A Digital Euro's Relationship with Data Protection, Anti-Money Laundering and Combating the Financing of Terrorism

Diogo Dá Mesquita

Dissertation written under the supervision of João Freire de Andrade.

Dissertation submitted in partial fulfilment of requirements for the International MSc in Management with Major in Corporate Finance, at the Universidade Católica Portuguesa, April 2022.

Abstract

***Title*:** A Digital Euro's Relationship with Data Protection, Anti-Money Laundering and Combating the Financing of Terrorism

***Author*:** Diogo Dá Mesquita

***Keywords*:** central bank digital currency; digital euro; AML/CFT; fintech regulation; data protection.

The study focuses on the possibility of a central bank digital currency (CBDC) for the euro area and its relationship with data protection and anti-money laundering / combating the finance of terrorism (AML/CFT) policies. Its objective was to identify the state of the art on the subject and some of the main opportunities, challenges and risks which should be considered in the ongoing process of a digital euro. The research was based on a critical review of reports and surveys about CBDCs produced by central bank community, international institutions and European Union agencies, the regulatory framework and international standards about data protection and AML/CFT, complemented by academic and professional experts' literature. It was conducted under a qualitative method following the premise that in Fintech innovation is crucial to understand current and emerging regulations that can be relevant. Digital euro's architecture, independently of the adopted model (account-based, token-based or hybrid), should: (1) allow CBDC holders identification and comprise traceability mechanisms in accordance with AML/CFT requirements; (2) respect the General Data Protection Regulation, namely data protection by design and by default through privacy-enhancing technologies. The status of the European Central Bank and national central banks of euro countries is incompatible with their subjection to the legislation on AML/CFT applicable to the participants on digital money transfers market, so all the operations related with the end-users must be full intermediated by private sector entities submitted, beyond financial supervision, to guidelines, regulation and supervision by AML/CFT authorities.

Abstract (Portuguese version)

***Título*:** A relação de um euro digital com proteção de dados, combate ao branqueamento de capitais e financiamento do terrorismo.

***Autor*:** Diogo Dá Mesquita

***Palavras-chave*:** moeda digital de banco central; euro digital; combate ao branqueamento de capitais e financiamento do terrorismo; regulação de fintech; proteção de dados.

O estudo tem como objeto a possibilidade de uma moeda digital de banco central (MDBC) na zona euro e a sua relação com proteção de dados e combate ao branqueamento de capitais e financiamento do terrorismo (CBCFT). Pretendeu-se investigar o estado da arte e principais oportunidades, desafios e riscos no processo em curso de um euro digital. A investigação baseou-se na revisão crítica de relatórios e estudos sobre MDBCs produzidos pela comunidade de bancos centrais, instituições internacionais e órgãos da União Europeia, do quadro regulatório e orientações internacionais sobre proteção de dados e CBCFT, complementados por estudos de académicos e outros especialistas. Foi adotado um método qualitativo à luz da premissa de que para a inovação Fintech é fundamental compreender regulamentações atuais e emergentes relevantes. A arquitetura de um euro digital, independentemente do modelo adotado (baseado em contas, em *tokens* ou híbrido), deverá: (1) permitir identificação dos titulares de MDBCs e compreender mecanismos de rastreamento conformes às exigências CBCFT; (2) respeitar o Regulamento Geral sobre Proteção de Dados, nomeadamente, proteção de dados desde a conceção e por defeito através de tecnologias de proteção da privacidade. O estatuto do Banco Central Europeu e dos bancos centrais dos países do euro é incompatível com a sua submissão às exigências CBCFT aplicáveis aos participantes no mercado de transferências digitais de dinheiro, pelo que as operações relativas aos utilizadores finais devem ser integralmente intermediadas por entidades privadas sujeitas, além da supervisão financeira, a diretrizes, regulação e supervisão pelas autoridades de CBCFT.

Table of Contents

List of Abbreviations

AI - Artificial intelligence

AML - Anti-money laundering

BIS - Bank for International Settlements

BOJ - Bank of Japan

CBDC - Central bank digital currency

CCPA - California Consumer Privacy Act of 2018

CDD - Customer due diligence

CFT - Combating the financing of terrorism

CPMI - Committee on Payments and Market Infrastructures

DLT - Distributed ledger technology

EC - European Commission

ECB - European Central Bank

ENISA - European Union Agency for Cybersecurity

EP - European Parliament

EU - European Union

FATF - Financial Action Task Force

Fed - Federal Reserve

FI - Financial institutions

FIU - Financial Crime Intelligence Unit

FX - Foreign exchange

G7 - Group of Seven

G20 - Group of Twenty

GDPR - General Data Protection Regulation

HLTF-CBDC - High-Level Task Force on CBDC

IMF - International Monetary Fund

KYC - Know your customer

ML - Money laundering

NCBs - National central banks of euro area

NLP - Natural language processing

OECD - Organization for Economic Co-operation and Development

P2P - Peer-to-peer

P2B - Peer-to-business

PET - Privacy-enhancing techniques

PIP - Payment interface provider

PIPEDA - Personal Information and Electronic Documents Act of Canada

PKI - Public key cryptography infrastructure

PoC - Proof of concept

PSI - Private sector intermediaries

PSP - Payment service providers

SNB - Swiss National Bank

TF - Terrorism financing

TIPS - Target instant payment settlement

UK - United Kingdom

US - United States

USD - United States Dollars

VA - Virtual asset

WEF - World Economic Forum

1. Introduction

Over the last few years, central bank digital currency (CBDC) has been on the agenda of the Eurosystem. In that context, the European Central Bank (ECB) launched on 24 July 2021 the "Investigation phase of digital euro project" to last 24 months.

The dissertation focuses on retail CBDC, used by the public for day-to-day payments, and on the opportunities and threats in two different but related areas: data protection and anti-money laundering / combating the finance of terrorism (AML/CFT).

The study begins with a brief framework of the current global debates and research about CBDC foundational principles, core features and design. After that, the developments at the Euro zone are analysed, in particular ECB reports, and some of the possible features and designs in an environment of a physical currency and a digital currency, the two issued by ECB.

An ECB`s report about a public consultation concludes that "privacy is considered the most important feature of a digital euro by both citizens and professionals participating in the consultation" (ECB, 2021a: 3). The technical and political options on the CBDC euro should have into account also the privacy policy of the European Union (EU), especially the General Data Protection Regulation (GDPR) which imposes obligations both to public and private organizations.

The privacy issues are related with the mechanisms against illegal activities and its compatibility with a full or partial privacy of the transactions. Globally, a "key liability of central banks serves to reduce the costs of criminal activity" (Williamson, 2019: 1) and in Europe the financial system must respect a vast legal framework with multiple obligations to prevent money laundering (ML) and the terrorism financing (TF).

There are multiple connections between currencies, privacy, and fight against crime. Two simple demonstrations: (a) In 2016, the ECB put a term to the production of the 500 euro note considering that bill had grown far too popular in the funding and facilitation of drug trafficking, human smuggling and terrorism (Jones, 2016); (b) Four days before the ECB launched the "investigation phase of digital euro project", the European Commission presented an ambitious package of legislative proposals to strengthen the EU's anti-money laundering and countering terrorism financing rules taking into account the "new and

emerging challenges linked to technological innovation" which "include virtual currencies" (EC, 2021b: 1).

The purpose of this study is not to advocate the issuance of a digital euro or its specific design but identify the state of the art on the subject and summarize some of the main challenges and questions that should be considered in the ongoing process of a digital euro. It will be developed a methodological approach centred on FinTech, but also considering the social and legal circumstances, such as data protection and crime prevention, in relation to a digital euro, under the premise that for the Fintech actors it is crucial to understand which current and emerging regulations could influence their ability to succeed (e.g., Freij, 2018: 35).

2. Literature Review

2.1. What is a central bank digital currency?

A definition of CBDC simultaneously synthetic and analytical is the following: "a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank" (BIS, 2020: 4). So, a CBDC is the virtual format (no physical value) of a fiat currency for a particular country or region; it is an electronic record or digital token (below 4.1.3 about the ledger types) of the official currency issued and regulated by its monetary authority (below 4.1.2).

CBDCs' discussion involves a vast complex of dimensions with plurality of goals, challenges and risks (below 4.1 and 4.4, figure 4, tables 2-8).

2.2. What is a crypto-asset or cryptocurrency?

Crypto-assets, also often called cryptocurrencies, are one type of virtual asset (VA), i.e., a digital representation of value that can be digitally traded, or transferred, and can be used for payments or investment purposes, whose distinctive feature is that they are digital units created and transferred between users through the use of cryptography (e.g., Söderberg, 2018: 1).

There isn't a worldwide established concept of crypto-asset, but in the EU, there is a proposal of a legal definition already accepted by the EU institutions as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology (DLT) or similar technology" (EC, 2019: 39). In this context, DLT means "a type of technology that support the distributed recording of encrypted data".

The first decentralised cryptocurrency was Bitcoin which began operating in 2009. Currently, there are competitors using Bitcoin's original open-source protocol, with a number of changes in its underlying codes (e.g., Litecoin and Monero) and others based on their own protocol and DLT (e.g., Ethereum and Ripple).

The lack of a clear regulatory framework for crypto-assets "remains a significant constraint to broader based acceptance" (Mandeng / Velissarios, 2019: 14) but the threats of price volatility, speculative trading, hack attacks and ML/TF are giving cause to regulatory responses. EU's emerging regulation is based on a legal distinction, crypto-assets "issued by central banks acting in their monetary authority capacity or by other public authorities should not be subject to the Union framework covering crypto-assets" (EC, 20019: 20), so for the EU legal framework crypto-assets' classification is reserved for the ones issued by private entities (despite potential technological similarities with CBDCs, below 2.3, 2.4, 4.1.3 and 4.2).

Crypto-assets have been used as a means of payment at a very small extent, but the hypothesis of big tech participation on that market could change that. The emerging regulatory responses determined some dropouts and nowadays the question about the issuance of CBDCs is beyond crypto-assets risks (below 4.1.1, 4.1.4 and 4.2).

2.3. How can a CBDC be implemented in eurozone?

ECB announced in July 2021 "our aim is to be ready, at the end of these two years, to start developing a digital euro, which could take around three years" (Panetta, 2021a).

Since the start of the digital euro project, ECB's experimental testing has shown there are no major technological constraints on the issuance and there are many options and techniques in which it could be designed; however, easy accessibility, robustness, safety, efficiency, privacy, and regulatory compliance are critical requirements that must be met.

In accordance with the 2020 ECB`s "Report on Digital Euro" (below 4.2) there are four work streams under test with the purpose to determine the most comprehensive and economical solution that best meets all the fundamental requirements: accessibility, efficiency, safety and privacy.

In order to test the issuance and distribution of a digital euro, the first group of expertise focused on the existing infrastructure and architecture, such as the TARGET Instant Payment Settlement (TIPS) launched by the Eurosystem, in November 2018, to enable people and businesses to transfer money amongst themselves in seconds, regardless of their local bank's hours of operation.

The second one still relied on the existing infrastructure (TIPS) but, in this case, intending to examine the potential compatibility between centralised and decentralised technologies to develop innovative features. The approach establishes a clear division between the issuing process, attributed to the central banks and the distribution process, which would be dealt by the private sector.

The last two revolve around new solutions and concepts. The first assessed the integration of blockchain technology as developed by cryptocurrency issuers. Since there is no existing substance to serve as a base in this case, the studies had to focus not only on the potential scalability of such platform but also on the infrastructure's capacity to cope with the various degrees of privacy demanded and to comply with regulation on AML/CFT, two key dimensions for the eurozone.

