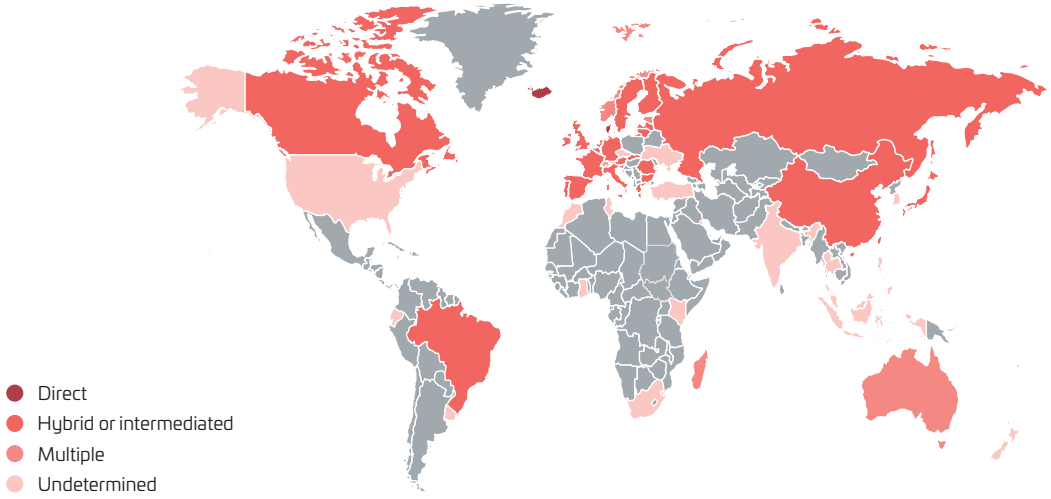
1.4. Project development

The successive pronouncements by official bodies like the Bank for International Settlements in Basel or the International Monetary Fund have been instrumental to the issuing of reports and proofs of concept by the central banks and monetary authorities of various countries around the world. This growing interest in the possibilities of issuing CBDC can largely be put down to the reasons set out in the point above, combined with the fact that the CBDC is regarded as a crucial aspect in the development of innovative techniques of the financial systems of states. Eventually, it is a matter of seeking out alternatives and maintaining the sovereignty and effectiveness of the means used by institutions to consolidate their interests in the international economic area.

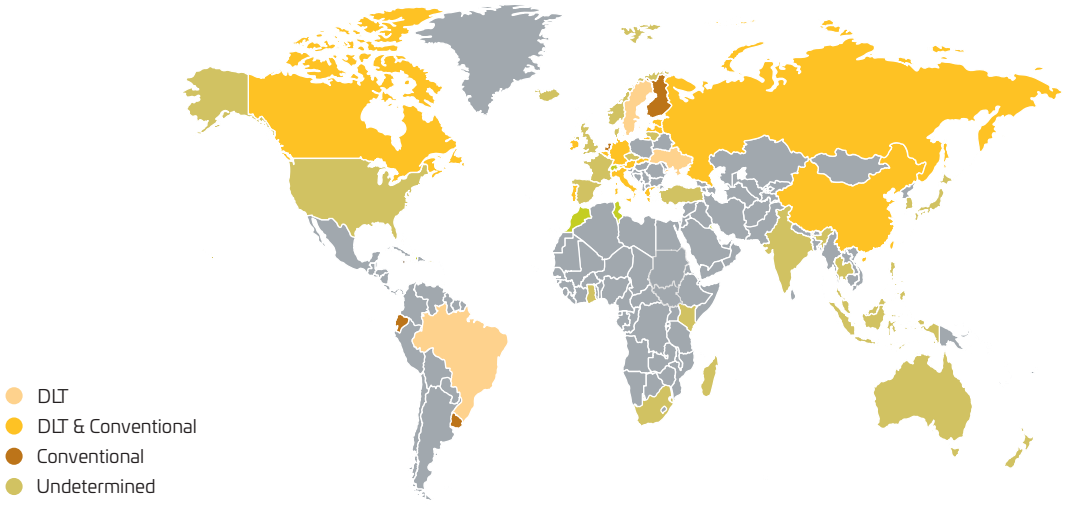
The analysis of this subject encompasses the carrying out of prospective studies on the impact and consequences of the issuance of a CBDC to the development of proofs of concept. During this time, it has been common for central banks to form associations to draw up these studies, such as the one carried out by Hong Kong SAR and Thailand in 2020 in the BoT-HKMA project, or the creation of the working group at BIS formed by six central banks to investigate CBDCs.

The most important variables looked at in the studies and initiatives on CBDCs in different countries have been set out below, in accordance with BIS sources:

Architecture

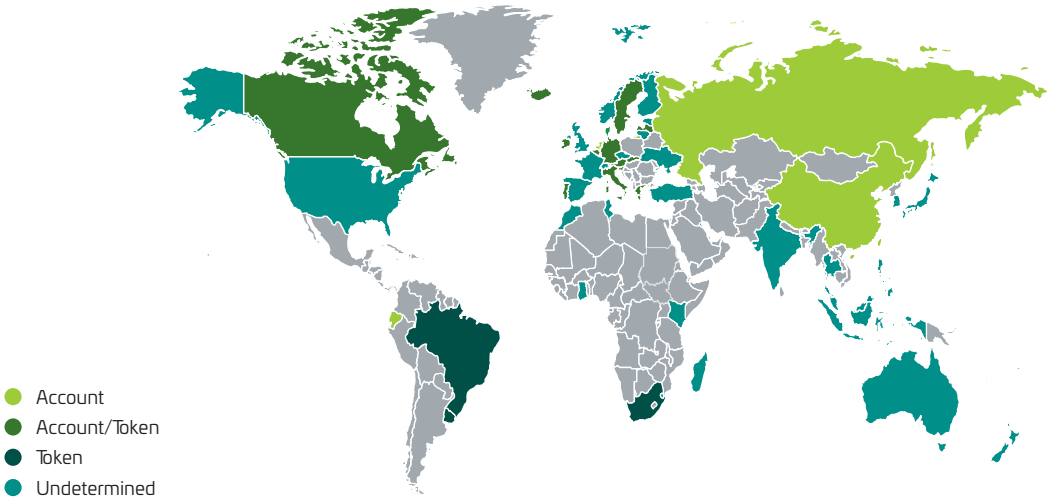


Infrastructure

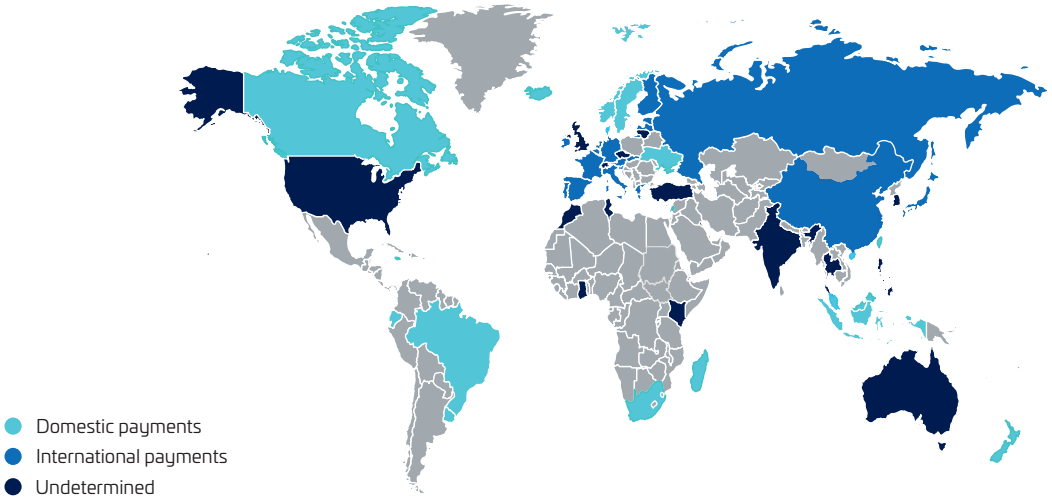


Source: BIS database, April 2021

Access



Cross-border payments



Source: BIS database, April 2021

1.4.1. People's Bank of China: the DC/EP (pilot) project

In recent decades China has achieved a prime level of technological development, with ever higher internal development and consumption, thereby becoming consolidated as the second largest economy on the planet, closing in on the United States. The trials and studies with CBDCs in which the country has been involved have set out to achieve the financial integration of national companies and services like Alipay and WeChat which are used every day by hundreds of millions of people.

The design of the Chinese project is based on a hybrid model in which different intermediaries take part and in which the People's Bank of China maintains a record and control over transactions. This two-tier scheme is particularly pronounced, and it is even considered that the distribution entities are the owners of the digital currency issued and hence the guarantors of the system from a technological perspective[31]. The project seeks to promote different payment solutions around a single concept of e-CNY or digital yuan. In this way, it is intended to expand the development options for these companies and maintain the supervision of the Chinese financial system by the monetary authorities.

As regards the infrastructure system used, it is not clear whether the DLT system has been excluded though, in theory, a model is sought which supports at least 300,000 transactions per second as, for example, Alipay alone currently registers 250,000 transactions per second.

The first tests for this pilot scheme started in April 2020, located in certain cities and users, achieving in autumn of that same year an approximate transactions value of almost 162 million dollars. According to the latest information[32], several state banks and technological companies are said to be building interfaces and distribution systems for the platform. The aim of the Chinese government could be the presentation and start-up of this instrument in 2022 to coincide with the Winter Olympics to be held in Beijing[33].

Further details of the project have not been reliably disclosed yet and official statements in this regard have been few and far between. Some publications assert that as far as data management is concerned, the PBOC will have unlimited access on the network and the receipt of these data could be asynchronous and be issued by the intermediaries at the end of the day or a specific time. Despite this, it seems possible that the users themselves may limit the exposure of their identity to the counterparty of the transaction provided that the amount does not exceed certain limits.

1.4.2. Riksbank: Sweden, the e-krona Project

The oldest central bank in the world has warned that over the last decade the use of cash is becoming increasingly lower and in fact, many businesses have started not to accept this means of payment. This body's proposal is based on a hybrid model which, through decentralised technology, involves intervention by various intermediaries in the management and registration of the digital currency issued. The system used is that offered by Corda R3.

Users can access e-krona through an account-based model, though the issuing of portable instruments such as prepaid cards is also contemplated.

At present, the project is still under study. The issue of adapting this type of currency to the legislation and functions of Riksbank is still being analysed and the optimum technical method for the system which would support the issuance is also being studied. Both concerns require subsequent research which means that the decision must not be rushed into as to whether construct the e-krona or to improve the current Swedish payments

[31] Zhou, X (2020): "Understanding China's Central Bank Digital Currency", China Finance 40 Forum. http://www.cf40.com/en/news_detail/11481.html

[32] Fanusie, Y and Jin, E (2021): "China's Digital Currency. Adding Financial Data to Digital Authoritarianism", CNAS https://www.cnas.org/publications/reports/chinas-digital- currency

[33] Gov.cn (2020): "Central Bank: Digital RMB closed test will not affect RMB issuance and circulation". http://www.gov.cn/xinwen/2020-04/17/content_550371 1.htm

system in other respects. For the time being, the body is observing social and economic changes and prefers to postpone this issuance until all the alternatives have been analysed in-depth.

1.4.3. The digital dollar: public and private approaches

The development of the digital dollar is currently under study, both by public bodies and by private associations and foundations.

From the public perspective, there is still no clear line about the intention to create a digital version of the dollar. Some responsible parties of the US Federal Reserve[34] acknowledge the duty to adapt and study the technical advancements in view of the importance of the dollar, though they warn about the need not to rush into a project of this scale, with far-reaching consequences and implications. Besides, some leaders have expressed their wish to take part and cooperate in international forums for the definition of this instrument[35].

One of the first steps in this regard has been the creation of the Federal Reserve Technology Lab (TechLab) which is responsible for expanding experimentation with technologies related with digital currencies and other innovations in payments' areas. The TechLab undertakes practical research into improving the Federal Reserve's understanding of payment technologies and supporting strategies from a political perspective. It boasts a multidisciplinary team comprising staff from the Federal Reserve Board and Bank endowed with experience in payments, economics, law, information technology and computing.

As regards the experiments and research carried out in this regard, worthy of special mention is that developed by the Federal Reserve Bank of Boston[36]. The research project undertaken along with MIT consists of the creation of an American CBDC of the retail type, which has an estimated time period of two to three years. The first stage will be focused on the creation of a cryptographic scalable architecture which complies with the requirements in terms of speed, security, privacy and resistance, which are expected of an instrument like the digital dollar. At the successive stages, a proof of development and the evaluation of the impact on macroeconomic variables is expected.

In turn, from a private perspective, the Digital Dollar project[37] is worthy of mention, backed by a private foundation "The Digital Dollar Foundation", which sets out to study the possibility of issuing a tokenised dollar, in other words, an American CBDC. The reasons behind the need for this issuance would be, first and foremost, participation in the digital and financial revolution of recent years. Secondly, it would seek to improve, in terms of efficiency, the time and cost parameters for making payments and, thirdly, to maintain the current status of the dollar as a reference and world reserve currency.

The project advocates the digital dollar as a third form of money to complement banking reserves and cash. The form of distribution would be through a two-tier system between the Federal Reserve and commercial banks, thereby avoiding any possible damage to the latter and to allow compatibility with projects of a private nature. Furthermore, it is committed to a tokenised model similar to cryptocurrencies and with a speedier, simpler object-value association. Finally, the project highlights some themes yet to be studied such as the privacy model and compliance with the other regulations for the financial sector.

As has been explained, it is a private analysis initiative which has not been endorsed yet by the US authorities. The Federal Reserve (FED), through its senior manager[38], believes in continuing to analyse the possibility of issuing a CBDC through the working groups of BIS.

[34] Weber, A; Torres, C and Look, C (2021): "Cryptocurrencies: Fed's Powell and Peers Aren't Rushing Into Digital Currencies", Bloomberg. https://www.bloomberg.com/news/articles/2021-03-22/fed-s-powell-and-peers-aren-t-rushing-into-digital-currencies-kmkp6667

[35] Brainard, L (2020): "An update on digital currencies", BIS speeches by central banks. https://www.bis.org/review/r200814a.htm

[36] Reynolds, T (2020): "The Federal Reserve Bank of Boston announces collaboration with MIT to research digital currency", Federal Reserve Bank of Boston. https://www.bostonfed.org/news-and-events/press-releases/2020/the-federal-reserve-bank-of-boston-announces-collaboration-with-mit-to-research-digital-currency.aspx

[37] Digital Dollar Foundation y Accenture (2020): "The Digital Dollar Project. Exploring a US CBDC". https://www.digitaldollarproject.org/

[38] Federal Reserve System (2021): "Federal Reserve Chair Jerome H. Powell outlines the Federal Reserve's response to technological advances driving rapid change in the global payments land-scape". Press release. https://www.federalreserve.gov/

2

The digital euro in Europe

2.1. Context and motivations behind the issuance of a digital euro

Although the majority of innovations with regard to payments have not substantially altered the instruments deployed so far, the development of the loT ("Internet of Things"), the arrival in the sector of major technological companies with important network economies, or the appearance of cryptoassets, is giving rise to major changes in the current context in which the issuance of a digital currency is being studied. The development of new forms of payment initiation such as instant credit transfers, contactless payments, through "wearables", or even without the need for devices, thanks to advanced authentication technologies such as biometrics, are examples of how technology has brought about a rapid evolution in the sector in recent years.

In light of this circumstance, on 24 September 2020 the European Commission adopted a new package of measures[39] on digital finance, including a Retail Payments Strategy.

Under this strategy, the European Commission outlines the issuance of digital currency, leaving the design of payment solutions to the private sector. The aim is to deal with the fragmentation of the single market by creating a digital payment solution which can be used throughout Europe.

The aim is for the digital euro to serve as an engine for continuous innovation in payments, strengthening the international relevance of the euro and the open strategic autonomy of the EU. In addition, the European Commission considers that the issuance of a digital euro could contribute the rendering of resilient, fast and less expensive payment services, as well as allowing automated, conditional payments.

The possibility of issuing a digital euro has emerged from studies, particularly highlighting the one published by the ECB[40], drawn up by Eurosystem. Although it is still too soon to talk about a specific design of the digital euro, the basic principles and requirements have been determined which this CBDC should comply with. They include: accessibility, robustness, security, efficiency and privacy, as well as compliance with the applicable legislation.

In turn, the ECB has already warned that the implementation of the digital euro requires a new infrastructure. With this in mind, it is committed to taking advantage of the current infrastructure of the Eurosystem, incorporating new technologies.

2.2. The Eurosystem report on the digital euro

In this drive by the European authorities to prepare the economy and legislation for the potential issuance of a digital euro, in October 2020 the Eurosystem launched a report[41] in which it analysed the most relevant aspects of this issue. It highlighted in the report that the Eurosystem must be prepared for the launch of a digital euro if this proves necessary, in line with the initiatives of other central banks. Although the document warns that it is of an introductory and explanatory nature, it is particularly useful as it introduces some of the design lines and characteristics that this instrument could have.

In this way, the report identifies scenarios which could justify the issuance of a digital euro and what the possible basic characteristics and desirable principles of its design would be. It highlights the aim of configuring the digital euro as a means of payment accessible throughout the Eurozone, also designed as a complement to cash and current bank money (and not as an investment asset).

One of the main interests of the Eurosystem in light of a possible issuance of the digital euro is to ascertain the potential negative effects that this might have on the financial sector and the economy as a whole. Concern has been expressed in the event of a mass displacement of funds towards the use of this instrument, (particularly in terms of the control of monetary policy, financial stability and the financial intermediation role of the banking sector) and how these would impact the stability and security of

[39] European Commission (2020) "Package of measures on digital finance: the Commission presents a new ambitious approach to promote responsible innovation which benefits consumers and firms". https://ec.europa.eu/commission/presscorner/ detail/es/ip_20_1684

[40] Ferrari, M; Mehl, A and Stracca L (2020): "Central bank digital currency in an open economy", ECB, Working Paper Series. https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2488~fede33ca65.en.pdf?ac12ca088c73513aca6012ea1e3671d2

[41] Op. cit. (31)

the European financial system. The report underlines the importance of carrying out a proper design of the digital euro which avoids these effects.

