



BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

A digital euro: a contribution to the discussion
on technical design choices

by Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporrini,
Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti,
Gabriele Marcelli, Pietro Tiberi, Alessia Vita



BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento (Markets, Infrastructures, Payment Systems)

Questioni istituzionali (Institutional Issues)

A digital euro: a contribution to the discussion on technical design choices

by Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporrini,
Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti,
Gabriele Marcelli, Pietro Tiberi, Alessia Vita

In memory of Diego Toma, who left us alone too soon on this journey.

Number 10 – July 2021

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of the Bank of Italy in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of the Bank of Italy.

The series is available online at www.bancaditalia.it.

*Printed copies can be requested from the Paolo Baffi Library:
richieste.pubblicazioni@bancaditalia.it.*

Editorial Board: STEFANO SIVIERO, LIVIO TORNETTA, GIUSEPPE ZINGRILLO, GUERINO ARDIZZI, PAOLO LIBRI, CRISTINA MASTROPASQUA, ONOFRIO PANZARINO, TIZIANA PIETRAFORTE, ANTONIO SPARACINO.

Secretariat: ALESSANDRA ROLLO.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of the Bank of Italy

A DIGITAL EURO: A CONTRIBUTION TO THE DISCUSSION ON TECHNICAL DESIGN CHOICES

by Emanuele Urbinati,* Alessia Belsito,* Daniele Cani,* Angela Caporrini,** Marco Capotosto,***
Simone Folino,*** Giuseppe Galano,*** Giancarlo Goretti,**
Gabriele Marcelli,*** Pietro Tiberi,*** Alessia Vita*

Abstract

In the last decade, the advent of new technologies has dramatically changed the banking and financial ecosystem. Financial operators have transformed their services in the context of the Fintech phenomenon; households' payment habits are rapidly changing as well, embracing the revolution brought by the digital innovations. In this context, a number of central banks are devoting significant resources to examining the feasibility of introducing a digital currency as a complement to physical money.

After an introduction that illustrates the main characteristics defining a Central Bank Digital Currency (CBDC), the paper presents ongoing CBDC-related work around the globe, discusses how a digital currency could support a central bank in performing its functions, and analyses its key features. The paper then illustrates a possible digital euro solution based on the integration of an account-based platform with a DLT-based one. The integration of these two components would make it possible to reap the benefits of two complementary solutions, reciprocally balancing their advantages and disadvantages, as regards, for instance, privacy. Finally, the paper presents the findings of experiments on the digital euro carried out by experts of the euro-area National Central Banks and the ECB; according to the results of those experiments, the integration of an account-based platform with a DLT-based one may provide a sound basis on which to build a fully-fledged solution, capable of meeting both regulatory and retail users' needs.

Sintesi

Nell'ultimo decennio, l'avvento di nuove tecnologie ha cambiato radicalmente l'ecosistema bancario e finanziario. Gli operatori finanziari hanno trasformato i loro servizi nell'ambito del fenomeno Fintech; le abitudini di pagamento delle famiglie stanno cambiando rapidamente, abbracciando in pieno la rivoluzione portata dalle innovazioni digitali. In questo contesto molte banche centrali stanno dedicando risorse significative nell'esame della fattibilità dell'introduzione della valuta digitale come complemento del denaro contante.

Dopo una parte introduttiva in cui vengono illustrate le principali caratteristiche per definire una Central Bank Digital Currency (CBDC), il documento illustra i lavori in corso in questo ambito nel mondo, discute come una valuta digitale potrebbe supportare una banca centrale nell'espletamento delle proprie funzioni, e analizza le sue caratteristiche fondamentali. Il lavoro poi espone una possibile soluzione di euro digitale basato sull'integrazione di una piattaforma account-based con una DLT-based. L'integrazione di queste due componenti permetterebbe di raccogliere i benefici insiti in due soluzioni complementari, bilanciando reciprocamente i propri vantaggi e svantaggi, per quanto riguarda, ad esempio la privacy. Infine, il documento presenta i risultati di sperimentazioni sull'euro digitale condotte da esperti delle banche centrali nazionali dell'area euro e dalla BCE; secondo i

* Banca d'Italia, Directorate General for Markets and Payment Systems.

** Banca d'Italia, Directorate General for Currency Circulation and Retail Payments.

*** Banca d'Italia, Directorate General for Information Technology.

risultati di queste sperimentazioni, l'integrazione di una piattaforma account-based con una DLT-based può fornire una solida base su cui costruire una soluzione completa in grado di venire incontro sia alle esigenze regolamentari che degli utenti retail.

Acknowledgments

The authors would like to thank Massimiliano Renzetti and Eleonora Serrao for their valuable contribution and support.

JEL Classification: E42.

Keywords: digital euro, payment systems, financial market infrastructure, blockchain.

TABLE OF CONTENTS

1. INTRODUCTION	7
1.1. Scope of the document	7
1.2. What is a CBDC?	8
1.3. What has been done so far?	9
1.4. How a D€ could support the objectives of the Eurosystem	12
1.5. Central Bank Digital Currency: relevant dimensions	14
2. A POSSIBLE ARCHITECTURE FOR THE DIGITAL EURO	17
2.1. Elements of the solutions	17
2.2. Two complementary approaches: a centralized account-based model and a token-based model	18
2.3. The TIPS+ platform	21
2.4. The itCoin platform	25
2.4.1. Introduction	25
2.4.2. Technical functioning	27
2.4.3. Relevant policy choices	33
2.5. TIPS+/itCoin Bridge	35
2.6. eCash - an alternative token-based platform	37
3. RESULTS OF THE EUROSISTEM'S EXPERIMENTATION OF POSSIBLE TECHNICAL SOLUTIONS FOR THE D€	40
3.1. Overview	40
3.2. Ledger benchmarking	41
3.2.1. Work stream scope	41
3.2.2. Prototype architecture and technological choices	41
3.2.2.1. Account-based ledger	42
3.2.2.2. Request handler	42
3.2.2.3. Point of Interaction Interface	42
3.2.2.4. PSD2 Interface	43
3.2.2.5. SEPA Interface	43
3.2.3. Experimental results	43
3.3. Integration between the account-based and token-based components	46
3.3.1. Integration between TIPS+ and itCoin	47
3.3.2. Integration between TIPS+ and a programmable DLT platform	48
3.3.3. Experimental results	50
4. APPEALING FEATURES OF THE INTEGRATED ARCHITECTURE	51
5. CHALLENGES AND THE WAY FORWARD	55
6. CONCLUSIONS	57

ANNEX 1: CBDC PRELIMINARIES	59
1. Substance of ownership: knowledge and identity	59
2. Ledger types: account-based vs token-based	60
3. Distribution degrees of systems and infrastructures	61
4. Online vs offline models	62
5. Intermediation types and implications for central bank liabilities	63
ANNEX 2: ITCOIN DISCUSSION TOPICS	64
1. About on-ledger transactional capacity	64
2. About the off-ledger digital euro as a central bank liability	65
REFERENCES	67

1. INTRODUCTION

1.1. SCOPE OF THE DOCUMENT

The debate on the introduction of a Central Bank Digital Currency (CBDC), a digital form of money for retail users that would represent a claim on a central bank instead of on private institutions, is rapidly growing as a response to the decline in the use of cash, the higher demand for digital payments and the advent of global stablecoins. Several central banks (CBs) are currently engaged in experiments and pilot testing; one of them has already issued its own CBDC as a complement to cash (see Section 1.3 below). The Eurosystem, after several months of preliminary experimentation carried out in four different work streams (the results of the experiments are described in Chapter 3), has launched an investigation phase¹ to assess the possible design choices of a digital euro and the impact it could have on the current payment system landscape and on the broader objectives of the Eurosystem.

The success of a digital euro project will be determined by its adoption by the end users, which in turn depends on the wide participation of the financial industry and, in particular, of the payment service providers (PSP), who, being directly in touch with customers, can encourage or discourage the usage of the digital euro.

It is worth emphasizing that this paper does not in any way aim at putting forward a fully-fledged technical proposal for the digital euro, and even less does it aim at pre-empting any decision on its possible features, as this task remains the full responsibility of the ECB Governing Council alone. Rather, this paper intends to take stock of the technical discussion on the digital euro so far and illustrate the logic underlying a possible architectural design for it. To do that, the paper describes a model, based on the scaling up of TIPS,² integrated with token-based systems, which are either based on Distributed Ledger Technology (DLT), i.e. itCoin (see Section 2.4)³ or based on different digital representations of money, i.e. eCash (see Section 2.6). It then looks at how such a model could meet the requirements defined in the report produced by the Eurosystem High Level Task Force (HLTF) on CBDC. Moreover, the paper briefly reports on the results of two experiments carried out by Banca d'Italia, the ECB and other euro-area central banks. The paper discusses how the results of the experimentation could provide valuable input to open design questions and support the policy discussion on design choices. Finally, the main open points and challenges are addressed, together with a possible way forward.

¹ “Eurosystem launches digital euro system“, ECB press release, 14 July 2021. For more details, see <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html>.

² TIPS (TARGET Instant Payment Settlement) is the pan-European platform for the settlement in central bank money of instant payments, i.e. electronic retail payments that have to be settled within a few seconds, following the SEPA Instant Credit Transfer (SCT Inst) scheme. For further details, see Renzetti *et al.* (2021).

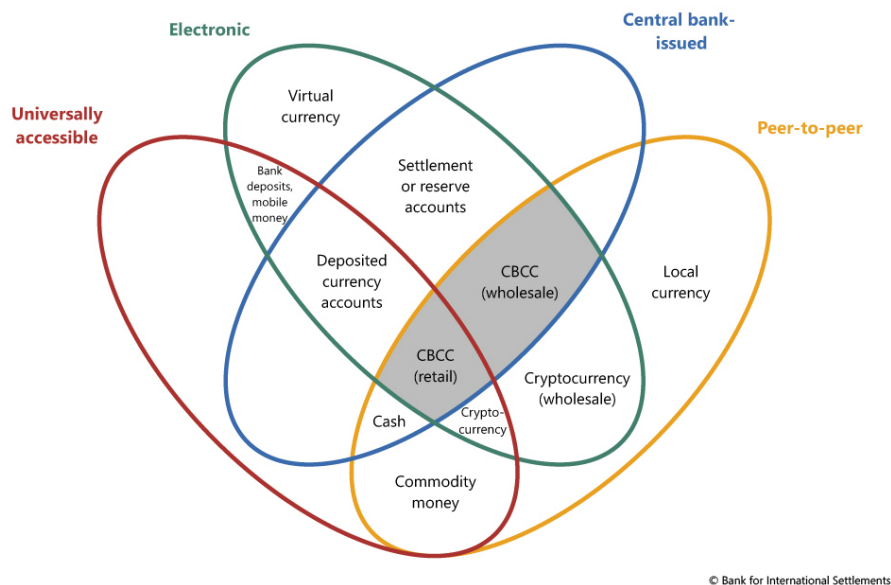
³ Both the scaling up of TIPS and itCoin have been developed by Banca d'Italia.

1.2. WHAT IS A CBDC?

Digital innovation has totally reshaped the banking and financial ecosystem: intermediaries have transformed their way of providing financial services, new technological companies (i.e. Fintech) emerged and households' habits have radically changed. In view of the continuing transformation towards a more digital landscape, the use of cash is gradually declining as a means of payment. People increasingly prefer to pay digitally and this trend appears to have accelerated further during the coronavirus pandemic.⁴ In addition, the potential growth of "crypto assets with a payment function" (such as the so-called stablecoins)⁵ is transforming the traditional concept of money. In this context, to evolve and to preserve confidence in the payment systems in a changing digital environment, the world's main central banks have started exploring the feasibility of introducing a digital currency (see Section 1.3).

The "money flower" graph (see Figure 1 below) proposed by Bech and Garratt⁶ and further adapted, can help in framing digital central bank money in a broader context that includes other types of money, according to their defining characteristics (issued or not by CBs, restricted or general purpose, token or account-based, digital or tangible nature).

Figure 1 - "Money flower" graph



⁴ See European Central Bank (2020a).

⁵ The recent Digital Finance Package released by the European Commission in September 2020 and in particular the legislative proposal "Markets in Crypto Assets Regulation (MiCAR)" defines a crypto asset as a "digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology". According to the MiCAR proposal, stablecoins can be included in one of the following categories of crypto assets: "Asset Referenced Token" (if the crypto asset refers to the value of several fiat currencies which are legal tender, one or several commodities or one or several crypto assets, or a combination of such assets) and "E-money token" (if the crypto asset refers to the value of only one fiat currency that is legal tender).

⁶ See Bech and Garratt (2017); see Bank for International Settlements (2019).

This graph identifies several forms of digital CB money: in particular digital central bank money has already been available for some time in reserve accounts of CB-managed wholesale payment systems such as TARGET2.⁷ However, this particular type of CB digital money is reserved mainly to banks and, occasionally, to other selected institutions.

Other forms of digital money depicted in the graph (such as cryptocurrencies used for wholesale payments by non-banking institutions) remain mainly speculative.

Although the notion of a CBDC has been around for some years, a completely clear-cut definition is still missing. For the purpose of this paper, a CBDC for retail transactions available to the general public which replicates to some extent the features of cash (i.e. a retail CBDC), is defined as a means of payment that is:

- issued by the central bank, i.e. a liability in the Central bank's balance sheet;
- in a digital form;
- available for retail use by the public.⁸

1.3. WHAT HAS BEEN DONE SO FAR?

CBDC's exploratory and experimental phase worldwide is already well under way, and the interest in understanding how the new technologies can support the creation of a new form of money is constantly growing. Indeed, in 2019 more than eighty per cent of Central banks reported being engaged in CBDC projects (Bank for International Settlements, 2020a). In October 2020, a joint report on CBDC (issued by seven major central banks – the Bank of Canada, the Bank of England, the Bank of Japan, the European Central Bank (ECB), the Federal Reserve, Sweden's Riksbank and the Swiss National Bank – and the BIS)⁹ pinpointed the fundamental principles that a CBDC must meet:

- coexisting with cash and other types of money in a flexible and innovative payment system;
- supporting wider policy objectives and doing no harm to monetary and financial stability;
- promoting innovation and efficiency;
- being resilient and secure in order to maintain operational integrity;
- being convenient and available at very low or no cost to end users;
- being backed by appropriate standards and a clear legal framework;
- assigning an appropriate role to the private sector, as well as promoting competition and innovation.

⁷ TARGET2 is the payment system owned and operated by the Eurosystem. For more details, see <https://www.ecb.europa.eu/paym/target/target2/html/index.en.html>.

⁸ For sake of completeness, it should be clarified that cash, and hence a cash-like CBDC, also fulfils the roles of unit of account and store of value. In any case, it should be kept in mind that, even if "store of value" is a natural function of any currency, this does not mean that a CBDC should also necessarily serve as a means of investment.

⁹ See Bank for International Settlements (2020c).

Central banks have engaged in work streams related to CBDCs with different degrees of progress, ranging from research and conceptual analysis to actual issuance.

The first CBDC to go live ever was the so-called “sand dollar”, officially launched in the Bahamas on 20 October 2020, gradually reaching nationwide coverage. The CBDC represents for the Bahamas a great opportunity to overcome the challenges in circulating and exchanging physical cash and to bring financial inclusion to communities that live in the most remote areas of the archipelago. Issued by the Central Bank of the Bahamas, it is distributed to end users through authorized financial institutions, which are in charge of Know Your Customer (KYC) and Anti-Money Laundering (AML) checks and responsible for providing citizens with the digital wallets to store sand dollars as well as offering custodial services. At the end of March 2021, the Eastern Caribbean Central Bank went live with the pilot of its central bank digital currency: DCash. The project was developed in partnership with the Barbados-based Fintech company, Bitt Inc. and, since April, the digital currency is open for business on the islands of Antigua and Barbuda, Grenada, Saint Christopher (St Kitts) and Nevis and Saint Lucia.

Among the largest economies in the world, Sweden and China have had the most advanced CBDC experiences. The Riksbank is conducting a pilot project, in partnership with the consulting company Accenture, to develop a technical solution for an e-krona that could be used by the general public as a complement to cash (Sveriges Riksbank, 2021). In the test environment, simulated users hold e-kronas in a digital wallet and make payments, deposits and withdrawals via a mobile application or via cards and wearables. The pilot is also examining the possibility of using e-krona offline. E-krona is based on a Distributed Ledger Technology (DLT) – a blockchain technology. Its distribution model is reminiscent of the one for cash: only the Riksbank can create e-kronas, which are then distributed to the general public through intermediaries such as banks and payment service providers. The pilot project will run until February 2022.¹⁰

In October 2020, China issued a draft law to provide a regulatory framework and legitimacy for a forthcoming CBDC that would provide a digital alternative to cash for retail use. Recently, in July the People’s Bank of China (PBoC) published a white paper on the digital renminbi, or e-CNY, which clarifies the background, objectives and visions, design framework and policy considerations.¹¹ The e-CNY is currently being tested in multiple areas including Beijing and Shanghai, possibly leading to its launch as early as next year. The e-CNY would be issued by the PBoC and distributed by authorized operators. It would be a value-based, quasi-account-based and account-based hybrid payment instrument, with legal tender status and loosely coupled with bank accounts, featuring managed anonymity. As at last June, more than 20 million personal wallets

¹⁰ <https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2021/riksbank-extends-test-of-technical-solution-for-the-e-krona/>.

¹¹ See People’s Bank of China (2021).

and over 3.5 million corporate wallets had been opened, with a volume of over 70 million transactions and a value approximating 34.5 billion renminbi.

Looking at the United States, work is still in its initial phase, but the Federal Reserve Bank has recently announced a collaboration with the Massachusetts Institute of Technology (MIT) to build and test a hypothetical digital dollar.

The Bank of England has been exploring the topic of CBDC for several years and has recently speeded up its investigations. In April 2021, it announced the creation of: a CBDC Taskforce jointly with HM Treasury to coordinate the exploration of a potential digital pound; a CBDC Technology Forum to gather input on all technology aspects; a CBDC Engagement Forum on all non-technological aspects; and, lastly, a CBDC Unit within the Bank of England itself to lead its internal exploration around CBDC.¹²

In Europe, the Governing Council of the ECB established a High-Level Task Force (HLTF) on CBDC in January 2020, bringing together experts from the ECB and the 19 National Central Banks (NCBs) of the euro area. On 2 October 2020, the ECB released a report¹³ summarizing the main findings of the HLTF, concerning the possible benefits and challenges as well as the economic, technological, legal, societal and strategic implications associated with the introduction of a CBDC in the euro area – i.e. a digital euro (hereinafter, also D€). No decision has been taken yet on the issuance of a D€, but the Eurosystem is committed to being ready to do so in the future, should the need arise. Under the aegis of the HLTF, the Eurosystem has just launched the project's investigation phase.

THE ECB'S REPORT ON A DIGITAL EURO

As per the report, the digital euro would be a liability of the Eurosystem recorded in digital form as a complement to cash and central bank deposits, an electronic form of central bank money accessible to all citizens and businesses for their retail payments.

The digital euro could be issued: (i) to support the digitalization of the European economy and the strategic independence of the European Union; (ii) in response to a significant decline in the role of cash as a means of payment; (iii) if there is significant potential for foreign CBDCs or private digital payments to become widely used in the euro area; (iv) as a new monetary policy transmission channel; (v) to mitigate risks to the normal provision of payment services; (vi) to foster the international role of the euro; and (vii) to support improvements in the overall costs and ecological footprint of the monetary and payment systems.

The Report elaborates on core principles, scenario-specific requirements and general requirements for the digital euro.

Core principles are properties that must fully comply with the Eurosystem's mandate, policies and principles. The digital euro has to be: convertible at par, a liability of the Eurosystem, a European solution, market-neutral and trusted by end users.

¹² See Bank of England (2021a) and Bank of England (2021b).

¹³ See European Central Bank (2020b).

Scenario-specific requirements depend on the Eurosystem's objectives and the potential users' needs that are to be fulfilled. These consist in enhanced digital efficiency, cash-like features, competitive technological features, options for monetary policy transmission, resilience to extreme events, international accessibility, cost-efficiency, and environmental sustainability.

General requirements are needed in all foreseeable scenarios to protect both the Eurosystem and the European economic and financial system from any unwarranted implications arising from the issuance of a digital euro in relation to: controllability of the amount in circulation, cooperation with market participants, compliance with the regulatory framework, safety and efficiency, easy accessibility throughout the euro area, conditional use by non-euro area residents, and cyber resilience.

While a clear preference is expressed towards an access model to the D€ intermediated by the private sector, many other aspects are left open for further conceptual analysis and assessment through practical experimentation, the most relevant of which are: the design of the back-end infrastructure and its underlying technology, the level of privacy, remuneration and holding limits.