The final work category leans on offline payment solutions to be assessed in terms of feasibility to both Peer-to-Peer (P2P) and Peer-to-Business (P2B) transactions, the different levels of privacy they may establish, the security and safety provided, their geographical limits and ease of use, and the costs they entail.

The technical and policy issues would be subjected to a final decision of EU institutions (below 4.2).

2.4. What is the Blockchain Ledger Technology?

A blockchain is a type of database – a collection of information stored on a computer system, which can be accessed, filtered and manipulated quickly and easily by several users at the same time. It requires a big number of computers (processors) in order to have the computational power and storage capacity necessary for many users to access the database simultaneously.

A blockchain collects information together in groups, the blocks, that hold sets of information. These blocks have certain storage capacity, which when is filled is chained to the previous storage block (Conway, 2021). All the data gathered in the different blocks creates the “blockchain” and each block in the chain is given an exact timestamp when it is added to the chain. This ledger technology makes use of cryptographic and algorithmic methods to

generate and validate a continuously increasing data structure in the blocks (Bashir, 2017: 56).

Blockchain technology allows people and organisations who may not know or trust each other to collectively agree on and permanently record information without a third-party authority. Adding to this, "the transparency of blockchain implies that all transactions are recorded", despite the fact they "can be made anonymously or configured to a varying degree of pseudonymity, all transactions are traceable" (Mandeng / Velissarios, 2019: 13).

2.5. What types of approaches and techniques could be used to differentiate CBDC's levels of privacy?

An anonymous user may function or communicate in a way that keeps him/her unrecognizable. On the other hand, someone who uses a pseudonym operates or communicates in a way that allows him/her to be recognized. "Digital signatures are encrypted code that verify someone's unique identity and are used to validate ownership of crypto-currency for transactions, but do not reveal the identity of the owner" (Wadsworth, 2018: 11). Hence, in the case of digital transactions, one should talk about pseudonyms rather than anonymous, as there is a sender and there is a receiver linked to an individual identity; even if there is no personal information, there is an IP address associated.

In terms of pseudonyms options there are some which can be applied and incorporated in a blockchain ledger (ECB, 2021b*:* 6): one-time pseudonyms (a different pseudonym used for each transaction, which makes it difficult for the receivers to link the pseudonyms with the senders' identity); transaction mixing (multiple users can mix their transactions, so the pseudonym linkage and traceability is avoided); payment channel network (a system of bilateral channels in which the amount of privacy varies based on the agents authorized to enter the system).

While certain privacy methods solutions, such as traceability solutions, may give legally valid alternatives, others may necessitate further study to ensure that the high level of privacy does not breach AML regulatory standards (below 4.4.2).

3. Methodology

The central banking community and international institutions (e.g., IMF, BIS, World Bank, Asia Development Bank, World Economic Forum, G7, G20) have promoted comprehensive discussions, reports and surveys on the adequacy and feasibility of issuing CBDCs. A critical review of that work is the basis of the investigation.

The research was based fundamentally on secondary data collected by ECB, other central banks and international financial institutions, but also on historical and comparative studies on money, specifically on digital money, which are essential to understand these developments. The massive resources of the financial entities, which promote studies and surveys on CBDCs, implies that an individual collection of data on the items already developed by these institutions can be pointless, so the main goal here is the selection and interpretation of the most important public data to the subject.

It was also considered standard documentation of international organizations on matters directly related to the subject of the thesis, for instance the Financial Action Task Force Organization`s (FATFF) standards on AML/CFT. Additionally, previous analyses were taken into account (based on the collection, integration and interpretation of trustworthy investigations and reports from credible sources) alongside with the knowledge obtained by the reading of expert studies on AML/CFT, the participation in conferences which supplemented, validated, and extended ideas achieved in the previous stages.

The thesis is conducted under a qualitative method. It is adopted an analytical approach considering regulations and regulatory changes as a vital element to the main object of the study, a euro CBDC.

The academic investigation on digital currencies regulation is commonly divided in two different typologies: (1) “concrete or tangible proposals such as tools, protocols, methods, models” and (2) “theoretical or intangible solutions such as frameworks and knowledge” (e.g., Silva / Silva: 17).

The focus of the present work is the second approach mentioned above but it also comprehends an effort to point out a critical connection with the first one.

The studies about value chain in public sector unanimously stress the importance of trust, mainly what they call “a posteriori trust generated by service satisfaction” (Heintzman /

Marson, 2005: 554). And trust is crucial to the money issued by a central bank, a condition to be accepted in exchange for goods and services.

Empirically, there is not enough data to evaluate the impact of different possible models and designs of CBDCs in data protection and AML/CFT. Particularly, in the public sector it should not be forgotten there is a value chain gap between the policy and legislation for one hand and its implementation for the other (Walt, 2016), and the analytical distinctions between the different stages and their impacts (cf. figures 42-44).

The options about money transfers, privacy and AML/CFT are related with rule of law principles and the equilibrium between the powers of the state and individual rights, in particular the right to restrain governmental and private actions that threaten the privacy of individuals.

Considering that the theme of the dissertation is a digital euro, one must bear in mind that the rule of law is one of the fundamental values upon which the EU is based on. Accordingly, special attention is taken to the works of some central banks with economies and political systems compatible with EU constitutional values who have already launched projects and/or experimental testing on retail CBDC and independent studies about these efforts. Countries with whom it is possible cooperation and harmonization in the creation of common standards about how the design of a CBDC should take into account the necessity of dealing with data protection and AML/CFT issues (namely the works of seven other central banks: Sveriges Riskbank, Bank of England, Norges Bank, Federal Reserve, Swiss National Bank, Bank of Canada and Bank of Japan). The specific scope of the work and its economy does not allow a detailed approach and the study of the bibliography about Bahamas, Eastern Caribbean and Venezuela CBDCs because they operate in a very different ecosystem; with respect to China, despite the different rule of law, it was studied some of its bibliography about its digital currency experience on AML.

Based on the bibliographic research, the work begins with a systematic review about retail CBDC as a new type of money and key factors to the regulatory analysis relating CBDCs with data protection and AML/CFT.

To the second step of the analysis (the project about a digital euro and policy assumptions of ECB), the reports of EU institutions and the analysis, interviews and public material of ECB's leadership and staff were decisive.

The third part of the analysis concerns the EU legal regimes on data protection and AML/CFT (also its further process of reform). It must be highlighted that it is a work in the context of a Fintech investigation with a specific subject, wherefore one should not appreciate the global legal problems related to a CBDC in the eurozone (namely its foundations under ECB law and its treatment under EU monetary law). However, it is essential to understand privacy and AML/CFT in EU.

The subsequent chapter is dedicated to the discussion of the challenges, risks and necessary efforts posed to a digital euro on the issues of data protection and AML/CFT with the help of the most important literature on that subject.

The final chapter summarizes the most important conclusions of the previous analyses and discussions.

4. Analysis and Discussion

4.1. Central bank digital currency as a new type of money

4.1.1. Historical background

Technology plays a critical role in the finance industry. Although this is an obvious fact it is still pertinent during the third phase of Fintech, initiated in 2008, with intense innovations in payment systems and credit markets (figure 1), in which the link between disruptive technologies and the Fintech business models is a critical factor [Tien et al., 2021: 400; in 2021 the global Fintech funding more than doubled, in comparison with 2020, to reach a record of USD 132B (CB Insights, 2022: 11)].

The beginning of the present phase of Fintech was contemporary of the regulatory shifts occurred after the 2007/2008 financial crisis which had a massive impact on the current and future Fintechs' landscape (Felländer et al., 2018: 154, especially in everything concerning big data, Chishti / Barberis, 2016: 100-105). Regulation constraints are a key factor to the old (e.g., banks and other FI) and new participants (as Fintech start-ups) in order to have success in multiple fields.

Nowadays more than 85% of central banks are researching and, in some cases, at advanced development stages of CBDCs (Labonte / Nelson, 2022: 2; figure 2). The rapid interest of central banks on CBDCs is one more event in the history of monetary transformations and another example "that technological change in money and finance is inevitable, driven by the financial incentives of a market economy" (Bordo, 2021: 2). The fact that a large number of central banks is pressing ahead causes reciprocal investment in sister institutions because they all want to be prepared for what may lie ahead even if it is still very dubious what will be the future designs and goals of CBDCs.

In the last two centuries there were a lot of substantial changes on money currencies driven by different forces, which influenced namely the two most tradable currencies, the USD and the Euro.

In the United States (US) the commercial banks and the Treasury issued their own paper currency until the 20th century (and until 1864 without any federal regulation of private bank-issued currency); the Federal Reserve (Fed) was not established until 1914 and the USD value was fixed to precious metals until 1933, when the US abandoned the gold standard (Elwell, 2011: 9-11), a decision determined by a quick and dramatic succession of events – the stock market crash in October 1929, the first banking crisis (October 1930 to March 1931), the second banking crisis (March to June 1931), Britain's departure from the gold standard in September 1931, the USD 1 billion open market purchase the Fed conducted, under congressional pressure (from April to June 1932) and the banking holiday of March 1933 (Bordo, 1989: 28-29).

The euro was a product of a political choice assumed on the 1991 Maastricht Treaty, born virtually on 1 January 1999 before notes and coins began to circulate, which only happened in January 2002. The Eurosystem, comprising the ECB and the national central banks (NCBs) of the 19 countries which have adopted the euro, has as main goal the maintenance of price stability and acting as a leading financial authority.

The hypothesis of a central bank issuing a CBDC involves multiple reasons and dimensions conformed by the institution objectives, risk, policy and design considerations and legal, governance and regulatory perspectives (figure 4; tables 1-8).

The emergence of CBDCs also involves cooperation and harmonisation in international fora (e.g., the works of BIS, IMF, World Bank, G7[1] or G20[2]). Multilateral collaboration is also essential in different but related areas [e.g., cross-border transactions or foreign exchange (FX)] and compliance with legislative and international obligations must be considered, namely about AML/CFT requirements (below 4.3-4.4).

4.1.2. Central bank digital currency and other types of money in euro area

History shows that retail CBDCs should be framed in a dynamic interaction of different types of money. Taking that into account, Bech / Garratt (2017: 60) offer a useful taxonomy of money based on some key attributes: who is the issuer, what is its form, who can

[1] Canada, France, Germany, Italy, Japan, UK and US.
[2] Composed of most of the world's largest economies, including EU countries and the EU as a regional organization.

access and/or hold it (universal or not) and how is it transferred (centralized or decentralized) (figure 3). In that context it's possible to capture some of the key elements of retail CBDCs, adopted by ECB and NSBs research and the projects of other central banks mentioned (above 3): a currency issued by a central bank on a digital form with universal access (above 2.1).

Currently, ECB and NCBs issue two types of money: (1) reserves only disposable to selected FI (about the Eurosystem's policies on reserves, Åberg et al., 2021) and (2) currency in the form of banknotes and coins which are legal tender throughout the euro area and available to the public (in practice, only the NCBs physically issue and withdraw euro cash, the ECB oversees the activities of the NCBs and initiates further harmonisation of cash services within the euro area).

One basic idea, useful to capture features of a digital euro in confrontation with other official types of money issued in the euro area, is the possibility of a legal claim on the issuer. On that matter, a digital euro should be equivalent to cash, which "implies that the amount of central bank money issued in the form of digital euro should always be under the full control of the Eurosystem" (ECB, 2020: 8, figure 5). In other words, the nuclear feature of a retail CBDC comparing with the other types of money is that it would be a virtual, not physical, money that the public can have "without facing counterparty risk" (Berentsen / Schär, 2018: 101).