From a legal perspective, it analyses some of the possible regulatory changes and effects required, based on these amendments to the TFEU (Treaty on the Functioning of the European Union). Furthermore, it considers the effects it could have on technical security and the cyber-risks of operating this type of digital instruments. Finally, the risks are also pointed out regarding the potential use of the digital euro by foreign citizens and companies and the potential mass adoption of this CBDC as a reserve currency abroad.

As regards the forms of design, several alternatives are considered about the access mode, infrastructure and distribution of the digital euro:

- Centralised infrastructure: end users would be the holders of accounts in digital euros with a centralised infrastructure provided by the Eurosystem. In this regard, a warning is made about the technical and organisational challenges that would be entailed by processing a high volume of payments, for which the current infrastructure is not prepared, as well as the need to strive to comply with the regulations on the prevention of money laundering and the financing of terrorism.

  Under this alternative there are two possible options:

  - Direct access: end users would have an account in digital euros at the central bank. The report warns about the difficulty of this model, not only at a technological but also operational level, owing to the extremely high volume of transactions and users to be managed.

  - Hybrid or intermediated access: financial entities would be responsible for handling the accounts with the central bank on behalf of the end users. Financial entities would incorporate digital euro services into their business models.

- Decentralised infrastructure: an infrastructure with a certain amount of decentralisation could be used to provide a digital euro in which the end users, or the supervised intermediaries acting in their name, would verify any payment. This could be achieved through either of the two models, direct model or private/public collaboration model (hybrid/intermediated).

The Eurosystem seems to be committed a priori to a private/public collaboration model in which the ECB would issue digital euros and the supervised intermediaries would collaborate on their distribution, similarly to that which occurs today with cash distribution. It has also been pointed out that the digital euro could be designed with a view to replicating some characteristics of cash, for example, the possibility of making payments offline as well as online.

The Eurosystem is committed to public-private collaboration with the financial sector, backed up by supervised financial intermediaries to manage the distribution of the digital euro and to undertake value-added services for the end users. The design of the digital euro is intended to allow interoperability with private payment solutions, which would facilitate the offer of Pan-European products and additional services for consumers. In this regard, it will be necessary to understand how both types of solutions would co-exist and whether, in practice, the digital euro could actually compete with the multiple options available for making payments.

As regards the issue of privacy, the report acknowledges the permanent dichotomy between the user's rights in terms of data protection and need for control and supervision by the authorities in the context of anti-money laundering regulations; in this regard, it raises the possibility of applying selective privacy which varies in line with the amount or frequency of the transactions. This type of limitation could also be used to control the volume operated by the users, possible remuneration and even the use of the digital euro outside European borders.

Finally, although it refers to the possibility of issuing one or other type of digital euro, the body itself argues and justifies the possibility of carrying out a dual issuance. In other words, an offline-type digital euro, with a greater degree of privacy and a fixed rate of return, interoperable with the private payment circuits and, secondly, an online option with a variable rate of return, without being associated with a specific device or access, without an anonymous nature and also interoperable with the private payment circuits.

2.3. Current status of the initiative

The Eurosystem, in line with the widespread positioning of many central banks, seeks to keep studying those aspects described in the previous points above. It urges private and public institutions to take on the challenges regarding the design and management of a potential digital euro from different perspectives: technical, economic and legal.

In keeping with this purpose, the body started a public consultation on 12 October 2020 to evaluate the needs, benefits and challenges that society and the financial sector are expecting from the issuance of a digital euro. This consultation ended in January with 8,221 replies, a record figure[42], demonstrating the great interest of companies and citizens to help to give shape to this new instrument.

Of the main conclusions drawn, it highlights that privacy, security and the pan-European scope were the characteristics most requested by European citizens regarding a potential digital euro.

In addition to the consultation, the ECB raised the possibility of starting to try out possible models as can be gleaned from the words of Christine Lagarde in this regard: "As the economy continues to evolve and new expectations about the nature of money emerge, the Eurosystem must be ready to respond and ensure that European payments adapt to changing consumer preferences and remain inclusive and efficient[43]".

The start of a potential investigation stage would be set for mid-2021. According to Fabio Panetta "after the public consultation and a period of preparatory work, the ECB's Governing Council will decide – towards the middle of 2021 – whether to initiate a fully-fledged project that should lead us to define the specific characteristics of a digital euro and get ready for a possible launch. This journey will require prudence and perseverance[44]".

If the Eurosystem is committed to starting a project to develop the digital euro, this would be intended to put into practice the technical and methodological concepts that would allow the evaluation of the best option for a possible real issuance when deemed opportune.

2.4. Possibility of issuing commercial bank digital money or a banking stablecoin as an alternative to the digital euro

As has been explained, the issuance of the digital euro by the Eurosystem is still uncertain, as it is still necessary to keep analysing the different technical, economic and legal options, as well as their attendant impacts on the financial system as a whole. Concurrently, public and private bodies are studying alternatives to improve payments systems and services and the digitalisation of the economy.

Recently, Deutsche Bundesbank[45] carried out a study on the possibilities of creating a programmable payment system. The body defines programmable payments as predesigned transfers of money in which the execution time, the payment amount and/or the type of payment are determined by conditions specified beforehand rather than being established *ad hoc* at the time of payment.

To achieve these forms of payment it sets out different alternatives: the modernisation of current payment systems, the creation of connectors between the current systems and the DLT type applications (in line with Iberpay's Smart Payments proof-of-concept),

[42] ECB (2021): "The ECB consultation on the digital euro ends with a record number of replies to the public consultation", Press release. https://www.bde.es/fZwebbde/GAP/Secciones/SalaPrensa/ComunicadosBCE/NotasInformativasBCE/21/presbce2021_11.pdf

[43] Lagarde, C (2020): 'The future of money - innovating while retaining trust". ECB. https://www.ecb.europa.eu/press/inter/date/2020/html/ecb.in201130~ce64cb35a3.en.html

[44] Panetta, F. (2020): "A digital euro for the digital era". ECB. https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201012_1~1d14637163.en.html

[45] Deutsche Bundesbank (2020): "Money in programmable Applications Cross-sector perspectives from the German economy". https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf

cryptocurrencies of a private nature, the "tokenisation" of bank money and CBDC.

Particularly interesting amongst all of them is the alternative of "tokenising" bank money. In summary, this would entail that this type of money could be managed not only through bank accounts and deposits, but also in the form of tokens. This would allow this instrument to incorporate specific preprogrammable functionality with regard to the implementation of payments.

In view of the fact that the exchange of "tokenised" bank money means assuming the counterparty risk of each bank in question, it is proposed to carry out various intraday clearing and settlements in central bank money. In order for these clearances and settlements to be effective, it would be necessary to find a standard that would ensure the acceptance of this money between banks, an acceptance which could derive from the joint issue by the banking sector of tokenised bank money in legal tender. Furthermore, it is proposed to create a legal vehicle operated by the banks, responsible for issuing the tokenised money and hence responsible for dealing with any possible exercising of rights by private individuals. Notwithstanding, the report suggests that the application of the rules on deposit guarantees under this model should be stricter.

Other analysis, such as the one carried out by Iberpay in 2020 in the context of the Smart Payments initiative, have looked at the possibility of the issuance of private digital money by the banking sector, indicating that a neutral entity, for example, Iberpay, could be the issuer of this money. This alternative was looked at based on the assumption that Iberpay could be the holder of an account at the central bank as a solution for issuing a synthetic CBDC or a sectoral sCBDC[46].

With this alternative, Iberpay would need to be specifically empowered to have its own account at the central bank and it would be the entity responsible for issuing tokens (electronic money) as its liabilities. The tokens would be 100% backed by funds in the Iberpay account at the central bank, in other words, they would always be prefunded and they would also be endowed with a maximum solvency level (sCBDC).

The start-up of this alternative may require the modification of the regulation and an ad-hoc authorisation by the supervisory authorities, both so that Iberpay could be allowed to obtain a license to become an E-Money Institution authorised to issue digital money (required to issue sCBDC), as well as for being holder of an account at the central bank.

The entities may be responsible for acting on behalf of Iberpay in the distribution and reimbursement of sCBDC, in other words, they would act as distributors, as through them the client could request an exchange of euros for tokens and vice versa. The entities would also be responsible for applying the due diligence measures which may outsourced in accordance with article 8 of Law 10/2010 up to a certain limit, with the exception of the follow-up of the business relationship. In turn, Iberpay, as electronic money institution, would assume the responsibility for issuing tokens, in other words, it would be the entity responsible for ensuring the precise match between the monetary value received for conversion into electronic money and the value of the latter effectively issued (the entity against which the end user "holds the credit or claim").

If the model is successful, this could entail challenges to the stability of bank financing. The supervisor and the regulator, in any case, could adopt different measures to limit this impact. By way of example, limitations could be applied similar to those to be found in the case of cash to restrict unexpected large movements in deposits outside the entities.

[46] An sCBDC is a digital currency issued by a private entity which holds an account at the central bank and which is thus 100% backed by the money held in the account opened by the entity at the central bank.

This alternative should also consider its adaptation to the proposal for a regulation of the cryptoassets markets (MiCA)[47].

In accordance with the proposal for a regulation, the sCBDC designed in this alternative would fit into the category of "e-money token", which implies, as has already been indicated above, the need to adapt to the regulation pertaining to electronic money institutions. Moreover, it is worth mentioning the category of significant e-money token, a category which the sCBDC designed in the context of this initiative would probably acquire, owing to the dimensions of its client base, the high number of expected transactions or the interconnection capacity with the financial system, among other. Precisely because of the impact that this type of token could have on the financial sector, the proposal demands compliance with additional requirements by the issuing entity.

In this regard, the categorisation of the sCBDC as a significant e-money token would have some major legal implications in the event of the coming into force of the proposal for a MiCA regulation, particularly as regards the guarantee requirements. In this way, the provisions of article 7 of Directive 2009/110 on access to the activity of electronic money institutions would cease to apply, applying articles 33 and 34 of the MiCA regulation which are more thorough in terms of custody and reserve assets. In addition, the issuing entity, in this case Iberpay, would be submitted to higher capital requirements than those applicable to other issuers of e-money tokens, to interoperability requirements and to the need to adopt a liquidity management policy.

As can be observed, both the model designed by the Bundesbank and that analysed by Iberpay in 2020 require major legislative and/or normative amendments. The usefulness, pros and cons of issuing private digital currency by the banking sector must thus be considered with the possible issuance of a CBDC by the ECB.

Although, basically, both models afford a particularly liquid means of payment, there are differences in terms of the degree of diversity and innovation of the currency itself. In the CBDC model, the currency forms part of the digital applications and stimulates new assets. The sCBDC model, by contrast, promotes the innovation run by the private sector at a more fundamental level. Private companies would compete to offer the form of private digital currency which was easiest to use and the most efficient settlement platform[48]. Even so, the central banks must supervise the security, solidity and operating resistance, ensuring financial stability.

[47] European Commission (2020): "Proposal for a regulation of the European Parliament and of the Council on markets in Crypto-assets and amending Directive (EU) 2019/1937". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

[48] Adrian, T. (2020): Speech- "Evolving to Work Better Together: Public-Private Partnerships for Digital Payments", IMF. https://www.imf.org/en/News/Articles/2020/07/22/sp072220-public-private-partnerships-for-digital-payments

3

Smart Money sectoral initiative

3.1. Background: Smart Payments initiative

Iberpay is the company responsible for the Spanish Payment System (SNCE), a critical infrastructure for interbank retail payments specialised in the processing, clearing and settlement of payment instruments based on the current account: credit transfers, instant credit transfers, direct debits and cheques, as well as other domestic payment instruments. Iberpay also plays a key role in the distribution of cash to Spanish financial entities as manager of the oficial cash distribution system (SDA), as well as providing other sectoral, technological and digital services with high added value in the context of payments.

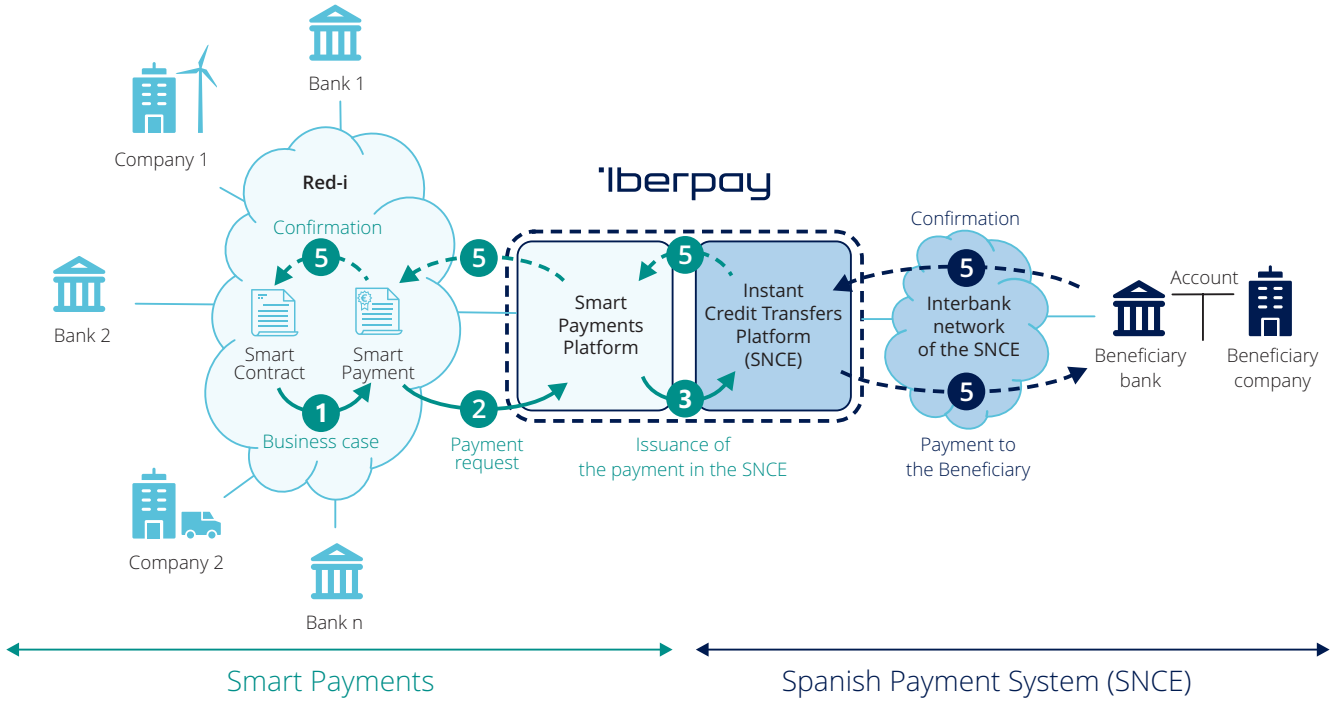
Iberpay fulfils a critical mission in society. Through its payment mechanisms and infrastructures, it facilitates the rapid circulation of funds between citizens and companies.

In June 2018 Iberpay started driving forward the sectoral initiative Smart Payments in response to the need to resolve the execution of payments on digital networks with the maximum guarantees, making use of instant credit transfers to complete the process. In January 2019, the Smart Payments Group was formed, a discussion forum for payment experts of the various entities and also in innovation, blockchain and public policy, which enjoys the participation of representatives from the Banco de España as observers. This group became the catalyst for the sectoral initiatives of Smart Payments and, more recently, Smart Money.

The Smart Payments initiative sets out to offer programmable payment services in digital networks, blockchain or IoT, as the response of the Spanish financial sector to cryptocurrencies such as Bitcoin, stablecoins like Libra/ Diem and other private e-money solutions.

September 2019 saw the start-up of a Proof-of-concept (PoC) to test the connection of blockchain networks with the Spanish Payment System (SNCE), particularly, with its instant credit transfer system, in such a way that any payment initiated in a blockchain network could be processed and settled efficiently, securely and in real time

Smart Payments sectoral initiative
Interoperability between blockchain network and the Spanish Payment System (SNCE)
Instant, programmable and smart payments



Source: own elaboration

through the current payment systems. The top five banks in Spain took part in the PoC (Santander, CaixaBank, BBVA, Sabadell and Bankia, before the latter's merger with CaixaBank), along with Iberpay and the Banco de España as an observer. For the start-up of the PoC, the Red-i network was created, an interbank blockchain network formed by seven nodes, and the Smart Payments platform, for the connection of the Red-i network with the Spanish Payment System (SNCE). In addition, a first governance framework was developed which allows the management of all aspects of the network and the legal feasibility of the initiative was studied.

The connection of the Spanish Payment System (SNCE) with blockchain networks allows the development of numerous usage cases regarding this technology which require a payments solution. With a view to testing the programmability of business cases and the automatic implementation of payments after complying with the conditions programmed previously under smart contracts, a business case related to the management of bank guarantees was tested: in other words, the complete life cycle management of a bank guarantee in a blockchain network and the processing and automatic settlement of the payment associated both with its fees and immediately after the enforcement of the guarantee.

The PoC was successfully completed in May 2020, having carried out more than 20,000 payments in the test environment. The network, in a version with limited resources and in a test environment, attained an average processing time, as from when the payment order is issued until confirmation is received in the blockchain network, of around 2.5 seconds[49].

These tests confirmed the feasibility of developing use cases in blockchain networks whose associated payments are carried out automatically after meeting certain conditions programmed in smart business contracts. It was also concluded that the solution does not introduce any distortions to compliance with the strict payments regulations, particularly in terms of the irrevocability and finality of the transactions and the legal validity of the transactions carried out in the system.

Subsequently, with a view to solving the implementation of payments on other sectoral blockchain networks, an API was developed on the Red-i network which allows interoperation with the maximum guarantee and security with these sectoral blockchain networks and the association of the implementation of payments in the Spanish Payment System (SNCE) with non-banking usage cases.

In October 2020 a proof-of-concept of this second scope was successfully completed, in collaboration with the blockchain specialists of Allfunds Bank. These tests confirmed the possibility of executing payments on the Red-i network, originating from another blockchain network, conducted via an API.

At present, participation in the Smart Payments initiative was extended to other Spanish entities, and so a total of 17 nodes were enabled on the Red-i network, as well as the nodes of Iberpay and Banco de España. In addition, the Red-i network is currently operational awaiting its application in a banking or sectoral use case on blockchain networks.

3.2. Objective and scope of the project

Practical experimentation is undoubtedly necessary to assess the various technological alternatives and explore their technical feasibility, as well as the capacity to meet users' needs. In light of this need for exploration, the Spanish financial sector launched, in late 2020, the Smart Money sectoral initiative.