1.4. HOW A D€ COULD SUPPORT THE OBJECTIVES OF THE EUROSISTEM

This section briefly outlines the authors' view on how a digital euro could support the objectives of the Eurosystem. A more detailed analysis of these aspects will need to be conducted before any decision can be taken on the issuance of the D€ .

The Eurosystem's main objective is to ensure price stability,¹⁴ mainly implemented through monetary policy.

The introduction of the D€ would inevitably entail direct effects on the most essential functions of the Eurosystem (monetary policy, financial stability, payment system security and efficiency). It could also have broader implications, as regards, for instance, issues relating to anti-money laundering/combating the financing of terrorism (AML/CFT), strategic and technological independence, taxation, and environmental issues.

As regards monetary policy, since the D€ would be another tool to provide liquidity, the implications for the transmission of monetary policy could vary depending on how the CBDC is actually designed. Just to mention one aspect, the outcome would be very different depending on whether the D€ is remunerated or not.

Moreover, hypothetically, the diffusion of Global Stablecoins¹⁵ or even foreign CBDC in Europe could weaken the monetary policy transmission channels. In the worst-case scenario, there could be a currency substitution and a loss of control over domestic liquidity by the Eurosystem, that the D€ could help in countering.

The risk of a downscaling of commercial banks' role in money creation and deposit taking are likely to have implications for financial stability, which need

¹⁴ Article 127 of the Treaty on the Functioning of the European Union.

¹⁵ The Global Stablecoin is a stablecoin (a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets) with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume (see Financial Stability Board, 2020).

to be thoroughly analysed as well. For example, a shift from commercial bank to D€ holdings might increase the cost of funding for banks and might result in higher interest rates on bank loans, potentially reducing the volume of bank credit to the economy.

In the context of the Eurosystem, Banca d'Italia, jointly with the other central banks, promotes the security and efficiency of payment systems by carrying out payment system oversight, directly provisioning payment clearing and settlement services (both in wholesale and retail scenarios) or performing the role of catalyst. According to the Eurosystem oversight policy framework, as payment instruments and payment schemes are an integral part of payment systems, the Eurosystem includes these in central bank oversight of payment systems.

With reference to the retail payments landscape, the rapid changes that characterize this sector require the Eurosystem to promote innovation, paying attention to the connected risk profiles and their mitigation. In this context, the issuance of the digital euro could increase the range of innovative payment services available to citizens, market operators and businesses, introducing a secure payment instrument that would complement cash and other existing electronic means of payment, without replacing them.

Cultural trends, such as the one that is being observed in northern European countries, or temporary shocks, such as the one caused by the COVID-19 pandemic, push towards a shift in payment habits and represent a driver for the public to willingly substitute cash in favour of alternative electronic means of payment. The introduction of a D€ could represent an effective response in the face of a possible sharp decline in the usage of cash connected to structural or cyclical phenomena,¹⁶ offering an additional form of public and risk-free money to European citizens.

Moreover, the D€ could enhance cross-border payments and allow smoother exchanges with other currency areas. However, should the D€ be made available for cross-border and cross-currency operations, one should keep in mind that this could affect financial stability in various ways, which would need to be properly investigated in order to prevent undesired spillovers and additional international linkages.

In addition to the effects on the main objectives of the Eurosystem described above, the D€ would have an impact on some other aspects that are not part of the traditional set of objectives of the Eurosystem.

On the one hand, the D€ could give a major forward impulse to the digitalization of the European Union (EU), as its issuance could facilitate the development of

¹⁶ See the HLTf Report on a digital Euro, European Central Bank (2020b) and Study on the payment attitudes of consumers in the euro area (SPACE), European Central Bank (2020a). According to the SPACE report, in 2019 adult consumers in the euro area used cash for 73% of their retail transactions (48% in value terms). Both figures declined with respect to 2016, when, according to a previous ECB study (see European Central Bank, 2017: "The use of cash by households in the euro area"), cash accounted for 79% of transactions (54% in value terms). The gradual shift towards cashless payments has gained momentum due to the COVID-19 pandemic. According to an ad hoc survey carried out by the ECB in July this year, four out of ten respondents replied that they had used cash less often since the start of the pandemic.

a full range of services by European intermediaries for their customers and, as such, benefit not only the financial system as a whole but, ultimately, all citizens. On the other hand, from a strategic perspective, this would also support the independence of the EU from private and public entities that propose themselves as providers of payments solutions capable of extensive adoption. The digital currency issued by the Eurosystem should be designed in such a way as to limit its ecological footprint; first evidence on how a TIPS-based D€ could mark an initial step towards a more general reduction of the environmental costs of payment solutions and instruments, are provided in Section 3.2.3.

Financial inclusion should also be taken into consideration in defining the features of the D€: similarly to banknotes, which do not require a high degree of digital or financial literacy, it is important that the D€ is designed to involve the widest possible “audience”, guaranteeing ease of use even to people that are not accustomed to digital technologies. Moreover, a D€ would also be essential to include citizens temporarily excluded from central bank money; for instance, in the case of natural disasters, access to standard payment channels or to cash withdrawals from automated teller machines (ATMs) could be temporarily or even persistently not guaranteed. The D€ could offer, both in ordinary and emergency situations, an alternative recovery payment method, with a view to improving the resilience and overall availability of the payment system infrastructure.

Lastly, some configurations of the D€ could effectively discourage tax evasion, money laundering, terrorism financing and other illicit activities which usually rely on anonymous means of payment. At the same time, the D€ should be designed in a way that ensures an adequate degree of privacy of transactions. It is worth noting, however, that if personal data related to D€ transactions were ultimately managed under the responsibility and the control of public authorities such as the Eurosystem, this would already guarantee compliance with the privacy protection standards, especially compared with cases in which transaction data are managed by big private institutions.

1.5. CENTRAL BANK DIGITAL CURRENCY: RELEVANT DIMENSIONS

This section summarizes the most significant operational and technological dimensions of a CBDC, which here are dubbed “facets”: each facet constitutes a different point of view on a specific characterization of a CBDC, possibly, but not necessarily, orthogonal¹⁷ to other facets. More specifically the facets that have been identified are briefly described in this section, while being detailed in Annex 1.

- Substance of ownership: identity-based vs knowledge-based. A first way to attest ownership of D€ is based on identity verification: in this model, users’ holdings are recorded by a third party and transactions are authorized thanks to the ability of the third party to verify the identity of the payer.

¹⁷ The mathematical concept of “orthogonality” is here used to refer to the non-correlation of dimensions. Two facets are orthogonal if it is possible to combine them arbitrarily with consistent results; e.g. a decision made with respect to one facet does not influence a decision in another. It should be observed that the concept of “orthogonality” should not be taken literally: arbitrarily combining every possible value for every facet might lead to a characterization of a CBDC that is possibly meaningless or virtually unfeasible.

This is the approach currently followed by the vast majority of digital payment solutions (e.g. electronic money and credit cards),¹⁸ since there are simple and convenient ways to verify the user's identity. A second option to attest ownership of D€ is based on the concept of knowledge possession, in analogy with physical cash:¹⁹ in this case, no identity verification is required to complete a transaction; rather, the fundamental requirement is the ability to prove the knowledge of a secret piece of information (e.g., a private key or a secret number); the validity of the proof must of course be verified. While in the case of physical cash the requirement is satisfied through the physical possession of valid banknotes, in the case of digital currencies ownership is attested by means of cryptographic signatures, whose validity can be verified by the parties involved in the payment transaction, including the ledger operator. In this second scenario, there is no need to link the digital currency to an identity and anonymity can be enabled.

- Ledger types: account-based vs token-based. An account-based system records the state of the ledger as a list of accounts, each of which has a corresponding balance.²⁰ When a transaction occurs, the system updates the records by increasing and decreasing the balances of the accounts in question, usually the payer account and the payee account. Most payment systems, including TARGET2/TIPS, operate according to the account-based model. Another example of this kind is the Ethereum DLT (Buterin, 2013), in which the ledger state is made up of objects called "accounts", with associated balances. By contrast, a token-based system records the state of the ledger as a list of individual objects, called tokens, each of which has a corresponding value, which can also be a decimal value (e.g. in order to address the need of giving change), but this does not change over the whole lifetime of the token (e.g. €10.53). The fundamental characteristic of tokens is that, when a payment is made, they are either created or destroyed (and usually replaced with other, equivalent, tokens), but cannot be partially spent. The ledger operator creates or destroys the tokens while keeping track either of the set of tokens that have already been destroyed (i.e. spent) or that are still in circulation (i.e. unspent). Examples of this kind are the Bitcoin DLT and eCash²¹ protocol.
- Distribution degrees of systems: centralized vs distributed vs decentralized. From the organizational viewpoint, three different system architectures exist: centralized, distributed and decentralized. A centralized system is controlled by a single entity or organization, which is trusted by the users. In distributed systems, instead, the control is spread over some pre-defined and identifiable organizations: in this case, there are multiple

¹⁸ Nowadays most credit cards are associated to a unique secret number, such as the Personal Identification Number (PIN). Nevertheless, the knowledge of the credit card secret number does not entail ownership of the funds that can be spent with the card. In fact, the card and the PIN are used as a convenient technology to verify the identity of the card owner, and not as a proof of ownership itself. For these reasons, the electronic money that can be spent with credit card remains identity-based. On the contrary, value stored on anonymous prepaid cards or other anonymous gift cards (such as the ones that can be bought at the supermarket) would be knowledge-based.

¹⁹ Another similarity may be drawn with bearer securities: holding a valid paper certificate bestowed certain rights to the holder, and physical coupons were attached to bonds, each one corresponding to payments of interest at a defined date. See Bank for International Settlements (2020b).

²⁰ See Bank of England (2020).

²¹ See Chaum (1983).

system owners that have a part or a copy of the resources. With systems of this kind, the users do not have to trust a single organization or entity.²² Lastly, in decentralized systems control is spread over many unidentifiable entities, possibly unknown to each other.²³

- Distribution degrees of infrastructures: centralized vs distributed. From a technological viewpoint, two different infrastructure types come into play: centralized and distributed. Centralized infrastructures are designed with a single node in charge of executing the system goal (one classic example being the so-called client/server architecture), where one or more client nodes are logically connected to a central server. A distributed infrastructure, instead, is a collection of different and separated autonomous computing elements²⁴ working together to achieve a common goal, in order to appear as a single coherent system and reach the goal, including in the presence of failures of one or more members of the group.
- Operational model: Online vs offline. The online model relies on permanent connectivity to the ledger, which acts as a unique source of truth. The offline model, instead, operates in the absence of connectivity to the ledger, and offers an opportunity to expand the availability of services. The offline model may imply considerable risks, usually related to the so-called “double spending problem” or to the risk of counterfeiting. Considering the wide variety of possible offline scenarios, it is proposed to narrow them down to two main theoretical categories: eventually online and permanently offline. The eventually online category refers to a scenario in which a payer executes a transaction with a payee in the absence of connectivity to the ledger. This implies that the transaction is completed, but it is recorded only after a process of data reconciliation with the online system (i.e. written on the ledger). The permanently offline category refers to a D€ which works completely offline, and therefore transaction finality does not require data reconciliation with the online system, but only relies on hardware devices, whose security is fundamental to guarantee that transactions happen in a safe mode. The feasibility of a permanently offline D€ is questionable: physical tampering of devices is the main vulnerability of such a model because it creates economic incentives for users to attack their own secure hardware devices (Allen *et al.*, 2020), soliciting the need for new security features (e.g. the no-cloning theorem).²⁵
- Technical intermediation types: settlement agent intermediation vs gatekeeper intermediation vs direct access.²⁶ This last facet refers to the technical relationship between the user of the CBDC and the ledger infrastructure operated by the central bank. It is important that the safety of the digital currency is guaranteed independently from the intermediation type, in all circumstances, including when the user queries the payment system for account information (e.g. balance or list of transactions), and when the user is willing to initiate and authorize a new payment. Three possibilities can

²² DNS (Domain Name System) is an example of a distributed system.

²³ Peer-to-peer systems are an example of a decentralized system.

²⁴ See Van Steen and Tanenbaum (2017).

²⁵ See Aaronson *et al.* (2012).

²⁶ The terminology used in this report for gatekeeper and settlement agent is taken from Section 6.1 of European Central Bank (2020b). A different classification would be possible if the focus were shifted from technical intermediation to the way in which accounts are managed, as in the model presented in Bank for International Settlements (2021).

be envisaged: settlement agent intermediation, gatekeeper intermediation and absence of intermediation. In the settlement agent intermediation, intermediaries execute transactions on behalf of their customers and possibly, provide storage facilities for D€ holdings.²⁷ Unlike settlement agents, the gatekeepers are in charge only of authenticating end users and provide the technical connectivity between users and the payment system infrastructure. Finally, the user access to the ledger can, technically, not be intermediated (i.e. it is direct), as is the case with many crypto-assets and stablecoins.

2. A POSSIBLE ARCHITECTURE FOR THE DIGITAL EURO

2.1. ELEMENTS OF THE SOLUTIONS

The D€ should be designed so as to ensure that its introduction helps the Eurosystem achieve its core objectives and mandate, minimizing potential risks to the current financial environment and smoothly coexisting with cash, while at the same time being appealing to end users.

To support the digitalization of the European economy, the D€ solution should be based on state-of-the-art technology with high-end performance and 24/7/365 availability; it should also be low cost, interoperable with existing payment solutions (e.g., credit transfers, direct debits, e-money and card payments) and compliant with current regulations (e.g., PSD2)²⁸ throughout the entire euro area, thus leaving room for private initiative to develop advanced features and value-added non-core services for their customers, so that it becomes as attractive as the most popular private solutions.

While the D€ should of course be attractive, it should not be viewed as a form of investment; should this happen, the ensuing disintermediation of the banking system would result in undesirable implications for the conduct of monetary policy and for financial stability. Therefore, the design of the D€ should consider features to limit the excessive conversion of bank deposits into D€; this could be done with a two-tier remuneration system²⁹ and/or the imposition of limits on individual holdings.³⁰ Remunerating the deposits with a time-varying interest rate that also depends on the amounts held would be instituted to ensure that the Eurosystem fully retains the ability to control the total amount of D€ in circulation. Applying a zero or a relatively attractive remuneration rate up to a relatively low ceiling, even in a context of low or negative policy rates, will incentivize the use of the D€ by households and merchants; at the same time, a lower interest rate for amounts beyond the threshold will discourage its use as a form of investment or safe harbour.

²⁷ See European Central Bank (2019) for a D€ model with settlement agents.

²⁸ See European Parliament and Council of the European Union (2015).

²⁹ A two-tier remuneration system is discussed in detail in Bindseil (2020) and Panetta and Bindseil (2021).

³⁰ Other aspects about the thresholds/limits that the CBDC back-end platform should support to be considered: e.g. compliance with local laws limiting transactions that can be done anonymously (e.g. in some countries limits on the maximum amount of cash transactions are currently established by law).

A blue circular logo with the text "ECB PUBLIC CONSULTATION" in white, uppercase letters.

Scoring a record participation for an ECB public consultation of over 8,200 responses, the consultation on a digital euro cast light on the main characteristics of the digital euro according to citizens and professionals: privacy (43%), followed by security (18%), pan-European usability (11%), the absence of additional costs (9%) and availability offline (8%).

The introduction of a limit on individual holdings could mitigate the risks of undesirable fallout for the banking system and serve AML/CFT purposes. The implications of a tiered remuneration and/or limits to individual holdings are still being investigated by the HLTF-CBDC and the relevant Eurosystem Committees. Regardless of the conclusions of this investigation and the Eurosystem's final decision, it is clear that the design of the D€ should allow for the possibility of applying limits to holdings and/or tiered remuneration.

The ever-rising use of electronic payments means that the Eurosystem should include cash-like features in the design of its digital currency, to ensure the financial inclusion of unbanked people (and possibly non EU-residents, too). The D€ should protect the privacy of transactions; at the same time it should comply with the existing regulations on anti-money laundering (AML) and combating the financing of terrorism (CFT), which includes the customer due-diligence (CDD) obligations. The design of the D€ should strike the right balance between privacy and AML/CFT compliance.

To ensure the proper functioning of the payment system, the D€ should be sheltered from cyber threats and other extreme events. It is therefore of the utmost importance to complement its infrastructure with advanced business continuity solutions and innovative cyber resilience controls, while digital wallets, cards and other possible devices must be tamper-proof and protected via cryptographic techniques to the extent possible.

Cost impacts and the ecological footprint of the D€ are two further aspects that should be kept in mind when designing any technological solution; as to the former, it may be desirable to "reuse" an already existing Eurosystem infrastructure; as to the latter, solutions such as the mining mechanism typical of some DLTs should be avoided.

2.2. TWO COMPLEMENTARY APPROACHES: A CENTRALIZED ACCOUNT-BASED MODEL AND A TOKEN-BASED MODEL

The D€ design should take into account the characteristics described in the previous section and the results of the public consultation launched by the ECB at the end of 2020 (European Central Bank, 2021a).

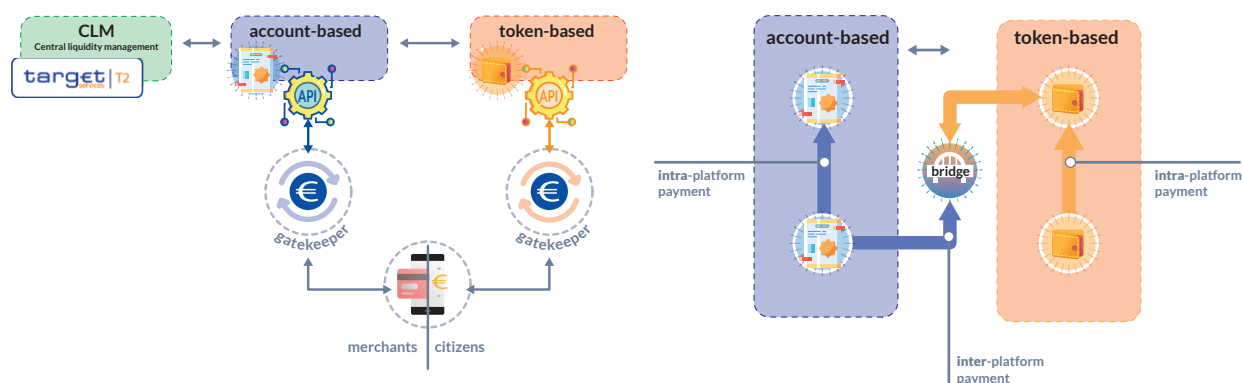
While the intrinsic characteristics of the D€ should *per se* guarantee an efficient and secure means of payment, both at a national and a European level, regarding privacy, it must be pointed out that there could be different degrees of it in transactions. These include completely anonymous payments for cash transactions where there is no link between the identity of the payer and the possession of the banknotes, and electronic payments that are known only to the payer and payee, but that for purposes of verification by the judicial authorities could be possibly linked to the parties' identities.

Hence, based on the results of the public consultation and the requirements of the HLTF report, a wide set of requirements has been identified that are sometimes in conflict with one another and cannot be satisfied simultaneously by a single solution. For instance, a token-based solution could easily mimic some of the characteristics of cash, including a high degree of privacy; at the same time, it would make it harder to comply with the current AML/CFT requirements for e-money and to implement remuneration policies. An account-based solution, on the contrary, would be able to meet many of the requirements, except for some of the cash-like features.

Considering the above and in order to contribute to the ongoing discussion on the digital euro, this paper illustrates the features of a model, graphically presented in Figure 2 below, that integrates a digital currency account with a token-based instrument, i.e., the integrated model:

- the account-based component would provide a proven highly performing infrastructure and would give the Eurosystem the possibility to fully control the amount of D€ in circulation, to set holding limits per balance or per transaction and/or to remunerate balances;³¹
- the token-based instrument would offer variable levels of privacy, as well as financial inclusion to the unbanked, and possibly programmability.

Figure 2 - Graphical representation of the integrated model



Furthermore, as the technical analysis will show in detail, the two models have a different capability in terms of volume of transactions processed and recorded in the ledger: the account-based component would be able to process a higher rate of transactions than the token-based one, which is less scalable in terms of volumes. However, the token-based or other DLT-based component could be designed to better foster the development of high value-added applications by market operators, leveraging a higher programmability with respect to the account-based model, thanks to the

³¹ In an account-based/identity-based system, gatekeepers identify and enrol end users, storing account data in a centralized directory kept under the Eurosystem. This directory would store for each end user a unique identifier that allows the identification of the account owners so that specific remuneration or holding limits could be applied to their account balances.