4.1.3. Central bank digital currency and the token model *versus* account model

The bigger picture of CBDCs comprises a difference between wholesale (only available to FI) and retail CBDCs (work's object, above 1) and concerning the later there is a discussion centred on the underlying data structure and on the authentication and funds transfer process (figure 6). Related to that there is a contraposition between account-based model *versus* token-based model.

There are two main and different criteria used in the distinction between account and token-based models.

Following a criterium adopted by the past differentiation between bank accounts and cash: (1) in the account-based model, the ownership is linked to an identity, meaning that in order to make a transaction the user must provide his identity (as in today's bank accounts)

and the record is updated by increasing or decreasing the position of the account on its database; (2) in the token-based model, the ownership is linked to a proof which can be achieved through the use of public key cryptography infrastructure or other authentication service (as it is synthetized in figure 7).

This criterium is related with a historical economic approach. It presents a way to understand some key aspects of retail CBDCs and frame it in the history of money. Traditionally, money is based on dualistic models, tokens of stored value *versus* accounts, with implications for the difference between the transfer of cash and the transfer between bank accounts (Mersch, 2017; Berentsen / Schär, 2018: 98; Kahn / Rivadeneyra / Wong, 2018: 3-4; CPMI, 2018: 10-12, 17; Barontini / Holden, 2019: 2; PWC, 2020: 15; Auer / Böhme, 2020: 93-95; Bindseil, 2020: 4; Giancarlo et al., 2020: 17-19).

However, this criterium can sometimes be a little dubious for computer scientists (Auer / Böehm, 2021: 9n12). It is not a completely comprehensive criterium as in the account-based model the identification of the owner is needed and in the token-based there is a verification if the token is genuine, thus later it is also possible that an intermediary verifies the identity of the wallet holder (Barontini / Holden, 2019: 2, figures 6 and 8). In some DLT token-based models, there is the need of verification through a central node in the system, a so-called notary node, which could be operated by an intermediary and require that all transactions are recorded in a ledger (Armelius et al., 2020: 87).

Furthermore, the simplistic approach of the supposed resemblance between CBDC token-based and cash (below figure 7) can lead to misguided illusions that token-based technology in opposition to account-based may achieve cash-like properties. It has the risk of obscuring or oversimplifying the relationship between alternative CBDC designs and regulatory constraints (below 4.4).

It is important to consider the structural difference between tangible cash and all virtual types of money: only the former circulates freely in the economy without any intrinsic necessity of being kept records. The only thing CBDCs have in common with cash is the legal claim on the issuer (figure 5).

An analysis linked to the theory of the regulatory approach should bear in mind the empiric and technologic structural difference between cash and digital money. Cash is the only liquid asset for payments that can operate without any intermediaries while all systems of digital transfers of money involve the mediation of a ledger. They all are just “another form

of scriptural money" (Grym, 2018: 13) and, in a certain sense, it can be said that "as long as there is a ledger involved […] there is a third party involved (the ledger)" (Armelius et al., 2021: 11), i.e., in virtual payments or transfers it is always necessary a digital register and, contrary to cash, it is impossible that the payer hand delivers the money to the payee.

The criterium adopted in the present work concerning the distinction between token and account CBDC models is more focused on a Fintech point of view and will be based on the alternative ledger types used (e.g., Mancini-Griffoli, et al., 2018: 8-9; Urbinati et al., 2021: 15).

A criterium focused on technology and also on legal definitions is that "tokens are bearer instruments and represent in themselves ownership of a monetary value" and an account-based "indicates ownership of a monetary balance" in some form of conventional financial technology recorded by a central bank or a financial intermediary (Armelius et al. 2020: 87).

The way the operations are recorded is quite different: a token based system "records the state of the ledger", as individual tokens, and 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)" (Urbinati, et al., 2021: 15); it's the case of protocols like Bitcoin and Corda (Longchamp et al., 2020: 2-5; Zellweger-Gutknecht, 2021: 3; Urbinati, et al., 2021: 15). In the account model, when a transaction happens, "the system updates the records by increasing and decreasing the balances of the accounts in question, usually the payer account and the payee account" (Urbinati, et al., 2021: 15) and it can be operated the same way of many of the payments systems (namely TIPS, above 2.3), but also protocols as Ethereum, Quorum and Ripple (Longchamp et al., 2020: 5-9; Zellweger-Gutknecht, 2021: 3).

In conclusion, the key factor is the information carried by the information asset, tokens or accounts: in the former, it is carried "information about their value and the entity that issued the token"; in the later, accounts "are associated with transaction historical movements that include all of the credit and debit operations involving the accounts" (Chaum et al., 2020: 9).

The perspective that the terms token *versus* account model perhaps "should be retired to avoid further confusion" (Garratt, et al., 2020) is not followed in the present work. Here, token *versus* account model is considered an useful conceptual distinction, if based in ledger

types criteria, to approach the risks and challenges regarding CBDCs and regulations constraints on data protection and AML/CFT (but not only because it also brings advantages on the matter of equilibrium on other security risks as counterfeiting (Kahn / Rivadeneyra / Wong, 2018: 8-16), as long as it is rejected the idea one must choose between account-based and token-based (Lee et al., 2020), so the "choice may not be binary" (Bank of England, 2021: 19).

In the present work this classification, including the possibility of hybrid models (i.e., a digital currency can be simultaneously token-based and account-based), is preserved for three main reasons: (1) it captures a key factor on the operation schemes mentioned above (how the information is carried), having potential relevance to the comprehension of regulatory problems; (2) it can be useful to discuss key features, even in the case of the adoption of hybrid, mixed or integrated models with an account-based component and a token-based instrument (e.g., Tinn / Dubach, 2021; Urbinati, et al., 2021: 19, below figures 11-12); (3) it is frequently used by the literature in the discussion of multiple issues (e.g., trade-offs on privacy and AML/CFT) and the majority of central banks and consultant companies (as Accenture, who is working with ECB, the Fed, Riksbank and Bank of Canada) rely on the distinction in the development of their researches (e.g., Gürtler et al., 2017: 6; Mandeng / Vellisarios, 2019: 11; Giancarlo, et al., 2020: 11; Kahn / Rivadeneyra, 2020; Chaum et al. 2020: 12-24; Bindseil, 2020: 4, 24-25; Armelius, 2021: 11; Norges Bank, 2021: 26; BIS 2021: 85; Carstens, 2021: 7-14; Cecchetti / Schoenholtz, 2021: 57, 62).

Beyond the alternatives based on the ledger types there are other key features to understand the relationship of CBDC architecture alternatives with regulatory needs on data protection and AML/CFT.

Decentralized preferences are compatible with token-based and with features of account-based systems because they can exist without a centralized ledger. What makes these "decentralized systems account-based is that transactions require updating a balance, as opposed to providing an object (token) that can be further transmitted without verifying a balance on the ledger" (Giancarlo et al., 2020: 18; figure 10). Variants between different kinds of centralised and decentralised architectures (figures 10 and 13-17) which involve the level of tasks and responsibilities assumed by the central banks (figure 18) have enormous impact on regulatory issues, namely AML/CFT (below 4.4).

The complexity of the distinction increases when integrating very different perspectives about the main goals of CBDCs and risks that should be addressed, some of them based on multiple-level architectures (especially two-tier). In fact, in what Auer / Böhme call a "Direct CBDC" model, the central banks handle all payments and are the entities responsible for all retail holdings (top of figure 19). In contrast to that model, possible alternative solutions include different kinds of division of tasks between private entities and central banks.

Theoretically, the central bank responsibility can range from the maximum of cumulating issuance, distribution and management of payment system, user devices or accounts to the minimum of only having regulatory and supervision authority besides acting as an issuer (for an illustration from the point of view of the central banks, figure 18). Division of tasks between private entities and central banks can be expressed in plural designs (figure 19 for one illustration, but there are multiple alternatives, figures 13-16).

The two-tier alternatives will be analysed only from the perspective of potential impacts on data protection and AML/CFT, letting aside the monetary policy foundational issues as the risks of structural disintermediation of banks or systemic runs on banks in crisis situations (e.g., Bindseil, 2020: 30; below 4.4.1).

4.1.4. Central bank digital currency as complement to other types of money

CBDCs, if implemented, would appear in advanced economies as new contenders on the money market in potential competition with cash, private digital currencies, existing private payment systems or the current commercial banking system.

CBDCs can be presented as an answer for the dangers posed to central banks by crypto-assets (Söderberg, 2019 pp. 2-3), but the main responses to those risks are regulatory (cf. 2.2 and 4.3), with an increasing number of countries that have banned or severely restricted cryptocurrencies (Quiroz-Gutierrez, 2022).

Beyond the pressure of countries and intergovernmental organisations, there are other doubts about its safety and its capacity to survive due to some economic and technological weaknesses. The majority of cryptocurrencies' prices frequent fluctuation make difficult its use as a method of payment (Amstad, 2019: 231). For some authors, even the strong features of Bitcoin (scarcity and cryptography) in the near future eventually won't be sufficient to guarantee exchange because of the huge energy-intensive protocol, called "proof of work", needed to process transactions and its economic dependence of the rewards of the miners with newly minted coins. As Auer points out, when Bitcoin will approach its maximum supply of 21 million coins, the monetary income ("seigniorage") of the miners will decline and delays will increase (Auer, 2019: 8-20, figures 22-23).

ECB, the Fed and other important central banks of the more advanced economies pointed out that the projects of its retail CBDC are about a new type of money which will exist alongside with the "traditional" ones (e.g., Auer / Corneli / Frost, 2020: 18-30; Rice et al., 2020: 42; Assenmacher / Bindseil, 2021: 111; Tinn / Dubach, 2021: 30). Theoretically, "it is possible that eCNY, China's new CBDC, could reduce the international dominance of the US dollar" (Duffie, 2021: 141), with studies concluding that for People's Bank of China it would be relatively easy to replace cash (Shirai in Amstad, 2019: 35) and it is attractive to the state control (4.4.2.4). Nevertheless, it would depend on international arrangements. There are instruments to block CBDCs on cross-border payments (4.4.2.2) and the issuers of the two contemporary dominant currencies (USD and euro) don't like the idea of issuing CBDCs to replace physical cash because "it would jeopardize these currencies' role in the global payments and monetary systems" (Nabouli, 2020: 17).

In democratic and advanced economies there may be scope for the market adoption of CBDC as a «potential replacement for cash for small-value, pseudo-anonymous transactions» (Mancini-Griffoli, 2018, 30-31). However, a conception of CBDCs as an «alternative to cash that also provides some privacy features» (e.g., Garratt / Lee, 2021: 17) can enter in collision with AML/CFT policies (below 4.3 and 4.4.2).

Dramatic money replacements aren't unprecedented (e.g., from metal-based money to metal-backed banknotes and to physical fiat money), so from an historical perspective there is no reason to say CBDCs can't one day fully replace physical cash (Mancini-Griffoli, et al.,

2018: 6). In a near future, cash will continue as "the only *liquid* asset for saving outside of the private financial system" (Berentsen / Schär, 2018: 100), and if a digital euro emerges it will be only a complement of other types of money (below 4.2) with its own features that the public can choose to use or not to use – for instance Rogoff / Scazzero "conjecture that the demand for non-anonymous CBDC will be considerably less than the pre-existing demand for paper currency" and calculate it would be "as much as 80 percent less" (2021: 572, 588-589).