The Smart Money initiative is based on the theoretical and practical base of the previous Smart Payments initiative. The aim of this new initiative is to test certain technology and functionalities for the sectoral distribution of a digital euro. In this way, in a controlled testing environment of the Red-i network, managed by Iberpay, the Spanish financial sector can also prepare for any Eurosystem decision to issue digital euros. To be precise, the opportunities identified in the Smart Money initiative are:

[49] This processing time includes the execution time of an instant credit transfer in the Spanish Payment System (SNCE) which has average time of 1.5 seconds in the test environment. It is estimated that the processing time would be lower in production, assuming that the average processing time of an instant credit transfer in the Spanish Payment System (SNCE) in this environment is around 0.7 seconds.

- To incentivise public-private collaboration with regulated payment systems and infrastructures, as is the case of Iberpay.

- To practically test and analyse some of the possible design aspects of the digital euro, studying their potential impact on the financial sector in accordance with the recommendations and preferences of the Eurosystem in its "Report on the digital euro".

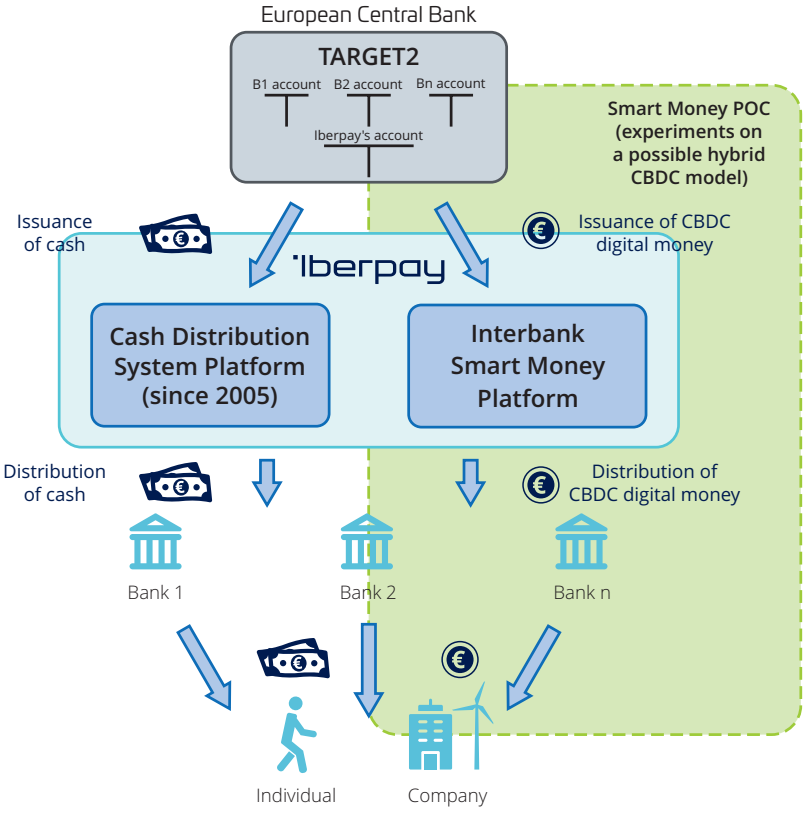
- To advance in a new digital alternative for making payments complementing cash, which helps to cut the total cost associated with the latter (issuance, manufacture, distribution, handling and recycling) and to better meet the needs of society.

- To help to configure a European response in the event of the mass use of CBDC in other foreign currencies, such as the digital dollar or the digital yuan, or in the event of the mass use of stablecoins created outside the financial sector (for example, Diem from Facebook), supporting the economic sovereignty strategy of the European Union.

- To promote innovation in payments and the digitalisation of the European economy, preparing new digital value-added services for companies and private individuals based on programmable digital money, entailing a new source of income for financial institutions and positioning the sector at the forefront of innovation vis-à-vis the technological giants.

The proposed model in this new proof-of-concept takes advantage of the Iberpay's experience in the management of the cash distribution system (SDA), as well as its status as a company regulated by Law and supervised by the Banco de España. Iberpay is already a central, neutral point for banking entities that allows the testing of digital money distribution models, aligned with the regulations and needs of the sector.

Smart Money sectoral initiative
Proof of Concept



Source: own elaboration

In particular, the Smart Money initiative is focused on testing two retail digital money distribution models, which would be carried out by the banks to their clients via the Red-i network: token-based and account-based models. In both models three parties are involved: the end user, the financial entity and Iberpay. In addition, there is a system which simulates the issuance of digital money by the monetary authority and the observer node of the Banco de España.

The study of these models seeks to provide a detailed comparison of the pros and cons of each of them, identifying the main obstacles and designing solutions in order to be prepared for distribution of a digital euro in the event that the Eurosystem decides to issue. The initiative also includes the development of different interfaces to study user's experience when interacting with the digital money. With this in mind, a mobile application has been designed to be used by clients of the entity (simulated for the PoC) compatible with Android and iOS devices.

The initiative also tests different forms of exchanging digital money between end users (online and offline), usage and holding limits of digital money and the possible application of negative interest to disincentivize its use as a store of value.

Finally, although the Smart Money initiative has not studied further the development of a digital identity for these tests, its future evolution is relevant as there will be a need to identify clients on the network. With the Smart Money initiative, a technologically agnostic digital identification tier has been created, compatible with any sectoral solution for sovereign, decentralised digital identity which may be developed in the future.

3.3. Project design

3.3.1. General description of the solution developed

The Smart Money proof-of-concept applies certain functionalities and designs for digital money distribution in the event of the possible issuance of a retail digital euro as a complement to cash, aligned with the "Report on the digital euro[50]" published by the Eurosystem and the latest announcements carried out by this body.

The state of the art regarding the issuance of digital money is not conclusive with regard to its optimal form of representation. The basic options studied in the context of the Smart Money project are representation by tokens and by account entries which have been tested separately and jointly. Both options would allow the end user to have a direct right to the digital money issued by the monetary authority.

In accordance with documents like the "Report on the digital euro" published by the Eurosystem or "The technology of retail central bank digital money" by the BIS[51], these models (token and account-based) are mainly based on the following premises:

[50] Op. Cit (21)
[51] Aurer, R and Bohme R. (2020) "The technology of retail central bank digital currency". BIS. https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf

Models analysed in the "Report on the digital euro" from the European Central Bank	
Token-based digital money (Bearer digital euro)	*Account-based digital money (Account-based digital euro)*
• The identity is verified at device level when the user demonstrates they know a cryptographic value (for example, through a public and private keys system). • The payer and the beneficiary are responsible for verifying and transferring value between each other. • The operation is similar to that for cash. The limits to the amounts and other restrictions to digital money may only be controlled at device level.	• It is a third party (bank entity) who verifies the identity of the payer and the beneficiary. • It is a third party who guarantees that a transaction is valid and updates the account balances accordingly. • It is the basis for the majority of current electronic payment solutions. The Eurosystem may continue to exert control over the digital money.

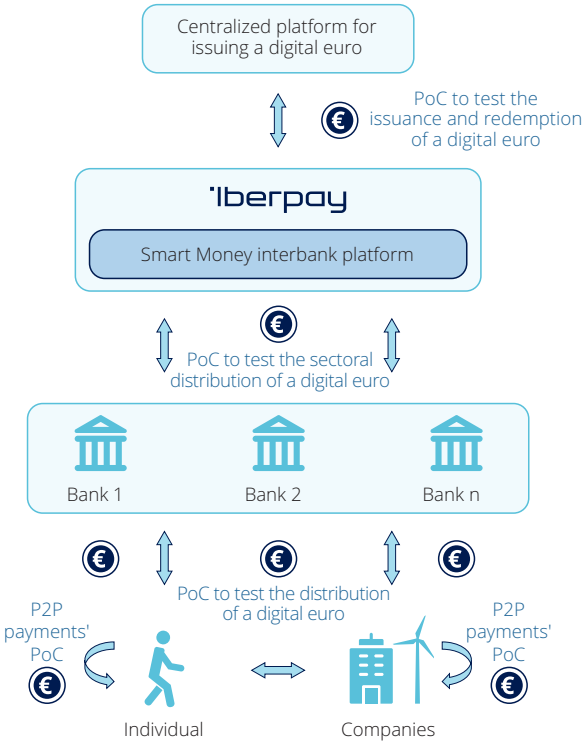
However, with a view to supporting innovation in the sector, testing blockchain technology in this regard and test the functionalities that the Eurosystem regards as desirable in both models (limits, remuneration, offline payments, etc.), the Smart Money initiative has limited certain aspects of the token-based digital money model set out in the previous table.

Hence, the solution proposed in this initiative involves a scheme in which the end users do not have direct access to the blockchain network (Red-i network), instead, all the transactions necessarily involve bank entities (intermediated model), who verify the identity of users and validate the transactions carried out between them. In the token-based digital money model, the cryptographic keys reside in the user's device, with a view to allowing offline operation, whilst in the account-based digital money model the keys are safeguarded by the entities. Programmability deriving from the use of blockchain technology pertains to the entities who, through it, have the capacity to provide new services or create new business models based on the digital money. The digital money models tested in the context of PoC and analysed in the following sections, use these premises as their basis.

This solution solely meets the criteria used in the Smart Money PoC whose aim has been, inter alia, to assess the potential that the digital money combined with blockchain technology may bring to the financial sector, without reducing the controls which, as of today, are mandatory (and which, in the case of a pure "bearer euro" model, are still difficult to apply). Under no circumstances does the solution used in the context of these tests constitute an official recommendation or final solution. In fact, it is expected to continue with future stages of the initiative to delve into aspects not studied in the context of this PoC and which could entail analysing possible solutions with regard to the modus operandi of token-based digital money as set out in the reports mentioned above.

The solution developed is based on a two-tier model in which Iberpay would be responsible for distributing digital euros on behalf of the monetary authority at the request of the entities, crediting or debiting the amount into the financial institution's reserves in TARGET2, TIPS or any other platform deployed for these purposes, all in a test environment. In turn, the financial entities would be the distributors of the digital money to their clients and responsible for diligence measures as set out below:

Smart Money sectoral initiative
Testing sectoral distribution of a digital euro



Source: own elaboration

As can be observed, the issuance and the redemption of digital euros would be centralised on the upper tier (Eurosystem, the tier simulated in the project). In turn, the intermediate tier, where Iberpay takes part, would be responsible for distributing the digital money amongst the financial entities who, in turn, through the lower tier, would distribute it to its clients. The distribution of digital money would be limited to those authorised intermediaries with a view to avoiding risks to the financial system.

Five parties take part in the environment created:

- **Orchestrator or simulator:** this consists of a server that receives the issuance and redemption digital money transactions, and which simulates communication with the monetary authority/central bank. For the purposes of PoC, this upper centralising tier also simulates the issuance and redemption of digital euros for the Red-i network.

- **Iberpay:** is the management institution who coordinates and administrates the digital money issued in a given context or environment through the Smart Money interbank platform (intermediate infrastructure between the central bank and the Red-i network). In other words, it acts as a link between the digital money issuer and the distributing financial entities. Iberpay, as manager of an ancillary system in TARGET2 and soon in TIPS, has the capacity to settle in the accounts of financial entities on the TARGET2 and TIPS platforms of the Eurosystem. This could allow, in the event of any issuance of the digital euro, Iberpay to connect directly to the platform used by the monetary authority to request or return digital euros at the request of the

entities, through a sectoral and collaborative solution. Iberpay also controls and validates technically (see section 5.1) the wallets[52] involved in each transaction in the Red-i network and has the visibility of the whole network (limited to the degree of privacy configured initially).

- **Financial entity:** it acts as an intermediary and distributor of digital money amongst its clients. It transfers to Iberpay the request to receive or return digital money, it is responsible for the necessary identification of the clients and it has the visibility of its own transactions and those of its clients.

- **The end user:** this is the client, a natural or legal person, of a financial entity, from which it obtains (or returns) digital money and it may transfer it to other users, with the visibility of all its transactions. The end user may operate alternately with account-based or token-based digital money, or both.

- **Observer authority:** the BdE participates in the network as an observer, having access to the information of the transactions carried out (balance in account), although not the user to which it belongs.

3.3.2. Design of the digital money

The digital money designed in the framework of the Smart Money project offers universal access and so the end client may receive it and transfer it (within the limits set initially) through the digital money accounts and/or wallets enabled to operate in the Red-i network. The most important characteristics are indicated below:

- **Form of representation of the digital money:** both representation models of the digital, token and account-based, with the specifications previously set out in point 3.3.1 have been tested. The difference between both, from a technological perspective, mainly lies in the storage location of the private keys (in the case of the token-based model, they would reside, in theory, in the user's device, whilst in the case of the account-based model, the keys would be managed by the banks). In both models it is necessary for the end user to have a previous bank account to associate it either with the wallet (in the case of the token-based model) or with the digital money account (in the case of the account-based model), or with both if the two models coexist. The aim is to allow conversions of bank money to digital money and vice versa. Both models are interoperable and so a client may send or receive digital euros within the network in transparently and independently from the model that the counterparty uses. The decision as to whether the user has a bank account associated with the digital money account or wallet was adopted in the context of the Smart Money initiative. However, there is nothing to prevent the final solution from allowing access to unbanked people in line with the pronouncements by the ECB ("a digital euro would contribute to the financial inclusion, affording an additional option as to how to pay along with cash"). In this regard, it should also be highlighted that the legislation[53] already foresees the right of consumers to have access to a basic payments account or e-money. Digital money could thus make a positive contribution to promoting and facilitating the use of this type of account.

- **Possibility of making offline transactions:** the account-based digital money may only be used when the user has internet connection: it is not connected to a specific device and its access is controlled by the intermediary entities. In turn, token-based digital money allows its use both online and offline and it is connected to a specific device, usually a mobile phone (where the keys reside, in order to sign transactions on the blockchain network). To prevent the loss of the device entailing the loss of the digital money, entities could have key regeneration systems or contingency solutions, or

[52] In the context of the Smart Money initiative tests, Iberpay was responsible for technically designing both the master wallets (those used by the entities to obtain/return digital money to the simulated Eurosystem and distribute it to its clients) and the wallets provided to the users.

[53] As regards unbanked population and with regard to whether a current account is required to support the digital money account and wallet, due consideration must be given to the regime foreseen by Royal Decree-law 19/2017, of 24 November, regarding basic payment accounts, account switching and comparability of payment account fees, which transposes the EU Directive 2014/92 of the European Parliament and Council, of 23 July 2014, on the comparability of fees related to payment accounts, payment account switching and access to basic payment accounts. One of the objectives of the Directive is precisely to facilitate the access of potential clients to basic banking services, in accordance with Commission Recommendation 2011/442/EU, of 18 July 2011, on the access to a basic payment account, which seeks to cater for those situations in which potential clients are not able to open a payment account either because they are denied this possibility, or because they are not offered a suitable product.

even acquire the function of key safeguarding, as will be explained later.

In the context of the PoC, the offline transmission of token-based digital money has been designed to be triggered by means of a code system. In this way, when an individual wishes to send digital money to another, the beneficiary will activate the "receiving tokens" option on their mobile application, generating a QR code for scanning by the payer. This QR code would allow the beneficiary's address to be filled in automatically on the payer's mobile who would also indicate the amount to be sent and any other data that proves necessary.

Once the issuer has entered all the data required to complete the offline payment, their wallet generates and signs the transaction to transfer the funds to the beneficiary. It should be noted that the generation of this transaction does not entail the processing of the order nor, accordingly, the settlement of the funds, which will be completed when one of the parties (the issuer or the beneficiary) sends this transaction to its respective entity for introduction in the blockchain network[54].

Although the payment transaction using token-based digital money can be carried out offline, its processing and settlement will only take place when one of the two participants has an internet connection and sends the transaction to their financial entity. At this time, the synchronisation and conciliation of the payment is carried out, in such a way that the balances of all the participants are updated automatically, as part of the execution of Smart Money smart contracts.

- **Prevention of duplicated payments due to the application of blockchain technology:** the blockchain technology employed by the Smart Money platform prevents the problem of double-spending. In the case of duplicating the same transaction, the platform will only process the first transaction received and so ensuring that the funds will only be transferred once. To this end, the platform identifies the transactions generated by the issuer which contain the same "nonce" and it rejects those with "nonces"[55] which have already been processed, meaning that the funds will be transferred only through the first transaction received. In view of the fact that this situation could occur in the event of intentional fraud by the user, this point must be investigated thoroughly in the future to apply mitigation measures proven necessary.

- **Use of smart contracts and programmability:** the whole modus operandi of the digital money is carried out through the execution of smart contracts deployed on the Red-i network. Hence, transactions such as the issuance and redemption of digital money, the distribution of digital money to the clients of the entities or payments between users, are executed by means of transactions sent to the blockchain network. Hyperledger Besu technology's programmability guarantees the possibility of bringing use cases of various natures to the Red-i network, automating the relations and associated processes which will require an individualised analysis and, potentially, will allow innovation in this field.

- **Security:** the Red-i network allows the application of complementary security measures owing to the fact that financial entities may process and verify the content of the transactions sent by their clients before being introduced into the blockchain network. In addition, the PoC incorporates basic security measures to guarantee the correct implementation of the tests.

- **Limitations in the usage and holding of digital money:** regarding the amount of available digital money, the Eurosystem proposes, amongst other tools, the possibility of establishing quantitative limits

[54] For further information see section 5.2.

[55] The nonce is a whole number which serves as an incremental counter of the transactions sent by a user, which allows the ordering of the execution of blockchain transactions. In this way, the first transaction sent by a client has nonce 0, the second nonce 1, and so on. If a user sends two transactions with the same nonce, only the first is processed, whilst the second will be rejected.

by individuals. These limits have been tested in the framework of the Smart Money project, both in wallets and digital money accounts, jointly with tools that facilitate the management of digital money liquidity.