SMART CONTRACT

A smart contract is a computer program that is intended to automatically execute actions according to the terms of a contract defined in digital form, using a specific programming language. Executing such instructions makes it possible to simplify the exchange of money and other types of assets.

possibility of using advanced programming languages to implement smart contracts³² that are self-executed when certain conditions are met.

One of the fundamental characteristics of the integrated model would be its high degree of flexibility, which would make it possible to combine it with innovative private solutions with an open and client-sided approach, and to make it interoperable with current operational models. This in turn would enable intermediaries to offer D€-based services to their customers.

The Eurosystem will decide whether the front-end solution (e.g. D€ mobile application, web application or smart card) is developed by the private sector. In any case, the integrated model does not force a priori the adoption of a specific solution.

The integrated model proposed in this paper does not take into account “offline” use, namely the possibility for users to send and receive payments in D€ using devices like hard tokens or smart cards. Offline transactions would be the closest to cash due to the absence of intermediation and P2P exchange without the need for a constant internet connection.³³ The extension of this model to also encompass mechanisms for offline usage of the D€ will still be possible, provided that a comprehensive analysis of the security aspects of this model is performed in order to ensure its robustness. Moreover, providing a secure way to enable offline use still depends on the state-of-the-art technology, which currently does not allow the handling of long chains of consecutive offline payments without severe security concerns. At any rate, the choice of the “core” model for the D€ does not in any way precludes the choice of the most appropriate “offline” solution down the road.

The two approaches are complementary, so that the combination of both models in a seamless way without hierarchical order is able to provide a fully-fledged solution. This system would result in a versatile D€ that could satisfy both retail user needs, for instance in term of privacy or programmability, and public needs such as control over the monetary base.

Sections 2.3 and 2.4 will present in more detail the two sides of this integrated model, respectively a TIPS-based platform and itCoin, a DLT platform for token-based instruments. Section 2.5 will then present how the two platforms interact with each other. The integrated model provides a highly flexible architecture and can host different technical solutions for the token-based instrument; to illustrate this point, Section 2.6 will briefly describe integrating the TIPS-based platform with a token-based (non-DLT) infrastructure, as an alternative to itCoin.

³² See Buterin (2013).

³³ It should be noted that, for integrity reasons, transactions cannot be merely offline because balances of devices will be eventually reconciled with the online ledger.

2.3. THE TIPS+ PLATFORM

Drawing upon the facet-based classification of CBDC characteristics introduced beforehand, an account-based solution may be classified as presented in the following Table 1.

Account-based systems are probably the most well-known and widespread solution for payment systems. As a 4CB³⁴ technology provider, Banca d'Italia has built, on behalf of the Eurosystem, a 24/7/365 payment system that is, in fact, an account-based system: TIPS.

Since its introduction in November 2018, TIPS, which is based on an advanced IT architecture,³⁵ has proven to be a reliable central platform that has become a reference system when it comes to high-volume/high-speed transactions. TIPS may provide a reference architecture that complies with the technical performance requirements of a digital euro platform; it combines the scalability of a distributed architecture with the security of a centralized system whose operations leverage the experience of the Eurosystem.

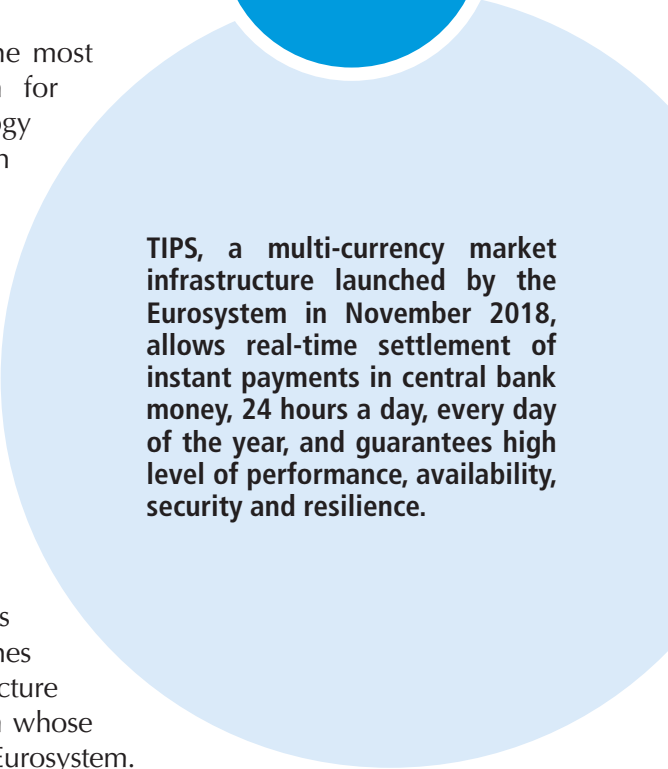
Taking TIPS as the starting point, the authors believe it is possible to design a new account-based system, called TIPS+, that includes new features and enhances existing ones so as to satisfy many of the requirements for the digital euro, at least those reported in the digital euro report.

The design model for TIPS+ is based on a TIPS-like architecture, where a central platform directly holds individuals' accounts while access to them is provided via third parties (gatekeepers), responsible for the enrolment and identification of the users (KYC principle). Figure 3 provides a graphical representation of the TIPS+ high-level model.

TIPS+ addresses the D€ requirements described in the previous sections, such as privacy, support to bearer instrument,³⁶ accessibility³⁷ and programmability. Availability and scalability, which are cornerstones of the current TIPS design, are also confirmed as fundamental requirements in TIPS+.



TIPS



TIPS, a multi-currency market infrastructure launched by the Eurosystem in November 2018, allows real-time settlement of instant payments in central bank money, 24 hours a day, every day of the year, and guarantees high level of performance, availability, security and resilience.

³⁴ In their capacity as the CBs building and operating the TARGET Services, Deutsche Bundesbank, Banco de España, Banque de France and Banca d'Italia are also referred to as the "4CB".

³⁵ See Arcese, Di Giulio and Lasorella (2021).

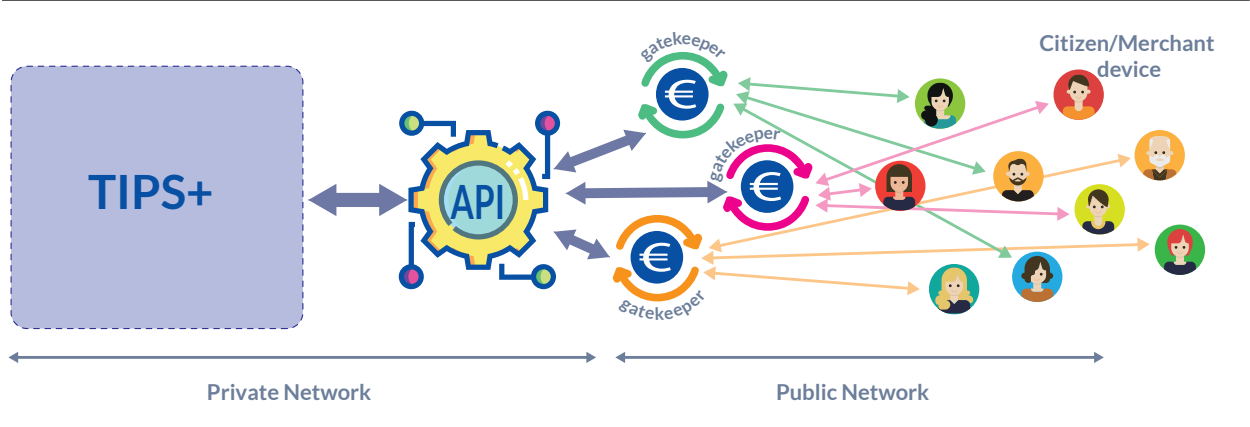
³⁶ TIPS+, with the introduction of technical positions, is open to pre-paid cards and any other type of bearer instruments

³⁷ The possibility to give access to a broader set of users (i.e. outside euro zone).

Table 1: Facets characterization of account-based model

Facet	Characterisation	Remarks
Ownership	Identity-based	Possibly knowledge-based for pseudonyms accounts
Ledger type	Account-based	
Distribution (systems)	Centralised	The core ledger is fully controlled by the Eurosystem
Distribution (infrastructure)	Distributed	
Operational model	Online	
Intermediation type	Gatekeepers or Settlement Agents intermediation	Intermediaries responsible for fulfilling KYC/AML regulatory obligations. A contingency module might provide users' direct access for emergency purposes.

Figure 3 - TIPS+ high level design model



Considering the high volume of transactions and the huge number of users, scalability is a key aspect that any CBDC system has to ensure. For this reason, TIPS+ must be designed in such a way that it is able to cope with the large increases in the volume of transactions, while preserving the average latency per transaction.

Availability is a crucial feature too. In order to build a 24/7/365 payment system characterized by very high (and actually enhanced) availability, the same principles underlying TIPS³⁸ are exploited: fault tolerance of nodes in the infrastructure and multi-site distribution. TIPS+ allows implementing

³⁸ TIPS+ can leverage the experience of the Eurosystem to manage existing gross and retail payment services in term of performance, availability and security.

coarse-grained Application Programs Interfaces (APIs) to grant interoperability with the central platform, and letting the private sector create value-added services on top of the CBDC.

In particular, TIPS+ intends to provide a predefined set of APIs that enables the carrying out of operations of even high complexity: for example, grouping and ordering into an atomic operation based on an all-or-nothing paradigm, scheduling payments and executing cross-currency payments.

TIPS+ is built with programmability in mind and is designed to offer public APIs. These APIs are provided to allow private sector companies to develop new applications.³⁹ The evolution of the APIs should occur in close cooperation with the stakeholders, in order to address the latter's desiderata and to embed state-of-the-art technologies and standard on the market (Wong and Maniff, 2020).

To better cope with the "need to know" principle, TIPS+ replaces the concept of "account" with that of "position": the latter implies that the central system is not aware of real users' identities, it just keeps track of technical identifiers (called pseudonyms); these are referred to as "positions". In order to get the job done, the central platform does not need to know real users' identities, but collects the minimum amount of information necessary to settle transactions. The detection of users' identities is the responsibility of intermediaries, to the extent needed and deemed appropriate by the policymakers. Moreover, since the central platform does not collect all the information that is needed to fully track a payment, authorities that may need to retrieve such information will have to collect it from all entities involved in the transaction. So thanks to the usage of pseudonyms, TIPS+ protects privacy of end-users that are only known to the central bank in the form of technical identifiers that hide their real identities from the central platform.

TIPS+ takes a further step forward and differentiates between end-user positions and technical positions. The former refers to positions created by individuals businesses and merchants; the latter refers to positions created by intermediaries (on behalf of customers) in order to offer their services.

Users can transfer money from every types of positions but only to end-user positions. Technical positions are provided with an initial balance at creation time and cannot be charged after creation; they can be used only to transfer D€ to end-user positions, as long as there is availability of money. The balance of a technical position can only decrease up to availability. Intermediaries could open technical positions in TIPS+ to offer pre-paid cards or other pre-paid services to unbanked users or non-euro area residents visiting a euro zone country. For example, a tourist may ask for a pre-paid card from a supervised intermediary against a payment in a foreign currency. The pre-paid card can then be used to buy goods and services during the journey and at the end of the stay the pre-paid card can be returned to the intermediary for eventual

³⁹ Fintech companies can develop applications in any modern language using platform APIs that follow standard and modern communication protocols.

disposal. The residual amount of D€ stored on the card may be converted back into the foreign currency.

A public key identifies each position and users own a private key that makes it possible to sign operations and to prove the ownership of a position in the system. The use of a public key to reference a position implies that a pseudonym⁴⁰ in the central system is the only information that TIPS+ needs to work properly.

Moreover, to effectively remunerate positions and set limits on holdings at the centralized level, one should make sure that users can only hold a single position in the system. This can be achieved, for instance, by enhancing the TIPS+ platform with a centralized directory used to identify the same entity across different gatekeepers.

TIPS+ does not place any technical constraint regarding forms of intermediation, such as settlement agents or gatekeepers. An intermediary organization can play the role of an access point for the CBDC: it may own a private registry of identities that maps positions in the TIPS+ system or provide a value-added service for the storage of private keys on users' behalf. For instance, gatekeepers could create some technical positions linked to prepaid services (physical cards or token-based mechanisms). Customers can buy these prepaid services from their intermediaries or authorized shops (users' identities may or may not be traceable, depending on the policymaker's preferences). Services of this kind can favour the inclusion of the unbanked and allow the usage of the D€ by non-resident people in the euro zone, similar to current currency exchange offices.

Intermediaries provide access to the central platform, however D€ is a central bank liability and the Eurosystem may be accountable to customers that are unable to access their positions in TIPS+.⁴¹ For instance a gatekeeper may be unavailable or unexpectedly/suddenly quit the business.

In these situations, customers might not be able to access their positions in TIPS+, so it is fundamental to consider solutions that allow them to access the central platform even in a contingency scenarios.

For example, the Eurosystem may provide a shared database⁴² with customer information in order to enable the migration of end users from a previous unreachable gatekeeper to a new one.⁴³

⁴⁰ The pseudonym is an identifier for each end user from which it is impossible to derive any end user personal data. All the pseudonyms would be stored in a directory at Eurosystem level, while personal data would remain under the responsibility of the gatekeepers that are in charge of the onboarding and identification of the users (KYC).

⁴¹ As previously said, the digital euro would be a central bank liability, issued by the Eurosystem as a digital representation of cash and therefore a risk-free form of central bank money, regardless of the technical solution chosen.

⁴² A database for customer data would be shared among gatekeepers. Each gatekeeper would be allowed to handle only the portion of information it owns. From a technical point of view, this database could be implemented with a blockchain technology, considering that the main requirements for such a service are resilience and security.

⁴³ Eurosystem may reallocate, inside the shared database, customer information that belong to an unavailable gatekeeper to a new active gatekeeper.

This database would provide a service at the platform level and would make it possible to mitigate both gatekeepers' overall costs to keep track of users' information and the risks associated with protecting data from cyber-attacks. Moreover, the choice of having a common service to manage customer data would sustain the data portability of customers from one gatekeeper to another even in normal situations.

2.4. THE ITCOIN PLATFORM

This section describes the authors' vision of a possible token-based D€, which is implemented on a platform called "itCoin". Section 2.4.1 briefly introduces the platform and the objectives that it aims to tackle, while Section 2.4.2 illustrates in more details the technical functioning of itCoin, and how it could be used to provide the D€ infrastructure to retail users, in collaboration with supervised intermediaries. Section 2.4.3 focuses on how the technology can accommodate different policy choices of the Eurosystem; the most relevant options and trade-offs that arise in that context are also briefly discussed (e.g. the trade-off between controllability and anonymity).

2.4.1. INTRODUCTION

The token-based leg of the combined architecture model can possibly be provided by the itCoin DLT platform, whose objective is to broaden the cash-likeness and competitive features of TIPS+. The itCoin platform is a blockchain-based back-end infrastructure, based on Bitcoin technology and prototyped by Banca d'Italia. Starting with the free and open source Bitcoin codebase, a few but substantial modifications have been made to accommodate the needs of the D€. In particular:

- 1) the issuance of the currency is controlled by the Eurosystem;
- 2) the core back-end infrastructure is operated by the Eurosystem;⁴⁴
- 3) the block latency and transaction volume are slightly better than Bitcoin's, e.g., a 1 minute block latency on average (compared to 10 minutes block latency on average), and a transaction volume of about 50 Transactions Per Second (vs. 5 TPS in Bitcoin).

Everything else has been left unchanged in the prototype in order to maintain compatibility with the Bitcoin protocol and to inherit all the existing ecosystem of protocols and applications that are built on top of its core infrastructure. For example, among other things: (i) the itCoin platform is open and directly accessible 24/7 to retail users and intermediaries via the Internet; (ii) the

⁴⁴ In Bitcoin, the consensus on transactions to be recorded in the ledger is reached via "Proof of Work" (PoW). This requires heavy computation involving enormous power consumption, but is necessary to the functioning of the network because transactions are confirmed by a set of anonymous validators. For D€, the context is completely different: since the Eurosystem is a trusted central authority, it is unnecessary to resort to techniques to prevent Sybil attacks in unrestricted systems like "Proof of Work" or "Proof of Stake" (PoS), and it is possible to use a "Proof of Authority" (PoA) approach, where the Eurosystem validates transactions to be recorded on the blockchain, by means of its own cryptographic signatures on the blocks. This would remove one of the biggest drawbacks of public blockchains based on PoW, namely the high carbon footprint.

BLOCKCHAIN

A blockchain is an ordered list of append-only records that contain transaction data. The blocks are linked together using cryptography: each block has a reference to the previous one, thus forming a chain, and the link is implemented using a cryptographic hash function. The data contained in a block cannot be altered retroactively without altering all subsequent blocks. Each block also contains a timestamp, which can be used to prove that the transaction data existed when the block was added to the blockchain.

UTXO-based data model,⁴⁵ the fee structure, the cryptographic primitives and the scripting capabilities are the same; (iii) ownership of the funds is attested by means of knowledge of some secret cryptographic information (e.g. private keys); in order to transfer ownership, it is necessary and sufficient to prove this knowledge to the ledger; (iv) the prototype does not implement remuneration (i.e., the interest rate is set to 0%).⁴⁶

As in the case of the TIPS+ platform, Table 2 provides the facet-based classification of the D€ that circulates on itCoin, without addressing the issues linked with offline usage.

Thanks to the previously mentioned ecosystem of protocols and applications, the itCoin-based D€ would be able to offer, among others, the following key characteristics:

- it would replicate some distinctive features of cash in the digital domain. In particular, and depending on certain policy design choices, the D€ could be designed to be easy to use for vulnerable groups, free of charge for basic use and, furthermore, it could provide a very high level of privacy protection;
- much freedom could be left to market operators, such as supervised intermediaries and Fintech players, paving the way for the possibility of building high value-added services on top of the central bank core infrastructure, by means of a widely and directly accessible open ledger, that resorts to well-known and state-of-the-art cryptographic technologies, inherited from Bitcoin. In this way, the D€ could have features that are at the technological frontier and offer the basis for providing functionalities that are at least as attractive as those of the payment solutions available in foreign currencies or through unregulated entities.

⁴⁵ The Unspent Transaction Output data model is an abstraction to implement a token-based system. Each UTXO is analogous to a coin, and holds a certain amount of value. It also represents a chain of ownership implemented as a chain of digital signatures where the owner signs a transaction transferring ownership of their UTXO to the receiver's identifier. The term UTXO refers to the output of a blockchain transaction that has not been spent and can be used as an input in a new transaction.

⁴⁶ In principle, other modifications to the protocol may be implemented, e.g. remuneration on a UTXO ledger could be theoretically envisioned. Nevertheless these changes are: i) incompatible with the ecosystem of applications that are already available in open-source, such as wallets, layer-2 nodes, etc., that in case of significant deviations will have to be heavily readapted; ii) an obstacle, and to some extent a "technical debt", to the merging of new and innovative features that will be developed in the future with the original protocol. As long as itCoin maintains a high compatibility with the Bitcoin protocol, any technological innovation that is developed in open-source for the Bitcoin protocol may be easily ported to the itCoin solution, also thanks to the strong commitment to long-term backward-compatibility of the Bitcoin project. This would allow the itCoin D€ to stay at the technological frontier of crypto-assets and stable-coin while retaining technological control of the solution. For these reasons, the choice has been to reduce to the bare essentials the number of modifications of the itCoin prototype with respect to Bitcoin.

Table 2: Facets characterization of itCoin token-based model

Facet	Characterisation	Remarks
Ownership	Knowledge-based	Ownership based on knowledge of cryptographic information, e.g. private keys
Ledger type	Token-based	Platform modelled on Unspent Transaction Outputs (UTXO)
Distribution (systems)	Centralised	The core ledger is fully controlled by the Eurosystem
Distribution (infrastructure)	Possibly distributed	Block creation may be distributed among multiple Central banks of the Eurosystem
Operational model	Online	
Intermediation type	Any	Direct access to itCoin is technically possible and depends on user choice. Note that liquidity access is different from technical access, and depends on policy choice (see 2.4.3).

2.4.2. TECHNICAL FUNCTIONING

The core back-end infrastructure of itCoin is a blockchain-based Distributed Ledger Technology, which is operated by one or more central banks of the Eurosystem. The itCoin DLT provides an open, trusted, append-only and moderately programmable ledger, which could be technically accessible by the public, via the Internet, 24/7/365. This allows end users to autonomously verify the authenticity of the transactions without trusting any intermediary but the Eurosystem.