4.2. The project about a digital euro and policy assumptions of ECB

The Eurosystem (above 4.1.1 to 4.1.2) prime objectives are the maintenance of price stability, safeguard of financial stability and promotion of European financial integration. The ECB and national competent authorities are also responsible for Single Supervisory Mechanism. Beyond the EU treaties there is a vast legal framework about the ECB and NCBs, including matters about articulation with private entities, namely the designated "credit institutions and other market participants" (articles 17 and 18 of the Statute of the European System of Central Banks and of the ECB).

ECB and the Fed don't want to be among the pioneer central banks with a retail CBDC. However, if the digital USD and digital euro are to be born, its issuers want to get it right and shaped by their specific interests and core public responsibilities (above 4.1.1). Some of the public speeches of ECB`s top staff have common points with the Fed, namely the final decision to launch it must be from the political bodies. Accordingly, in US the Fed "does not intend to proceed with issuance of a CBDC without clear support from the executive branch and from Congress, ideally in the form of a specific authorizing law" (Board of Governors, 2022: 3) and in EU was highlighted that the European Parliament (EP) has a "fundamental role to play in the discussions on the framework that would be needed to issue a digital euro" (Panetta, 2021a) and the EU finance chief, Mairead McGuinness, already announced the EC`s "goal is to table legislation in early 2023" (Smith-Meyer, 2022).

EP, EC and the finance ministers of the euro area countries are political institutions with the power to do the final step (e.g., Council of the European Union, 2021a, § 23: 7) but their decision must be preceded by cautious research promoted by the ECB.

ECB was not among first central banks with an enthusiastic view about the possibility of issuing a CBDC; in a 2018 global survey it appeared as one of the most sceptic central banks about the issue (Mancini-Grifolli et al., 2018: 29). Still, ECB was one of the first central banks with official reports on VA and, in October 2012 released one which concluded "virtual currency schemes" "do indeed fall within central banks' responsibility as a result of characteristics shared with payment systems, which give rise to the need for at least an examination of developments and the provision of an initial assessment" (ECB, 2012: 46).

Subsequently, ECB promoted multiple digital asset research papers and was involved in collaborative research efforts with other central banks and international financial institutions, like BIS (founded in 1930 and composed by 62 central banks), to better understand DLT and the potential effects of CBDC issuance. By the end of 2016, ECB created a CBDC task force prompting more public discussions (Todd / Rogers, 2020: 107) and, in 2017, research to study DLT market infrastructure use cases (named Project Stella, ECB / BOJ, 2017) was initiated with the Bank of Japan (BOJ). Project Stella has explored DLT application use cases through conceptual studies and practical experiments. Its financial market infrastructure results have been released in four phases; the fourth, in February 2020, analyses a broad range of privacy-enhancing techniques (PET) aimed at balancing the confidentiality and auditability of payments in a DLT environment. However, project Stella findings were examined through a technical scope without considering all the legal and regulatory constraints.

In January 2017, ECB`s board member, Yves Mersch, launched the first institution insights about the possibility of a euro CBDC that he considered "characterized by two features" "like banknotes in circulation […] is a claim on the central bank" and "in contrast to banknotes" is "digital" (Mersch, 2017). It is a speech based on the traditional division between cash and bank accounts that pointed in the direction that CBDC in euro area should "mainly replace cash" and should be "as cash-like as possible, at least initially" (about the hypothetical resemblance with cash, above 4.1.3 and below 4.4.2).

Contrary to the perspective of some authors that "unlike cash, CBDC is no more anonymous than other traded debt" (Rogoff / Scazzero, 2021: 588), in 2019 the Eurosystem experts explored ways to issue small value payment cards that allow anonymity; it was developed a proof of concept (PoC) for enhancing privacy in a CBDC payment system aiming

to show if it is possible to monitor illicit activities while still allowing users to make a small number of low-risk, low-value payments with limited sharing of information (ECB, 2019).

Suddenly, during the first year of the COVID-19 crisis, they were taken rapid steps, probably induced by the apparent shift in payment habits towards contactless payments and e-commerce (ECB, 2020: 7 and 11).

In 2020, the ECB established a High-Level Task Force on CBDC (HLTF-CBDC) composed by experts from the ECB and the NCBs, whose initial main findings about benefits and challenges concerning introduction of a digital euro were the object of a report released in October 2020 (ECB, 2020); it puts in context the hypothesis of a digital euro accepting some core features of the digital euro like the characteristic of legal claim which brings important implications, "design options in which private entities would act as custodians of digital euro holdings, thereby leaving users with a claim on the intermediary rather than on the Eurosystem, are excluded in line with the core principle that the digital euro should always be a claim on the Eurosystem" (ECB, 2020: 36; above 4.1.2).

The October 2020 report developed a comprehensive study about conditions, objectives, core principles, scenario-specific requirements and general requirements for the digital euro, reaching conclusions that will frame the regulatory challenge: a digital euro as a CBDC complement to cash and central bank deposits universally accessible. It identified conditions and objectives to the launch of a digital euro. Among the main goals are (i) the contribution to digitalization of the EU economy and the strategic independence of the EU as a response to the decline role of cash as a means of payment; (ii) to mitigate risks to the normal provision of payment services; (iii) to foster the international role of the euro; (iv) to support improvements in the overall costs and ecological footprint of the monetary and payment systems.

Since one basic goal is that digital euro must not have negative consequences in the financial sector, two important requirements with impact on AML/CFT issues are required: (1) that it should be mainly used as a means of payment and not become an instrument for financial investments; (2) that supervised intermediaries should be involved in the handling of a digital euro.

Coherently, the 2020 report expressed a preference towards an access model intermediated by the private sector but it left open many aspects for further conceptual analysis and assessment through practical experimentation, some of them quite important like the design of the back-end infrastructure and its underlying technology, the level of privacy,

remuneration and holding limits. The ECB highlighted the future research should connect the "fast evolution of the payments ecosystem" with the needs of enhanced privacy for users and risks of ML/TF (ECB, 2020: 7).

The HLTF-CBDC work was a starting point for a public consultation published in April 2021 (ECB, 2021a). It was possible to verify the importance and the caution with which the ECB treats this possible innovation by the number of people surveyed, a record number (more than 8000 respondents) in ECB public consultations, from European citizens to professionals and business in the payment sectors. Citizens and experts who took part in the public consultation on the digital euro largely believe that the digital euro should be integrated into existing banking and payment systems and that additional services should be given in addition to basic digital euro payments (figures 24 to 26).

After the results of the public consultation, the Eurosystem launched the project's investigation phase (ECB, 2021c).

In the last year and a half, many declarations and speeches give signals that the EU bureaucracy has already reached a broad consensus about the reunion of the decisive elements to the possibility of a digital euro (EC, 2021a: 11-12; Council of the European Union, 2021, § 24 p. 8; EP, 2021: 7; Lagarde, 2021; Guindos, 2021). EU institutions, though its cautious declarations and reports, apparently have a consensus to prepare a retail digital euro in the context of an impressive rise worldwide of research and development effort on CBDCs (above 4.1.1, below figure 2).

The possibility of a digital euro related with the "direct and indirect evidence" that "strongly suggest that the use of paper currency in transactions is steadily declining" (Rogoff / Scazzero, 2021: 590) and the necessity of the ECB won't be outdated by its competitors on the money issuing (above 4.1.1). So, it should be framed in the broader problem of digital payments in Europe and its continuing transformations, an area where ECB was precursor among central banks when it provided TIPS as a fast-payment solution (Mancini-Grifolli et al., 2018: 12 put it in a global perspective).

Something that is related with a strategic analysis present in the Eurosystem reflection about CBDCs and specific goals as an answer to economic concerns, namely the idea that "Europe has underperformed in recent years in the global competition among payment instruments" (Assenmacher / Bindseil, 2021: 112). So, the participation of intermediaries is more than an operating need, it is a goal to economic policies.

ECB needs to define the digital euro model in collaboration with three key stakeholders: consumers, merchants and supervised intermediaries (Bindseil et al., 2021: 31). For that, it set up a Market Advisory Group (including 30 professionals from the retail payments industry) to provide advice on the design and potential role of a digital euro in the payments' ecosystem (ECB, 2021d) which is regularly discussing the project with the Euro Retail Payments Board (the Eurosystem's established forum for institutional dialogue on retail payments), academics and think tanks (Panetta, 2022).

Another key is the international dimension and the need of cooperation with other major central banks (above 4.1.1; Panetta, 2021c), namely about the potential for foreign CBDCs or private digital payments to become widely used in the euro area.

The issuance of a digital euro involves multiple trade-offs (e.g., privacy, traceability of operations and end-users) that are foundational for specific design features such as the technology platform, the degree of transparency, availability and usage limits (Kiff et al., 2020: 47). The progress of the political option to launch a digital euro and the design of the new retail CBDC must be constrained by the specific EU framework, so it is "key to address any potential challenges for EU policies", including "those related to" AML/CFT and data privacy (EC, 2021a: 21).

4.3. EU legal and regulatory frameworks for data protection and AML/CFT relevant to digital money

There are three essential legal principles in the context of Fintech: legal certainty, technology neutrality and proportionality (Amstad et al. 2019: 48). The relationship between money, law and enforcement or regulatory powers of the states can produce significative impacts on the Fintech industry value chain, so GDPR and AML/CFT rules must be included in the decision tree (figure 36).

GDPR is one of the most protective data protection laws of individual rights (table 10) comprising a lot of rules relevant to digital money (table 11), namely, article 25 imposes "privacy by design", which implies data protection is best achieved if integrated in the technology when created, and "privacy by default", what means that without requiring any intervention by the user his data is used only in steps strictly necessary for the specific

purpose of determining whether a transaction is lawful, namely respecting AML/CFT requirements (Auer / Böhme, 2020: 88).

ML/TF is a financial crime that consists of making "dirty money" look clean and/or using money for illicit purposes.

FATF is an independent intergovernmental organization that sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating ML/TF. It has 37 members jurisdictions, including all the major economies, various EU countries and the EU as an international organisation (represented by EC as the EU's executive body).

FATF has set out recommendations for customer due diligence (CDD), including identity verification, record keeping, and suspicious transaction reporting requirements for financial institutions and designated nonfinancial businesses and professions (e.g., Mancini-Grifolli et al., 2018: 29).

AML/CTF activities are governed by a legal framework at EU level designed to prevent money transfers for ML/TF purposes. AML/CFT regulation has a complex procedure with the interaction of a plurality of institutions of EU and member states, between the private sector and law enforcement agencies (police, prosecution offices). The financial intelligence units (FIU) are state authorities who work as intermediaries between the private entities subject to AML/CFT obligations and the law enforcement agencies, receiving, analysing and transmitting reports of suspicions identified and filed by the private sector (figure 27).

The EC announced on 20 July 2021 a new AML package, which consists of four legislative proposals (EC 2021b, 2021c, 2021d, 2021e and 2021f, figures 28-29) that should be applied by the end of 2025.

European policies on AML/CFT comprise different strategies to different types of money.

EU policies have been based on FATF standards, namely the "follow the money" approach, thus, in the centre of the AML/CFT efforts is the scrutiny of wire transfers of funds.

Cash, differently from virtual money, isn't traceable so the "follow the money approach" can't be adopted and AML/CFT measures are directed to transactions and money transport (FATF, 2015; Europol, 2015). The 2021 package spreads to all EU countries the limit of EUR 10000 cash payments for purchases of goods and services permitting member

states to keep lower limits (EC, 2021b) as EC concluded that systemic identification requirements for selected operations present issues on speed and effectiveness.