- The possible limits imposed by the Regulator: configurable limits have been established with a maximum amount per transaction and with a limited weekly amount in digital money transfers, both for digital money accounts and wallets. Furthermore, to carry out the tests, a maximum limit of digital money available between the wallet and/or the digital money account of 10,000 digital euros was parameterised, although the final amount is still under discussion[56]. Given that the scope of the PoC has been limited to each user having only one account, the limits of the holders of multiple wallets or accounts through which they can operate with digital money have not been tested. However, in a productive environment, the ideal is to apply these limits to the total amount of digital euros that a user may have in the system, regardless of whether he decides to operate with one or multiple wallets or accounts, to which end, a homogenous digital identity layer will be required in the whole system (see C12 in section 3.4 Results and conclusions).
- Limits administered by the users to automate the management of liquidity: within the limits established by default, an individual may, in turn, set their own limits. Additionally, they may set minimum thresholds when the amount of digital money in the account and/or wallet is lower than the minimum threshold that was established, the automatic conversion of bank money from the individual's account into digital money until it reaches the amount set as the base position. The effect would be the same as if the user always wanted to have an amount of money available in their wallet.
- Management of excess digital money: the amount that exceeds the limit (for example, sending digital money from one individual to another causing the recipient to exceed their digital money limit permitted in their account or wallet) is automatically transferred in the form of bank money to the client's account associated with the digital money account or wallet.

- **Return/rate of interest of digital money:** digital money has been designed to be able to apply remuneration policies in accordance with the Eurosystem guidelines. In this manner, the tests conducted in the framework of the project include two different types of remuneration, one for entities and another one for the accounts and/or wallets of end clients.

  Remuneration of the wallets/accounts of clients is calculated according to the total balance of digital money which is available at any time. In this regard, an interest rate is applied by, for example, positively remunerating the holding of digital money up to a certain amount. If this amount is exceeded, no remuneration would be applicable (remuneration at zero interest rate) until it reaches a fixed amount as from which a negative interest rate would be applied. The objective of this type of measures is to prevent digital money from being hoarded as an instrument of store of value, and, in this way, using it exclusively as a means of payment.

  Regarding the remuneration of the entities in the context of the tests carried out during the PoC, this has always been set at a negative rate.

  In any case, there is still an ongoing debate about the need or not to apply remuneration policies to digital money, and so, the tests carried out in the framework of the PoC do not imply, under any circumstances, any recommendation nor decision in this regard.

[56] Panetta, F (2021): "Evolution or revolution? The impact of a digital euro on the financial system". BCE. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210210~a1665d3188.en.html

3.4. Results and conclusions

The tests carried out in the framework of the Smart Money initiative have given rise to the conclusions presented below.

C1: A two-tier model facilitates the provision of added value services by the sector:

A two-tier model would allow a form of access to the digital euro that would be under the supervision of the competent authority while facilitating the use of the digital euro by users, maintaining a significant degree of autonomy in the provision of value-added services by the banking sector, especially interesting in the field of money programmability.

Consequently, the entities would continue to ensure the distribution of central bank money, executing due diligence controls, and they would be responsible for the necessary infrastructure to reach all citizens and companies, maintaining the necessary attention to issues such as cyber-security and third-party privacy. This would allow a better adaptation of the digital euro to the needs of the end users (clients) thanks to the knowledge and the relationship of the commercial bank with the end client. On the other hand, the implementation of this model could also imply less investment in the infrastructure by the monetary authority, which would not be obliged to adapt its access to end users.

The two-tier model would also facilitate the possibility of creating synergies with existing financial services, taking advantage of the current banking model (integration with the Eurosystem, supervision, regulation, full competence in terms of money laundering prevention and the financing of terrorism and consumer protection). This idea also emerges from the responses to the public consultation on a digital euro[57] published by the ECB, according to which the vast majority of the citizens surveyed (73%) see a role for intermediaries, who can offer innovative services and contribute efficiency to the system, especially with regard to the offer of payment solutions to end users.

C2: The two-tier model facilitates appropriate risk management:

In the scope of the tests conducted, the access to digital money has been restricted to users that are already holders of a bank account. In other words, each digital money account or wallet must be linked to a current account at a bank.

In this manner, transaction banking can be guaranteed in the conversion between the commercial bank money and the digital euro, and vice versa. This circumstance also allows both models (token-based and account-based) to be based on the responsibility and experience of the entities in the management of onboarding processes, the application of Money Laundering Prevention and Terrorism Financing (PML-FT) measures, the control of fraud and security, amongst many others.

Furthermore, the model implemented would facilitate the application of security regulations in comparison with other models, for example, the direct model. Among other things, it would permit password backup mechanisms for the users in a simple way; also, access to central bank accounts would be less complex by limiting the number of participants in the system to supervised intermediaries.

In any case, the tests allow us to conclude how important it is for financial entities to be a vehicular part of the system, fostering the transition from the current model to a digital money model whilst maintaining the correlation between the potential end users and the banking entities.

[57] BCE (2021): "Eurosystem report on the public consultation on a digital euro". https:// www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

C3: The token-based digital money model and the account-based digital money model can coexist in the same infrastructure, although they present some significant differences:

From the perspective of technological design (and always in the scope of the PoC), the difference between developing one or the other model is minimal since the registration of tokens in the corresponding smart contract occurs in the same way as account-based registration. The main difference is the storage location of users' private keys.

In the token-based digital money model, these keys are stored in the individual's mobile, facilitating the possibility of making offline payments. With this in mind, any commissioning of the production system would require, among others, the availability of safe storage systems on the device used and the strict control of any possible double entries.

In the second case (account-based), these keys would be managed by the corresponding financial entity for use on behalf of the client, when the latter so requested. This difference between the two models could have consequences both in terms of the type of services provided by the entity, as well as in terms of the responsibility[58] for key security.

In an account-based model, the entity would be the guarantor of key security and hence of the client's digital money. On the other hand, in the token-based model, the role of the banking entity would be limited to recording transactions, with a lower capacity to guarantee the security of the client's account. In this regard, the risk of fraud both in user authentication and in transactions, or even the management of keys on devices whose security has been compromised, are characteristics that must be analysed in detail in the case of opting for this model, especially when the entities' responsibility would lack security guarantee mechanisms because the keys are stored on the user's mobile. This might entail reputational damage in the case of security incidents and in the case of the coexistence of both models (token and account-based), the risks could be carried over from one service to the other. In order to avoid risks, the keys could be stored at the entity itself which, in addition, could have recovery or new generation mechanisms in the case of loss, providing greater security to the system.

Even though, the token-based model presents challenges to the industry, it cannot be forgotten that it has the advantage of allowing payments to be made offline, in other words, without the need for an internet connection. This requirement has already been shown by the Eurosystem as a possibly desirable characteristic to consider in the future digital euro (see C6 and C7 for further detail) according to the results of the public consultation about the digital euro.

As can be observed, the storage location of the keys has a special relevance both for the user and the entity. With this in mind, it is necessary to consider mechanisms that allow the user to know the risk they are taking and the responsibility incumbent upon them in each case (for example, those cases in which the end client suffers an attack from a third party or another event and loses the keys for reasons unrelated to the network). The advantages entailed for the user of adopting the token-based model (with the possibility of making offline payments) in comparison with the risks assumed, must be assessed prior to the commissioning of any initiative.

[58] It should be borne in mind that if the wallet is going to serve as a payment instrument, article 42.2 RDLSP shall apply, which determines that the payment service provider will assume any risks deriving from the sending of a payment instrument to the payment service's user or from the sending of any personalised security elements thereof. And section 1 a) of the same law considers the obligation of the payment service provider to ensure that the personalised security credentials of the payment instrument are only accessible to the payment service's user entitled to use this instrument, without prejudice to any obligations incumbent upon the payment services user pursuant to article 41, section 23, article 3 of the RDLSP takes payment instrument to mean: "any personalised device or set of procedures agreed between the payment services user and the payment services provider and used to initiate a payment order".

C4: Both models (token and account-based) are compatible and combinable from a functional perspective:

After the commissioning of the Smart Money initiative, it can be concluded that the design of a mixed system that allows, on the one hand, the execution of offline payments through token-based digital money (probably limited to a certain amount) and, on the other hand, carrying out current transactions based on the account-based model, would allow us to count on the advantages of both models.

The combination of both models could even lead in the future to the possibility of adapting each model to a specific type of user or a specific use case. However, it could also entail difficulties for the user when conceptualizing each model as it may not be able to distinguish between them in practice. In this regard, it is necessary to reflect on how to communicate to the end user the advantages and disadvantages of using digital money in a general way and, specifically, for each model, in case they coexist.

The implementation of either of the two models, or their combination, highlights the need to clearly determine the distribution of responsibilities and obligations between the Eurosystem and the different intermediaries in the event of a possible technical error or a cyber-attack. Likewise, it will be necessary to adapt the governance and operational risk mechanisms according to the final characteristics of the digital euro.

C5: Iberpay could facilitate the digital money distribution infrastructure in both models:

Iberpay can act as a technological facilitator in both the token-based digital money model and the account-based digital money model. In both cases, Iberpay would be prepared to manage the new Spanish infrastructures that would constitute the wholesale distribution model and the sectoral transactional support of the digital euro, being a crucial party to interconnect the platforms of the issuing bank of the digital euro with financial intermediaries.

In this way, the access to digital money by users is guaranteed to be carried out through regulated, supervised and authorised infrastructures. On the other hand, thanks to Iberpay's vast experience of interconnecting with other counterpart infrastructures in the European area, it could also contribute to the development of European payment solutions based on the digital euro, interoperable with other countries in the Eurozone.

Iberpay could reuse, in part, the current infrastructure, platform and communications with banks, links with TARGET2 and TIPS platforms of the European Central Bank and other European infrastructures, as well as its capacities and processing technology, to offer a sectoral distribution service of the digital euro which is efficient, secure and reliable.

C6: The results of the offline payment tests reveal the complexity of finding an optimum solution comparable to cash:

In offline payments the client utilises the mobile device to sign the transactions whereby they transfer their funds. Since the signature keys associated with the token-based digital money wallet reside on the mobile, only offline payments could be made with this device.

Within the framework of the project, this functionality has been addressed by enabling the exchange of QR codes between the payer and the beneficiary, allowing the payment order to be generated without the need for an internet connection and settling the latter at the time when either of the two users reconnects to the network.

In this context, the following challenges have been identified:

- QR codes are not standardised at European Union level, which restricts their acceptance, particularly when it comes to cross-border transactions. Therefore, it is concluded that this may entail difficulties when

offering businesses and consumers convenient and affordable payment solutions based on the use of unified QR codes as an alternative to payment cards. Other technologies such as Near Field Communication (NFC) are not without their challenges either. There are device manufacturers that restrict the access of payment method providers to this technology on their mobile phones[59].

The Euro Retail Payments Board (ERPB)[60], in cooperation with the multi-stakeholder group for Mobile Initiated SEPA Credit Transfers, is exploring the possibility of preparing a single standard for QR codes. In any case, standardisation is required to be able to process offline payments in the Eurozone.

Additionally, if this form of offline payments were finally implemented, it should be noted that it would be necessary for financial entities to make investments, as it is not currently one of the widespread systems used in the field of payments, unlike other countries like Argentina or China. It should also be emphasised that it would be necessary to guarantee the appropriate security standards for this new system.

- The final design may require looking more closely at cryptographic solutions that allow digital money to be processed offline in a similar way to cash, so that the beneficiary can spend this money without the need for any type of connection, since, otherwise, offline digital money could end up resembling a kind of promissory note. This has important consequences, such as those in law (the capacity of cancelling debts of offline payments, the acceptance by the creditor of the payment or the time when it must be considered final) and security (secure storage systems on devices or mechanisms to avoid double spending), so we must continue studying the optimal way of implementing offline digital money.

Furthermore, the tests conducted in the framework of the Smart Money initiative have highlighted the need to analyse the nature of offline payments and, accordingly, the warnings that must be made to users. In this regard, the need to implement *ad hoc* legislative provisions cannot be ruled out.

Basically, the real challenge lies in obtaining an offline payment solution that behaves in a similar way to cash (in terms of instant payment settlement or digital money spending without an internet connection) but with the advantages of a token-based digital money (limits, security or fraud reduction thanks to traceability, depending on the designs selected for their implementation).

C7: It is possible to apply restrictions on the number of digital money transactions offline according to the reference standards, even though it is still necessary to keep analysing what the best design would be:

As indicated in Directive 2018/843 of the European Parliament and the Council on the prevention of the use of the financial system for money laundering or the financing of terrorism (hereinafter, PML-FT regulations), completely anonymous transactions, like those made through anonymous prepaid cards, can facilitate money laundering and the financing of terrorism. Besides, excessively high limits impact the effectiveness of the prevention, since the maximum amounts below which entities, otherwise obliged, are authorised not to apply some of the due diligence measures in regard to the client. This is why the Directive has duly reduced the maximum threshold amount for this type of transactions to 50 euros.

Even though offline payments should not be anonymous with the objective of PML-FT risk prevention, avoiding its usage as a store of value, it would be possible to introduce restrictions to offline payment amounts, based on the previous standard.

[59] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Law) studies this issue, although there are still years for its effective application.

[60] The body which, under the supervision of the Central European Bank, was formed to help promote the development of a retail payment market in euros in the European Union which is integrated, innovative and competitive. It is integrated by representatives from the supply and demand of payment services, as well as from the European Commission, the ECB and the national central banks.

[61] Coordination and decision-making body of the banking industry with regard to payment. The EPC defined SEPA payment instruments and the frameworks required to build the single payment market in euros.

C8: The necessary synchronisation mechanisms and service levels in the area of offline and online payments would be similar to the ones currently in use for instant payments:

Payments initiated offline would not be fully executed until one of the two parties has internet access and sends the transaction to its entity, at which point the payment synchronization and settlement takes place. Hence, the entities' information systems must be available at all times to receive payment orders in real-time and send them to the blockchain network which can occur at any time of the day.

In this regard, the service requirements for offline payments do not differ from others that currently exist, such as, for example, Iberpay's instant credit transfer service. In other words, the service levels for offline payments and, in general, for the Smart Money solution, would be similar to the instant payment services provided by Iberpay.

C9: It is possible to make privacy compatible with traceability in offline payments, although this makes it difficult to compare it to cash:

Based on the previous conclusions, and after carrying out the tests within the framework of the project, it can be concluded that payments made offline maintain privacy as long as none of the users obtains an internet connection. As soon as the payment enters the network, the entities involved will be able to view, as in any online transaction, the origin and destination of the transaction carried out offline. As in the rest of the transactions, only the entities involved in the operation will know its origin and destination, while for the rest, thanks to private channels, they will remain opaque.

Additionally, in line with the public pronouncements of the ECB[62], to satisfy higher levels of privacy for citizens, a scheme with different threshold levels could be proposed, where low-value offline payments could be allowed when users do not share their identity with the entities involved or through anonymity vouchers for offline payments up to a certain threshold.

C10: Offline payments have advantages when one of the two parties has a frequent internet connection:

After the tests conducted under the Smart Money initiative, it is possible to conclude that offline payments, unlike cash payments, prevent money from being lost. In this regard, when a transfer of funds occurs offline, the payer's mobile will store and send the transaction to the beneficiary. The validation carried out by the payer's mobile will be to verify that the money held in its wallet is higher than the amount to be sent offline. Once this has occurred, this transaction will be stored on both mobiles (payer and beneficiary) and it would only be lost if both mobiles were misplaced or stopped working. This entails an advantage over cash, as the chances of loss are reduced significantly.

However, this situation also has some disadvantages. Only when one of the parties (the payer or beneficiary) obtains an internet connection will the payment be effectively settled and stored in the network. This implies that the beneficiary cannot spend the money received offline until one of the two parties gets a connection to the network, which is why we may conclude that offline payment is less efficient and has greater limitations than cash.

It should be noted that offline payments will be stored in chronological order and the mobile offline payment validation system will always take into account the amount remaining in the wallet before sending an offline payment. During the period when the payer has no internet connection, this would prevent the digital money amount from being reduced prejudicing the first transactions.

At the time when the internet connection has been re-established by any of the users involved, the transactions will be executed in chronological order.

It can also be concluded that a specific study needs to be carried out as to which offline use cases may be more appropriate. An example of this could be to pay at a store in situations involving connectivity loss where the

[62] Panetta, F (2021): "A digital euro to meet the expectations of Europeans". ECB. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210414_1~e76b855b5c.en.html

terminal is connected to the internet most of the time and it is thus possible to guarantee that the transfer of digital money will occur rapidly.

On the other hand, it should be taken into account that the direct debit or other expenses in the wallet could cause additional difficulties since in the period that elapses between the initiation of the offline payment and the internet connection of either party (payer or beneficiary), online expenses may be incurred in the payer's account, generating a risk of lack of necessary funds to make the payment once the connection is restored.

C11: New standards for payments need to be developed:

In the context of the Smart Money initiative, the information exchanged between entities to make payments is mainly based on the customer's IBAN. The IBAN provides information about the account and the country of the citizen or company. However, it has limitations when it comes to providing information about certain aspects dealt with in the project, for example, whether the digital money transferred is token-based or account-based, what type of CBDC is being exchanged (domestic or foreign), among others. Hence, the review of the specific current standards in payments would be required, especially to facilitate payments with CBDCs between different countries.

Following the commissioning of the Smart Money initiative, it can be concluded that there are several design options for a new CBDC account identifier standard, the main ones being the following:

- CBDC IBAN: it would follow a similar format to the current IBAN, incorporating new characters that identify the type of CBDC in question, as well as additional information.

- Decentralised identifiers or DID: this is a standard for identifiers designed to facilitate digital authentication on the internet. The usage of DIDs at a national and European level could also smooth the path for the adoption of decentralised digital identities by end users.

In any case, the solution must be sufficiently flexible so as to be able to adapt and interoperate with digital money in other jurisdictions. With this in mind, technical and regulatory standardisation is required, to which end the ECB would play a key role. Likewise, a common orchestrator figure capable of conducting operations in each network according to the type of digital money could help solve part of the problem raised.

C12: It is possible to limit the amount of digital euros:

In the framework of the Smart Money initiative it has been established that it will be the responsibility of the entities to provide technological solutions for the digital money wallets and accounts of the final client. In turn, it will be the responsibility of Iberpay to authorise participation in the network of these wallets and to keep track of those enabled to operate on the Red-i network.

The Smart Money proof-of-concept, having a limited scope, has been based on the premise that each user only has one digital money wallet and/or account. However, in a real productive environment it is necessary to define whether an individual will have access to one or several wallets or accounts per entity through which they will operate with digital money. This decision gains particular relevance if it is intended to limit the amount of digital money available to users and for the effective application of progressive interest rates, such as the ones described previously, to the total balance of an individual for the purposes of avoiding any possible damage to the financial system (for example, a run on deposits), since each entity can only control the limit of the digital money account or wallet that it provides to its client.