Transactions that circulate on the itCoin DLT are:

- i) called “on-ledger” because they are validated and confirmed by the Eurosystem, by permanently writing them onto the itCoin ledger. Once this happens, they are considered final;⁴⁷
- ii) carried out between users identified by pseudonyms, whose association with real-world identities is generally unknown to the Eurosystem, but can become known to other intermediaries in certain scenarios;⁴⁸

⁴⁷ For the purpose of this paper, the legal implications related to the finality of the D€ transactions according to the Settlement Finality Directive (98/26/EC) have not been taken into account.

⁴⁸ Association between pseudonyms and real-world identities would be collected by third parties and not by the Eurosystem; for example, regulated intermediaries that end-users voluntarily choose as providers (e.g. wallet providers) will be asked to retain an association between the pseudonyms and real-world identities of their customers; similarly, commercial banks, which exchange the CBDC for commercial bank money and vice-versa, will know and maintain the association between pseudonyms and the real-world identity of people depositing/withdrawing the CBDC. In general, pseudonyms with an unknown relationship to a real-world identity may reside on the ledger itself. All the privacy and confidentiality implications that stem from the use of pseudonyms in a public ledger apply (i.e., pseudonymity in and of itself is not anonymity, but a sophisticated use of pseudonyms can provide some level of privacy/anonymity/untraceability).

- iii) visible to any user of the ledger, including retail users;
- iv) supported only within transactional limits, i.e., there is only a limited number of on-ledger transactions per unit of time that can be processed, such as 50 TPS. Similarly to Bitcoin, in order to prevent overload or abuses of the system (e.g. denial of service attacks to the open ledger system), there is a transaction fee mechanism in place, whereby users will have to bid for on-ledger transactional capacity;⁴⁹
- v) used to transfer a particular form of itCoin D€, called “on-ledger liquidity”, i.e., the D€ variety that circulates on the itCoin ledger, the core back-end infrastructure operated by the Eurosystem.

Because of the above characteristics, the authors foresee that the on-ledger transactions would not be a convenient form of payment to be used in the retail market and would be typically employed by intermediaries for gross settlement of large-value payments, or for settling the final net positions of many small value payments. In particular, the limited throughput and high latency would make on-ledger transactions unsuitable for use in everyday payments. In addition, the ledger is public and readable by everyone, and for this reason the techniques needed to preserve privacy and confidentiality on a public ledger are sophisticated and would require ad-hoc technical skills,⁵⁰ which are likely not present in an average retail user. Finally, the transaction fee mechanism would make this system unpalatable for the retail market.

In fact, the itCoin infrastructure would be one layer of the system, built by the Eurosystem for intermediaries, which in turn would be in charge of building, on top of it, a layer for retail users. It is crucially important to highlight that the itCoin ledger would offer programming capabilities,⁵¹ paving the way for the development of innovative smart-contracts applications by the market, including, but not limited to, payment applications. Among many others, the programmability model of itCoin would support the development of applications that make use of multi-signature arrangements (e.g. multi-signature escrows, or shared wallet control) and applications for the synchronization of D€ payments with external events, including the delivery of securities or payments taking place on different platforms (e.g. via Hashed Timelock Contracts)⁵² or based on external data feeds that are communicated by third parties called “oracles” (e.g. future contracts based on Discreet Log Contracts).⁵³ But above all, the most significant application in the context of a retail D€ is the Payment

⁴⁹ See Annex 2 for a detailed description of itCoin’s on-ledger transaction capacity aspects.

⁵⁰ See European Central Bank and Bank of Japan (2020) for a description of the most relevant techniques to preserve confidentiality in a DLT environment.

⁵¹ As mentioned, itCoin is based on the Bitcoin technology, i.e. a programmable platform. Nevertheless, its programmability is moderate in comparison with other crypto assets, such as, notably, Ethereum. Therefore, the choice of relying on Bitcoin-level programmability would restrict the attack surface, in order to better address the overall CBDC security requirements.

⁵² See European Central Bank and Bank of Japan (2018) (2019) and Bank of Canada and Monetary Authority of Singapore (2019).

⁵³ See Dryja (2019).

Channel Network (PCN),⁵⁴ which would allow two parties to execute a high volume of fast payments “off-ledger”.

The off-ledger payments would not be directly validated or individually confirmed by the central bank, and would not end up being individually recorded on the central bank ledger, but would be executed by bilaterally exchanging a sequence of digital, cryptographically signed, private contracts.

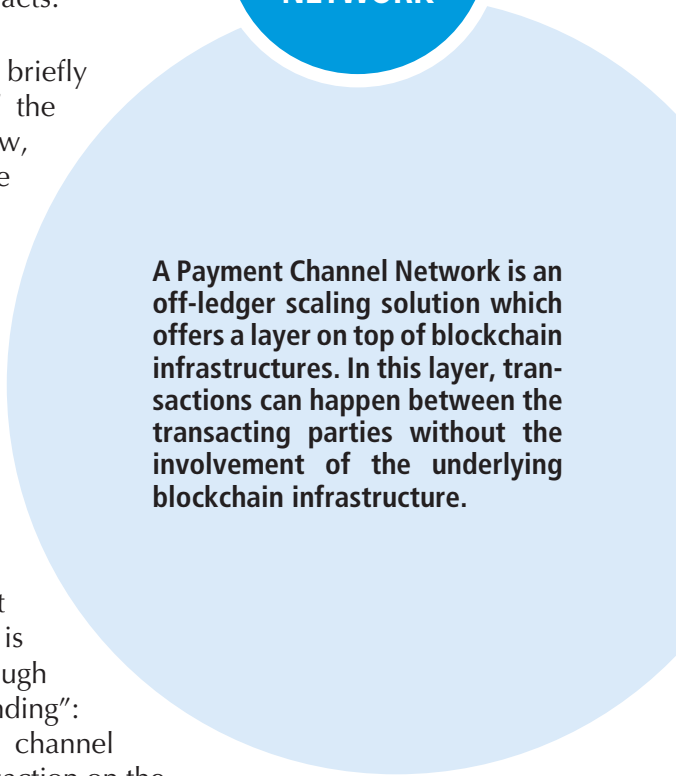
The remaining part of this section will briefly describe the technical functioning of the payment channel technology and how, according to the authors’ vision, the itCoin core ledger could be used by supervised intermediaries to create a PCN, which would represent the infrastructure for exchanging retail payments using the D€.

A payment channel can be conceptually described as a relationship between two parties, which agree on mutually exchanging payments up to a certain amount, without the need for on-ledger payment transaction recording. The channel is initially set up by the parties involved through a process that is similar to a “pre-funding”: in other words, opening a payment channel essentially consists in committing a transaction on the public ledger, thereby reserving for that payment channel a predefined amount of on-ledger liquidity, which is called the “payment channel capacity”. The process of pre-funding is crucial in two ways: (i) it defines once and for all the payment channel capacity, effectively imposing a limit on the amount of liquidity that can be owned on it; (ii) it is a necessary condition to ensure that there is no counterparty or credit risk involved in the future payments exchanged on the channel.

After the setup phase, the two parties can execute payments in the channel, within the limits of its capacity, by bilaterally exchanging a sequence of digital, cryptographically co-signed, private contracts. In principle, one or both parties may decide, but are not required to, to terminate the relationship and close the channel, by sending the last of these cryptographically co-signed contracts to the ledger, and retrieving the off-ledger liquidity in the form of on-ledger liquidity.



**PAYMENT
CHANNEL
NETWORK**



A Payment Channel Network is an off-ledger scaling solution which offers a layer on top of blockchain infrastructures. In this layer, transactions can happen between the transacting parties without the involvement of the underlying blockchain infrastructure.

⁵⁴ See Poon and Dryja (2016).

In other words, the functioning of a payment channel guarantees that:

- i) it is not possible to hold in the channel more off-ledger liquidity than the amount initially agreed upon, i.e., the payment channel capacity;
- ii) each payment exchanged in a channel is mutually signed by both the payer and the payee, and is always non-disputable before the ledger;
- iii) it is unambiguously possible to order the set of payments exchanged in a channel, thus defining a totally ordered set of “payment channel states”, which is known both to the sender and the receiver;
- iv) each party can independently decide to terminate the relationship (i.e., “close” the payment channel) and receive the corresponding amount of on-ledger liquidity that was previously held off-ledger.

To execute off-ledger liquidity transfers between any given owner of D€, it is not necessary to establish a complete set of payment channels between each possible pair of participants, which would be effectively unfeasible.⁵⁵ In fact, it is possible to route payments from a payer to a payee without a direct payment channel between them, as long as it is possible to establish a path of payment channels with enough capacity and liquidity that allows the latter to be reached by the former. This is the same principle that allows communications over the Internet, where each node of the network can communicate with any other even without a direct connection. By establishing a Payment Channel Network, shown in Figure 4 below, any two participants connected to the network can exchange off-ledger payments in D€, which are:

- i) called “off-ledger” because they are not directly validated or individually confirmed by the central bank, and do not end up being individually recorded on the central bank ledger;
- ii) peer-to-peer, in that individual payments are routed from user to user across a network of intermediaries over the Internet, without putting undue strain on the infrastructure of the central bank; the throughput of a PCN is effectively limited only by the ability of the parties involved in the process of routing payments, and thus not by the on-ledger performance of the underlying platform (i.e. itCoin), but only by the parties’ own technological infrastructure (e.g. network capacity, computational capabilities);
- iii) end-to-end encrypted, with an high degree of privacy; this is made possible by a routing mechanism known as “Onion Routing”,⁵⁶ which is used to deliver payments from payer to payee in an encrypted way;

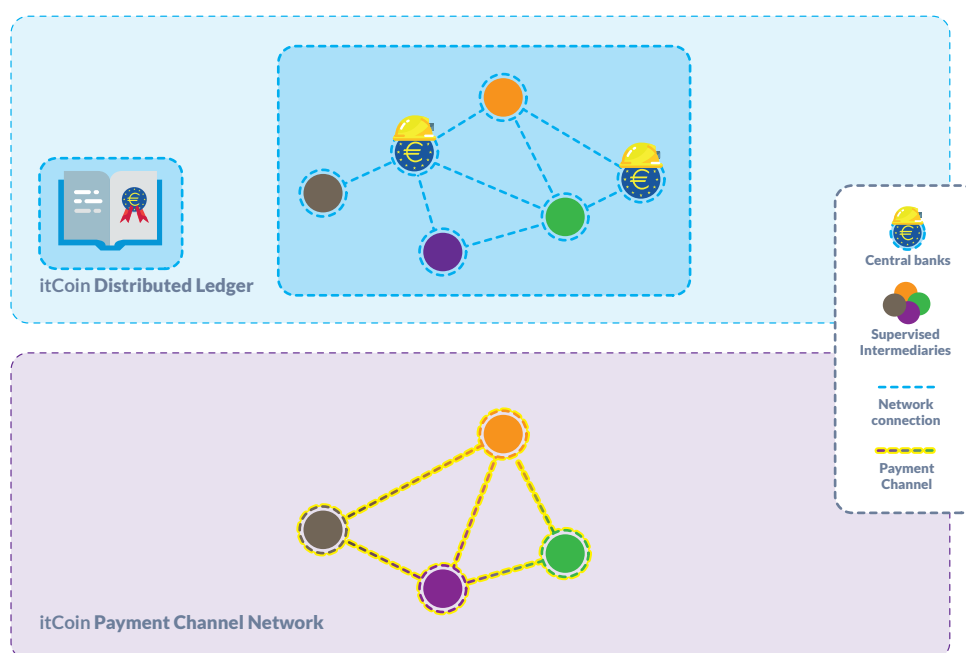
⁵⁵ The observation stems from the number of possible bilateral relationships in a set of N elements, which amounts to $N*(N-1)/2$ – thus growing as a quadratic polynomial in the number of elements. In a retail payment system with millions of participants, that would entail the necessity to establish “millions of millions” of payment channels.

⁵⁶ Onion routing networks were developed in the 1990s by the U.S. Naval Research Laboratory to protect Internet connections initiators and responders from eavesdropping and traffic analysis. The most widely known implementation of Onion Routing is the TOR Project, allowing for high degree of privacy in the usage of Internet (<https://www.torproject.org>). For more details see also US Patent n. US6266704B1, “Onion routing network for securely moving data through communication networks”.

- iv) not immediately final; this notwithstanding, the off-ledger liquidity may be considered as a liability of the Eurosystem,⁵⁷ in that it is free from credit/counterparty risk for the end-users, thanks to the availability of a direct technical access to the itCoin ledger, combined with the previously described pre-funding mechanism, which would allow each user (who is online and owns the cryptographic keys of their own wallet) not to incur a loss on its own off-ledger funds, even in case of a failure of the supervised intermediary.⁵⁸ In other words, in case of problems of the intermediary providing access to the PCN, the retail user can activate a backup procedure that closes the channel and allows the retrieval of their own off-ledger funds, in the form of on-ledger liquidity;
- v) possibly free of charge for the end users, depending on policy choices (see Section 2.4.3);
- vi) used to transfer another particular variety of the itCoin D€, called the itCoin “off-ledger liquidity”, i.e. the variety of D€ that circulates on the itCoin Payment Channel Network, a payment infrastructure operated by private sector market players.

Because of the above characteristic, off-ledger payments could be employed by retail users for their everyday payments. From a business perspective, it can be envisioned that supervised intermediaries would be the ones that will effectively create the PCN of the D€, establishing direct payment channels among them.

Figure 4 - The itCoin payment channel network construction is carried out by market players

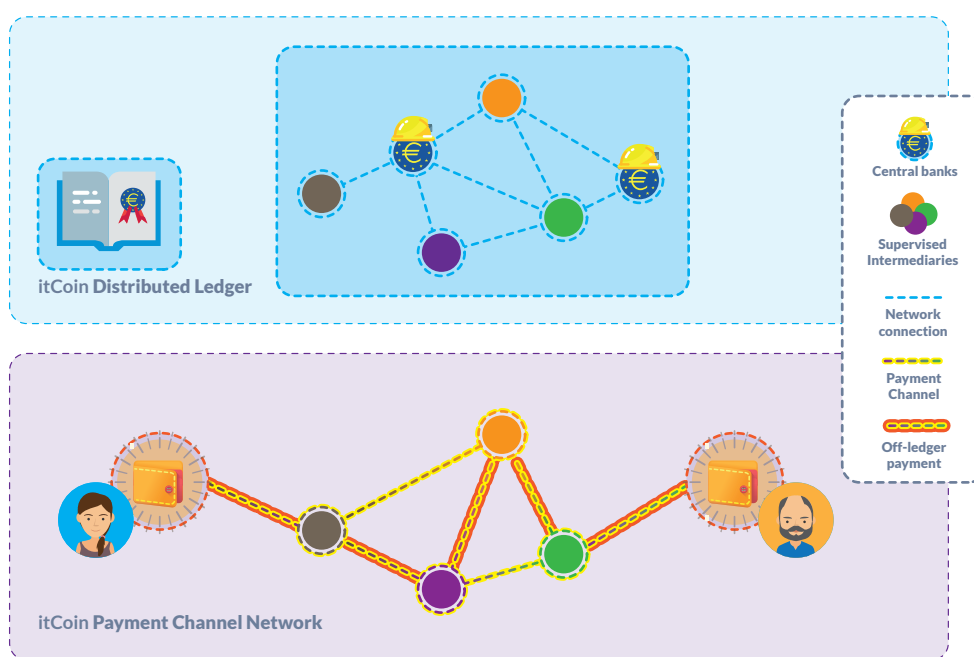


⁵⁷ This has to be confirmed subject to further investigation and in light of the legal framework that would support the issuance of the D€.

⁵⁸ A more detailed description of how off-ledger D€ could still be considered a liability of the central bank can be found in Annex 2.

Once the off-ledger infrastructure is ready, retail users would be allowed to connect to the network by opening payment channels with supervised intermediaries. It should be noted that, in this design, a D€ retail wallet is technically implemented with a payment channel (or set of payment channels) that is opened between a retail user and a supervised intermediary (or a set of supervised intermediaries). The overall payment channel capacity can be used to implement a wallet cap, which prevents the D€ from competing with commercial bank deposits: when the user wallet is empty, it can be topped up by withdrawing off-ledger D€ from commercial bank money accounts; when the wallet cap is reached, it will not be possible to receive payments in D€ and the excess liquidity may be deposited into a commercial bank account.

Figure 5 - The itCoin two-layer payment infrastructure allows retail payments to be exchanged in the PCN



To summarise, a two-layer payment design is described above, where the first layer is the itCoin distributed ledger (the light blue box in Figure 5) and the second layer is the itCoin payment channel network (PCN, the purple box in Figure 5). The first layer is managed by the Eurosystem and can be exploited by intermediaries to build an off-ledger infrastructure, D€ PCN, which would allow retail users to exchange high volumes of fast and off-ledger payments with a high degree of privacy and possibly free of charge. The two layers correspond to two different forms of D€, respectively called the on-ledger liquidity and the off-ledger liquidity, which exhibit different properties. The on-ledger liquidity, i.e. the D€ that circulates on the distributed ledger of the central bank, would constitute a digital euro with many useful features for supervised intermediaries, including programmability. On the other hand, the off-ledger liquidity, i.e. the D€ that circulates off-ledger in the PCN, would constitute a digital euro that functions online, with many cash-like features, and available to retail users for their everyday payments.

2.4.3. RELEVANT POLICY CHOICES

Within the technological boundaries of the solution, many design options are available to the Eurosystem, e.g. depending on whether the Eurosystem policies wish to prioritize the need of controllability and AML/CFT or the need to foster market innovations that guarantee very strong privacy protection to retail users, possibly including anonymity.

One of the most important policy decisions that the Eurosystem would face is whether to allow retail consumers to have access to on-ledger liquidity, i.e. to withdraw on-ledger D€ from supervised intermediaries. This key aspect is better explained by describing two different extreme scenarios.

At one extreme is the case in which on-ledger liquidity is tightly controlled by the central bank, which makes it available only to supervised intermediaries; in this scenario, retail users would access the digital euro only in the form of off-ledger liquidity on the Payment Channel Network infrastructure and via supervised intermediaries, which would on-board users upon verifying their identity. Under this policy, retail users would not be able to exchange commercial bank liquidity for on-ledger liquidity (i.e. withdrawal limits for on-ledger liquidity are set to zero). This set of policy decisions would implement a controlled access to itCoin, because it is expected to guarantee high controllability of the liquidity,⁵⁹ thus mitigating the risks related to bank disintermediation and to the possible use of the D€ for illicit activities, while still offering a good level of privacy protection.⁶⁰ As a result of the controlled access policy, the off-ledger liquidity would circulate privately in the PCN among retail users, but within the limits of the individual wallet caps that is set by the policy authority and is enforced via the payment channel capacity.

At the opposite extreme is the case in which on-ledger liquidity could be allowed to circulate also in the retail and unsupervised market, for instance to foster innovation, facilitate the development of payment applications by Fintech players, improve financial inclusion and privacy, or spur the cross-border use of the D€. In this scenario, end users could withdraw D€ from commercial bank money accounts also in the form of on-ledger liquidity (likely subject, at least, to the same kind of limits that are currently in place for physical cash) and the retail wallets would effectively have two balances, a balance for the on-ledger D€ and a balance for the off-ledger D€. In case of unlimited access to on-ledger liquidity, a user could autonomously (and

⁵⁹ On-ledger liquidity could flow into the retail market only upon the closing of a payment channel previously opened with an intermediary, and subsequently closed; this can be (i) discouraged, by not providing mobile app functionalities for the manual closing of non-empty payment channels and (ii) detected by a supervised intermediary, and made potentially subject to reporting to financial control authorities.

⁶⁰ In this scenario, privacy is guaranteed by the fact that there is no single party that is able to observe all the details of end user payments, which are spread among the intermediaries routing the off-ledger payments. Nevertheless, in this scenario the privacy level is not comparable with cash, and there is no anonymity. In particular, in a scenario of controlled access to itCoin, the risks for privacy stem from the fact that the topology of the PCN is constrained by the policy decision. The metadata learnt by the routing intermediaries may be merged and this would allow traceability of payments. A proper legal framework on the treatment and protection of off-ledger payments metadata should be put in place in this scenario.

potentially anonymously, in case they opt for an “un-hosted wallet”)⁶¹ send and receive on-ledger payments through their wallet, by means of an on-ledger address; this would improve the overall level of “cash-likeness” of the D€, at the expense of controllability and compliance with AML/CFT: as a result of this policy, the wallet cap and limits on transaction amounts cannot be enforced technically, but only via regulation, similarly to what happens with physical cash.