The evolution of assets poses new challenges for AML/CFT, for instance FATF follows a Recommendation-by-Recommendation approach to the VA (FATF, 2021b: 5). In particular, crypto-assets (above 2.2 and 4.1.4) are thought to be very suitable for ML/TF purposes because of their anonymity, cross-borders nature and quick transferability (Houben / Snyers, 2017: 17). 2021 EC package have relevant measures for crypto-assets, namely: the list of entities obliged to prevent ML and TF is expanded to include crypto-asset service providers and other sectors; internal policies, controls, and procedures for risk management are clarified, in particular CDD measures are detailed; beneficial ownership requirements are streamlined to ensure an adequate level of transparency across the EU, and new requirements to mitigate risks that criminals hide behind intermediate levels; measures against the misuse of bearer instruments are strengthened; anonymous crypto-asset wallets are forbidden.

AML/CFT depends on the efficacy in supervising and scrutinizing suspicious financial transactions, which involves a link between prudential supervision and AML/CFT authorities (Council of EU, 2018; European Banking 2019; 2021).

In the exercise of its prudential supervisory tasks, ECB shall act upon ML/TF concerns that may have impact on FI' safety and soundness and has the duty to cooperate with AML authorities. For example, the ECB cannot monitor KYC procedures in individual cases, but it can check whether a failure of a bank in conducting KYC procedures is the result of more fundamental governance deficiencies.

The AML authorities have the power to investigate breaches on AML/CFT rules and, for instance, to impose fines.

The breaches on AML/CTF provisions can be a ground for the withdrawal of a bank's license, which is an ECB's task. For that, ECB should rely on facts investigated by the authorities competent for AML/CTF (European Banking Authority, 2019).

A need for closer cooperation on the supervision field is taken into account in the 2021 EC package, which proposes the creation of a new EU supervisory authority to control financial activity in member states, monitor and audit large transnational FI that will "be entrusted to develop guidelines in coordination with the ECB, the European Supervisory Authorities, Europol, Eurojust, and the European Public Prosecutor's Office on cooperation between all competent authorities" (EC, 2021e: 29, 71, 73 and 75, figures 28-29).

4.4. Challenges on data protection and AML/CFT posed to a digital euro

4.4.1. Compliance needs, digital euro architecture and the division of tasks between central banks and private sector intermediaries

In the EU the political independence of the ECB and NCBs is laid down in the institutional framework for the monetary policy which has important practical implications: they are forbidden of seeking or taking instructions from EU institutions or bodies from any agencies of EU Member States (article 130 of the Treaty on the Functioning of EU).

Theoretically, central banks (as ECB and NCBs) depending on its relations with the end-users of the currency can be bound to the same legislation of other market participants, especially AML/CFT regulations (World Bank, 2021: 16; Chaum et al., 2020: 9). It would be the case if the public held deposit accounts in central banks [figures 19 (top) and 21)] implying, therefore, a responsibility of these public institutions to ensure AML/CFT compliance, such as conducting KYC checks, authenticating customers for transactions, managing fraud, and dealing with false-positive and false-negative authentications.

It is not an executable system given the fact central banks aren't prepared to do all the necessary operations on a large scale. More important, that hypothesis, where the central banks have tasks related with distribution, payment system and/or user devices, is incompatible with the EU law about central bank status and AML/CFT framework (above 4.1.3, 4.3, below figure 18).

The alternative designs comprise a division of tasks between central banks and private sector intermediaries (PSI), selected banks and other PSP, because less information shared with ECB and NCBs means less exposition of central banks to the regulatory framework and more supervision of PSI is needed to ensure data protection and effective application of AML/CFT rules (figure 20).

Even a centralised digital euro, where the PSI should conduct KYC checks, isn't also legally possible if the NCBs still have a direct contractual relationship with the end-users [figures 13 and 19 (middle)], which can imply some CDD responsibilities incompatible with their status.

These are decisive reasons to reject architectures that require central banks to develop and establish AML compliance programs (without forgetting the risks of disruption in the financial sector). A conclusion beyond the complex policy issues concerning who would be the market participants with the right to act as selected and supervised intermediaries (Assenmacher / Bindseil, 2021: 113).

The only architectures compatible with the AML/CFT legal framework are the decentralised ones where central bank does not maintain the full record of retail transactions and, consequently, is released from the duty of supervising ML/TF. As examples of those architectures can be mentioned the designated "decentralized ledger system" (Armelius et al., 2020: 88-90, below figure 16), the "fully intermediated" (Auer / Böhm, 2021: 10-13, bottom of figure 19) or the "hybrid bearer infrastructure" (ECB, 2020: 41, below figure 15). In these solutions, central banks only record wholesale balances but maintain the responsibility to honour claims of which they have no records, so it is necessary a close prudential supervision of the PSI in order to verify the correspondence between the wholesale holdings communicated and the retail activity.

The effectiveness of these two-tier systems depends on clarification of the regulatory framework and sufficient economic incentives to private sector entities participate as intermediaries [e.g., fees, expansion of customers bases with additional embedded services" (BIS, 2021: 81; Bindseil, 2021: 31); some authors consider that CBDC can also potentially mitigate compliance cost for PSP on transaction monitoring and reporting (Fong, 2019: 9)].

In a two-tier system full intermediated, ECB and NCBs are not involved with CDD procedures but coordinate their prudential supervision of PSI with the AML/CFT public agencies (figures 32-33).

ECB has already to coordinate its tasks with AML/CFT authorities in the context of the 5th AML/CFT EU Directive, namely it has the responsibility "to ensure that practical arrangements are operational to allow AML/CFT concerns communicated to the ECB by AML/CFT supervisors to be consistently factored in when performing supervisory tasks" (Council of EU, 2018: 3). Harmonisation and coordination of prudential supervision with AML/CFT supervisors developed at the 2021 package in a way more evidently inadmissible with its accumulation with compliance roles (above 4.3, below figures 28-29).

In short: (1) if it is adopted an account-based system the entire servicing and maintenance of the accounts must be assigned to third-party providers (Bindseil 2020: 4), for

instance allowing customers to use their existing online banking access to initiate transactions from their CBDC account (Berentsen / Schär, 2018: 102); (2) if the adopted solution comprises electronic tokens it also needs the exclusive involvement of PSI on the performance of KYC checks and other AML/CFT procedures.

4.4.2. Digital euro and trade-offs involving data protection, anti-money laundering and combating the financing of terrorism

4.4.2.1. The record-keeping payments system comprehends a problem with three key elements, access, privacy and security, because "it is necessary to balance the extent of access (universal or restricted) with security risks (to the operator and users from admitting potentially risky participants) and privacy (relinquished by users to help control the risks)" (Kahn et al., 2018: 13, figure 34).

The EU law presupposes that there is a difference between anonymity, for one hand, and data protection, for another (above 4.3).

Regarding the design's research, the initial investigation about a digital euro, more focused on a technical scope (e.g., project Stella, above 4.2), should be followed by investigation concerning previous policy decisions about privacy, data protection, integrity of the financial system, fight against crime (including ML/TF) and protection of the ownership of intangible assets. Regulatory constraints shape technical developments in matters such as the "functionality that enables the features of the system (e.g., minting, transferring, governance, etc.)", "guarantees that ensure the privacy and confidentiality of the information" and "integrity or security requirements that ensure the system's robustness" (WEF, 2021: 160) which should be addressed "on the basis of a technology-neutral approach", as it is underlined in other areas of payment technologies at the point 6 of the Directive (EU) 2019/713 of the EP and of the Council.

The payment ecosystem of a euro CBDC should comply with requirements about the processing of personal data, such as specific data retention periods or reporting obligations, applicable to all other kinds of digital money in euro area (bank accounts, credit cards, cryptocurrencies). The guarantees of data protection and the AML/CFT legal requirements call for an architecture that accommodates different data protection solutions as well regulatory rules designed to ensure monitoring AML/CFT (Norges Bank, 2021: 25-26).

Transactions reveal sensitive personal data, so there are two core decisions in the matter of privacy by default design: “the amount of personal information transaction partners” get and “the risk of large-scale breaches of data held by the system operator or intermediaries” (Auer / Böhme, 2020: 94; BIS, 2020: 19).

Consumers’ data protection can be an important competitive advantage of a digital euro because it must respect high privacy level configurations in accordance with the GDPR and European Charter of Fundamental Rights (Chavolla, 2018: 273, 281-286, 288-291). ECB, as a public and independent institution, has no interest in monetising users’ payment data (Bindseil, et al., 2021: 24) and consumers have clearly more trust in FI (potential PSI of a digital euro) in comparison with big tech (figure 35).

Digital euro operators would only process data to the necessary extent for performing their functions and in full compliance with public interest objectives and legislation. PET are “a coherent system of information and communication technologies measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system” (European Union Agency for Cybersecurity, 2022: 8). Hence, it is possible to use them while still complying with regulations on AML/CFT (Bank of England, 2020: 32; Tinn / Dubach, 2021: 10-13).

The investigations on the current experimental work of a digital euro include various work streams that “allow for different levels of privacy” and are “looking at possibilities for local storage in collaboration with developers of bearer payment instruments that could be used in offline transactions” (Panetta, 2021a, appendix; Deutsche Bank, 2021: 3; ECB, 2021b: 3-4).

4.4.2.2. The problems about privacy and AML/CFT have a significant cross-border dimension, but literature has been focused mainly on the domestic use of CBDC (Mancini-Griffoli et al., 2018: 4; BIS / CPMI / Innovation Hub / IMF / World Bank, 2021: 17) and digital euro project is “currently focusing on domestic needs in the euro area” (Panetta, 2021a; ECB, 2020: 22).

The functionalities for FX, cross-border payments and transactions, open questions that need international multilateral collaboration and harmonisation (which would include

agreements about AML/CFT compliance) to overcome the problems created by multiple and ambiguous rules.

The possibility of cross-border transactions with CBDC can be sustained by relevant policy reasons such as "regulatory expectations" on the AML/CFT matters (EC, 2021a: 11), "potential gains in cost and speed" (Labonte / Nelson 2022: 2; Panetta, 2021a, 2021c; ECB, 2021a: 26), "foster the international role of the euro" (ECB, 2020: 14; Bindseil et al., 2021: 4) or mitigation of "the impact of sanctions on ordinary citizens of sanctioned countries and [to] discourage them from switching to alternative payment methods with higher risk profiles" (Nabilou, 2020: 312).

Digital euro use outside the euro area depends on different arrangements concerning international payments with other currency areas (Bindseil et al., 2021: 25-29; BIS, 2021: 86-89). It involves unique issues to cross-currency systems such as FX conversion and liquidity management in foreign currencies and other "complexities of domestic systems" that "are amplified in a cross-border context", as conflict of laws issues, the universe of admissible end-users and adherence to multiple AML/CFT regimes (Bech et al. 2020: 53).

"Detection of cross-border ML/TF cases" is a key to AML/CFT policy related with the need of "supervisory cooperation" (EC, 2021e: 2, 3 and 5), in particular harmonisation of KYC checks to "further facilitate the registration, identification and authentication of users in payments" (Council of EU, 2021a: 6). So, the possibility of a digital euro to be used cross-border depends on mechanisms to ensure compliance with AML/CFT frameworks (e.g., Mancini-Griffoli et al., 2018: 31; ECB, 2020: 22; Council of EU, 2021a: 10; Bindseil et al., 2021: 28; WEF, 2021: 32-35).