Consequently, in the event that users may be holders of different digital money wallets and accounts (associated with different entities), it would be necessary for an orchestrating entity with visibility of the entire network to

control the individual's digital money limit, for example, linking all the digital money wallets and accounts of the user through their ID cards or through a digital identity layer (a European or international standard of digital identity could greatly facilitate this aspect). In this way, it would be possible to uniquely identify the individual and thus set a digital money limit per person (all without prejudice to the application of the measures that are necessary to comply with the personal data protection regulations).

Another alternative would be to create a unique sectoral wallet associated with a specific IBAN, with a default balance limit. In this case, the wallet designed should be portable from one entity to another in a simple way for greater user operation. The model could allow the wallet to be personalised by each entity in order to provide its own user experience, integrating it (or not) into their own applications, etc. This option would allow the entity responsible for the wallet in each case to be responsible for monitoring the individual's digital money limit without the need for a higher layer of control.

Although both alternatives are not exclusive, in order to limit risks to financial stability and to be able to adequately control operating limits, wallets should only be provided by regulated and supervised intermediaries. Additionally, and regardless of the solution finally chosen, it is necessary to have a standard that allows interoperability between wallets, not only at national level, but also at the international level.

Finally, it should be noted that, although technically it is possible to limit the amount of digital euros per individual or penalise their accumulation through negative interest rates, it is necessary to analyse in detail whether these measures will be effective to mitigate the risks and possible negative effects for the financial system of a significant outflow of bank deposits to digital euros (either in crisis situations, or in normal times[63]).

C13: It is possible to apply different limits to digital money depending on the desired user experience:

In the framework of the Smart Money initiative, it has been sought to configure a maximum limit for holding of digital euros and a limit on the number of transactions carried out with digital money. These limits have been applied generically to all digital money wallets/accounts and their objective is none other than to direct digital money to its use as a means of payment and not as a store of value (avoiding a transfer of bank funds to digital money), as well as to ensure proper control of transactions. However, the configuration options are very varied and it will be necessary to attend to the final design of the euros and the business models that are finally developed to make a decision in this regard.

In this regard, a cumulative limit may be proposed for transactions in euros in a given period (for example, one month), to determine limits based on the related transaction and customer profile (consumer, professional, company, Public Administration, also considering any complications that may be entailed in terms of usability) or making the limits similar to those already in place for transactions carried out in cash. In any case, the setting of limits should be aligned with the on tax evasion laws.

C14: There are efficient mechanisms in place to manage any excess of the digital money limit:

Regarding the management of the excess of digital money limits, the tests conclude that the simplest option would be to automatically convert the surplus of digital money into commercial bank money when the maximum threshold for holding digital euros has been exceeded, as this is a sound, simple rule. This surplus would be deposited in the bank account linked with the digital money wallet or account, in the same way as any other usual deposit.

[63] Op. Cit (48)

Another alternative could be to reject the transaction that causes excess digital money in the digital money wallet or account, sending a communication to the payer and the beneficiary, although, to this end, it would be necessary to develop a prior authorisation layer of the transaction before finally processing the payment, which would add complexity to the transaction in addition to discouraging the use of digital money as a means of payment.

C15: It is viable to apply remuneration policies to digital money, though their effectiveness is still being studied:

Setting a remuneration rate might be necessary to strike a balance between promoting the use of the digital euro as a means of payment and deterring its use as a store of value. To this end, the possibility has been raised that this remuneration rate does not affect only retail customers, but also digital euros that are owned by authorised intermediaries.

In the framework of the Smart Money initiative, applying a remuneration rate has been tested, both for banking entities and users. The interest applied to clients varies according to the balance whilst the one applicable to banking entities is always negative. The remuneration is customisable and configurable allowing the adaptation of the regulations that are issued at any time from the competent authorities and bodies. However, it is still necessary to delve into this question in order to determine whether remuneration is an effective measure to discourage the use of digital money as a store of value, or whether, on the contrary, these objectives can be met by only applying limits to balances and to transactions.

Finally, it is important to continue studying the scenario in which end users may be holders of several digital money accounts or wallets in different entities, in which case it will be necessary to know the total balance of a client in order to use it to calculate remuneration (see C12).

C16: Both models (token and account-based) allow the application of due diligence measures within the framework of the rules for the prevention of money laundering and the financing of terrorism:

During the Smart Money initiative, a way of operating with digital money has been proposed similar to the one currently produced with private bank money because it is a familiar operation for the client and because it allows entities to fit their operation into their internal processes in a simpler way.

The requirement of having an open current account in an entity as a step prior to the creation of a digital money wallet or account allows entities to maintain the client identified and to keep applying their due diligence procedures, knowledge of the customer and security measures. However, the obligation to identify the client must be maintained in any other possible scenario in which there is the possibility of having independent digital money wallets or accounts not associated with current accounts.

Likewise, the operation tested within the framework of the Smart Money initiative allows operational validations to be carried out on the transactions specific to the banking system: fraud, money laundering, the smooth execution of transactions, validating amounts or other parameters. In addition, a financial institution could block the digital money wallet or account of a client if it detects suspicious operations as a necessary aim to maintain system[64] integrity.

Finally, the application of limits on the number of transactions allows better control within the framework of the PML-FT regulation.

[64] It should be determined whether the wallet, if it is defined as a payment instrument, and the digital money account, if it is defined as a payment account, are subject, for the purposes of carrying out this block, to the provisions of art. 40 RDLSP, in particular as regards the user notification and blocking obligations.

However, although this mechanism for using digital money has its advantages, it also prevents the separation of digital money from normal banking operations, which may have consequences in areas such as financial inclusion, one of the objectives indicated both by the ECB and by other international organisations as one of the driving forces in the study of CBDC models. In this context, it is still necessary to step up the development of mechanisms that make it possible to offset the use of CBDCs by underbanked segments with guarantees in compliance with PML-FT regulations, for example, allowing easier client registration procedures through traditional financial intermediaries.

On the other hand, the digital euro would also offer new opportunities to facilitate compliance with the PML-FT regulation by payment providers (for example, applying automatic controls or whitelisting), as well as for control and supervision by the authorities, who could, for example, have access to the underlying payments and the identification of beneficiaries and payers. This could significantly simplify the intermediary role of the obliged entities in the presentation of regulatory reports (requirements on centralized account registries, the communication of transactions with offshore financial centres, etc.) or the application of regulatory actions (sanctions screening and account blocking against EU sanctions lists), without calling to question the responsibility of the obliged entities to identify and report suspicious activities.

In any case, the technology used in the Smart Money initiative would make it possible to evaluate the implementation of new wallet opening models for the unbanked population, for example being able to request digital euros at ATMs by depositing cash. In this case, it would be necessary to reflect on the mechanisms for applying due diligence measures and the person responsible for applying them, even in those cases in which a less strict onboarding process may possibly be allowed.

C17: It is possible to apply privacy mechanisms on the Red-i network whilst complying with the regulations for the Prevention of Money Laundering and the Financing of Terrorism:

In any system architecture and privacy scheme, technical mechanisms must be established that allow the parties involved in the payment to comply with the current requirements for the Prevention of Money Laundering and the Financing of Terrorism (PML-FT), while protecting the holders from unauthorized accesses. After the tests carried out within the framework of the Smart Money initiative with the Orion privacy layer of Hyperledger Besu, it can be concluded that the technological privacy solutions, although effective today, must continue to mature in order to be used in real productive environments.

From a regulatory point of view, the data protection regulations protect the processing of data when it is necessary to comply with a legal obligation, as is the case of the PML-FT regulation. In this regard, the Smart Money project has been designed so that entities can view their clients' transactions, just as is currently the case with bank money.

Through the use of private transactions (on private channels), the accounting of each client would only be known by its entity. Iberpay and the observer node of the Banco de España will be able to see the accounting (the balances of each account), but they will not know the end user to whom it belongs. Likewise, once the storage period has elapsed, the data may be deleted, leaving the blockchain records anonymized (see point 4.3.1. for further information).

In the event that the digital euro is launched, it would be necessary to take a closer look at robust anonymization[65] techniques, so that the information stored on the private channel is irreversibly dissociated from the end user once the regulatory deadlines to this end have been met. In the same way, the address of the users, especially important

[65] Spanish Data Protection Agency (2019): "Introduction to the hash as a personal data pseudonymization technique". https://www.aepd.es/sites/default/ files/2020-05/estudio-hash-anonimidad.pdf

for the operation of transactions with token-based digital money, should be analysed to apply measures that prevent inferring information from users by parties that are no longer authorised on the private channel. In any case, the tests carried out to date make it possible to assert that the Red-i network is capable of considerably reducing the risk of re-identification, without being an anonymous network.

From a technological point of view, anonymity would mean that the solutions were executed at the device level. This, in addition to causing security risks beyond the control of the entity (and difficulty in identifying suspicious transactions), would in any case require the device to go online with a predetermined frequency to update the back-end infrastructure in order to maintain control of digital money in circulation, distribution by type of user, as well as limits on the holdership and/or the interest owed which would result in the network not being completely anonymous.

The foregoing does not prevent the provisions of Regulation 2016/679 for the protection of natural persons with regard to the processing of personal data and free circulation of the data (hereinafter, "GDPR") and Organic Law 3/2018 on Personal Data protection and the digital rights guarantee continues to apply. The GDPR establishes in its article 25 the need to consider privacy requirements from the first stages of the design of products and services. This means using, as from the design stage, a risk management-oriented approach and proactive responsibility to establish strategies that incorporate the protection of privacy throughout the entire life of the process (whether this is a system, product, service or software). Identifying, a priori, the possible risks to the rights and freedoms of the interested parties and minimizing them so that they do not materialize in damages is an obligatory task within the framework of the design of the digital euro, its infrastructure and its operations.

C18: The scalability and technical performance of the Red-i network is satisfactory:

Firstly, it should be mentioned that although the technology used in the Smart Money initiative has been Hyperledger Besu, there is nothing to prevent in the development and possible launch of the initiative from evaluating other alternatives that allow the enhancement of the functionalities designed, their scalability and performance.

After the tests carried out, it can be concluded that the digital money transaction processing rate may be much higher than the rate of transactions per second (TPS) allowed by the blockchain network. This is because in the service layer (back end), tried and tested traditional techniques can be applied to optimise transactionality, such as batch transaction processing, the parallel sending of transactions, the asynchronous response to end clients, among others, that allow the mass processing of payments and other types of operations. Additionally, the characteristics of the blockchain network can be configured to support high volumes of incoming transactions, including the configuration of the issuance time of the blocks, the maximum number of transactions for each block, the size of the pending transaction queue, etc.

In order to optimise performance, it might be useful to look more closely at a possible solution design geared towards batching operations. In this context, digital money transactions could be executed in real-time in an off-chain manner (in other words, without carrying out transactions on the blockchain network), grouping and subsequently sending all transactions in batches to the network. With this approach, theoretically, the performance of the system could be increased, since it would reduce the response time of each individual operation, since these do not involve the execution of transactions in real-time. Hence, starting from a theoretical exercise, it is estimated that the Red-i network could achieve metrics of over 10,000 payments per second. However, in order to design a solution in real production, a more detailed analysis is required, as well as performance tests that support these theoretical calculations.

C19: The Red-i network optimises the consumption of energy resources compared to other possible designs based on "Proof of work":

The Red-i network optimises the consumption of energy resources in comparison with some very popular cryptocurrencies, since it uses the "Proof of authority" type consensus protocol where the issuance of new blocks is based on the signature of the validating nodes (authorities) and on the exchange of messages between these nodes. In this way, it is possible to avoid less efficient protocols from an energy point of view such as the one known as "Proof of work", used by many of the best-known cryptocurrencies and whose electricity consumption has been valued by some studies[66] at between 52 and 111 Tw/h (exacerbated by using non-renewable energy sources). In actual fact, this year the crypto industry is expected to use 0.6% of the world's electricity production, which would exceed the annual consumption of countries like Norway, according to the University of Cambridge Bitcoin Electricity Consumption Index.

C20: Digital currency has the potential to compete with the supply of private cryptocurrencies used as means of payment:

As outlined throughout the report, the supply of cryptocurrencies is currently attaining its highest levels, with different types of issues associated with different projects or intentions. In this context, any potential digital euro would come into competition with private cryptocurrency services and functionalities which have a major added value associated with consumption and communication platforms (for example, compared with Facebook Diem).

In light of all the above, the digital euro has the backing and solidity of the central bank as the issuer and guarantor of the funds issued, besides being a currency which is legal tender, known and accepted by the majority of the population. Notwithstanding, a possible digital euro also needs functionalities which lend added value with regard to the current scenario and, as has been set out above, they are yet to be defined.

[66] Rauchs, M; Blandin, A; Klein, K; Pieters, G; Recanatina, M and Zhang, B (2018): "2nd global cryptoasset benchmarking study". University of Cambridge. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset- benchmark-study/#.YK5ugKgzaUk

4

Possible impact of a digital euro on the financial sector

Owing to the technical characteristics and the economic and legal implications, the digital euro appears as an instrument which requires careful study about its impact on the financial sector. The authorities responsible for its implementation must weigh up its possible negative effects so that it truly is an element that stimulates the financial market in accordance with the current digital revolution, demonstrates its security and protects the interest of citizens. This section sets out some of the possible effects of the digital euro on the financial sector.

4.1. Impact on bank deposits and on credit intermediation

Historically, the banking sector has acted as an intermediary between savers and investors. As a result, the credit creation has allowed the financing of major projects which, individually, would have been impossible to carry out.

At present, this activity is still one of the cornerstones of the banking business model and it entails an important reflection on the development and state of the economy in a given context at a given time.

As has been set out during the course of this report, the digital euro could be designed in different forms taking into account variables such as technology, distribution and its intrinsic characteristics. In this regard, it is essential for the digital euro to be designed to serve as a means of payment and not as a saving or investment instrument, in order to avoid any significant outgoings from deposits of commercial banks to the digital euro which could affect the lending capacity of the banking sector, impact the operation of the liquidity coverage ratio or affect the transmission of monetary policy.

In line with the above, it would be reasonable for the design to be based on a two-tier or hybrid model. It would also be necessary to have appropriate mechanisms for managing both the quantity of digital euros in circulation, as well as the limits on individual holdings or, should it be necessary, staggered remuneration (with penalty rates above a certain threshold). However, there is still no consensus about the suitability of using any of these mechanisms, as is particularly the case of remuneration.

First and foremost, concerning the form of distribution, if the ECB opts for the two-tier model, the presence of intermediaries in the system would be maintained and the digital euro would have a lesser impact for the application of PML-FT measures and KYC processes. As in the direct distribution model, if control mechanisms are not introduced, there would be a risk of flight of retail deposits in the form of digital euros, particularly in situations of stress or financial crisis. In the event of uncertainty about the sustainability of the banking system, the digital euro could be seen as a safe haven. Its digital characteristics will allow the mass movement of capital in real time, destabilising and prejudicing the solvency and liquidity of the private sector. Following the same line, the replacement of deposits could give rise to an increase in the financing costs of the banks and, accordingly, of the interest rates on bank loans which, in turn, could reduce the volume of bank credit in the economy.

As has been explained during the course of this report, although it is technically possible to implement control mechanisms on limits and remuneration or penalties in line with the digital currency thresholds that each user[67] has, it is still necessary to carefully analyse their effects and suitability in terms of mitigating any possible negative effects commented on previously. However, the innovation of the digital euro entails the need to analyse

[67] Op. Cit. (31)

the intrinsic risk in its modus operandi, updating the working systems and methodologies to adapt them to the digital euro.

Basically, it is a matter of preventing the digital euro from becoming a store of value which competes on an unequal footing with the private options of the market.

As regards the inclusion of an interest rate or rate of return, and although for the time being it remains as a merely theoretical aspect for study, there are still no clear conclusions about the effectiveness of this tool in a banking crisis scenario.

One of the reasons for establishing the accrual of an interest rate for the digital euro lies in the possibility of having a new instrument for applying monetary policy[68]. Using this instrument, the quantity of digital euros in the economy could be regulated, with its attendant impact on saving and consumption. However, the advantages or the need for a digital euro as an instrument of monetary policy[69] are not yet clear. Other publications in this regard have concluded that monetary policy could work in a manner similar to present policy, by means of relevant variations in the quantity, and that the transmission of the latter could even be increased[70].

As regards the effects on the deposits system, the accrual of interest by the digital euro would compete directly with public and private financial products. From the public perspective, the remunerated digital euro could be seen as a competitor with sovereign bonds issued for the financing of States[71].

Furthermore, the private sector would have to compete with the offer of the Eurosystem regarding the return on capital. The most likely consequences would be more expensive credit and a reduction in the liquidity of financial entities.

Basically, the key to avoiding any deterioration in the financial system after the arrival of the digital euro entails the limitation of the effects of disintermediation it could cause, becoming integrated within private initiatives that promote competition and innovation in the financial sector.

4.2. Impact on the payments system, means of payments and on cash distribution

The development of the digital euro may promote the modernisation of current payment systems and means of payment, and cut costs in the distribution and management of cash. In the current context, the appearance of new devices and payments applications, as well as payment facilities in businesses, have enabled increasingly faster, more automatic and simpler payments, in recent decades.

The future of the euro is inevitably linked to citizens' habits and this is why its design and format must be adapted to the new forms of payment used.

When examining the effect that the issuance of a digital euro could have on cash distribution, it is worth noting that its use is probably going to be reduced. This would entail a lower amount of cash in circulation and, in the long-term, it could result in a reduction of its distribution and management costs in the system. It is worth stressing that the forecast reduction in cash in circulation will occur insofar as there is a certain similarity between the

[68] Keister, T and Sanches, D (2019): "Should Central Banks Issue Digital Currency?". Federal Reserve Bank of Philadelphia. https://www.philadelphiafed.org/consumer-finance/ payment-systems/should-central-banks-issue-digital-currency

[69] Agustin Carstens (BIS) (2021): " Central banks today do not need to issue a CBDC for monetary policy reasons. Nevertheless, a CBDC would affect the transmission and implementation of monetary policy. It would affect the interaction with commercial banks and their reserve holdings, the monetary base and the transactional demand for money. These effects should be studied carefully. These effects should be studied carefully." https://www.bis.org/speeches/sp210331.pdf

[70] Meaning, J; Dyson, B; Barker, J and Clayton, E (2018): "Broadening narrow money: monetary policy with a central bank digital currency", Bank of England Staff Working Paper no. 724. https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2G18/ broadening-narrow-money-monetary-policy-with-a-central-bank-digital-currency.pdf?la =en&hash=26851CF9F5C49C9CDBA95561581 EF8B4A8AFFA52

[71] Yanagawa, N and Yamaoka, H (2019): "Digital Innovation, Data Revolution and Central Bank Digital Currency". Working Paper Series, Bank of Japan. https://www.boj.or.jp/ en/research/wps_rev/wps_2G19/wp19eG2.htm/ Danmarks Nationalbank (2017): "Central bank digital currency in Denmark?". https://www.nationalbanken.dk/en/publications/Documents/2017/12/ Analysis%20-%20Central%20bank%20digital%20currency%20in%20Denmark.pdf

characteristics of the digital euro and cash. In any case, the ECB has expressed its intention to issue a digital euro as a form of money complementing the current forms and not as a replacement.