In between these two extremes, many policy choices are conceivable and could be further investigated, such as allowing on-ledger liquidity into the retail market within strict withdrawal thresholds, so that the overall amount of on-ledger D€ in circulation (and its possibly anonymous portion stored in the “un-hosted wallets”) is limited; or by means of multi-signature arrangements that always involve at least one supervised intermediary, so that the on-ledger D€ could circulate in the retail market among known identities (“hosted wallets”).

Another important policy decision that the Eurosystem will face is whether the off-ledger digital euro, being cash-like, should be free of charge for retail users. The development and operation of the Payment Channel Network infrastructure would represent a cost for the supervised intermediaries, to be compounded by the cost of the liquidity that is allocated to the payment channels with retail users. These costs would need to be covered somehow, and this could either be done by the Eurosystem itself (in this case the D€ would be free of charge) or by the retail users via transaction fees.

In general, it is relevant for the success of the retail D€ to identify an incentive for market players to build and offer front-end solutions to retail users. This is even more relevant for the special case of the itCoin DLT, because the front-end solutions include a whole new payment infrastructure, i.e. the PCN. For example, in the situation of controlled access to itCoin liquidity described above, only supervised intermediaries have access to the on-ledger form of D€, and thus only supervised intermediaries can participate in the construction of the PCN; in this scenario, if charging service fees to retailers is insufficient or undesirable, an available option for the Eurosystem could be to remunerate at an adequate rate the liquidity that intermediaries allocate to payment channels with retail users and among retail users, e.g. by allocating up to a given amount of D€ per user identity. At the other end of the policy spectrum, i.e. unrestricted access to itCoin liquidity, there would be no restrictions deriving from the traditional financial architecture on how market players organize themselves into roles/categories of intermediaries, and thus any market player can participate in the construction of the PCN; in this scenario, incentives may stem from the fact that Fintech start-ups may be willing to seize the opportunities offered by this new market in terms of providing products and services related

⁶¹ An un-hosted wallet, also called a self-hosted wallet, is a type of wallet that is directly managed by the end user, who does not require the intervention of a service provider or financial institutions to conduct transactions. For this reason, the user could enjoy some degree of anonymity. By contrast, a hosted wallet is a wallet managed by the user in collaboration with a service provider or financial institution, and is usually linked to the identity of the user via a ‘know your customer’ (KYC) procedure.

to the D€. In between, there may be many options that are currently unknown to the authors and whose exploration goes beyond the scope of this work.

2.5. TIPS+/ITCOIN BRIDGE

Under the integrated approach, the centralized TIPS+-based D€ and the itCoin solution interact with each other through a bridge component. Even though this model encompasses the TIPS+ and itCoin platforms, this is not the only viable solution. Thanks to the openness of this model, the account-based platform can interact with other systems, which can be integrated on the basis of the value-added they may bring (see Section 3.3.2 for an example of alternatives).

TIPS+ and itCoin will be linked with each other by means of the bridge component as to create a seamless integrated model, in which there is no hierarchy between the two. In such a solution, both retail users and intermediaries can have accounts/wallets in either one or more platforms (with completely independent positions/balances), and payments can be exchanged either within the same platform or from one platform to the other. This section explains the processes of issuing the D€ and carrying out payments across different CBDCs. Because of the flexibility of the model, the same solution can be adopted if TIPS+ is integrated with a solution other than itCoin.

Liquidity would be injected in the system only through the TIPS+ component;⁶² in this way, the issuance process would rely on the mechanism already envisaged to fund any other TARGET Service such as RTGS, T2S or TIPS.

The sole source of liquidity would be that of the ECB's Central Liquidity Management (CLM) facility. Access would be restricted to authorized institutions,⁶³ which would be the only ones to hold accounts in it, as is already the case today for the existing TARGET Services. Intermediaries would obtain D€ by transferring liquidity from their accounts in the CLM platform to their accounts in TIPS+ (meaning the accounts in TIPS+ would be credited and their corresponding accounts in the CLM would be debited).⁶⁴

Intermediaries could move the liquidity into their wallets in the itCoin solution through the bridge component, which is operated by the Eurosystem, and finally to the wallet holder. The Eurosystem would play a key role, orchestrating the transfers across TIPS+ and itCoin based solutions.

Finally, the D€ can leave the CBDC system by becoming commercial bank money or cash, following the reverse process compared with the injection phase.

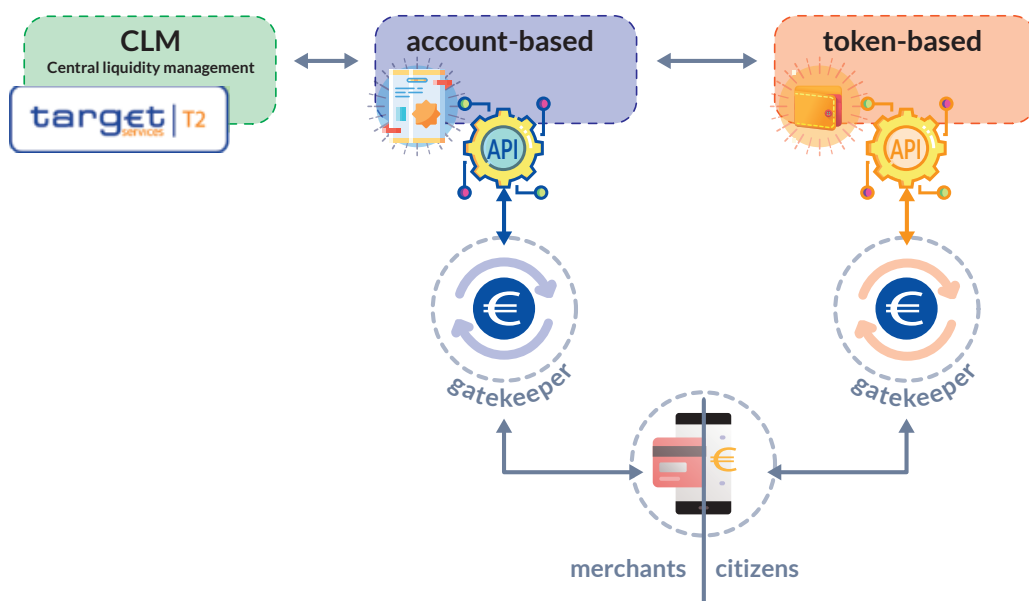
⁶² There would be no technical constraint to inject liquidity in all the components, but there would be also no practical advantage in doing so.

⁶³ Participation in TARGET Services is governed by the TARGET Guideline. See European Central Bank (2012).

⁶⁴ The issuance process relies on the same mechanism used for funding any other TARGET Service, with the difference that, in TIPS+, liquidity turns into a digital currency held in the TIPS+ positions accessible to end users.

Figure 6 below illustrates the process through which the D€ is issued:

Figure 6 - Process of issuance of digital euro



The interoperability between the platforms allows the Eurosystem to control a single digital currency, making the underlying technological duality of the system completely transparent.

Irrespective of how the D€ is stored, users can exchange payments between the two platforms: transactions within each D€ solution are possible, and so are solutions relying on both platforms. Hence, if in a D€ transaction the payer uses TIPS+ and the payee itCoin (or vice versa), the payment between the parties needs to cross the payer's platform domain – i.e., to go through the bridge component. In such case, the payment is sent to a special account/wallet on the payer's platform that is controlled by the Eurosystem, together with the instructions that are needed to forward the payment to the ultimate payee on the platform they use. The bridge component receives the payment, reads the incoming instructions and acts as a universal switch for the payment. Finally, the bridge component forwards the payment to the ultimate payee, on the appropriate platform according to the instructions received. This process is dubbed 'cross-pay through the central bank,' or XP-CB.

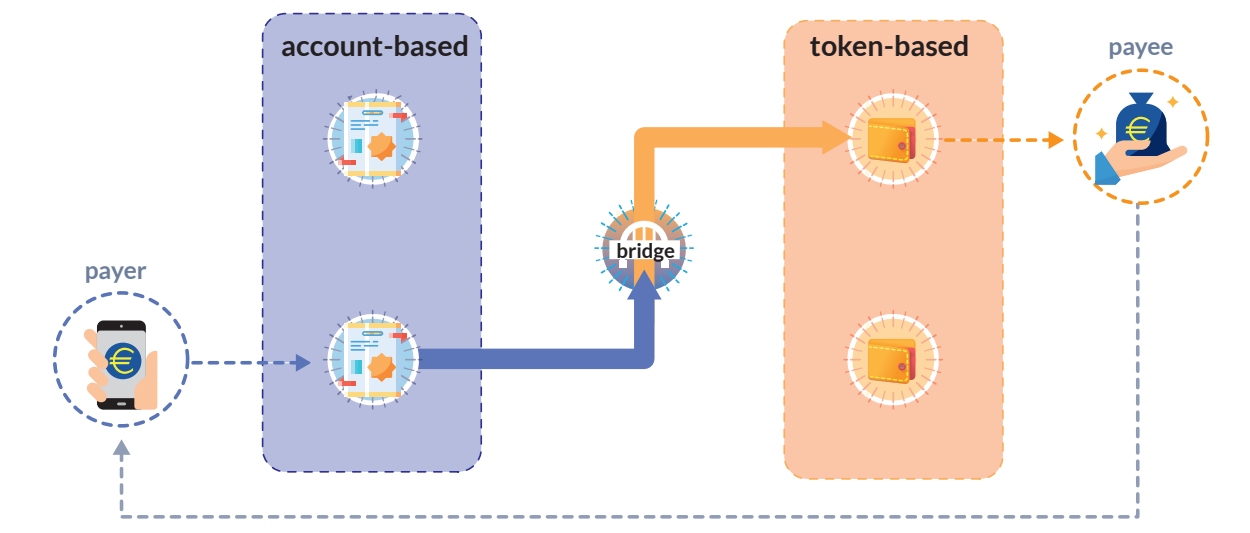
Therefore, the central bank, in its capacity as operator of the bridge component, acts as a trusted intermediary providing liquidity on all the platforms and routing inter-platform D€ payments.

For a better understanding, a possible scenario where the payment is originated from a payer's account in TIPS+ (e.g. a retail user) and successfully credits a payee's wallet (e.g., a merchant) in itCoin is described in Figure 7. The process consists of the following five steps:

- 1) The payee sends to the payer an itCoin payment request, containing the forwarding instructions.

- 2) The payer initiates a payment from its TIPS+ account to the payee's itCoin wallet. The payer's intermediary realizes that a cross-solution payment is needed and hence triggers the bridge component. The payment reaches the TIPS+ domain, where it triggers a payment order from the payer's account to the technical account in TIPS+, which is managed by the central bank.
- 3) The bridge component processes the incoming payment from the payer and successfully decodes the routing information, which identifies a payee within the itCoin domain.
- 4) The bridge component issues a new transaction from the technical wallet of the central bank in itCoin to the payee's wallet.
- 5) The payee acknowledges the settlement of the transaction.

Figure 7 - The XP-CB process



2.6. eCASH - AN ALTERNATIVE TOKEN-BASED PLATFORM

This section discusses the integration of TIPS+ with a non-DLT token-based system, eCash, meant to address the cash-like features in a person-to-merchant scenario.

eCash is a token-based payment scheme for which the earliest proposal was published by David Chaum in 1983; its possible usage in a CDLC system has been recently described by the Swiss National Bank (Chaum, Grothoff and Moser, 2021). It provides the technology to enable the exchange tokens directly from a payer to a payee, granting anonymity on the payer's side only. Anonymity for payers' transactions stems from the adoption of "blind signatures",⁶⁵ which come into play during the issuance of tokens. Because of the asymmetric anonymity property, the eCash technology is more suitable for

⁶⁵ See Chaum (1983).

a person-to-merchant use case, though it can be adapted to a person-to-person scenario.

Anonymity on the payer’s side reflects the common need to preserve privacy in case of some sensitive purchases by fully protecting payer’s identity vis-à-vis the payee or any other party. As mentioned above, the main scenario for eCash is, thus, person-to-merchant payments.

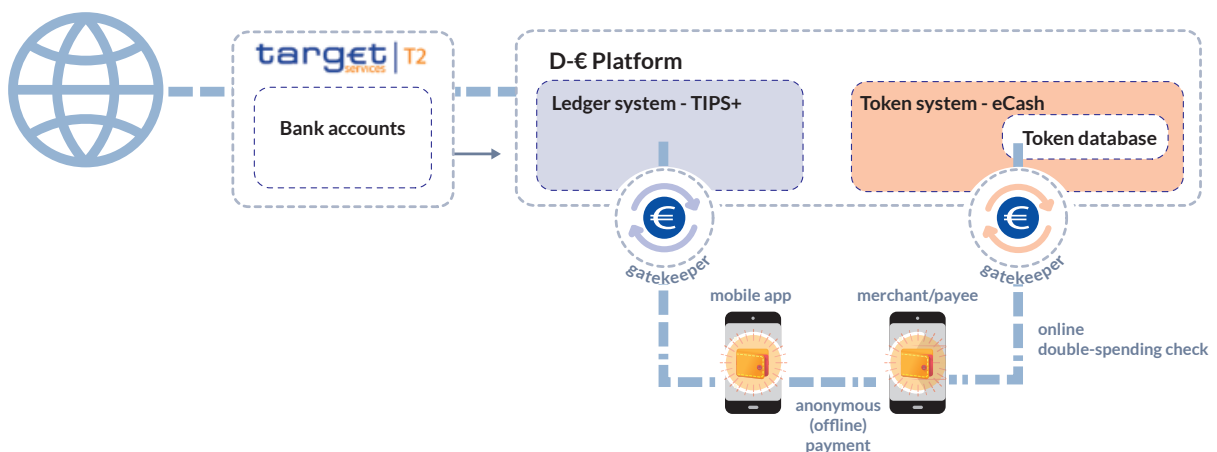
Looking at how eCash works, if users are in proximity, they can use mobile devices to exchange tokens as a means of payment. However, the transfer of tokens is not limited to mobile devices, and eCash can also support payments from mobile devices to web applications (e.g. e-commerce). With reference to the use case of mobile devices, people and merchants use two different types of mobile applications:

- the first type, developed for people, allows the user to request the issuance of tokens (i.e. issuance phase) and to perform transactions (i.e. payment phase); tokens are then stored in a wallet;
- the second type, developed for merchants, allows the user to accept tokens (i.e. payment phase) and ask the central platform for the conversion of tokens into D€ stored in their TIPS+ position (i.e. conversion phase).

In the issuance phase, end users utilize the mobile app to generate tokens and ask the central bank to sign them in “blindly” in order to complete and approve the issuance of the requested tokens. During this phase, the central platform debits end users’ positions for the equivalent amount of D€. The central bank receives tokens that are already “blinded” via cryptographic functions, and for this reason, it signs and confirms the issuance of the tokens without “seeing” them. Once the tokens are issued, the payer can spend them only once for transactions with merchants. During the conversion phase, the central bank is not able to identify the previously signed tokens and the identity of the user who first asked for the issuance of the tokens.

Therefore, in this alternative combined model (TIPS+ plus eCash, visually presented in Figure 8), end users can ask the central platform to convert D€

Figure 8 - The eCash model integrated with TIPS+



in their positions into tokens that will be stored locally on the user's device (i.e., their smartphone) inside a logical container called wallet.

By imposing limits on the amount of tokens – and therefore of D€ – that users can withdraw, the central bank can have control over transactions settled anonymously.

Looking deeper into the payment phase, a transaction is simply the transfer of tokens from the wallet of a payer to the wallet of a merchant. The wallet of a payer stores tokens that have not been spent yet in payment transactions, while the wallet of a merchant stores tokens already spent that can only be converted by the CB into D€ by crediting the end-user positions of merchants.

This transfer operation is completely secure against double spending if the merchant checks the tokens online; but the operation could be executed entirely offline if the merchant is willing to accept the risk of receiving a token that has already been spent.⁶⁶

As mentioned above, when merchants want to convert received tokens into D€, they initiate the conversion phase, whose objective is to destroy tokens in their wallets and to credit their positions in TIPS+. The central platform receives tokens and verifies them for authenticity and double spending; the tokens can then be converted into D€ in the end-user position of the payee.

Once spent by payers, tokens cannot be used anymore, and payees are not allowed to use them for other payments. At the end of a transaction, tokens received by payees represent nothing more than a medium of exchange for money in the central platform.

To summarize, the combination of TIPS+ with eCash leverages a token-based extension that makes use of advanced cryptographic techniques such as blind signatures, without relying on blockchain technology. As in the case of the other platforms, Table 3 provides the facet-based classification of the D€ that circulates on eCash, without addressing the issues linked with offline usage.

The advantages of using such a token-based platform is that TIPS+ leverages the adoption of a secure way to provide tokens – which even permits offline payments with no need to rely on secure hardware – to end users' devices by guaranteeing anonymity on the payers' side. From the TIPS+ side, the integration with eCash mainly consists in debiting the positions of payers when tokens are generated and crediting the positions of payees when tokens are converted in D€.

⁶⁶ eCash includes a way to disclose to the central bank the identity of a payer who used the same token multiple times.

Table 3: Facets characterization of eCash token-based model

Facet	Characterisation	Remarks
Ownership	Knowledge-based	Ownership is based on possession of the tokens, which are not linked to user identity
Ledger type	Token-based	The platform keeps track of the spent tokens
Distribution (systems)	Centralised	The token ledger is fully controlled by the Eurosystem
Distribution (infrastructure)	Possibly distributed	Transaction validation can possibly be distributed
Operational model	Online	
Intermediation type	Gatekeepers or Settlement Agents	

3. RESULTS OF THE EUROSISTEM’S EXPERIMENTATION OF POSSIBLE TECHNICAL SOLUTIONS FOR THE D€

3.1. OVERVIEW

In September 2020, the HLTf on CBDC, after the approval of the ‘Report on a digital euro’ by the Governing Council, established a new technical group of NCB and ECB experts with the mandate to gain further insights into possible technical solutions for a digital euro. The work was organized in four work streams:

- Work Stream 1 – “Scale the existing”: experimental activities concerning an account-based solution built on TIPS (and called TIPS+). Besides the benchmarking of the settlement ledger, the work stream also explored different forms of interaction with end users, privacy features, CBDC remuneration and technical possibilities for information exchange.
- Work Stream 2 – “Combined feasibility”: including two experiments, named “Flat approach” and “Tiered approach”, investigating different ways to integrate a centralized ledger with one or more distributed ledgers. The work stream focused, among other things, on programmability and privacy features.
- Work Stream 3 – “A new solution”: based on a blockchain solution with fixed value tokens called ‘digital bills’. In addition, the work explored the possibility of combining the blockchain solution with existing systems for the digital identity of users (e-ID). The work stream analysed both the performance aspects of the ledger and its interactions with different identification systems and privacy feature.
- Work Stream 4 – “Bearer instrument”: together with six companies selected via a procurement process, the research conducted by this work

stream focused on offline payment solutions (i.e. hardware-based bearer instruments) that were already on the market or under development, and that could facilitate the use of a digital euro as a bearer instrument.

The experiments assessed different design features – that are complementary to each other and may be combined into different architectures – with the main objectives of providing input for open design questions identified by the HLTf-CBDC that warranted analysis in terms of their technical feasibility and of acquiring a broad understanding of the compliance of the different possibilities with the principles stated in the HLTf Report on a digital euro. The experiments did not endorse any specific solution and the findings of this experimental phase do not pre-empt any decisions or commit the Eurosystem to providing a digital euro.⁶⁷

The remainder of this chapter illustrates the outcome of the experimental activities undertaken within Work Stream 1 and Work Stream 2 (for the “Flat approach” experiment), with specific reference to the possible architecture for the D€ described in Chapter 2.⁶⁸

3.2. LEDGER BENCHMARKING

3.2.1. WORK STREAM SCOPE

Work Stream 1 – “Scale the existing” focused on two main goals:

- 1) Experimenting on a solution for the issuing, redemption and distribution of the digital euro based on a new network architecture that builds on and extends the already existing, centrally managed, distributed architecture based on the TARGET Instant Payment Settlement system (TIPS).
- 2) Exploring how such a digital euro back-end solution could be embedded in and interoperate with the current payment landscape.