The design decisions taken on digital euro should be made "with a view to their domestic use also facilitate cross-border use in future" (Bindseil et al., 2021: 29; Urbinati et al., 2021: 54; Silva / Silva, 2022: 16), so it should be taken into account what design "can best enable cross-border efficiencies while preventing unintended international spillovers" (BIS, 2020: 19) – for instance, features to cross-border interconnection between identification ("beneficial ownership registers") and traceability mechanisms (EC, 2021e: 9, 19-25).

4.4.2.3. The decisions about a digital euro's design and rules should be based on public values like policy goals of the issuer (e.g., monetary, obstacles to risks of dangerous

disruptions) and other public policies (e.g., data protection and AML/CFT, figure 36). AML/CFT policies are not a core objective to the issuance of a CBDC, as it was highlighted by a group of central banks, including ECB (BIS, 2020), nevertheless, prevention policies on AML/CFT should shape the decision of introducing a CBDC and its future design (Bordo / Levi, 2017: 4).

For empirical and structural reasons, digital euro can't be cash-like (above 4.1.3) and shouldn't be treated like one for policy reasons. Only cash payments can operate without any intermediaries and the only hypothesis in which a CBDC doesn't leave digital footprints is in the case of tokens stored locally and when the payment is "made by handing over the device where the CBDCs are stored" (Armelius et al., 2021: 11).

Regarding privacy, the illusion of a cash-like CBDC blurs foundational issues on matters of data protection and AML/CFT.

Central banks must respect policy goals legally established, namely the circumstance that they didn't receive "a specific mandate to provide untraceable or anonymous payment methods" (Bank of England, 2020: 32) and they shouldn't forget that "most of the cash in circulation is in the top two largest denominations, often associated with illicit payments or store of value" (Mancini-Grifolli et al., 2018: 20).

AML efforts depend on the specific technology used on digital euro and tools used to manage the increasing amount of information generated by the CBDC. Regulated institutions need to invest in artificial intelligence (AI) based tools in order to improve their CDD processes (e.g., figures 37-39).

In principle, AML/CFT rules applicable to physical euro must be also applied to digital euro but this is not sufficient because CBDCs present different risks; if it had the liquidity of cash, it wouldn't suffer the limitations on portability that come with physical euro (FATF, 2020: 26). A CBDC will require AML answers beyond the amount allowed to transactions, attending to the incomparable power of computer tools used to fasten and multiply operations.

The potential use of "money mules" (people "who transfers illegally acquired money on behalf of or at the direction of another", FBI, 2019: 2) is a problem that should be addressed with preventive measures relative to digital transfers and transactions used on ML (FATF, 2021b: 42), including specific CDD guidelines (European Banking Authority, 2021:

193) – a reason for a designated "European Money Mule Action" being established in 2016 by the initiative of Europol, Eurojust and the European Banking Federation (Europol, 2021).

CBDCs enables the replacement of people as "money mules" by wallets and programs, generating possibilities for criminal entities "to distance themselves from the illicit source of funds" (Dupuis / Gleason / Wang, 2021: 11). There are various computer science tools that can be used in "money mules" operations with CBDCs "more intricate than traditional ones"; for instance, "with smart-contract functionality, a single person could potentially manage hundreds of digital wallets and exploit various automated features (many of which probably have not been thought of yet)" (Fanusie, 2020: 13, the author illustrates it with hypothetical illicit finance scenarios in pp. 17-20).

It is true that the old instruments to ML will still be available (Dupuis / Gleason / Wang, 2021: 12), but from a regulatory point of view the AML/CFT standards and enforcement strategies adopted to other types of money can be insufficient to the potential flexibility of CBDCs transfers in an environment based on a new architecture which can be explored with creativity for criminal endings.

4.4.2.4. The risk level posed by a digital euro relates to the "actual design of the product" (FATF, 2020: 27). A type of money which combines anonymity, portability and mass-adoption has huge potential for ML/TF.

In the medium term, the FATF`s risk-based guidance should be considered in a preventive manner to mitigate risks posed by different designs and possible evolutions of CBDCs (like cross border payments and FX) to develop specific and tweaked supervisory, regulatory and enforcement measures.

A digital euro should not be anonymous. The experience of China and its reasons to consider fully anonymous token-based wallets with low payment limits (Mancini-Grifolli et al., 2018: 29; Dent, 2020: 925 and 939; Amstad et al., 2021: 35, 177 and 182; Fong, 2021: 5-9; Auer et al., 2021: 5; Labonte / Nelson, 2022: 14) should be analyzed considering that China is: (1) an authoritarian state with broad surveillance programs and crime policies incompatible with foundational values of states submitted to the rule of law; (2) a global power which can have a faster transition from cash to CBDC based on a particular program against the dominance of USD and euro (above 4.1.1 and 4.1.4).

Although e-CNY Chinese experience (a distribution of wallets to more than 140 million people, since October 2021) is recent, there are already reports of situations of uncovered instances of ML using its pilot CBDC, confirming the "yuan's controlled anonymity" attractiveness for "scammers, fraudsters and hackers" (Ledger Insights, 2021). Solutions presented to overcome the problem are typical of a society with massive surveillance mechanisms ("locally stored face scan or fingerprint […] associated with the wallet" and the obligation for users to "scan their face to make a payment" and, even in these cases, there is the risk of people being forced "to scan their faces or fingerprints").

In democratic countries, various solutions have been discussed concerning the possibility of anonymity and offline transfers, like limiting the ability for anonymous P2P transactions (FATF, 2020: 27) and/or the withdrawing of a certain amount per day. Associated with that, Eurosystem Committees and HLTF-CBDC are studying the introduction of limits to individual holdings of digital euros, namely, to mitigate ML/TF risks (Uribati, 2021: 18).

In the current context, where a cautious approach should prevail, anonymity seems inacceptable for four main reasons: (1) it would be incoherent with the 2021 AML legislative package which prohibits anonymous crypto-asset wallets in the EU (above 4.3); (2) there isn't a pressure on the demand side for a new anonymous money because it was ensured that cash remains usable (above 4.1.4 and 4.2); (3) distribution of anonymous wallets only controlled by initial identity verification create bigger ML/TF risks than cash because it doesn't have the limitations on portability, allowing, without physical contacts, a massive number of operations and leaving open doors to schemes with "money mules"; (4) empirically, it isn't possible to evaluate AML/CFT tactics under a digital euro regime before it is fully implemented and crime history teaches that the public authorities can't anticipate all the potential schemes that criminals and terrorists may create in innovative money ecosystems.

Even moderated solutions with amount limitations (as anonymous pre-paid cards, token-based wallets with low payment limits or limited number of "anonymity vouchers" within permitted quantitative limits, ECB, 2019, above 4.2) pose big threats of ML/TF and can create a "black market" for these products (Chaum et al., 2021: 28; Gürtler et al. 2017: 5).

Digital identity is an emerging field in many jurisdictions (BIS, 2020: 19) with a broad range of public and private solutions for digital identification (below figure 40) and multiple

technical alternatives (e.g., public key cryptography infrastructure system or another central authentication service).

Token-based instruments aren't necessarily anonymous because the register can be controlled using cryptographic codes, the reason why it can be called "pseudo-anonymous" (Norges Bank, 2021: 26; Chaum et al. 2020: 12-24). Token-based options must be preventively "shaped to facilitate crime-fighting activities […] as determined by the regulating body", "guaranteeing traceability and the existence of a ledger (central or otherwise)" to leave "the state and various levels of law enforcement agencies with the capacity to examine granular data at leisure" (Dupuis / Gleason / Wang, 2021: 12).

On the other hand, account-based CBDCs solutions (which link identity with holdings, below 4.1.3) are compatible with data protection, for instance with the use of application programming interface (BIS 2021: 74, below figure 41).

Naturally, a hybrid model with account elements and token instruments is also a possible way of looking for an equilibrium between privacy and AML/CFT necessities without forcing a specific front-end solution as mobile application, web application or smart card (Urbinati et al., 2021: 20).

In short, since a digital euro comprises tools to identify the users, the objectives of "enable appropriate regulatory entities" to "more effectively identify suspicious outlier transactions" while providing data protection "of individuals" can "be achieved in an aggregated way, by utilizing techniques (e.g., differential privacy)" (WEF, 2021: 171) independently of the alternative ledger types used. Something different of anonymity is in certain limited wallets, cards or vouchers to adopt simplified measures preserving a minimum of AML/CFT requirements (e.g., identification procedure and traceability). Anyway, all the hypothesis (like the possibility of "stored value card like the London Oyster card" referred by Bindseil, 2020: 24) need a previous study of the global cost-benefit ratio which shall include ML/TF risks.

Identity verifications can also be important to the effectiveness of a system based on the control of the supply (Auer / Böhme, 2021: 8) and, if associated with the introduction of limits to individual holdings of digital euros eventually, it would be also relevant to mitigate risks of undesirable fallouts for the banking system (Uribati, 2021: 18).

In conclusion, considering the social, criminal policy and market risks in the EU, the maintenance of cash in the euro area, the rule of law constraints to enforcement agencies, FATF standards, legislation and treaties about AML/CFT requirements, empirically it would be imprudent admitting any type of a fully anonymous digital euro. A conclusion that must be related with a previous one: the use of PET would be indispensable to comply simultaneously with AML/CFT and data protection rules (above 4.2 and 4.4.2.1).

4.4.2.5. When compared with physical euro, a digital euro presents unique ML/TF risks. As a digital representation of a fiat currency, it doesn't fall within the scope of the current FATF definition of VA (FATF, 2021a: 10-11). Regulatory requirements are essential to the integrity of the financial system, hence the planification of a digital euro architecture must consider which entities will be subject to AML/CFT rules and its implications on the CBDC design before the digital euro is launched.

The AML/CFT law enforcement agencies and supervisors must have greater information on the digital euro transactions than the ones with physical euro, but the effectiveness level of AML/CFT will depend on digital euro's design, especially its traceability extension and the way users are identifiable.

Customers transacting with a digital euro should be at least subjected to the same CDD measures of other electronic transactions using fiat currency. The third-party providers (banks and non-bank Fintech) must be responsible for implementing the AML/CFT rules, independently of the use of account-based, token-based or hybrid solutions. PSI should remain the guardians of KYC information and the transactions associated with the relevant customer contracts and be responsible for all CDD procedures. If unusual patterns (like merchant income) are detected, the law enforcement authorities should have the possibility of obtaining and inspecting business contracts (eventually using AI technics).

By implementing privacy-by-design and privacy-by default, merchants won't learn the identity of their customers, banks will only have limited insights about their customers' activities and central banks "are blissfully divorced from detailed knowledge of citizens' activities" (Chaum et al., 2021: 25; Grothoff / Moser, 2021: 4). A digital euro that protects identity secrecy by making difficult the linking of tokens with individual identities isn't anonymous since it preserves technical solutions to establish links between a record and personal data to AML/CFT ends.

This requires technical testing and the final decision won't be made by ECB but by the political bodies of EU simultaneously responsible for the proposal and approval of a euro CBDC and AML/CFT framework (above 4.2 and 4.3).