As regards the effects on payment systems, we need to highlight, first and foremost, that the creation of new means of payment entails long processes to develop commercial rules and standards, and investments to implement the solution, market it and enable it to reach a critical mass of users.

Also, the possibility of incorporating programmable functionality into the digital euro has been proposed[72]. This characteristic (controlled by the entities in the context of the PoC) could be particularly useful in large-scale, cross-border automatic payments, as well as those payments carried out with the administration and public services, such as the payment of taxes, charges or receipts by the Public Administration (execution of transfers which depend on compliance with certain conditions).

Furthermore, a digital euro would in effect become a new means of digital payment which, depending on its design, would compete with and could displace private initiatives in this regard. It is important for the digital euro to be integrated and interoperable with current payment systems and means of payment.. The innovation of this means must be in harmony with the current architecture so as not to cause unnecessary changes and to avoid duplications in the management of capital flows in the Eurosystem.

The ideal integration would require the use of the same industrial standards, payment solutions and channels which are used for commercial bank money, in order to guarantee the interchangeability and interoperability of the digital currency.

With a view to improving the time to market for new payment solutions, such as digital currency, present infrastructures, networks and standards could be reused, at least partially. It would be necessary to carry out a detailed analysis here, as the reuse of components and the efficiency with which the new means of payment develops, should not diminish the possibility of being used as an alternative or contingency solution in the event of incidents in current payment systems.

In general, payment systems could be affected by innovative design options regarding the digital euro and its form of management by users. With this in mind, both current payment systems and private solutions offered by entities should be aligned with the new standards and systems.

4.3. Other aspects to be borne in mind

4.3.1. Personal data protection

The protection of privacy has been identified as one of the characteristics most highly rated by citizens and professionals in the public consultation concerning the digital euro.

Compliance with personal data protection regulations means matching the design of the digital euro with the guarantee of the rights of individuals throughout the development process (in line with the principle of privacy in terms of design). With this in mind, it is vital to define at least the following aspects:

[72] Op. Cit (24)

- **Functionalities and operability of the digital euro:** the definition of the operating outlines of a potential digital euro is vital in order to identify the personal data involved in its operation, in other words, the data required for direct or indirect identification of an end user. For example, the use of the digital euro to make payments directly impacts data like the IBAN, address and identification of the payer or beneficiary, etc., which will foreseeably be necessary to enable its functionality. And their processing must comply with the provisions of the GDPR. In the same way, the development of a digital banking identity requires a thorough analysis of its operation and of the data involved.

- **Operational scope**: the possibility of carrying out, for example, cross-border transactions outside the Eurozone involves considering the provisions regarding international data transfers in the context of the digital euro.

- **Parties involved in the operations:** identification of the natural or legal persons who will have access to the personal data of users and who will be regarded as data controllers, co-controllers and processors. It is important to analyse the whole functionality, case practice and tiers of digital euro operation, with a view to properly identifying the roles applicable in each case and establishing a tier of governance in this regard, particularly if a decentralised system is involved. In this regard, it is foreseeable that measures and agreements should be applied which are similar to those already in place in the payments sector to ensure compliance with the GDPR.

- **Technology deployed:** intimately linked to all the previous issues is selection of the technology deployed to implement the digital euro. Although no decision seems to have been taken yet in this regard, one of the alternatives proposed is to use DLT technology, to be precise, Blockchain technology. The use of this technology requires an assessment, in the context of an impact evaluation for data protection, the need for and proportionality of its use compared with other possible alternatives and the additional risks introduced by its own definition and design. The type of network and governance, the distribution of roles and responsibilities, the security levels, the management of obsolescence time (particularly relevant in cryptographic terms to ensure data anonymization), the exercising of the rights of stakeholders or the data storage time are issues which will need to be carefully studied.

Furthermore, the decentralised, traceable and immutable nature of Blockchain may generate some difficulties in terms of compliance with some principles or the exercising of some rights.

The design of the system developed in the Smart Money initiative has taken into account, within the scope of the PoC, compliance with data protection principles. In this regard, the PoC has been based on a design focused on the use of those data key to ensuring the smooth operation and security of the system, though it is still necessary to expand those measures that allow the maximum possible reduction in the risks identified in the points above (see C17). In this way, the data visible to each of the parties involved are those shown in the table below:

Information visible in the context of the PoC		
Party	**Information visible**	**Possible mitigating measures**
Iberpay and Banco de España	Pseudonymous data (address, balances and hashes[73] of certain parameters of a transaction)	Absence of identifiers and/or pseudo-identifiers associated with the hash, separation and securitisation of additional information which will allow the assignment of personal data to a specific person. The visible information and applicable measures could vary in line with the final design proposed as well as the degree of supervision required in each case (for example, automatic reporting).
Entities (private channel)	Transaction data (source, destination, amount), hash of certain parameters of the transaction and their respective association with the client of the entity (the latter information on a separate database)	Storage of personal data outside the private channel. In the event of the exercising of the right of erasure of any references/hashes registered on the private channel which could be regarded as personal information, anonymisation mechanisms are applied, eliminating any personal data related with the hashes. These references/hashes could, in turn, combine hash and encryption techniques to prevent brute-force[74] attacks or subsequent re-identification. Absence of identifiers and/or pseudo-identifiers associated with the hashes.
Entities (public channel)	Hash of a hash of certain parameters of a transaction	Storage of personal data outside the private channel. In the event of the exercising of the right of erasure of any references/hashes registered on the private channel which could be regarded as personal information, anonymisation mechanisms are applied, eliminating any personal data related with the hashes. These references/hashes could, in turn, combine hash and encryption techniques to prevent brute-force attacks or subsequent re-identification. Absence of identifiers and/or pseudo-identifiers associated with the hashes.

However, article 32 of the GDPR determines that the appropriate technical and organisational measures are defined to ensure the appropriate security level for the risk involved, in line with: the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

In other words, static measures are not established when ensuring the privacy of a system and, accordingly, guaranteeing the rights and freedoms of natural persons and it is thus necessary to know the specific context and final functionalities of any potential digital euro in order to apply the appropriate measures in each case.

What's more, the data controller will be responsible for determining those measures required to ensure the confidentiality, integrity and availability of personal data.

In addition, having procedures which allow period risk assessment to keep it at minimum levels throughout the data life cycle is a crucial task in the context of the implementation of the digital euro. This objective is intimately linked to the definition and implementation of procedures for exercising data protection rights, lodging claims or revoking the consents provided by the stakeholders, as well as mechanisms to ensure, by the data controller, the evaluation of compliance and the effectiveness of the obligations determined for it by the regulations, which contributes to respecting the principles of proactive responsibility and accuracy set out in the GDPR.

All the previous points permit the setting out of an initial approach capable of combining the protection of the rights of individuals and the implementation of an innovative system like the digital euro.

[73] A hash function is a one-way process which transforms any arbitrary set of data into a new series of characters with a fixed length, regardless of the size of the input data. The result obtained is called a hash, summary, digest or image.
[74] Op. Cit (57)

4.3.2. Prevention of money laundering and the financing of terrorism

The application of PML-FT measures provides for the maintenance of the solidity, integrity and stability of the financial and credit entities, as well as trust in the financial system as a whole. Their application requires coordination, not only nationally, but also at the level of the European Union and internationally.

To apply this type of measures, it is necessary to provide to financial entities with mechanisms which allow identification of their clients, application of due diligence measures, obtaining of information about suspicious activities, storage of records or notification to the authorities. These mechanisms can also be transferred to the context of the digital euro in which compliance with PML-FT regulations requires a certain level of auditability.

The existence of auditability, besides being possible in any technological system, is compatible with the application of personal data protection regulations. In actual fact, both Directive 2015/849 and Law 28/2010 make reference to the application of regulations concerning personal data protection in the context of PML-FT. In turn, the GDPR indicates that the need to comply with a legal obligation applicable to the data controller constitutes one of the legitimate bases for personal data processing.

Although the digital euro can reproduce many of the advantages of cash, the complete comparison of both currencies can generate certain risks as it could involve, besides the technological challenges and depending on its final design, the creation of an anonymous instrument difficult to trace.

Anonymity is inherent to the nature of physical money: the level of privacy that cash can attain is unparalleled and it is perhaps one of the purest examples of a fungible asset. This is why the fight against financial crime has been facing the “problem of anonymity” for some time now. If the CBDCs have to reproduce a similar situation, concurrently overcoming the material limitations, major issues may arise.

It should not be forgotten that there are privacy mechanisms which fluctuate within a gradual range of possibilities. Although absolute anonymization would generate major challenges in the application of PML-FT measures, pseudonymization, the use of encryption or the application of specific traceability measures may prove useful in a digital euro model in which privacy and auditability are compatible.

With this in mind, the most appropriate system would be the hybrid or intermediated two-tier system, not only because the financial entities already have mechanisms and experience in this field (which would result in lower implementation costs), but also because it would be possible to attain greater capillarity compared with a direct model. As the digital euro model is being defined, we will need to focus on new hotbeds of crime and, foreseeably, apply the majority of the mechanisms already in place to detect unlawful activities.

4.3.3. Cybersecurity

The issuance and distribution of digital euros entails, at the very least, the same risks as those which affect the current means of payment such as bank accounts or cards.

It is also possible to identify other risks such as:

- The actual security of the network, which must be adapted to security and data protection standards in a uniform and complete manner.

- The security of the nodes or access points of each of the entities involved in the network management process.

To mitigate the previous risks, it would be necessary to extend the cyber resilience standards of the infrastructures of the financial markets to the new platform, considering cyber resilience in the design of the infrastructures and platforms, as well as including the technical and operating procedures to face cyber-attacks, which must include coordination between participants. In this context, a wallets model managed by regulated entities would allow the application of the new operational resilience directives and compliance with the outsourcing and cybersecurity guidelines. In addition, there are some risks and threats which have to be studied carefully in the context of the CBDC in general. Some of the short, medium and long-term risks have been set out below in the context of digital currency, from the perspective of security:

- Risk regarding the control of access to information by users: during the course of their activity, users must have the information they can access limited, in line with their role and the functionality specific to them.

- Risk of external attack on the network: there is the risk and the threat of suffering an attack by external elements who are seeking to destabilise the network along with the capture of certain data of an extremely sensitive nature.

- Risk of network collapse: for example, when exceeding a given volume of transactions.

4.3.4. Financing of the necessary investment

To determine the investment required to implement the initiative, it is important to separate the investment that the ECB should undertake, the investment in sectoral infrastructure, the investment made by commercial banks and companies and administrations for their adaptation. The smooth development of the project largely depends on the perspectives about its cost and the resources available for its financing.

The forecast cost and planning of the project is essential, not only to evaluate any possible impacts analysed in this regard, but also by dint of the reputational risk assumed by the Eurosystem in undertaking this project. An exaggerated excess cost or an erroneous diagnosis of the impact on the parties involved or on the system could be particularly negative for the reputation and trust in the body. In actual fact, some publications question CBDC's option in some regions owing to the cost[75] of its development and implementation.

Although the final cost shall depend on the final model and the associated times, there are elements common to all the alternatives which may allow the necessary investment level to be estimated as high.

First and foremost, the need for the adaptation and/or development of new interfaces and connectors both with the users as well as with the infrastructures is an aspect that needs to be borne in mind whatever the scenario. Although the adaptation is expected to be progressive, it will also be necessary to develop standards, appropriate compliance mechanisms, control and cybersecurity systems or developments in current payments solutions to accept payments in digital currency, not only for individuals, but also for companies of all types. This latter aspect is particularly important, as it cuts across the whole industry in view of the fact that all terminals should adapt to a same standard in order to be able to receive payments in the form of digital euros.

The implementation of a project of this scale also requires investment in technological training, change management, communication and marketing, as well as the devising of potential new market strategies, amongst many other aspects. However, even taking into account the economic effort entailed by the development and implementation of a CBDC, during the course of this document it has also been set out how it could facilitate the saving of resources and an improvement in the current monetary system. Although it is true that the initial

[75] Cámara, N; Dos Santos, E; Grippa, F; Sebastian, J; Soto, F and Varela, C (2018): "Central bank digital currencies: An assessment of their adoption in Latin America". BBVA. https://www.bbvaresearch.com/en/publicaciones/central-bank-digital-currencies-an-assessment-of-their-adoption-in-latin-america/

investment and cost of simultaneously maintaining cash and digital currency entails an effort, in the long-term it could considerably reduce the expenses incurred for its production, distribution, follow-up and control.

In this regard, analysing the projects and trials of other central banks, those in which the private sector participates stand out for their high rate of development, both through direct financing or through the actual design and planning of the CBDC. The distribution of costs, a better adaptation to the market and the knowledge and approximation to the needs of the end user ensure greater probabilities of success and cost reduction. This is demonstrated, for example, by the pilot scheme developed in China in which payments and communications services companies have taken part, or the project by the Central Bank of the Bahamas which has private financing and partners[76].

At each of the levels of the financial sector, costs and their financing encounter different challenges and opportunities. The ECB would bear the main expenses incurred for the development and definition of the digital euro and it would play an essential role when defining its distribution. The economic effort entails a major investment in specialised IT staff and development, the acquisition of technological infrastructure, software and administration services and project strategy, among others[77].

Furthermore, the sectoral intermediaries will have to adapt their current infrastructure to the new requirements of the central bank. The progressive adoption of the TARGET2 system by different countries may be illustrative when weighing up the risk and costs of these changes.

Finally, commercial banks and other financial agents which participate in the distribution of the digital euro should adjust their operations to this new product, with regard to business model and strategy. What's more, a drive to educate clients to get to know this product and the consequences of its acquisition is also foreseeable. Commercial banks could take as a reference the transformation processes such as that deriving from the PSD2 directive. The legislative change affected the data management technology of banks and it has entailed increased competitiveness with so-called "open banking". As has been described in this chapter, the design of the digital euro must, in any case, avoid any possible negative effects of its issuance on the stability of the European financial system.

The financing of these projects could come from different sources from each of the participants, which may be public or private. From an institutional perspective, it is worth mentioning the so-called Multiannual Financial Framework (MFF) of the EU, projected until 2027 and the NextGeneration EU funds created to mitigate the consequences of Covid-19. Both instruments have available a budget of 143.4 billion euros[78] to improve the single market, innovation and the digital economy which could be used both by large companies and by SMEs to adapt to the digital euro, providing support which could wholly transform the economy of European countries.

The awarding of this type of funds is led by the European Commission which publishes notices of convening and programmes on specific themes. Participation in them is preceded by compliance with the legal and financial requirements and the process usually consists of one or two stages in line with the technical difficulty and the number of proposals. Studying it would be particularly positive in terms of the interoperability and optimisation of developments[79].

Finally, for the sectoral intermediaries and commercial banks there may be specific financing alternatives from the ECB. Loans for the development and adjustment of business models and systems which adopt the digital euro could entail a minimum cost to promote transformation. Another option could consist in establishing a remuneration by the monetary authority per transaction or for the volume operated on the network which would allow the recovery of the investment made.

[76] Sand Dollar: "Key players". https://www.sanddollar.bs/keyplayers
[77] Kiff, J; Alwazir, J; Davidovic, S; Huertas, G; Khan, A; Khionarong, T; Malaika, M; Monroe, H; Sugimoto, N; Tourpe, H and Zhou, P (2020): "A Survey of Research on Retail Central Bank Digital Currency". IMF.
[78] European Commission "Recovery plan for Europe" https://ec.europa.eu/info/ strategy/recovery-plan-europe_es
[79] European Commission: "Financing, tenders". https://ec.europa.eu/info/funding- tenders_es

5

ANNEX

Technological issues

5.1. Network architecture

The Red-i network is a DLT network based on Hyperledger Besu technology which has been deployed as a permissioned Blockchain comprising a total of seventeen nodes for participating financial institutions and five additional nodes for Iberpay and Banco de España. Hence, seventeen of them are used to carry out the activity of the financial entities and the end users, three are assigned to Iberpay as the network manager and the last two nodes are reserved for Banco de España, in its role as an observer. These nodes are hosted at instances of the Amazon cloud ("AWS").

Although the technology selected for these tests has been Hyperledger Besu, there is nothing to prevent, during the evolution and possible production start-up of the initiative, the assessment of other alternatives that allow the full potential of the functionalities designed to be exploited.

Hyperledger Besu allows private transactions to be undertaken, ensuring the confidentiality of the information. This type of transactions is processed on private channels on which only a set of authorised participants can view the transactions carried out, such as the distribution or transfer of digital money or the balances available. Iberpay and Banco de España also have access to the transactions (though they do access the data of the person who carries them out) as they take part in all the private channels. The private information resides in a component called Orion which is a transactions manager and it acts as a information repository. Each participant has its own Orion component where the private information to which it has access resides.

As regards the consensus algorithm, the Red-i network implements the consensus protocol IBFT 2.0 Proof-of-Authority (PoA). On IBFT 2.0 networks, the approved accounts, known as validators, validate the transactions and the blocks. The validators take turns to create the next block. Before inserting the block on the chain, a majority (greater than 66%) of the validators must sign the block. The existing validators propose and vote to add or eliminate validators. To add or eliminate a validator, the majority vote (> 50%) of the existing validators is required.

At present, the network is deployed on cloud environments. To be precise, the information systems belonging to each entity, Iberpay and Banco de España (applications' servers, Hyperledger Besu nodes, Orion, databases, among others) are deployed at independent cloud instances. The communication between participants is carried out by means of the protocols HTTPS, TCP and UDP. What's more, only those ports and IPs which are strictly necessary for the smooth functioning of the platform are enabled.