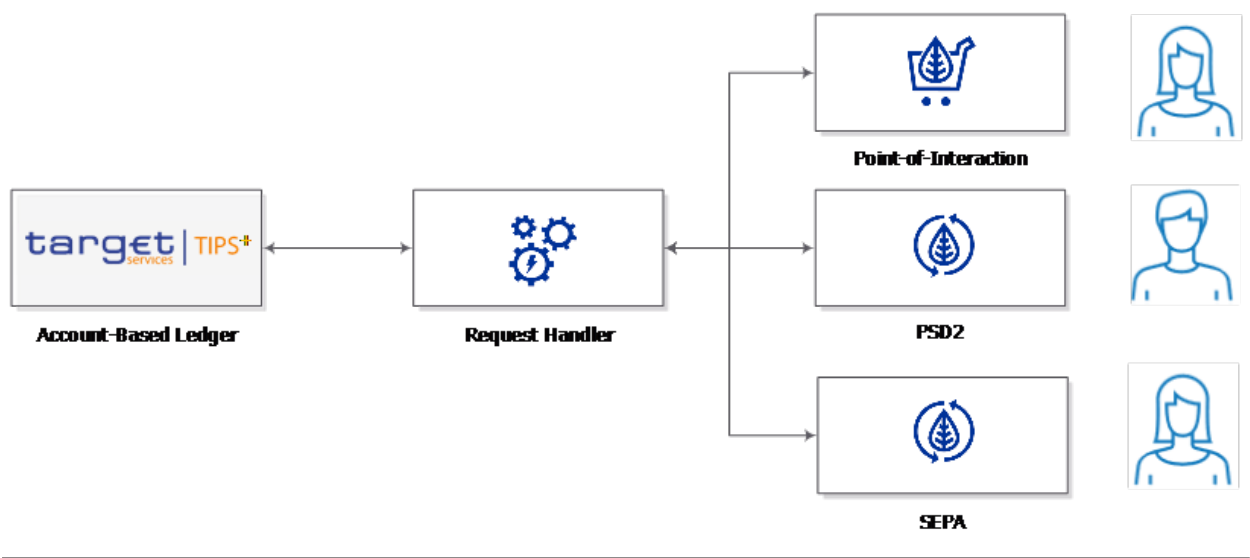
3.2.2. PROTOTYPE ARCHITECTURE AND TECHNOLOGICAL CHOICES

Figure 9 outlines the technical architecture of the prototype built and tested within Work Stream 1:

⁶⁷ Banca d’Italia participated in all the work streams and wishes to thank all the central banks who joined the work teams for their valuable contribution and for the excellent co-operation throughout the whole experimental phase. With particular reference to the work streams that are described in this section, we would like to express our thanks to the European Central Bank, Banque de France and the Oesterreichische Nationalbank for participating in both Work Stream 1 and Work Stream 2 (for the “Flat approach” experiment); De Nederlandsche Bank, Deutsche Bundesbank, Bank of Greece, Latvijas Bank and Banco de Portugal for participating in Work Stream 1; Banco de España and Banque centrale du Luxembourg for participating in Work Stream 2 (for the “Flat approach” experiment).

⁶⁸ For a complete description of all the experimental activities and results relating to all the work streams, please refer to European Central Bank (2021b).

Figure 9 - Prototype’s technical architecture



3.2.2.1. ACCOUNT-BASED LEDGER

TIPS+, the account-based ledger, relies on a TIPS-like architecture, i.e. a centrally managed, technically distributed infrastructure.

For the sake of the experimental activities, a dedicated public cloud tenant hosting all systems was built, along with the necessary middleware clusters.

At the application level, the software was deployed in its production version (i.e. as the current TIPS service) and then made available in an enhanced version (i.e. as TIPS+, with account-based ledger behaviour), after implementing the adaptation required for the work stream. In this respect, the main changes that have been implemented are:

- the use of pseudonyms to identify digital euro accounts and
- a new set of PSD2-like APIs for retrieving information on digital euro account balances and for instructing digital euro transactions.

3.2.2.2. REQUEST HANDLER

The role of the Request Handler is to regulate access to (and from) the core ledger and interact with the interfaces. The Request Handler and the PSD2, POI and SEPA interfaces (see sections below) compose the *network architecture*. The Request Handler translates valid instructions coming in through the interfaces into core ledger instructions. Invalid instructions are rejected. The result of an incoming request is communicated back to the originator of the request through one of the interfaces.

3.2.2.3. POINT OF INTERACTION INTERFACE

The Point of Interaction (POI) implements a business scenario wherein a physical terminal accepts payment from a mobile wallet and forwards it to the

Request Handler for settlement in TIPS+. For this purpose, an external partner delivered (i) physical POI terminals (as are currently used for POI payments), (ii) with an integrated back-end solution that communicates with the network architecture and (iii) specifically created mobile wallets to initiate payments on the prototype.

3.2.2.4. PSD2 INTERFACE

The PSD2 interface provides third party access to the D€ system via standardized ways with which the payment market is already used to communicating. The implemented interface provides PSD2 APIs as defined by the Berlin Group standard.⁶⁹ Additionally, a mobile web application was created in order to simulate a third-party service. To achieve a minimum viable product, the developed services provide a defined set of functionalities to their users. It is possible to check account balances, initiate transactions and view an account's transaction history based on IBANs. The mobile web application supports the managing of multiple D€ accounts simultaneously.

3.2.2.5. SEPA INTERFACE

The SEPA interface is used for converting commercial bank money to D€ and vice versa by using an instant payments infrastructure. It can receive (and send) messages from (and to) the mock-up SCT-Inst processor (of a commercial bank). The message format is based on the obligatory fields for the regular processing flow as described in the SCT-Inst Rulebook⁷⁰. In this model, the digital euro holders can be both the originator and the beneficiary as defined in the SCT-Inst scheme. If the digital euro holder acts as the originator, the correspondent account in the core ledger is debited, essentially destroying the digital euro. If the digital euro holder is the beneficiary, its account in the core ledger is credited and the digital euro is created.

3.2.3. EXPERIMENTAL RESULTS

Work Stream 1 aimed at benchmarking a TIPS-like architecture against the following dimensions and Key Performance Indicators (KPIs):

- throughput (number of transactions per second), with a KPI of 10,000 transactions per second with an account cardinality (total number of accounts defined in the system) of 100 million;
- settlement latency (processing time per transaction), with a KPI of 95% of transactions processed within 5 seconds and 99% of transactions processed within 10 seconds;
- carbon footprint (CO₂ equivalent), with no specific KPI.

⁶⁹ <https://www.berlin-group.org/>

⁷⁰ <https://www.europeanpaymentscouncil.eu/what-we-do/sepa-payment-schemes/sepa-instant-credit-transfer/sepa-instant-credit-transfer-rulebook>

The aim was to test whether a TIPS-like architecture can fulfil the performance requirements of a digital euro platform.

Performance (transaction throughput, settlement latency and account cardinality)

During the experimentation, as already mentioned, a PoC was created in a cloud environment to reproduce the part of the TIPS production installation necessary to process Application-to-Application (A2A) type payment requests.

Using this installation, tests were carried out to understand how many more front-end servers (i.e. the *Message Routers* that are in charge of processing incoming and outgoing messages) would be necessary for the current production system to manage the number of agents required by the experimentation (target KPI set to 10,000 payments per second).

The number of servers to be added has been set as equal to 6, thus bringing the number of front-end servers required to a total of 10.

Figure 10 - Average and 95% Pctl Latency (ms) vs Incoming Traffic (payments/sec)

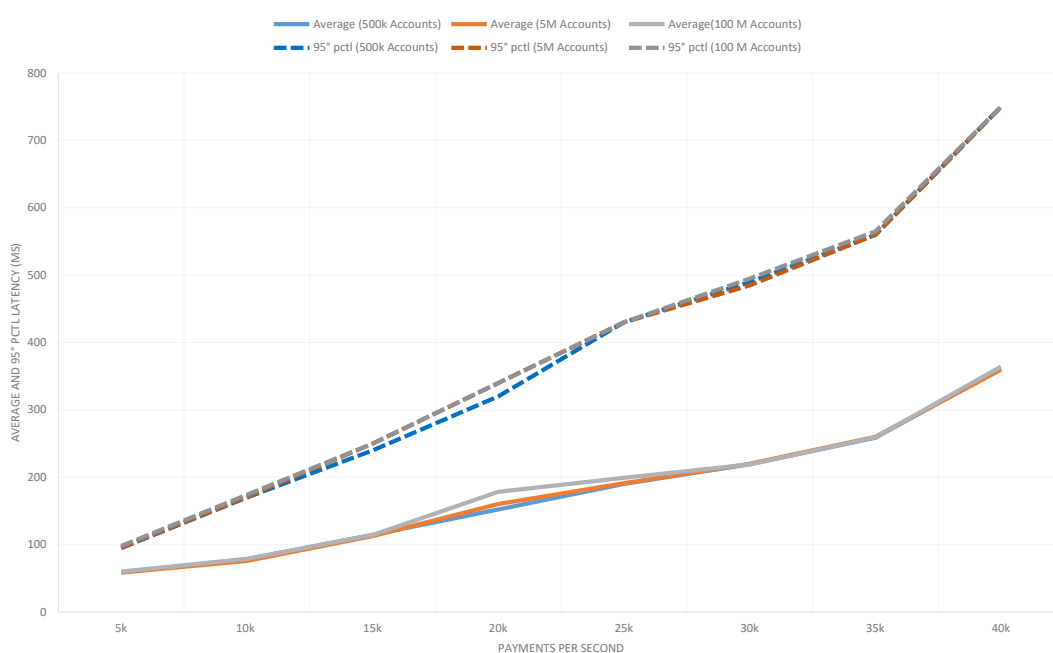


Figure 10 above shows the result obtained for the three different setups with a varying number of accounts, corresponding respectively to 500 thousand (500k), 5 million (5M) and 100 million (100M) accounts.

The graph shows, for each measurement, the average value of the latency calculated on the totality of payments injected during the test and the latency value within which 95% of the payments subject to the test are included (95 pctl).⁷¹

⁷¹ Both latency values are calculated end-to-end within the TIPS+ boundary, i.e. not including network, gatekeepers and users' processing time.

For each configuration (number of accounts and incoming traffic, i.e. transaction throughput), measurements were taken over a period of one (1) hour (sustained incoming traffic).

As can be seen in the graph, the throughput target KPI of the experiment (10,000 payments/sec) was reached and the average latency measured at this value was 59 ms, with a value of 95 pctl equal to 95 ms.

An important finding is that the number of accounts has no influence on the settlement latency of individual payments. This result is in line with expectations (i.e. greatly exceeding the given KPIs), due to the use of in-memory processing techniques and serial payment processing performed by the TIPS+ settlement engine. Tests have shown that these techniques can be effectively applied to the target number of accounts of the experiment. Nevertheless, the TIPS design may also be improved to limit serial processing to payments that debit the same account and to distribute account balances across multiple machines, in such a way as to remove any theoretical limit to the scalability of the system.

The system, sized to manage 10k payments per second, proved to be able to withstand an incoming traffic reaching 40k payments per second, with an average latency of 361 ms and a value of 95 pctl equal to 750 ms.

In all test cases, 100% of payments were settled under 5 seconds, thereby going beyond the initially given KPI.

It also follows for the technical design that a different setup of the cloud environment, with a greater number of front-end servers, would have made it possible to reach even higher throughput values, but this aspect has not been tested as the results obtained with the given configuration were already four times better than the proposed KPI.

Carbon footprint

The carbon footprint of the hypothetical TIPS-based D€ production system (sized to manage 10k transactions per second) was calculated on the basis of the configuration of the test system implemented in the PoC, which showed that the simple addition of only 6 (virtual) front-end servers was enough to achieve the expected result.

Starting from the electricity consumption values of the TIPS production system and knowing the number of virtual servers to be added, the total electricity consumption value of the TIPS-based D€ production system was estimated, including all the servers necessary to supply the service, develop, test and manage it. Therefore, the estimate provided does not relate to the PoC conducted in cloud, but instead refers to a hypothetical fully fledged production system.

The values reported in Table 4 were obtained:

Table 4: Carbon footprint estimations

Total Electrical Power consumption per year	170.687 kWh/year	This includes all Development, Test and Production servers needed including the ITSM ¹ tools.
Total Emitted CO₂e per year	86.367 kgCO₂e /year	Assuming the system is running in the current Banca d'Italia Datacenter, i.e. using the current PUE ² value.
Emitted CO₂e per single payment	0,00027 gCO₂e / payment³	Assuming a sustained rate of 10k payments per seconds for 1 year.

1) Information technology service management (ITSM) are the activities that are performed by an organization to design, build, deliver, operate and control information technology (IT) services offered to customers. – 2) Power Usage Effectiveness (PUE) is a measure of how efficient a data center is in using the electricity that powers it. It is a parameter that gives a figure of how much electrical power is dedicated to the power supply of IT equipment compared to auxiliary services such as air conditioning or UPS losses. – 3) According to many estimations publicly available on the web, this figure is about 6 orders of magnitude smaller than the carbon footprint of Bitcoin. More information can also be found in Tiberi, 2021: “*The carbon footprint of Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures*”. *Markets, Infrastructures, Payment Systems*, nos. 2021-5.

3.3. INTEGRATION BETWEEN THE ACCOUNT-BASED AND TOKEN-BASED COMPONENTS

Within Work Stream 2 – “Combined feasibility”, the “Flat approach” explored how the TIPS+ account-based platform (described in Section 2.3) could be complemented by another platform, based on a Distributed Ledger Technology (DLT), which would provide some of the features that may be missing in the former. In particular, in order to show different combinations of systems aiming to solve different kinds of problems and to address different requirements, two versions of the combined feasibility model were explored:

- the first version combines TIPS+ with itCoin, the token-based DLT described in Section 2.4, which enables the creation of an online bearer digital euro; this solution is best suited to addressing the requirements of cash-like features and competitive features of the HLTF report on the D€;⁷²
- the second version combines TIPS+ with a permissioned and programmable DLT based on Ethereum technology, which will be described in Section 3.3.2. This second DLT enables the creation of a programmable digital euro aimed at addressing requirements of enhanced digital efficiency and competitive features, as referred to in the HLTF report on the D€.

The fundamental idea of this combined feasibility model is that both the account-based and DLT-based platforms offer platform-specific functionalities, by means of platform-specific Application Programming Interfaces (APIs); they

⁷² As highlighted in Section 2.6, a non-DLT platform based on the eCash scheme could also be used to complement TIPS+ in terms of cash-like features. This scheme has not been part of the experiments for two reasons: (i) The focus of Work Stream 2 was explicitly on the combination of centralized platforms with distributed ledger technologies, while the eCash scheme is not based on DLT; (ii) Banca d'Italia had already developed a first itCoin prototype at the end of 2019, while no previous experience was available for the eCash payment scheme.

operate at the same level (hence the label ‘flat’): retail users and intermediaries can have accounts/wallets on either one of the two platforms or on both (with completely independent positions/balances); payments may occur within the same platform or may involve both of them. The result of the integration is the emergence of a D€ available to retail users in multiple and interchangeable forms that can accommodate their different needs along a number of dimensions, such as latency, volume of payments, privacy level, and programmability.

The integration solution developed in this work stream builds upon and extends an existing model in which a cross-platform payment is routed via a trusted intermediary.⁷³ It relies on the role of the central bank as a ‘bridge’ between the account-based and the DLT-based domains, as also described in Section 2.5. When a payment is made that needs to cross the borderline between the two domains, e.g. from a payer in a DLT system to a payee in TIPS+, then the payment is routed to the payee via the central-bank-operated bridge. In this solution, the central bank thus fulfils three functions; specifically, it acts as: (i) a trusted orchestrator of payments (i.e., the payer sends the payment to the central bank trusting it will forward the payment to the payee); (ii) a source of liquidity (i.e., the central bank ensures that enough liquidity is available on both platforms at all times to forward any payment to the payee’s wallet or account); and (iii) a technical operator of the platforms and of the bridge. During the experimentation phase, a Proof-of-Concept (POC) for the bridge component between the TIPS+ platform and the DLT platform was implemented. The POC aimed at presenting the basic functionalities of the bridge and the feasibility of the XP-CB process described in Section 2.5. Other requirements of the bridge service, including the performances, the high availability and the atomicity guarantees of the cross-transfers in the presence of failures were not tested during this experimentation phase and may be the subject of further investigation.

3.3.1. INTEGRATION BETWEEN TIPS+ AND ITCOIN

In this implementation, the DLT-based leg of the integrated solution is given by itCoin. As described in Section 2.4, itCoin is a public blockchain infrastructure which, for experimentation purposes, has been operated by Eurosystem central banks. The objective of this flat model is to show that a blockchain-based digital euro and an account-based one complement one another and jointly accommodate a variety of user needs. In particular, as described in Section 2.4, a back-end infrastructure based on a moderately programmable, open and public ledger (i.e. a ledger that anyone can access via the Internet, 24/7/365), such as itCoin, can be exploited by intermediaries to build an off-ledger infrastructure, namely the payment channel network (PCN), thus allowing retail users to quickly exchange high volumes of off-ledger payments, which exhibit many cash-like features.

The technical activities that were performed during the experimentation with reference to the TIPS-itCoin implementation are the following:

⁷³ See the “Trusted intermediary transfer” as described in Banque centrale du Luxembourg (2020).

- development and deployment of a centralized itCoin network prototype that is operated by a single central bank, in its own public cloud;
- development and deployment of an itCoin network prototype in a distributed infrastructure that is operated by two Eurosystem central banks in their respective public cloud infrastructures; this experiment is useful to show a proof-of-concept in which the operation of a CBDC infrastructure could be distributed among multiple central banks;⁷⁴
- development and deployment of simulated on-ledger payments among intermediaries on the itCoin ledger;
- development and deployment of a simulated payment channel network, where retail users open payment channels with intermediaries, exchange off-ledger payments, and payments are routed via financial intermediaries and possibly central banks;
- development and deployment of the bridge prototype between itCoin and TIPS+ to support the liquidity transfer use case, i.e. commercial banks moving their own liquidity from TIPS+ to itCoin and vice-versa.

3.3.2. INTEGRATION BETWEEN TIPS+ AND A PROGRAMMABLE DLT PLATFORM

In the second version of the integrated model, the DLT-based leg of the integrated solution is given by an Ethereum-like permissioned blockchain. An objective in developing this solution is to show that TIPS+ is compatible with various choices for the complementary platform, including various DLT-based platforms.

The facet-based classification, as shown in Table 5, can be also used to classify the D€ that circulates on a permissioned Ethereum-based DLT.

Table 5: Facets characterization of the Ethereum-based programmable DLT

Facet	Characterisation	Remarks
Ownership	Knowledge based	Identity-based D€ may be built on top of the Ethereum-based DLT
Ledger type	Account-based	Platform based on Ethereum accounts
Distribution (systems)	Centralised	The core ledger is fully controlled by the Eurosystem
Distribution (infrastructure)	Distributed	Block creation may be distributed among multiple nodes
Operational model	Online	
Intermediation type	Gatekeepers or Settlement agent intermediation	

⁷⁴ The distributed infrastructure is deployed with for demo purposes only. The development of a production-ready solution that implements a consensus algorithm for a reconfigurable and strongly consistent itCoin multi-node network would require further effort and investment, which was beyond the scope of the experimentation.

The most appealing feature of this second DLT is its ability to provide programmability to the resulting digital euro, which would allow the automation of some business processes. A back-end infrastructure based on a programmable DLT would allow supervised intermediaries to develop a software code to automate, directly on the digital euro ledger, arbitrarily complex business processes involving payments in D€. This capability is commonly referred to as ‘support for smart contracts’ or ‘programmable money’. Such smart contracts would, for instance, automatically send payments to TIPS+ accounts when some specific logical conditions are met.

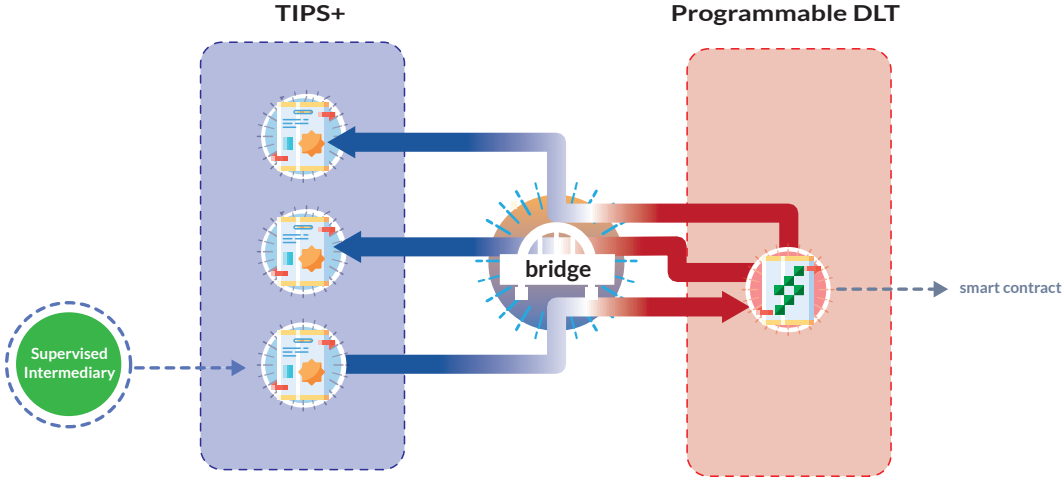
Technically speaking, programmable money is achieved with a powerful and expressive programming language, which can encode arbitrarily complex business logic.⁷⁵ After development, smart contracts can be deployed via the DLT and addressed as the destination of payments; when a smart contract receives a payment, it triggers the business logic that is encoded in its source code (i.e. a representation of the clauses of the contract), thus possibly generating a sequence of other payments and/or other types of updates to the ledger. The result of the integrated implementation is a D€ with two forms that are different along the programmability dimension. The TIPS+ D€ implements standard account-based money that is able to scale to hundreds of millions of accounts and transactions, while the DLT-based D€ would be highly programmable. As in the other implementation, the two forms coexist and are mutually convertible via the bridge. For example, a payment from a TIPS+ account could trigger a smart contract in the DLT, while a smart contract could also execute some complex business logic that credits one or more TIPS+ accounts.