5. Conclusions

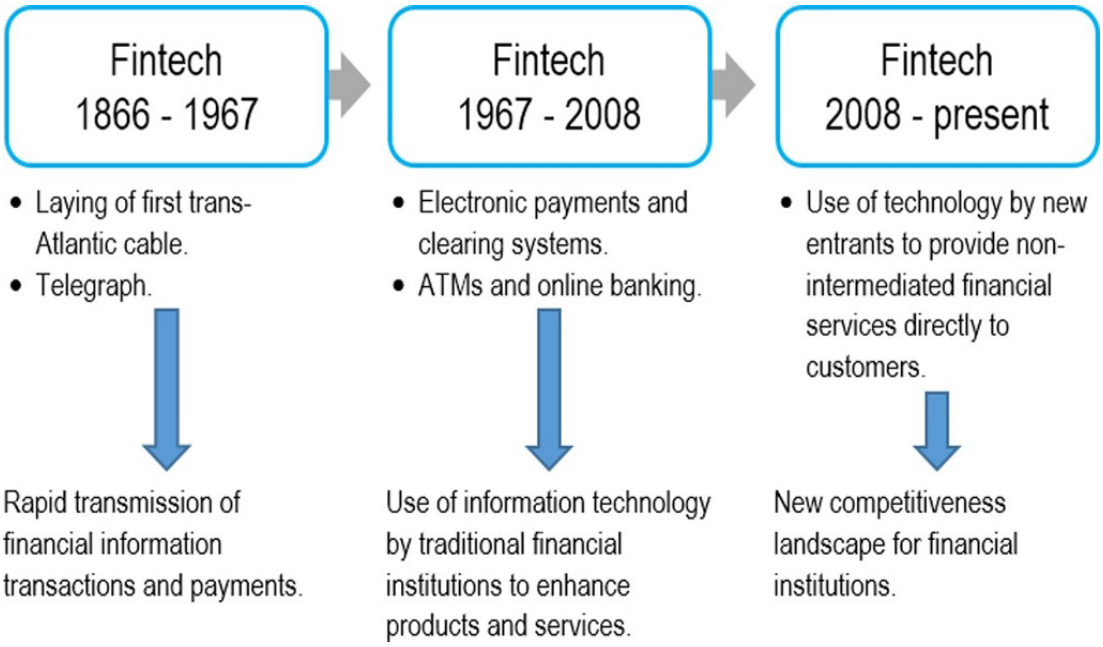
1. An eventual CBDC in the euro area should be a complement of cash mainly used as another means of payment.
2. Unlike physical money transfers, digital money transfers are always mediated by a technological mechanism, so all operations are recorded (digital footprint) and it's impossible for the payer to hand-deliver the money to the payee.
3. Following a criterium of the ledger types used, CBDCs can be classified in three models: account-based, token-based or hybrid.
4. The approach of a supposed resemblance between CBDC token-based and cash can generate misguided illusions that token-based technology, in opposition to account-based, would achieve cash-like properties.
5. The myth of a CBDC cash-like in terms of privacy blurs foundational issues on the matters of data protection and AML/CFT.
6. The status of ECB and NCBs is incompatible with their subjection to the legislation on AML/CFT applicable to the participants on digital money transfers' market.
7. Independently of the ledger types used, the architecture of a digital euro should comprise a two-tier system involving a public-private partnership, full intermediated by private sector entities, combining the credibility of a direct claim on the central bank with the specialized payment services of PSP who open accounts or wallets for the end-users.
8. In such a two-tier system, ECB and NCBs:
    a. Are not involved in KYC checks neither in other AML/CFT compliance procedures;
    b. Should coordinate their prudential supervision of PSI with the AML/CFT authorities.
9. Beyond prudential supervision, the PSI must be subjected to rigorous standards established by AML/CFT authorities to the effectiveness of regulatory requirements.
10. A digital euro can't be a tool to circumvent regulations on financial assets and must be coherently integrated with the policies of the AML 2021 EC Strategy, namely the prohibition of anonymous crypto-asset wallets in the EU.
11. A digital euro presenting a combination of anonymity, portability and mass-adoption would pose an unacceptable danger because of its huge potential for ML/TF purposes, so it would be imprudent to admit any type of fully anonymous digital euro.

12. In a first stage, digital euro should be confined to domestic transfers between residents, but with a flexible design prepared for the possibility of a safe and regulated evolution to cross-border transfers and FX (which is particularly dependent of agreements at an international level).
13. The payment ecosystem of a euro CBDC should comply with requirements about the processing of personal data, such as specific data retention periods or reporting obligations, applicable to all other kinds of digital money in euro area.
14. The use of PET is indispensable for a digital euro to comply simultaneously with AML/CFT and data protection rules.
15. A digital euro must create new opportunities for financial intermediation with its effective regulation on data protection and AML/CFT.
16. The PSI need to proceed its investment in putting in place AI-based tools to improve their CDD processes.
17. The final word about the project of a digital euro will be held by the political bodies of EU simultaneously responsible for the AML/CFT policies which should be considered for that decision.

Appendix

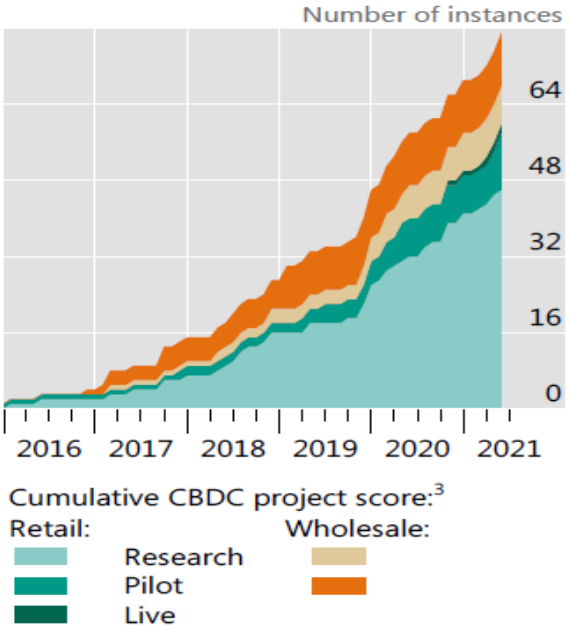
Appendix 1: Figures

Figure 1: Three phases of Fintech



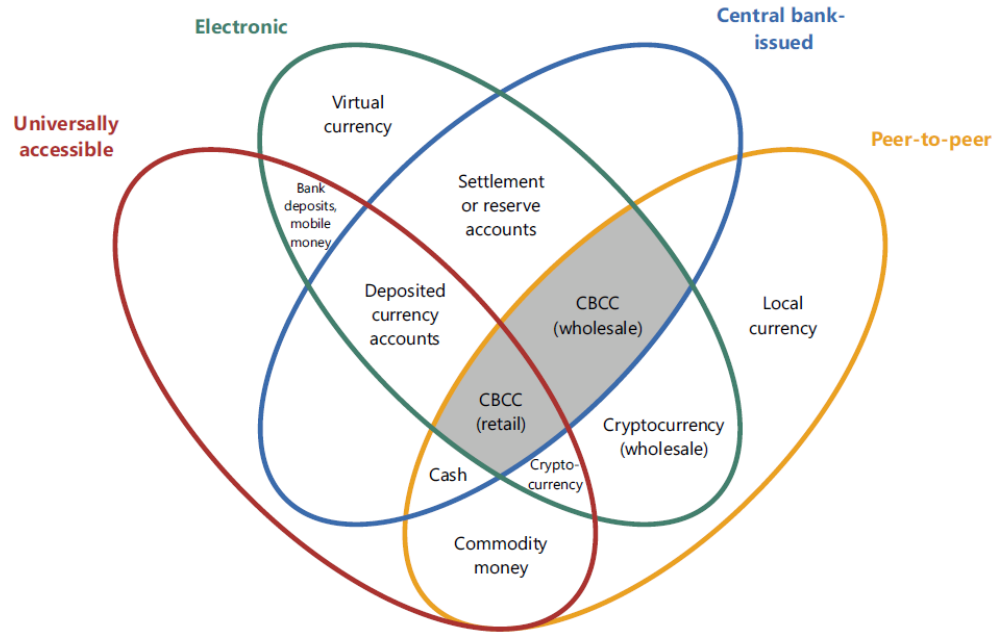
Source: Thakor (2019), p. 2 (based on Bates, 2017, p. 5)

Figure 2: Research and development effort on CBDCs



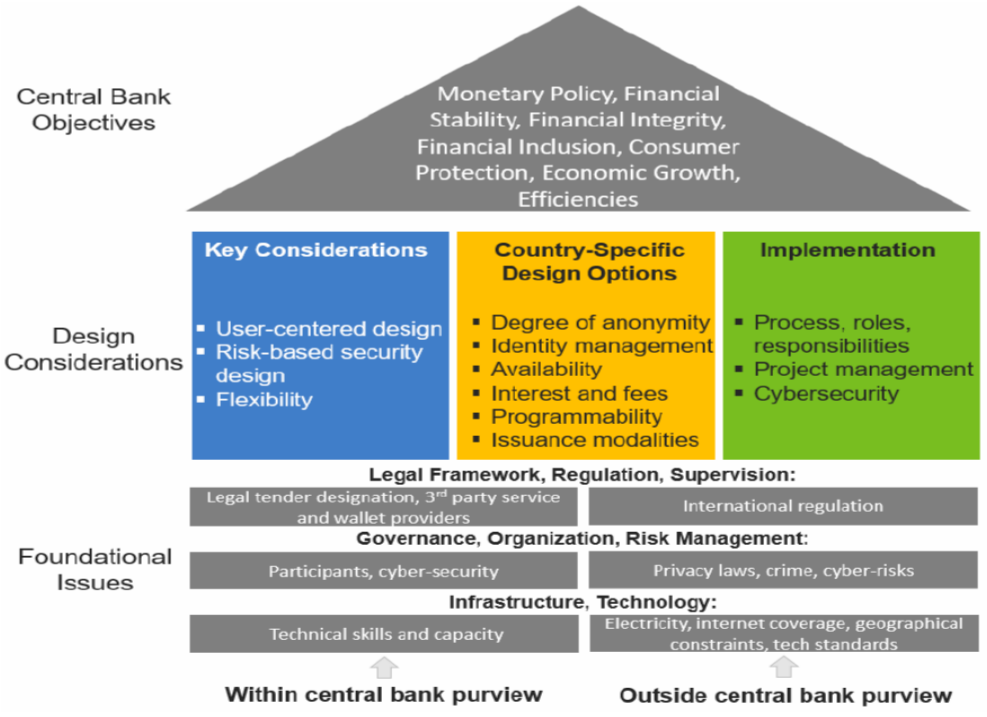
Source: BIS (2021), p. 67

Figure 3: A taxonomy of money



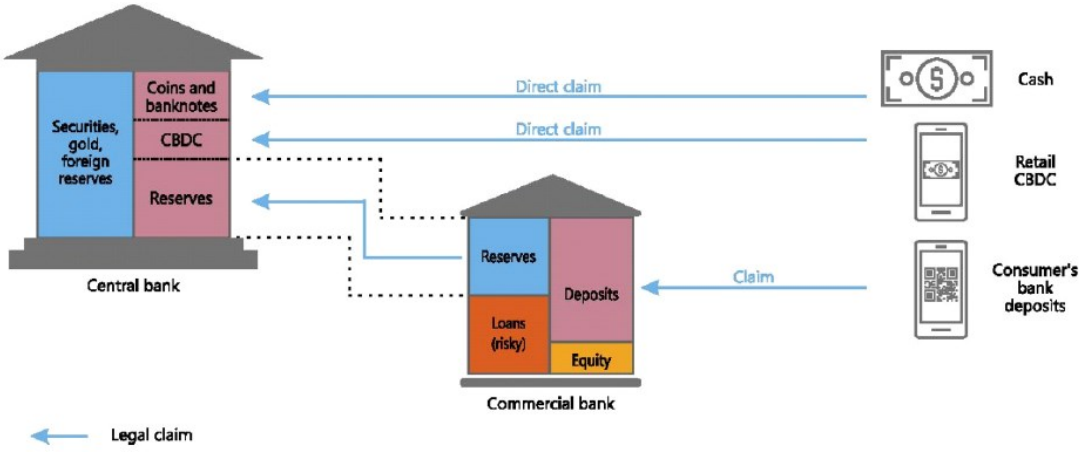
Source: Bech / Garratt (2017), p. 60

Figure 4: Overview on central banks reasons about exploring retail CBDC, policy and design considerations, legal, governance and regulatory perspectives and risk considerations