The Red-i network is for the exclusive use of the participants designated in the initiative, to which end it incorporates control mechanisms for the addition of new nodes, as well as to manage permissions to write on the Blockchain (block validation permissions) and other improvements to the management and monitoring of the transactions on the network.

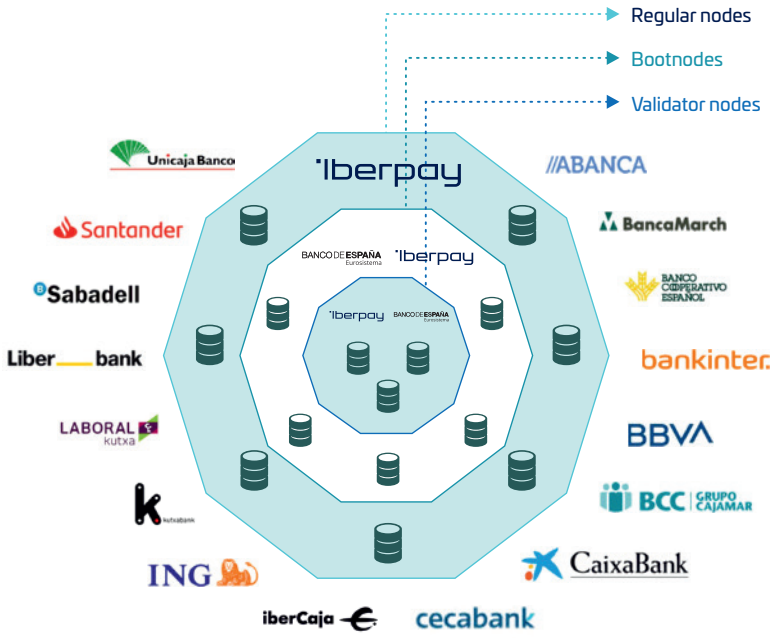
The main advantages of Hyperledger Besu technology and, hence, of the present Red-i network, are the following:

- Higher rate of transactions per second (TPS): the Ethereum networks with Hyperledger Besu technology afford one of the greatest TPS ratios in the current context of Ethereum technologies, by using the consensus algorithm IBFT2.0. In addition, it affords numerous infrastructure optimisation options that go from the configuration of the consensus algorithm to the personalisation of the resources used by the nodes implementation environment.

- Wider community and official support: Hyperledger Besu is an open source project with a considerable community of developers. What's more, the software is maintained and improved by Pegasys and other reference companies in the sector which offer official technical support.

The Red-i network is endowed with multitier architecture geared towards improving scalability and performance. In this design there are three types of nodes with different roles in the architecture.

Simplified topology of the Red-i network



Source: own elaboration

Simplified topology of the Red-i network

- Regular: nodes of the financial institutions. They have permissions to read on the blockchain and they interact with the external applications.

- Validators: Iberpay and Banco de España nodes. They have permissions to write, being exclusively dedicated to block validation and issuance.

- Bootnodes: Iberpay nodes. These are light nodes which maintain a list of existing peers to communicate it to new members.

Each entity also has a front-end or graphic interface, a back end responsible for the business logic (it receives the requests that are made from the user interface, it carries out the transactions on blockchain and manages the logs of the application), a database and a blockchain node.

The entities use the front end to control the transfers made by their clients. They can also carry out requests for the issuance and redemption of digital money which modify the funds of the entity on the blockchain network.

Furthermore, the back end processes all the client requests of the entity. There is direct communication with all the components of the architecture, including the database and the Hyperledger Besu nodes. Its main functions include that of sending transactions to blockchain to request or distribute digital money, introducing into blockchain the transactions signed by the clients of the entity in operations with tokens, storing and consulting information about the transactions on the database, among others.

Finally, a mobile application has been designed to be used by the clients of the entity (simulated for the PoC) compatible with Android and iOS devices.

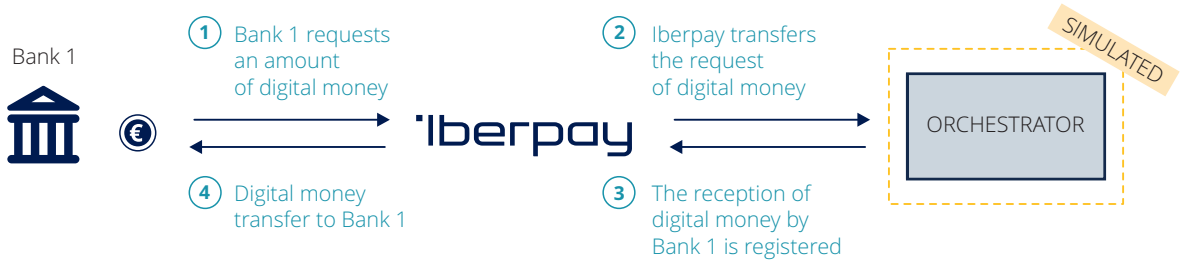
5.2. Operations on the network: user's experience

a. Distribution of digital money to the entities

The Smart Money initiative can be divided up into three major milestones. The first has to do with the movements which occur between the entities and Iberpay to request and return digital money. As explained in the illustration below, an environment has been simulated in which Iberpay transfers digital money requests by the banks and receives authorisation for their distribution amongst the entities.

The entities may also, where applicable, return digital money amounts, where necessary, using the same operation.

Requesting digital euros



Source: own elaboration

As regards the web interface developed for the entities, it is worth pointing out that they can view both the requests/returns of digital money carried out by the entity itself (either token-based or account-based) as well as the digital money requests/returns/transactions of their clients, in the same form in which it is currently possible to view the current account transactions of their clients.

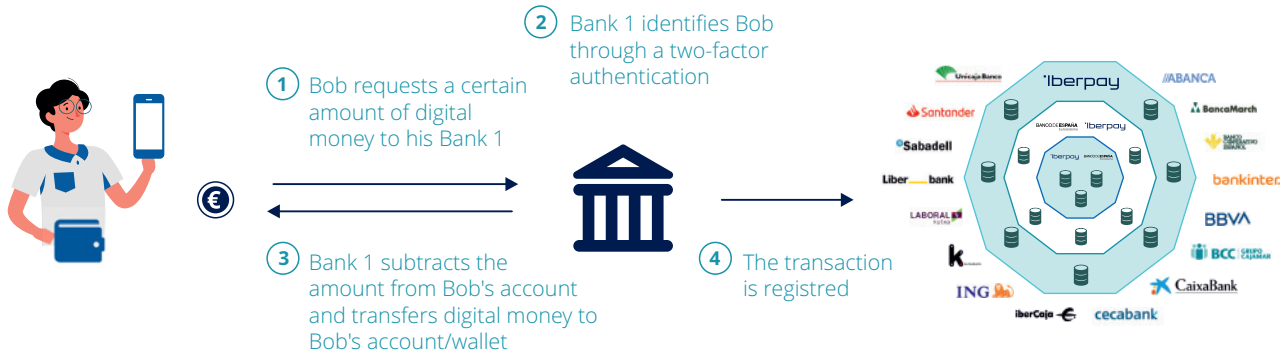
b. Distribution of digital money to the end users

The second milestone of the Smart Money project develops the modus operandi between entities and their clients. In this regard, the project has been designed based on a prior identification of the client by the attendant financial institution, via the usual channels. In this way, only the clients of duly identified entities holding a current account at the entity may access a digital money account and/or wallet which must be requested by the client from the entity via the channels established by the latter. Upon creation of the digital money account or wallet, a digital identity will also be created for the client.

Although the Smart Money initiative has not expanded on the development of a digital identity for these tests, its future development is particularly relevant owing to the need to identify clients on the network. With the Smart Money initiative, a technologically agnostic digital identification tier has been created, compatible with any sectoral solution for sovereign, decentralised digital identity which may be developed in the future.

Once the digital money account/wallet has been obtained (and the associated Ethereum ID), the client may request from their bank the amount of digital money they desire, respecting the maximum limit set by default through the attendant mobile application. As occurs with other transactions, the identification of the client at the time of the request will occur by means of two-factor authentication in line with the PSD2 Directive. The effect of this request on the client's current account will be the same as would occur if the latter had obtained money in cash, as illustrated below:

Requesting digital money

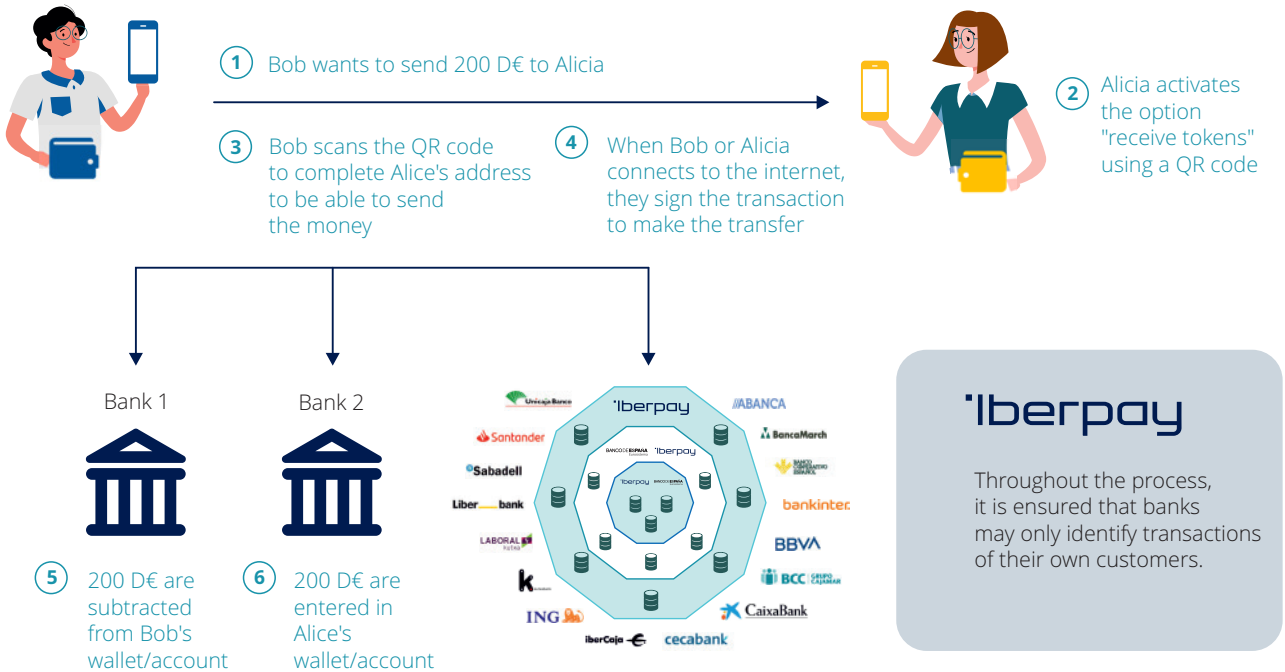


Source: own elaboration

c. Movements between end users

Finally, the third milestone pertains to the transmission of digital money between private individuals, either online or offline. In an online context, the modus operandi is simple in terms of user experience. The latter would use their mobile application to carry out a transfer to another private individual in the same way as currently occurs with bank money, except that this transaction is logged on the private channel of the entity and Iberpay (see section b. for further detail). From the offline perspective, the operation in accordance with the scheme is set out below:

Sending digital money offline



Iberpay

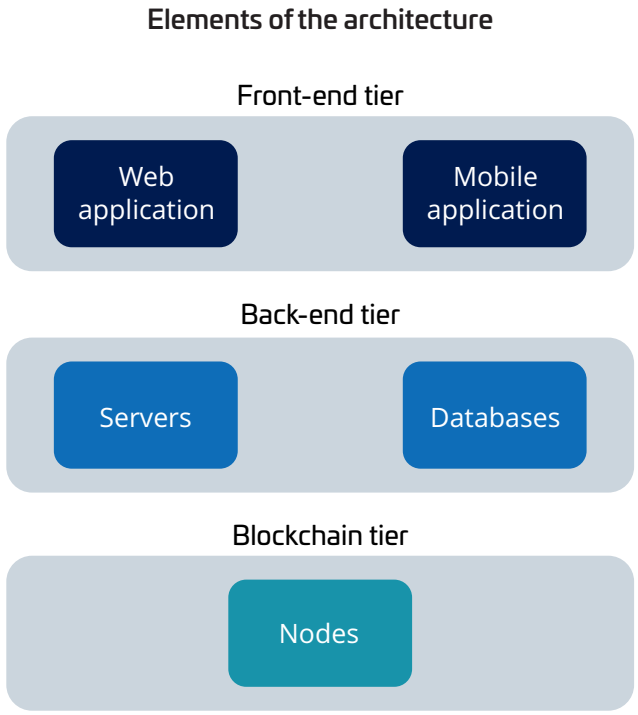
Throughout the process, it is ensured that banks may only identify transactions of their own customers.

Source: own elaboration

5.3. Intrinsic operation of the network

a. Components of the architecture

The technological architecture of the Smart Money solution can be divided into three tiers:



Source: own elaboration

- **Front-end tier.** This consists of user interfaces, used by the end clients and operators of the entities to trade with digital money. These interfaces (there is one for each entity) are: 1) the web system of the entity for managing the digital money and 2) the mobile application of the end clients. Both interfaces receive the interactions of the clients and send requests to the back-end tier for their subsequent processing.

  The web system of the entities allows their staff to view the movements of the end clients, as well as to manage the liquidity in digital euros of the entity, requesting the issuance and redemption of digital money, both token-based and account-based.

  Furthermore, the mobile application is used by the end clients and, within the scope of the PoC, it simulates the app of a banking entity whereby the clients can view and use their digital money. To be precise, clients can convert bank money to token-based or account-based digital money (and vice versa), make payments online and, in the case of tokens, also payments offline, as well as viewing their balances and movements.

The mobile application hosts the token-based digital money wallet of the client. In other words, it securely saves the private key used by the end client to sign transactions which, in turn, transfer money from the client to other beneficiary accounts via the Red-i network. Furthermore, it allows access to the account-based digital money account in an account stored in the back end of its entity, as it is the latter which manages the client's account.

- **Back-end tier.** The back-end tier is made up of an applications server and the database of the entity. The applications server receives all the requests sent by the front-end tier and so it is the point of entry of the modus operandi to the system. Its main functions consist of: 1) receiving and validating requests from users (operators and end clients), 2) generating and sending to the blockchain network transactions, to carry out the various transactions requested by the users and 3) updating the database where the information of the clients of the entities is stored, as well as their balances and movements, etc.

  On the other hand, the database saves the information that reflects the digital money transactions of the clients of the entity carried out on the Red-i network. In this way, logging of the movements made on the network is facilitated, for their subsequent presentation on the front-end tier, as well as data aggregations about the monthly expenses of clients, the number of transactions carried out by an entity, etc.

- **Blockchain tier.** This last tier consists of the blockchain nodes and the managers of private transactions, in this case implemented through Orion servers. The Blockchain nodes, whose technology is Hyperledger Besu, communicate peer-to-peer (P2P)[80] to form the blockchain network. The blockchain network stores the smart contracts which, in turn, save the digital money balances of clients and implement the business logic to operate this money. The blockchain network is permissioned and so only authorised participants can access it.

The contracts are based on the fungible tokens standard ERC20. They thus contain the functionalities of mint (issuance), burn (redemption) and transfer, respectively. Furthermore, the contracts have additional functions needed to manage the digital money balance limits of the clients and the payments of remuneration to clients and entities.

The digital money balances of the clients are recorded in these smart contracts. To be precise, in the contracts the Ethereum account or address of a client is associated with its current balance. The contracts are programmed so that only the client who owns the funds can transfer their digital money to other accounts.

All the transactions involved in the transactions with digital money are private. With this in mind, a private channels system of Hyperledger Besu has been designed which allows each entity to have access to the transactions related with its own funds or those of its clients.There is one private channel for each entity which includes Iberpay and the Banco de España. In the case of interbank payments, Iberpay carries out intermediation between the channels, moving the funds from one private channel to another. It is worth pointing out that other private channel designs may be adopted in which several entities take part.

b. Processing of transactions

In the context of this project, clients and entities have two digital money accounts: one for token-based money and the other for account-based money. Each account consists of a pair of Ethereum keys which allows participants in the Red-i network to send transactions to the blockchain network which trigger the execution of the transactions allowed at any time.

In general, the processing of transactions in the Smart Money solution can be divided into three sections:

- The user must start a session in the system, then requesting the execution of a transaction, using its

[80] A peer-to-peer network, a network between equals or between peers (P2P) is a network of computers, some or all of whose features work without fixed clients or servers, but rather a series of nodes that behave as equals between each other.

user interface. In the case of end clients, once they have been identified using two-factor authentication, they can obtain, return or transfer digital money from the mobile application, whilst the operator of the entity can make the digital money issuance or redemption request using the web system of the entity.

- The interface sends the user request to the back end of the entity. The back end verifies that the user is duly authorised to carry out the transaction and processes it in accordance with the type of functionality. Irrespective of the type of transaction, at least one transaction may be carried out on the blockchain network which will modify the balances of the players involved in the operation.

- Once the movement has been completed, the back end will store information about the transaction status on a database for its subsequent consultation and viewing from the user interfaces. In addition, the back end can update the transaction status, should this have been completed asynchronously.

c. Types of transactions

There are five transactions for each type of digital money in which various participants are involved:

- **Issuance and redemption of digital money.** This is the process whereby the entity asks the orchestrator or simulator through Iberpay to add or eliminate digital money from its account. Iberpay receives these requests on the Red-i network, it passes them onto the orchestrator and increases or reduces the digital money associated with the entity's account after receiving the digital euros issued by the orchestrator (this modus operandi has currently been simulated through the figure of the orchestrator).

  To be precise, the user of the entity sends the request to the back end via the web interface. The back end, using the master wallet of the entity, generates a transaction on blockchain to ask Iberpay for digital money which, in turn, requests the issuance of digital euros from the orchestrator. This transaction generates an Ethereum event which is received by Iberpay, informing of the amount requested. Iberpay then sends a request to the simulated service of the Eurosystem which simulates the blocking or unblocking of funds in the entity's account with the central bank. Once an affirmative response has been received, Iberpay generates a new transaction to request the issuance or redemption of the digital money associated with the bank's account, its balance on blockchain thus being updated.