The technical activities that were performed during the experimentation with reference to the integration between TIPS+ and the programmable DLT, described in Figure 11, are the following:

- development and deployment of the programmable DLT prototype network on a public cloud;
- development and deployment of the bridge prototype between the DLT and TIPS+ to support the same liquidity transfer use case as the itCoin implementation;
- development and deployment of a smart contract on the programmable DLT network that implements the following use cases: (1) the smart contract is triggered by a payment coming from a TIPS+ account, and targeting the DLT via the bridge; (2) the smart contract executes a business logic and implements specific “corporate actions”, such as the payment of dividends to stakeholders; (3) depending on the results, the smart contract triggers a sequence of payments from the DLT smart contract to a set of TIPS+ accounts, via the bridge.

⁷⁵ The programming language of Ethereum is usually said to be Turing-complete, while the Bitcoin programming language is not Turing-complete. In this context, the term Turing-complete is used to mean that the programming language of the DLT can approximately simulate the computational aspects of any other real-world general-purpose computer or computer language.

Figure 11 - TIPS+ and a programmable DLT integration - corporate action use case



It is important to note that programmability comes with high risks relating to the controllability of the smart contracts, which could contain bugs in their code that may lead to failures in the execution of the intended contract logic. In order to mitigate these risks, one may rely on a governance framework that mandates a set of policies and protocols for all participants, so as to fully preserve the security of the applications hosted by the programmable digital euro infrastructure. The development and an assessment of the effectiveness of such a governance framework were outside the scope of the experimental activity.

3.3.3. EXPERIMENTAL RESULTS

The fundamental result of the experimentation is that both of these solutions are technically feasible. In other words, this model leaves all options open: the choice between them depends solely on what scenario(s) is (are) deemed most relevant. Importantly, these choices are not mutually exclusive. Hence, an appealing feature of the model presented here is that it is by design fully suited to an incremental approach, whereby whatever choice is made now, the possibility of adding additional features further down the road remains open. This crucial finding implies that the solution outlined in this report delivers not only the benefits highlighted in Work Stream 1, but it also makes it possible to reap a potentially very wide range of further benefits in the future, by incrementally integrating new DLTs into the system as the need arises.

This incremental approach is very handy, in the event that one of the scenarios, as identified in the Report on a Digital Euro, materializes earlier than expected, thereby requiring an immediate issuance of D€. Therefore the following evolution is conceivable: the Eurosystem may initially choose to offer a purely account-based digital euro, thus enjoying all the benefits of this specific solution; the functionalities of the digital euro may then be further and progressively extended at a later stage, with the addition of one or more platforms, depending on which scenarios actually emerge as being most relevant or to accommodate the emergence of new specific needs from the market.

4. APPEALING FEATURES OF THE INTEGRATED ARCHITECTURE

Table 6 below describes how the integrated solution addresses each of the general and scenario-specific requirements defined in the HLTF Report on a digital euro. In the authors' view, by building upon the seamless integration of TIPS+ with other components (such as itCoin), a combined solution could better satisfy the requirements.

Table 6: How an integrated model could satisfy the requirements of HLTF report

Requirements of the HLTF Report on a digital euro vs. Integrated solution	
Requirement	Integrated solution
<p>Digitalization/ independence of EU [Requirement 1 (R1): enhanced digital efficiency]</p>	<p>The integrated solution relies on state-of-the-art technologies in compliance with IT best practices, also offering different levels of programmability on the basis of the technical solution adopted.</p> <p>It relies on the use of both a distributed architecture (TIPS+) and a DLT (itCoin) that permits a reliable and resilient system to be built. The programmability feature is achieved on three fronts:</p> <ul style="list-style-type: none"> • TIPS+ provides a predefined set of APIs that makes it possible to interact with the ledger of the account-based platform. Companies in the private sector can develop applications that use platform APIs to build additional services for their customers. • itCoin provides a moderate programmability that leverages on Bitcoin capabilities. • Different DLTs, as shown in Section 3.3.2, can provide a higher level of programmability leveraging on smart contracts. • The integrated solution reflects an intellectual property owned and operated by NCBs that establishes a suitable and distinctive payment service in the European area, with a strong European branding.
<p>Decline in the usage of cash [Requirement 2 (R2): cash-like features]</p>	<p>The integrated solution puts advanced cash-like features in place that leverage the possibility to offer a high degree of privacy in the off-ledger (PCN) in itCoin and anonymity on the payer's side in eCash.</p> <p>The integrated solution operates by keeping track of the minimum information required for it to work.</p> <p>For instance, the entire system protects privacy at different levels:</p> <ul style="list-style-type: none"> • through the use of pseudonymous identities in TIPS+; • through the use of PCN in itCoin; • through the use of blind signatures for token emission in eCash. <p>Offline functionalities are not covered at this stage.</p>

<p>Rise of a new form of money replacing euro [Requirement 3 (R3): competitive features]</p>	<p>The integrated solution offers the combined features of two different models:</p> <ul style="list-style-type: none"> • high speed payment platform and standard privacy features with the adoption of technical positions (TIPS+); • enhanced cash-like features with the usage of token-based platform features (itCoin, eCash); • programmability features with the usage of APIs (TIPS+) and Smart Contracts (itCoin, other programmable DLTs); • with the introduction of technical positions in TIPS+, for instance used for pre-paid services.
<p>Beneficial from a monetary policy perspective [Requirement 4 (R4): monetary policy option]</p>	<p>The integrated solution includes the possibility to remunerate accounts created in the account-based system.</p>
<p>Mitigation of the probability that a cyber-incident, natural disaster, pandemic or other extreme events could hinder the provision of payment services [Requirement 5 (R5): back-up system]</p>	<p>The integrated solution is based on two models that rely on distributed technologies that can be configured to implement a resilient solution. For instance, the adoption of geographical distribution is a powerful mitigation measure for a cyber incident or natural disaster.</p>
<p>The international role of the euro gains relevance as a Eurosystem objective [Requirement 6 (R6): international use]</p>	<p>Due to its intrinsic nature, both sides of the D€ integrated solution allow economic operators outside of the Eurosystem to have an easier and smoother access to central bank money for cross-border transactions, paving the way for a consolidation of the international role of the euro.</p>
<p>The Eurosystem decides to proactively support improvements in the overall costs and ecological footprint of the monetary and payment systems [Requirement 7a (R7a): cost saving] [Requirement 7b (R7b): environmentally friendly]</p>	<p>The integrated solution takes care of the ecological footprint: TIPS+ inherits the experience of TIPS in terms of low carbon emissions and itCoin does not use any mining mechanism typical of DLT private solutions.</p>

<p>Effects on the banking sector, monetary policy and financial stability [Requirement 8 (R8): ability to control the amount of digital euro in circulation]</p>	<p>Liquidity would be injected by the Eurosystem only through the TIPS+ component, as a transfer from the CLM accounts in the future TARGET2 service to TIPS+ accounts, thus knowing the total amount of D€ issued at the aggregate level. Liquidity from the CLM can be accessed by supervised intermediaries only, so that their role and expertise are preserved, mitigating the risk of bank disintermediation and the potential consequent financial instability.</p> <p>The TIPS+ component provides the possibility to set individual holding limits on the account balance as well as applying remuneration for financial stability purposes.</p> <p>In itCoin the control over the liquidity can be achieved by setting caps on off-ledger wallets (e.g. payment channels capacity). However, in case on-ledger liquidity is issued to end users, setting individual holding limits or applying remuneration would not be possible for on-ledger wallets.</p> <p>In the eCash integration with TIPS+, a threshold can be set to limit the amount of withdrawn tokens per end-user. The control over the amount of tokens emitted and not destroyed is covered by a central registry of tokens in the central platform. In addition, an expiry date can be implemented for different token denominations in order to force their conversion within a predefined time period.</p>
<p>Impact of a digital euro on the profitability and risk-taking of the central bank [Requirement 9 (R9): cooperation with market participants]</p>	<p>The integrated solution confirms the important role of intermediaries for customer relations.</p> <p>Intermediaries can build value-added services such as store of private keys on users' behalf or innovative services leveraging on programmability features.</p>
<p>Requirement 10 (R10): compliance with the regulatory framework.</p>	<p>The integrated solution is a flexible technical solution that can be tailored to comply with a wide range of Eurosystem's policy on D€</p>
<p>Effects on the safety and efficiency of retail payments [Requirement 11 (R11): safety and efficiency in the fulfilment of the Eurosystem's goals]</p>	<p>The integrated solution offers settlement in central bank money, in a system operated by the Eurosystem and, at the same time, programmability features allow intermediaries to develop non-core services to their customers.</p>
<p>Requirement 12 (R12): easy accessibility throughout the euro area.</p>	<p>The integrated solution, thanks to the connectivity of TIPS+ to Target Services for the injection of liquidity, is included effectively in the European payment system.</p> <p>The integrated solution does not offer a front-end solution itself, but it provides a set of API that makes it easy to build modern front-end solutions.</p> <p>The possibility to have a front-end application managed at the platform level to operate in the CBDC cannot be excluded.</p>

<p>Effects on the cross-border use of the euro [Requirement 13 (R13): conditional use by non-euro area residents]</p>	<p>It would be possible to apply limits and thresholds in TIPS+, depending on additional information collected by the platform and provided by gatekeepers, to set up accounts with specific characteristics for non-euro area residents.</p> <p>Moreover, the use of technical positions paves the way for the adoption of pre-paid cards to be used also by non-euro area residents. For example, following a light identity verification process, unbanked users may be provided with a low-capacity itCoin payment channel or with a limited amount of e-cash tokens.</p>
<p>Cyber risk [Requirement 14 (R14): cyber resilience]</p>	<p>By leveraging the experience of the Eurosystem in the operations of gross and retail payment systems, the integrated solution benefits from state-of-the-art methodologies and tools to ensure resilience to cyber threats.</p> <p>At the central platform level, a continuous IT process is established that makes it possible to identify vulnerabilities and pays a great deal of attention to them with high level of in each part of the development phases and in the operations.</p> <p>Considering that the solution combines the features of a central platform with those of a public ledger, accessible online via internet, and the possibility to create smart contracts, how to ensure that the whole system is properly secured should be further investigated.</p>

Such an integrated solution would be feasible, adaptable and open-ended. In fact, by combining the two components, it is technically possible to accommodate different end users with different needs in terms of privacy, inclusiveness, cash-likeness or programmability. The integrated solution would work as a bearer and a more private instrument as well as an account-based one closer to electronic money, shaped by what the market would value and demand.

Thus, it would make it possible to modulate the features of the D€ according to the use cases, having a component that can be remunerated and whose individual holdings can be controlled, coupled with a more cash-like one and also offering innovative features, such as the programmability of the money. The latter would pave the way for the development of innovative applications by market players to quickly interact with and build value around the CBDC infrastructure.

Using an open ledger for the DLT component would additionally broaden the openness towards Fintech companies, thereby fostering innovation and competition in the market, as they could perhaps implement additional solutions on top of the open ledger.

The TIPS+/itCoin integration, while allowing for planning interoperability with other solutions, would also make it straightforward to explore, and possibly enhance, cross-border and/or cross-currency transactions. As a matter of fact,

TIPS+ builds upon an infrastructure that is already multi-currency by design⁷⁶ and whose evolution towards a cross-currency transaction system is steadily progressing, opening the door to its future role as a central hub for cross-border/cross currency systems.

As said in the previous chapters, combining TIPS+ with itCoin would not be the only viable scheme.⁷⁷ In fact, a further advantage of the model is that it guarantees openness to other solutions. In this way, the solution would leave room for the private sector to structure its offer by building upon the blocks that best suit the service and technology that each actor plans to offer to the end users, in compliance with the broadest concept of technological neutrality.

With respect to privacy, this solution confirms its flexibility, as it allows for different degrees of privacy according to a combination of the platform used and the use case. The privacy that a user may enjoy would range from the standard privacy of electronic money, up to higher levels of privacy, closer to cash privacy. Interestingly, depending on their individual choices, the two parties of the same transaction may enjoy different levels of privacy. As already shown in Figure 11, the two end users may access the D€ from either component, each one enjoying their specific privacy features.

5. CHALLENGES AND THE WAY FORWARD

The issuance of a digital currency poses several questions about its strengths, critical issues, release methods and usability. Many of these topics have already been covered or cited in this paper. This section summarizes some of the implications related to the integrated model from both a technical and regulatory point of view and possible ways for handling them. It then outlines a way forward that would guarantee the security⁷⁸ and usability of the D€.

First of all, both systems in the integrated solution must be designed so the Eurosystem can control the amount and distribution of the D€ in circulation, so that its use as a form of investment is avoided. This, in turn, would prevent shifts of liquidity from sight deposits to the D€, which could otherwise lead to banking disintermediation and financial instability events.

The choice of allowing the creation of D€ starting from CLM accounts and injecting it in the market only through supervised intermediaries in TIPS+ is designed to always keep the amount of liquidity under the full control of the Eurosystem, according to the exact same methodologies applied to the other TARGET services.

⁷⁶ The Sveriges Riksbank is in fact migrating to TIPS for its instant payments in Swedish krona, leveraging the multi-currency capability of the service. See <https://www.bancaditalia.it/media/notizia/la-banca-centrale-svedese-aderisce-a-tips-il-sistema-pan-europeo-per-i-pagamenti-istantanei/>

⁷⁷ While it represents the only components prototyped by Banca d'Italia.

⁷⁸ Here security is meant in relation to a payment system based on a decentralized system.

Another critical aspect to address is how to reconcile privacy issues in transactions of a cash-like instrument with compliance to AML/CFT requirements. TIPS+ is less affected by this, as it allows for private transactions through the use of pseudonymous accounts. The Eurosystem would keep a register of transactions relating to the various accounts, without knowing the personal data of the account holders; however, with the support of the gatekeepers, it would always be possible to identify them, in case checks on suspicious operations need to be performed. Conversely, in itCoin, it is more complicated to track the money transfers within the PCN,⁷⁹ thus allowing a certain degree of privacy and possibly anonymity. Even if it were not possible to check the transactions on the PCN, or to set holding limits on the wallet as a result of the transactions exchanged, it would still be possible to set limits on withdrawal or conversion into another type of money (banknotes, account-based D€, commercial bank money). These limits, which are similar to some of the regulatory restrictions currently in place for cash, would help the monitoring of illegal activities including terrorism financing and money laundering, while emphasizing the cash-like features of itCoin. As far as eCash is concerned, anonymity is of an asymmetric type and is guaranteed only in the phase of using tokens for the payer. During the withdrawal phase, the system is able to apply all the limits and controls typical of an account-based system.

Another attractive feature of this combined model is its flexibility and openness to other DLT solutions proposed by the private sector, as shown in Section 3.3.2 (or even other token-based solutions as described in Section 2.6). It is undeniable that this is an advantage and a great stimulus for technological innovation, but there could also be some downsides. Indeed, if private operators offered incompatible technological products, a fragmentation of the market would ensue, potentially undermining the credibility of the whole D€, even though this risk might be mitigated by the need for such products to be interoperable with the TIPS+ platform.

Furthermore, nowadays the Eurosystem puts great emphasis on the possible vulnerabilities of systems under its responsibility. For instance, the features of a public ledger, accessible online via internet, and the development of smart contracts, could increase the attack surface and vulnerability risks of the D€. Moreover, integration with other DLTs or interactions with technical components outside the Eurosystem's control, pose other challenges from a cyber-security standpoint at the platform level and require an increase of defence mechanisms and protection of the D€ with ad hoc policies.

Considering, instead, the integrated solution from a performance standpoint, although with different characteristics, both components would offer reliable but different solutions. TIPS+ guarantees high scalability and large transaction volumes that make it suitable for retail users' needs, while itCoin, like many payment systems based on DLT, has reduced performance for on-ledger transactions (about 50 transactions per second), which could be significantly increased by resorting to off-ledger transactions supported by a Payment

⁷⁹ As stated above, intermediaries are only able to see only some metadata of the transactions and are therefore unable to track the payment activity.

Channel Network (PCN). However, the application of a PCN to central bank money requires in-depth analysis from a regulatory point of view. A payment channel between private individuals would represent an agreement to establish a means of exchanging money outside the Eurosystem infrastructure. The only transactions that should be written into the ledger would be those of opening and closing the payment channel, posing issues of how to classify transactions between these two events in terms of settlement finality.

The analysis carried out so far highlights both the benefits of the integrated solution and the points that need political guidance and/or more in-depth investigation of the technical and regulatory implications. As already pointed out, most of the principles and requirements published in the HLTf report on D€ would be widely fulfilled just by TIPS+ alone; itCoin or another platform (token-based or DLT account-based ones) would instead be needed only to tackle a few scenario-specific requirements, namely cash-like features (R2) and competitive features (R3).

6. CONCLUSIONS

The document aims at contributing to the debate on CBDC, by describing a possible technical architecture for the implementation of a digital euro and briefly illustrating the findings of the related Eurosystem experimentation, in which Banca d'Italia was involved.

The technical architecture described in this paper integrates TIPS+, an account-based platform obtained by enhancing TIPS, the existing retail instant payment system managed by Banca d'Italia within the framework of the 4CB, and itCoin, a token-based system based on a Distributed Ledger Technology. The need for a combined system reflects a number of requirements of the HLTf report on the D€ that are apparently difficult to satisfy with a single system. This paper highlights how the combination of these two systems through a bridge component would represent a versatile solution able to meet the different needs of end users in terms of privacy, inclusiveness, cash-likeness and programmability, while leaving the door open to the private sector to be involved and to offer high value-added services. This objective could also be pursued by adopting other token-based solutions, such as the one illustrated in Section 2.6, or an account-based DLT platform, as described in Section 3.3.2.

TIPS+ would be the access point in which to inject D€ from the RTGS system. To prevent an excessive use of D€ as a store of value, and consequently to avoid bank disintermediation, TIPS+ would be compatible with the implementation of individual holding limits and remuneration. As far as privacy is concerned, it would guarantee private, but not completely anonymous, transactions.

The second system would be a token-based platform (itCoin, eCash) or a programmable account-based platform, which would receive liquidity through TIPS+. Unlike TIPS+, these instruments would help address the HLTf-CBDC Report requirement on cash-like features. Additionally, the programmability

of DLT solutions would favour the introduction of programmable and value-added services by private market participants.

It is worth underlining that there are still some open questions that require an in-depth analysis of the regulatory and legal aspects, in particular those related to the token-based system, such as the possibility of introducing limits on wallet capacity and on convertibility into another type of money.

One of the most important features of this system would be its flexibility and openness to other DLTs or token-based solutions and the involvement of the market, including supervised intermediaries and Fintech players, that could build their value-added services on top of the central bank operated core infrastructure.

To conclude, this contributes to the ongoing discussion on the D€, by describing possible design choices that could be further analysed in the D€ investigation phase that the ECB Governing Council has just launched.

ANNEX 1: CBDC PRELIMINARIES

1. SUBSTANCE OF OWNERSHIP: KNOWLEDGE AND IDENTITY

The first facet concerns how authority is granted to a subject in order to execute a valid payment transaction and how ownership of value is verified.

A first possibility for certifying ownership is based on identity verification. In this model, users' holdings are recorded by a third party which, on behalf of the payer and payee, determines the validity of transactions and updates their respective positions accordingly. In this scenario, the enabler in transactions' authorization is the ability to verify the identity of the payer, which is the approach currently followed by checks and the vast majority of electronic payment solutions, such as credit and debit cards. As a consequence, a CBDC modelled on this paradigm requires the ability to verify and manage user identity.




A second option for verifying ownership is based on the concept of "knowledge possession", in analogy with physical cash: no identity verification is required to complete a transaction and, for this reason, the payment enjoys some degree of anonymity. The fundamental requirement of this second model is the ability to prove the "ownership" of a payment object and to verify its validity. While in the case of physical cash the requirement is satisfied through the physical possession of valid banknotes,⁸⁰ in the case of digital currencies ownership is certified by means of knowledge of cryptographic information, whose validity can be verified by the parties involved in the payment transaction, including the ledger operator. Therefore, in the latter scenario, the enabler in transactions' authorization is the payer's knowledge of a cryptographic key ("possession of knowledge"); ownership can be verified by anyone using publicly available information (e.g. the public key) and no verification of identity is needed.

A CBDC designed according to this paradigm thus requires a cryptographic infrastructure, where ownership of value is modelled as knowledge of some "secret information" about the payment object, and the payment object validity can be verified without disclosing the secret. This validation process requires the existence of some kind of "third party" – be it a centralized authority or a completely decentralized network of peers – acting as a common source of truth for CBDC users (see distribution degrees facet).

A comparison of the different ownership models, applied to the physical and digital world, is summarized in the following table.

⁸⁰ In the case of physical cash, the validity of a note is attested by means of security features such as watermarks, holograms, raised print, etc.

Table 7: Ledger types: Account-based vs token-based ledger

Ownership model	Physical world		Digital world	
	Medium	Key points	System	Key points
Possession	Cash 	Physical possession of a valid banknote Anonymity	Crypto assets 	Knowledge ("possession") of a secret - a cryptographic key stored in a wallet Potential anonymity
Identity			Bank deposits, or e-money 	Ability to prove identity (PIN, username/password, 2FA) Traceability

2. LEDGER TYPES: ACCOUNT-BASED VS TOKEN-BASED

The existing CBDC literature discusses the types of ledger that could support the circulation of a CBDC, and often classifies them into “account-based” and “token-based”.

An account-based system records the state of the ledger as a list of accounts, each of which has a corresponding balance.⁸¹ When a transaction occurs, the system updates the records by increasing and decreasing the balances of the accounts involved, usually the payer account and the payee account.

Most payment systems, including TARGET2/TIPS, operate according to the account-based model. Another example of this kind is the Ethereum DLT,⁸² in which the ledger state is made up of objects called "accounts", with an associated balance.

By contrast, a token-based system records the state of the ledger as a list of individual objects, called tokens, each of which has a corresponding value (e.g. 10€). Even if different tokens can be recorded on the same ledger, each of them would have a specific value, which can also be a decimal number (e.g. 10.55€),⁸³ but doesn’t change over the lifetime of the token.

The fundamental characteristic of tokens is that they are either created or destroyed, and cannot be partially spent. In fact, when a transaction occurs, the token value does not change. Unlike the account-based systems, in the token-based one the ledger does not update the tokens’ value. The ledger creates or destroys the tokens while keeping track either of the set of tokens that have already been destroyed (i.e. spent) or that are still in circulation (i.e. unspent).

⁸¹ See Bank of England (2020).

⁸² See Buterin (2013).

⁸³ In other words, a token-based ledger does not necessarily have fixed denominations.

An example of this kind is the Bitcoin DLT.⁸⁴ For each payment, a set of unspent tokens belonging to the payer is destroyed and (usually) two tokens with the same total value are created simultaneously: one going to the payee as payment and the other one being returned to the payer as exchange.

In order to prevent double spending, in both the account-based and token-based approaches, the accounts/tokens are stored on the ledger and updated by the ledger operator. In other words, neither tokens nor accounts are kept in the end user devices, which in general contains the cryptographic credentials that can be used to authorize transactions on the ledger. For this reason, neither the account-based nor the token-based approach refer to an offline and cash-like transfer, in which a payment is made without reference to any third party or intermediary.⁸⁵ Unless other arrangements are in place, the end user is always required to have a connection to the ledger, in order to safely receive payments.

3. DISTRIBUTION DEGREES OF SYSTEMS AND INFRASTRUCTURES

The modern applications' architecture has led to a dualism between system and infrastructure architecture, where system depicts the business and organizational view, while infrastructure refers to the technological and architectural one.

From a business and organizational point of view, three different system architectures exist: centralized, distributed and decentralized.

A centralized system is owned by a single entity or organization. In this case, users have to trust that the entity behaves correctly and in their interest. Currently, most of the internet applications are centralized (Amazon, Google, Facebook, etc.) and owned by a company or person that provides and maintains the source code to execute on a computer, server or even a cluster. As said, the centralized system concept regards a business view, irrespective of the actual technical infrastructure.

In the distributed systems, instead, the ownership is spread over some "well known" organizations. In this case, there are multiple central owners that have a part or a copy of the resources. With these systems the users don't have to trust a single organization or entity, but have different choices. Domain Name System (DNS) is a great example of a distributed system. It maps hostname to IP addresses and is implemented as a distributed, hierarchical database. Focusing on the root server, one of the three classes of DNS servers, 13 root name servers are available worldwide, run by 12 organizations, which the user has to ultimately trust.

⁸⁴ See Nakamoto (2008).

⁸⁵ See Bank of England (2020), Section 6.6.

Lastly, in the decentralized system, the ownership is spread over many entities, usually unknown to each other. Peer-to-peer file sharing services are a good example of decentralized systems.

From a technological and architectural point of view, two different infrastructure types can be distinguished: centralized and distributed.

Centralized infrastructures are designed with a single node in charge of executing the system goal. A typical implementation is the so-called client/server architecture, where one or more client nodes are logically connected to a central server.

A distributed infrastructure, instead, is a group of computers working together to achieve a unified goal. In this scenario, although the processes are separated, the system appears as a single computer to end-user(s). A distributed system is a collection of autonomous computing elements⁸⁶ that appears to its users as a single coherent system.

As a matter of fact, different systems could be designed with different types of infrastructure. With regard to payment systems, some examples follow:

- TIPS is a centralized systems with a distributed infrastructure;
- TARGET2 and T2S core services are centralized systems, with a centralized infrastructure;
- Ripple is a distributed system with a distributed infrastructure;
- Bitcoin is a decentralized system with a distributed infrastructure.

4. ONLINE VS OFFLINE MODELS

Looking at the connectivity requirement for a CBDC, two models are possible: online and offline.⁸⁷ The online model refers to payment systems based on a unique source of truth, such as a central register that does not require payers and payees to be connected at the same time. It relies on a resource being permanently up and always accessible: the ledger. The offline model instead operates in the permanent or temporary absence of the ledger, leaving the counterparties to bear the risk of being part of a disconnected subset of the entire network.

The adoption of the offline model offers the opportunity to augment the availability of services at the cost of considerable risks, usually related to the so-called “double spending problem” or the risk of counterfeiting: payments that are not verified against the payment service, cannot be checked in real time.⁸⁸

⁸⁶ See Van Steen and Tanenbaum (2017).

⁸⁷ See European Central Bank (2020b).

⁸⁸ See Sveriges Riksbank (2018).

Considering the large variety of possible offline scenarios, it is proposed to narrow them down to two main categories: “eventually online” and “permanently offline”. The “eventually online” category refers to a scenario in which a payer executes a transaction with a payee in the absence of connectivity to the ledger. This implies that the transaction is completed, but its finality is resolved only after a process of data reconciliation with the online system (i.e. when it is written on the ledger). In this scenario, the debt position for the payer will be active until the data reconciliation with the online systems ends and the payee is exposed to the credit risk (i.e. the risk of not receiving money). Because of this risk, an identity-based model would be more attractive for this offline category because the possibility of identifying a person in the event of problems on the debtor side could deter misbehaviour. Some knowledge-based models could also be suitable when the author of the double spending could be identified ex post (Chaum, 1983). In general, since the risk is proportional to the transacted value, this model might work mostly with low value transactions.

The “permanently offline” category relies on hardware devices, whose security is fundamental to guarantee that transactions happen in a safe mode. It works completely offline, therefore transaction finality does not require data reconciliation with the online system. The payer is freed, when the transaction is completed entirely offline. Such payments include cash-like transactions, as well as the transfer of a pre-loaded card from one person to another person after a purchase. Physical tampering of devices is the main vulnerability of this model, which can compromise not only the secure hardware environment but also the digital currency itself.⁸⁹ A major problem of the “permanently offline” category is that it creates economic incentives for users to attack their own secure hardware devices (Allen *et al.*, 2020), soliciting the need for new security mechanisms (e.g. the no-cloning theorem).⁹⁰

5. INTERMEDIATION TYPES AND IMPLICATIONS FOR CENTRAL BANK LIABILITIES

The last CBDC facet analysed is the intermediation type of the technical infrastructure in the payment process.⁹¹ It refers to the technical relationship between the end user of the CBDC and the ledger system operated by the central bank where the digital currency is issued and circulates. Usually three possibilities emerge from the literature: an absence of intermediation, gatekeeper intermediation and settlement agent intermediation.⁹²

All the above intermediation types may have implications for the safety of the central bank digital currency. Indeed, while the distinction between what can be considered a central bank liability and what cannot, is certainly a matter of legal definition, a central bank should consider the impact of technological

⁸⁹ The possibility of creating money from scratch in an arbitrary manner invalidates the foundation of a CBDC.

⁹⁰ See Aaronson *et al.* (2012).

⁹¹ The intermediation type in this facet does not refer to the intermediation in the CBDC distribution process, which is intermediated by commercial banks.

⁹² See European Central Bank (2020b), Chapter 6.1.

choices that could reduce outsourcing risks to the intermediaries and potentially increase the safety of the CBDC for end users.

In the settlement agent intermediation, intermediaries own the keys to access and authorize the payment in D€⁹³ and they execute transactions on behalf of their customers. As a result, a failure of the intermediary that acts as settlement agent, could result not only in the users being unable to access their CBDC balance and spend units, but also, potentially, in unauthorized transactions being sent to the CBDC ledger.

Unlike settlement agents, the gatekeepers are in charge of authenticating end users and of complying with the Know Your Customer (KYC), AML/CFT requirements; they also provide the technical connectivity between users and the payment system infrastructure. In this scenario, the gatekeepers may be technically unable to authorize transactions without cooperating with the end users.⁹⁴ This system avoids the case of unauthorized transactions being sent to the CBDC ledger when an intermediary, acting as a gatekeeper, defaults.

For both the above intermediation types, it is also important to guarantee that the information on the CBDC balance that is presented to the end user has not been compromised. If the end users need to trust an intermediary to report a correct balance, then a failure of the intermediary could result in the user believing more funds to be available than there actually are in the central bank account.

Finally, if end user access to the ledger is not intermediated, then safety derives from the fact that information written on the ledger can be directly accessed by the end users. Nevertheless, the absence of intermediation entails problems of a different nature, which can make intermediated access to the CBDC altogether preferable.

ANNEX 2: ITCOIN DISCUSSION TOPICS

1. ABOUT ON-LEDGER TRANSACTIONAL CAPACITY

The computational capacity of any payment system is a scarce resource because technological limits prevent it from being scaled indefinitely. In blockchain platforms like itCoin, this limit is related to two parameters: the amount of space available to describe new transactions per cycle (block space), and the period of the cycle itself (block time).

Knowing what this limit is and working with a pseudonymous ledger – where there is no possibility of distinguishing *a priori* well-intentioned transactions

⁹³ See European Central Bank (2019).

⁹⁴ For example, in order to authorize a transfer of CBDC units, the ledger may require that the end user explicitly provide a signature.

from spam and attacks – the central bank needs to find a way to protect this inherently scarce resource (transactional capacity) against spam transactions and/or targeted denial of service (DoS) attacks, which would prevent legitimate usage.

The universally adopted solution for this problem, at least in the field of crypto-asset-based solutions, is to have end users pay a fee for each on-ledger transaction they send to the central bank for inclusion in the ledger. The requirements of fee payment make it expensive (potentially even very expensive) to launch an attack on the CBDC or to fill its capacity with spam.

Unlike most traditional payment systems, the fee is not necessarily linked to the amount being transferred and is not chosen or imposed by the service provider (the central bank). A bidding process could take place, whereby everyone would be free to remunerate the central bank with an arbitrary fee, effectively competing for capacity. It is possible to say that “a market emerges” for the contended resource. Should the on-ledger transactional capacity come under pressure, then the higher the fee per transactional capacity unit, the more likely it is that the transaction will gain a seat in the very next block of validated transactions.

The criterion by which the central bank decides what transactions to include (if too many are pending) is that among all the queued transactions it will select the subset of candidate transactions that maximizes the total cumulative fee due from the next batch of confirmations.

It should be noted that this criterion is not ultimately geared to maximize income by fees for the central bank: this is not at all a design goal. It is instead used to offer a simple, market-inspired criterion that allows ledger users to form expectations about the fee that they will have to pay in order to obtain a certain quality of service (i.e. speed of processing for their own transactions), which in turn is a prerequisite for the correct and efficient functioning of the whole platform.

The TPS figure that is presented in this report, i.e. 50 TPS, is based on a very preliminary calculation. In a scenario where the adoption of the digital euro spreads rapidly after its launch, 50 TPS may be enough to bring onboard all citizens of the Eurozone to the digital euro Payment Channel Network in around three months (assuming 300 million users, one payment channel per user, and one on-ledger transaction per payment channel).

2. ABOUT THE OFF-LEDGER DIGITAL EURO AS A CENTRAL BANK LIABILITY

The thesis that off-ledger D€ are a liability of the central bank can intuitively be supported, although further investigation on the subject is needed, with specific regard to the CBDC’s overall legal framework.

Usually, the absence of immediate finality in existing payment systems is associated with credit/counterparty risk and this may lead to the conclusion

that off-ledger funds would appear as a liability on the balance sheet of some private entities rather than of the central bank. That, however, is not completely correct, or it is at least arguable, due to the specificity of the payment channel technology.

In fact, one of the main novelties of payment channels technology is that it may allow money to be conceived without any immediate transaction finality on the central bank ledger and, at the same time, in the absence of credit/counterparty risk.⁹⁵ The only risk that can be associated with the money owned by users in the off-ledger layer is, in fact, purely operational. It can be argued that the absence of credit/counterparty risk is sufficient to consider off-ledger funds as a liability of the central bank, also given new types of operational risk which need to be managed by end-user devices.

In fact, operational risks are also associated with central bank liabilities that are already present in the retail market, i.e. banknotes. These include, but are not limited to, risk of loss, damage, and theft. In the physical domain: retail users are indeed responsible for managing these risks themselves, e.g. by using a safe at home, or by not carrying too many banknotes in their pockets. For both physical and digital forms of central bank liabilities, a mismanagement of the operational risk could indeed cause a financial loss to the end user. In this respect, the only difference is related to the fact that operational risks are very easy to grasp for retail users in the physical domain, while in the digital domain they would be, at least initially, more complex to understand and manage.

In other words, with reference to the digital euro report, further investigation may support the idea that the off-ledger digital euro is risk-free, in the sense that “its holders should not be subject to any market risk or issuer default risk” (see page 10 of ECB 2020b), but not in the sense of operational-risk-free. In any case, the extent to which off-ledger D€ could fall within the definition of a central bank liability ultimately depends on the legal framework, which in turn would be applied to the characteristics of the underlying technology.

⁹⁵ A technical description of how payment channels are built and work can be found in Poon and Dryja (2016).

REFERENCES

- Aaronson, S., E. Farhi, D. Gosset, A. Hassidim, J. Kelner, A. Lutomirski (2012), *Quantum Money*, August 2012.
- Allen, S., S. Capkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostianen, S. Meiklejohn, A. Miller, E. Prasad, K. Wüst and F. Zhang (2020), *Design Choices for Central Bank Digital Currency - Policy and Technical Considerations*, July 2020.
- Arcese, M., D. Di Giulio and V. Lasorella (2021), *Real-Time Gross Settlement systems: breaking the wall of scalability and high availability*, Banca d'Italia, Markets, Infrastructures, Payment Systems, no. 2, 23 March 2021.
- Bank for International Settlements (2019), *Proceeding with caution - a survey on central bank digital currency*, BIS papers no. 101, January 2019.
- Bank for International Settlements (2020a), *Impending arrival – a sequel to the survey on Central bank digital currency*, BIS paper no. 107, January 2020.
- Bank for International Settlements (2020b), *International banking and financial market developments*, BIS Quarterly Review, March 2020.
- Bank for International Settlements (2020c), *Central bank digital currencies: foundational principles and core features*, Joint report by The Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and Bank for International Settlements, October 2020.
- Bank for International Settlements (2021), *CBDCs: an opportunity for the monetary system*, BIS Annual Economic Report, June 2021.
- Bank of Canada and Monetary Authority of Singapore (2019), *Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies*, Jasper-Ubin Design Paper.
- Bank of England (2020), *Central Bank Digital Currency, Opportunities, challenges and design*, Discussion Paper, March 2020.
- Bank of England (2021a), *Bank of England statement on Central Bank Digital Currency*, April 2021.
- Bank of England (2021b), *Discussion Paper on New Forms of Digital Money*, June 2021.
- Banque centrale du Luxembourg (2020), *DCB services & wholesale CBDC concept - EUROchain Hackathon*, BcL Technical Paper, January 2020.
- Bech, M.L. and R. Garratt, (2017), *Central Bank Cryptocurrencies*, Bank for International Settlements *Quarterly Review*, September 2017.
- Bindseil, U. (2020), *Tiered CBDC and the financial system*, Working Paper Series, no. 2351, ECB, January 2020.
- Buterin, V. (2013), *A next generation smart contract & decentralized application platform*, January 2014.
- Chaum, D. (1983), *Blind signatures for untraceable payments*.
- Chaum, D., C. Grothoff and T. Moser (2021), *How to issue a central bank digital currency*, March 2021.
- Dryja, T. (2019), *Discreet Log Contracts*, MIT Digital Currency Initiative.
- European Central Bank (2012), *Guideline of the European Central Bank of 5 December 2012, on a Trans-European Automated Real Time Gross Settlement Express Transfer System (TARGET2)*.

- European Central Bank (2017), *The use of cash by households in the euro area*, Occasional Paper Series, no. 201, November 2017.
- European Central Bank (2019), *Exploring anonymity in central bank digital currencies*, ECB In Focus, Issue no. 4, December 2019.
- European Central Bank (2020a), *Study on the payment attitudes of consumers in the euro area*, SPACE Report December 2020.
- European Central Bank (2020b), *Report on a digital euro*, October 2020.
- European Central Bank (2021a), *Eurosystem report on the public consultation on a digital euro*, April 2021.
- European Central Bank (2021b), *Digital euro experimentation scope and key learnings*, July 2021.
- European Central Bank and Bank of Japan (2018), *Project Stella phase 2, Securities Settlement Systems in a Distributed Ledger Environment*, March 2018.
- European Central Bank and Bank of Japan (2019), *Project Stella phase 3, Synchronised Cross-border Payments*, June 2019.
- European Central Bank and Bank of Japan (2020), *Project Stella phase 4, Balancing Confidentiality and Auditability in a Distributed Ledger Environment*, February 2020.
- European Parliament and Council of the European Union (2015), *Directive (EU) 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*, Official Journal of the European Union, Vol. 58, 23 December 2015.
- Financial Stability Board (2020), *Report on Regulation, Supervision and Oversight of “Global Stablecoin” arrangements*, October 2020.
- Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, November 2008.
- Panetta, F. and U. Bindseil (2021), *Digital central bank money for Europeans – getting ready for the future*, the ECB Blog, March 2021.
- People’s Bank of China (2021), *Progress of Research & Development of E-CNY in China*, July 2021.
- Poon, J. and T. Dryja (2016), *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, January 2016.
- Renzetti, M., S. Bernardini, G. Marino, L. Mibelli, L. Ricciardi and G.M. Sabelli (2021), *TIPS - TARGET Instant Payment Settlement*, Banca d’Italia, Markets, Infrastructures, Payment Systems, no. 1, 29 January 2021.
- Sveriges Riksbank (2018), *The Riksbank’s e-krona project Report 2*, October 2018.
- Sveriges Riksbank (2021), *The e-krona pilot – test of technical solution for the e-krona*, April, 2021.
- Tiberi, P. (2021), *The carbon footprint of the Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures*, Banca d’Italia, Markets, Infrastructures, Payment Systems, no. 5, 12 May 2021.
- Van Steen, M. and A.S. Tanenbaum (2017), *Distributed Systems*, 3rd ed., 2017.
- Wong, P. and J.L. Maniff (2020), *Comparing Means of Payment: What Role for a Central Bank Digital Currency?*, FEDS notes, August 2020, revised in April 2021.