- **Obtain and return of digital money.** This consists of the conversion of bank money to token-based or account-based digital money and vice versa, for an end client of an entity. In this process, the balance of the current account of the client (simulated) is reduced or increased, inversely to its digital money balance registered on blockchain.

  In this operation, the client sends to the back end a request to obtain or return digital money using its mobile app. The back end uses the master wallet of the entity to generate a new transaction which transfers digital money from the entity's account to the client's account or vice versa. In addition, the back end adds a new movement to the database, recording this operation and updating the balance in euros of the client's current account.

- **Bank and interbank transfers.** This involves the implementation of payments between private individuals from the same entity or different entities, which transfer the digital money units between the accounts.

  Payments are started on the mobile app when the payer (client) enters the beneficiary's data and sends a request to the back end, indicating the metadata of the payment as well as the beneficiary's account and the amount. In the case of payments in token-based digital money, this request includes a blockchain transaction which is generated and signed by the mobile app itself, using the pair of Ethereum keys of the client.

Once the back end receives the request, it processes the transaction in a different way in line with the type of digital money. In the case of token-based digital money, it forwards to blockchain the transaction received from the client, whilst in the case of account-based money, it debits the client's account (stored on the database) and generates and signs a new transaction to carry out the transfer of funds which it finally sends to blockchain.

Under smart contracts, the implementation of payments works differently when involving payments between users of the same entity or different entities. When the payer and the beneficiary of a payment are from the same financial institution, the payment is made in a single transaction which deducts the units of digital money from the payer's account and increases them in the account of the party receiving the payment.

Furthermore, if the beneficiary belongs to an entity other than that of the payer, the smart contract cannot carry out an automatic transfer of funds owing to the fact that it does not know the balance of the beneficiary client, but rather of the payer. Hence, the contract shall issue an event which is received by Iberpay as manager of the interbank platform of Smart Money. Iberpay will carry out two additional transactions, concurrently, which are sent to the respective private channels of each entity: 1) one to deduct the transaction amount from the money balance of the payer client and 2) another to increase the balance of the beneficiary client. Each transaction shall issue an event that will be received by the respective back ends of the entities which will store on the database the data pertaining to the movement carried out, for their subsequent display on the interfaces.

It is worth pointing out that for all transactions, the back end carries out additional checks which have been omitted for the sake of clarity. There is a verification that the payer client is registered with the entity or checks that the client has not exceeded the weekly payment limits or limits per transaction, to quote just a few examples.

5.4. Technology

The Smart Money initiative has allowed the traditional developments of web platform management and mobile apps to be adapted, along with the latest advances in data storage and the management of blockchain nodes. As regards the elements and tools deployed, the following are worth highlighting:

- **Client for Ethereum "Hyperledger Besu"[81],** whereby access to and participation in the Ethereum protocol is possible, creating a blockchain network with unique privacy characteristics.

- **EthereumSmart contracts[82]:** they contain the business logic required to digitally represent monetary units, as well as to carry out transactions (transfer, issue and redeem or burn tokens). The Smart Money contracts are based on the standards ERC-20, ERC-777, ERC-1411, among others. For the development, the good practices which are a reference in the community were used, mainly the widely tested and audited OpenZeppelin framework techniques.

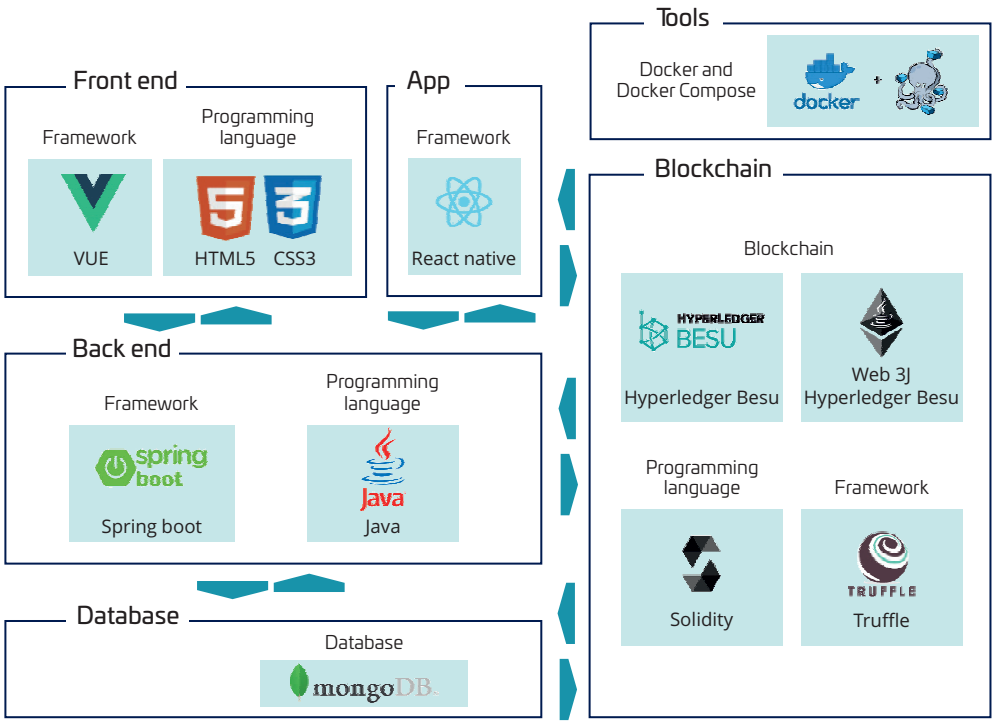
- **Application servers:** they implement the data processing required so that the players can interact and view their tokens on the network. These functions include the extraction and storage of information deriving from blockchain, the management of client wallets, the creation and sending of transactions, etc.

- **User interfaces:** the clients of the entities, as well as the users of the entities, Iberpay and the observer node of the Banco de España, have the user interfaces needed to operate and view the tokens, in accordance with the permissions assigned to each role. Furthermore, a mobile application has been developed which simulates a possible future application which would allow the client to manage its digital money. This application includes a technologically neutral digital identity layer which would allow, in the future, adaptation to digital identity solutions driven forward by the sector.

[81] Hyperledger Besu (2021): "Besu Enterprise Ethereum Client".
[82] Ziechmann, K (2021): "Introduction to smart contracts". Ethereum. https://ethereum. org/es/developers/docs/smart-contracts/

The technological services used in the Smart Money initiative are set out below:

Technological services
used in the Smart Money initiative



Source: own elaboration

5.5. Security

During the PoC, due consideration was given to security from the design stage, paying particular attention to privacy and implementing essential security checks.

As far as privacy is concerned, the following characteristics may be highlighted:

- Private transactions are used to limit the visibility of the entities with regard to client balances and transactions. To be precise, each entity may only view and process the balances and transactions of its own clients, whilst Iberpay and the Banco de España have full access to all the information shared on the Red-i network.
- Personal data are not shared visibly in interbank transfers, nor in other transactions.
- Although Iberpay knows the Ethereum addresses and balances to be found on the network, in the PoC there is no record of any other personal data of the end clients.

As regards the technical measures implemented in the PoC, the following have been included:

- Use of HTTPS for communications between the interfaces and the back end.
- Authentication and authorisation of end clients and the operators of the entities by using the user and password and JWT tokens.
- Use of user and password to access the database from the back end.

In addition, the request for digital money by the client requires the application of a two-factor authentication with a view to detecting attempts to use the personalised security credentials of the user which have been misplaced, stolen or misappropriated (in compliance with the provisions of the PSD2 Directive). European Banking Authority Guidelines provide a non-exhaustive list of the various alternatives valid for each of the authentication factors (sending of OTP on apps, for example). These security measures, amongst many more, must be combined with data protection measures, avoiding the exposure of the user to any additional processing in the event of an eventual system entry into production.

6

BIBLIOGRAPHY

- Adrian, T (2020): Speech "Evolving to Work Better Together: Public-Private Partnerships for Digital Payments". IMF. https://www.imf.org/en/News/Articles/2020/07/22/sp072220-public-private-partnerships-for-digital-payments

- Agencia Española de Protección de Datos, 2019: "Introducción al hash como técnica de seudonimización de datos personales". https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf

- Álvarez, R 2019: "Visa, MasterCard, eBay, Stripe y Mercado Pago anuncian su salida de la Libra Association: la criptomoneda de Facebook pierde adeptos". Xataka. https://www.xataka.com/empresas-y-economia/visa-mastercard-ebay-stripe-mercado-pago-anuncian-su-salida-libra-association-criptomoneda-facebook-pierde-adeptos

- Aurer, R. y Böhme R, (2020) "The technology of retail central bank digital currency". BIS. https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf

- Auer, R; Cornelli, G and Frost, J (2020): "Rise of the central bank digital currencies: drivers, approaches and technologies". BIS Monetary and Economic Department, no. 880. https://www.bis.org/publ/work880.pdf

- Auer, R; Haene, P and Holden, H (2021): "Multi-CBDC arrangements and the future of cross border payments". BIS Monetary and Economic Department, no. 115. https://www.bis.org/publ/bppdf/bispap115.htm

- Ayuso, J and Conesa, C (2020): "Una introducción al debate actual sobre la moneda digital de banco central (CBDC)". Banco de España. https://repositorio.bde.es/handle/123456789/10443

- Banco de España (2021): "Joint press statement by the CNMV and the Banco de España on cryptocurrency investment risks". Press release. https://www.cnmv.es/portal/verDoc.axd?t=%7B52286f9f-c592-4418-9559-b75bf97115d2%7D

- Bank for International Settlements; World Bank Group; Committee on Payments and Market Infrastructures (2020): "Payment aspects of financial inclusion in the fintech era". https://www.bis.org/cpmi/publ/d191.pdf

- Bank for International Settlements – Committee on Payments and Market Infrastructures (2020): "Enhancing cross-border payments: building blocks of a global roadmap". Stage 2 report to the G20. https://www.bis.org/cpmi/publ/d193.pdf

- Bank for International Settlements (2020): "BIS encourages central banks to continue adapting to the challenge of digital payments". Press release. https://www.bis.org/press/p200624_es.pdf

- Bank for International Settlements, (2020): "Central bank digital currencies: foundational principles and core features". Report no. 1 in a series of collaborations from a group of central banks. https://www.bis.org/publ/othp33.pdf

- ECB (2020): "Report on a digital euro". https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

- ECB (2021): "Eurosystem report on the public consultation on a digital euro". https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

- ECB (2021): "La consulta del BCE sobre el euro digital finaliza con una cifra récord de respuestas a la consulta pública". Press release published by the Banco de España. https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/ComunicadosBCE/NotasInformativasBCE/21/presbce2021_11.pdf

- Bossu, W; Itatani, M; Margulis, C; Rossi, A; Weenink, H and Yoshinaga, A (2020): "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations". International Monetary Fund. https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827

- Brainard, L (2020): "An update on digital currencies". BIS central bank speech. https://www.bis.org/review/r200814a.htm

- Brennan, C: "Libra: Understanding Facebook's Digital Currency". Consensys. https://pages.consensys.net/understanding-libra

- Cámara, N; Dos Santos, E; Grippa, F; Sebastian, J; Soto, F and Varela, C: "Central bank digital currencies: An assessment of their adoption in Latin America". BBVA. https://www.bbvaresearch.com/en/publicaciones/central-bank-digital-currencies-an-assessment-of-their-adoption-in-latin-america/

- Codruta, B and Wehrli, A (2021): "Ready, steady, go? – Results of the third BIS survey on central bank digital currency". BIS Monetary and Economic Department, no. 114. https://www.bis.org/publ/bppdf/bispap114.pdf

- European Commission (2020): "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions". https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0067&from=es

- European Commission (2020): "Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses". Press release. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

- European Commission (2020): "Proposal for a regulation of the European Parliament and of the Council on markets in Crypto-assets, and amending Directive (EU) 2019/1937". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

- European Commission: "Funding, tender opportunities". https://ec.europa.eu/info/funding-tenders_es

- European Commission: "Recovery plan for Europe". https://ec.europa.eu/info/strategy/recovery-plan-europe_en

- Financial Stability Board (2020): "Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements". FSB, Final Report and High-Level Recommendations. https://www.fsb.org/wp-content/uploads/P131020-3.pdf

- Danmarks Nationalbank (2017): "Central bank digital currency in Denmark?". https://www.nationalbanken.dk/en/publications/Documents/2017/12/Analysis%20-%20Central%20bank%20digital%20currency%20in%20Denmark.pdf

- Darbha, S and Arora, R (2020): "Privacy in CBDC technology". Bank of Canada. https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/

- Deutsche Bundesbank (2020): "Money in programmable Applications Cross-sector perspectives from the German economy". https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf

- Digital Dollar Foundation and Accenture (2020): "The Digital Dollar Project. Exploring a US CBDC". https://www.digitaldollarproject.org/

- Directorate-General for Financial Stability, Financial Services and Capital Markets Union (2020): "Digital finance package". European Commission. https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

- Directive 2009/110/EC of the European Parliament and of the Council, of 16 September 2009, on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC

- Directive (UE) 2015/849 of the European Parliament and of the Council, of 20 May 2015, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

- Directive (UE) 2015/2366 of the European Parliament and of the Council, of 25 November 2015, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC

- Directive 2018/843 of the European Parliament and of the Council, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

- Esselink, H and Hernández, L (2017): "The use of cash by households in the euro area". ECB, Ocassional Paper Series. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op201.en.pdf

- Fanusie, Y and Jin, E (2021): "China's Digital Currency. Adding Financial Data to Digital Authoritarianism". CNAS. https://www.cnas.org/publications/reports/chinas-digital-currency

- Ferrari, M; Mehl, A and Stracca, L (2020): "Central bank digital currency in an open economy". European Central Bank, Working Paper Series.

- World Economic Forum (2020): "Central Bank Digital Currency Policy Maker Toolkit". http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf

- G7 Working Group on Stablecoins (2019): "Investigating the impact of global stablecoins". BIS. https://www.bis.org/cpmi/publ/d187.pdf

- Gov.cn (2020): "Central Bank: Digital RMB closed test will not affect RMB issuance and circulation". http://www.gov.cn/xinwen/2020-04/17/content_5503711.htm

- Hubbard, B. (2021): "Federally Chartered Banks and Thrifts May Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities". OCC. https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2.html

- Hyperledger Besu (2021): "Besu Enterprise Ethereum Client".

- Keister, T and Sanches, D (2019): "Should Central Banks Issue Digital Currency?". Federal Reserve Bank of Philadelphia. https://www.philadelphiafed.org/consumer-finance/payment-systems/should-central-banks-issue-digital-currency

- Kiff, J; Alwazir, J; Davidovic, S; Huertas, G; Khan, A; Khionarong, T; Malaika, M; Monroe, H; Sugimoto, N; Tourpe, H and Zhou, P (2020): "A Survey of Research on Retail Central Bank Digital Currency". IMF.

- Lagarde, C (2020): "The future of money – innovating while retaining trust". BCE. https://www.ecb.europa.eu/press/inter/date/2020/html/ecb.in201130~ce64cb35a3.en.html

- Spanish Law 10/2010, of 28 April, prevention of money laundering and terrorism financing

- Spanish Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights.

- Lux, T and Mathys, V (2020): "Libra Association: FINMA licensing process initiated". FINMA. Press release. https://www.finma.ch/en/news/2020/04/20200416-mm-libra

- Meaning J, Dyson, B; Barker, J and Clayton, E (2018): "Broadening narrow money: monetary policy with a central bank digital currency". Bank of England Staff Working Paper No. 724. https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2018/broadening-narrow-money-monetary-policy-with-a-central-bank-digital-currency.pdf?la=en&hash=26851CF9F5C49C9CDBA95561581EF8B4A8AFFA52

- OMFIF, IBM (2019): "Retail CBDCs the next payments frontier". European Central Bank: "What are retail payments?". https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf

- Panetta, F (2020): "A digital euro for the digital era". ECB. https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201012_1~1d14637163.en.html

- Panetta, F (2021): "Evolution or revolution? The impact of a digital euro on the financial system". ECB. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210210~a1665d3188.en.html

- Panetta, F (2021): "A digital euro to meet the expectations of Europeans". ECB. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210414_1~e76b855b5c.en.html

- Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector

- Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937

- Draft Law on measures to prevent and combat tax fraud published in the Official Gazette of the Spanish Parliament, transposing Council Directive (EU) 2016/1164 of 12 July 2016, laying down rules against tax avoidance practices that directly affect the functioning of the internal market, modifying various tax regulations and in matters concerning gambling regulations

- Rauchs, M; Blandin, A; Klein, K; Pieters, G; Recanatina, M and Zhang, B (2018): "2nd global cryptoasset benchmarking study". University of Cambridge. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-cryptoasset-benchmark-study/#.YK5ugKgzaUk

- Royal Decree-Law 19/2017, of 24 November, on basic payment accounts, account switching and comparability of payment account fees

- Commission Recommendation, of 18 July 2011, on access to a basic payment account

- Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- Reynolds, T (2020): "The Federal Reserve Bank of Boston announces collaboration with MIT to research digital currency". Federal Reserve Bank of Boston. https://www.bostonfed.org/news-and-events/press-releases/2020/the-federal-reserve-bank-of-boston-announces-collaboration-with-mit-to-research-digital-currency.aspx

- Sand Dollar: "Key players". https://www.sanddollar.bs/keyplayers

- Federal Reserve System (2021): "Federal Reserve Chair Jerome H. Powell outlines the Federal Reserve's response to technological advances driving rapid change in the global payments land-scape". Press release. https://www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm

- Weber, A; Torres, C and Look, C (2021): "Cryptocurrencies: Fed's Powell and Peers Aren't Rushing Into Digital Currencies". Bloomberg. https://www.bloomberg.com/news/articles/2021-03-22/fed-s-powell-and-peers-aren-t-rushing-into-digital-currencies-kmkp6667

- Yanagawa, N and Yamaoka, H (2019): "Digital Innovation, Data Revolution and Central Bank Digital Currency". Working Paper Series, Bank of Japan. https://www.boj.or.jp/en/research/wps_rev/wps_2019/wp19e02.htm/

- Zhou, X (2020): "Understanding China's Central Bank Digital Currency". China Finance 40 Forum. http://www.cf40.com/en/news_detail/11481.html

- Ziechmann, K (2021): "Introduction to smart contracts". Ethereum. https://ethereum.org/es/developers/docs/smart-contracts/

Graphic design: outinup.com