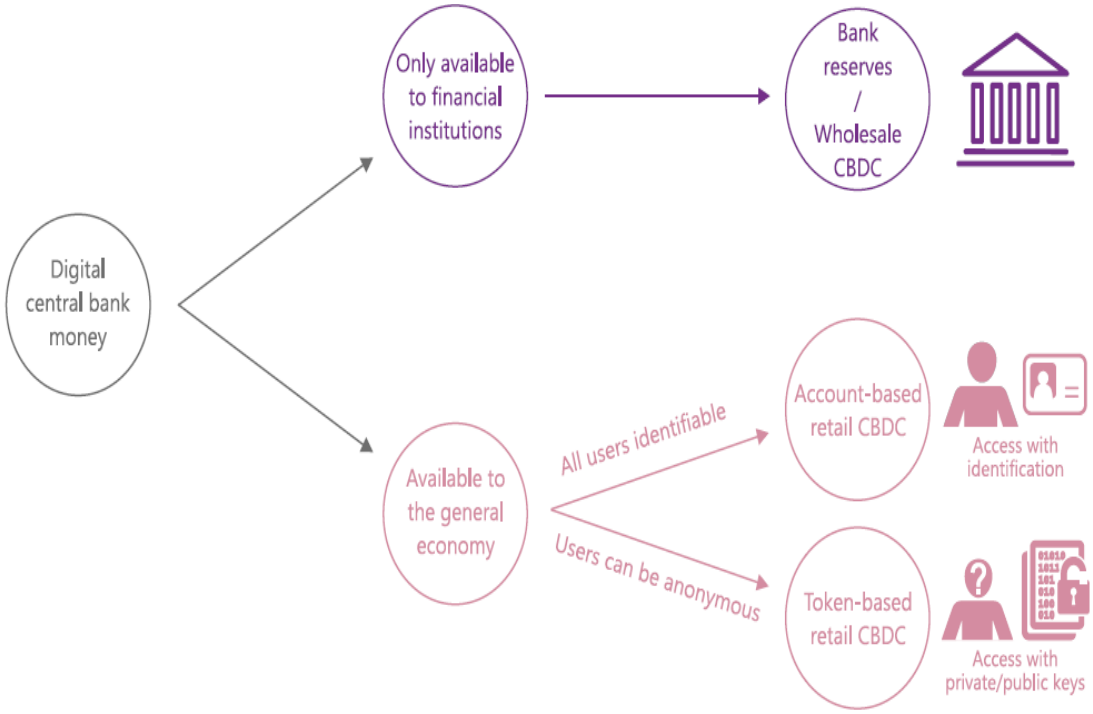
Source: Kiff, J. et al. (2020), p. 19

Figure 5: Legal claim of cash, electronic payment instruments and retail CBDC



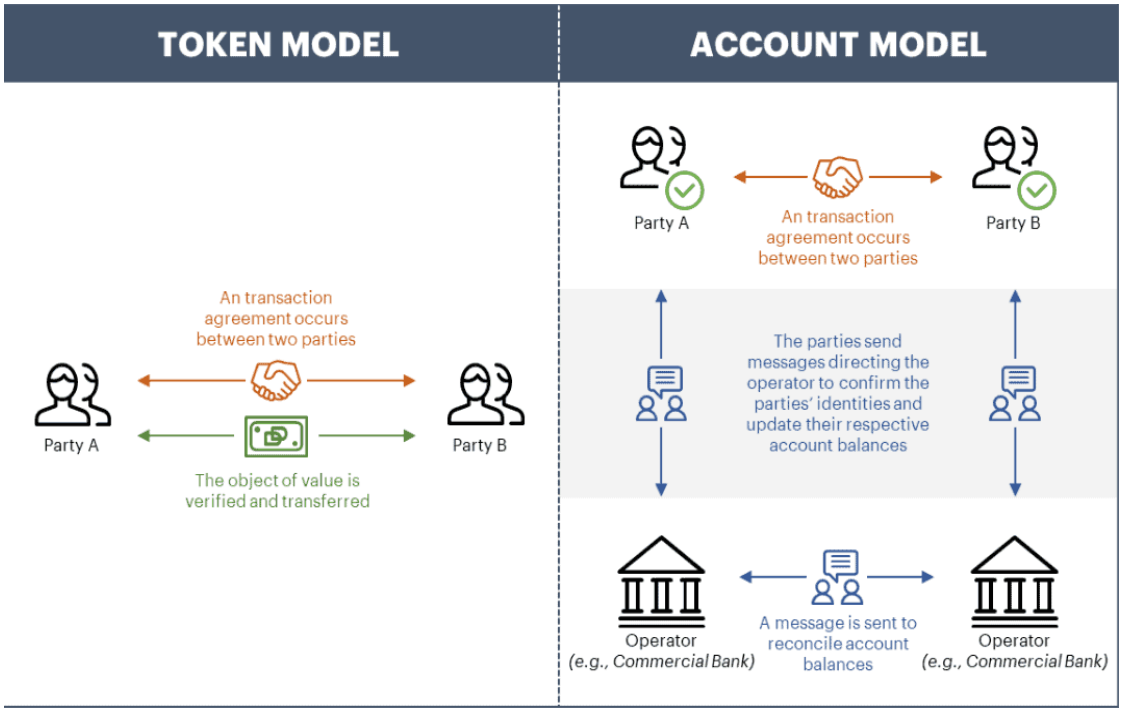
Source: Auer / Böhme (2021), p. 6

Figure 6: Forms of CBDC



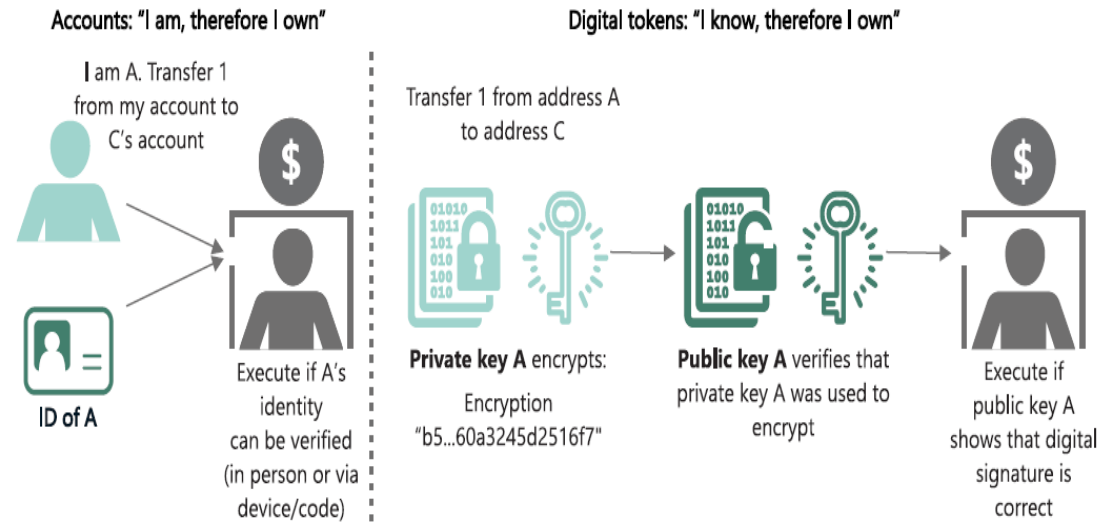
Source: BIS (2021), p. 74

Figure 7: Token *versus* account model using as criterium the identification of the object being transferred *versus* the identification of the individual whose account is being debited



Source: Giancarlo, C. H. *et al.* (2020), p. 17

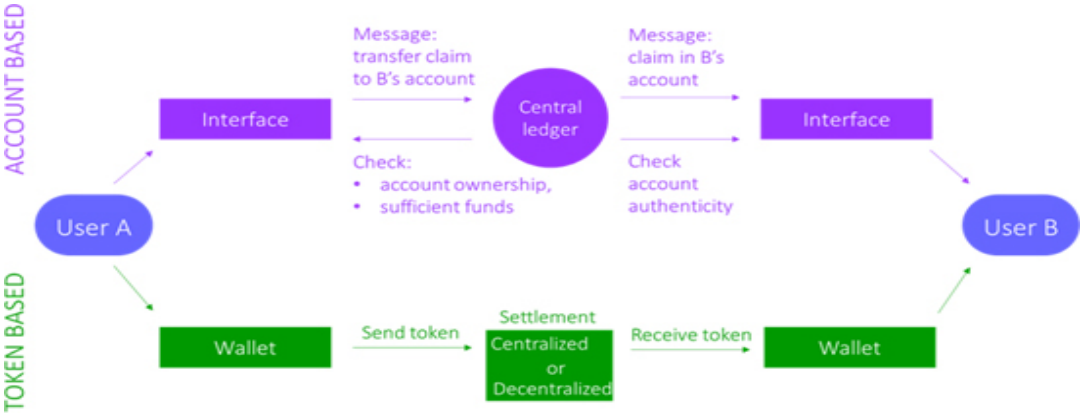
Figure 8: Account-based access compared with token-based access



In an account-based CBDC (left-hand side), ownership is tied to an identity, and transactions are authorised via identification. In a CBDC based on digital tokens (right-hand side), claims are honoured based solely on demonstrated knowledge, such as a digital signature.

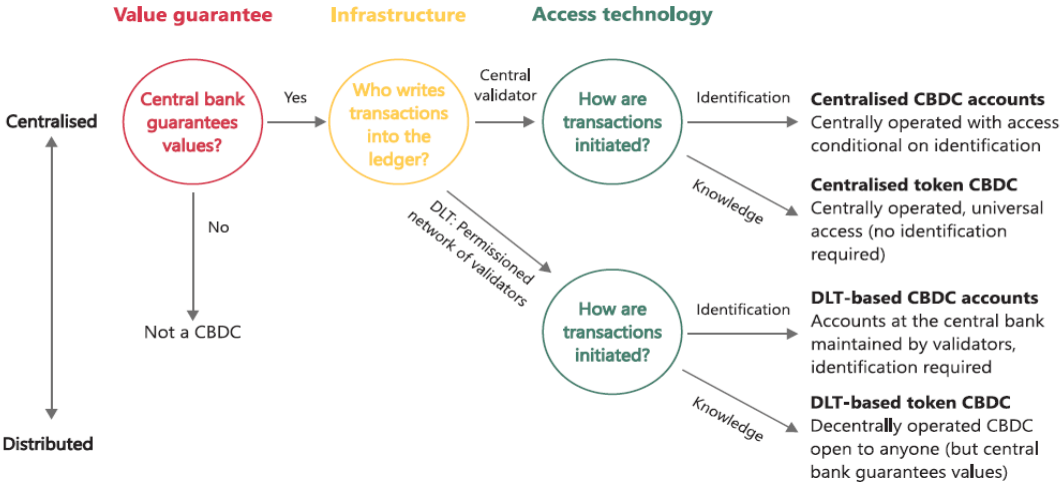
Source: Auer, R / Boehme, R. (2020), p. 94

Figure 9: Centralized account-based and token-based CBDC: basic mechanics



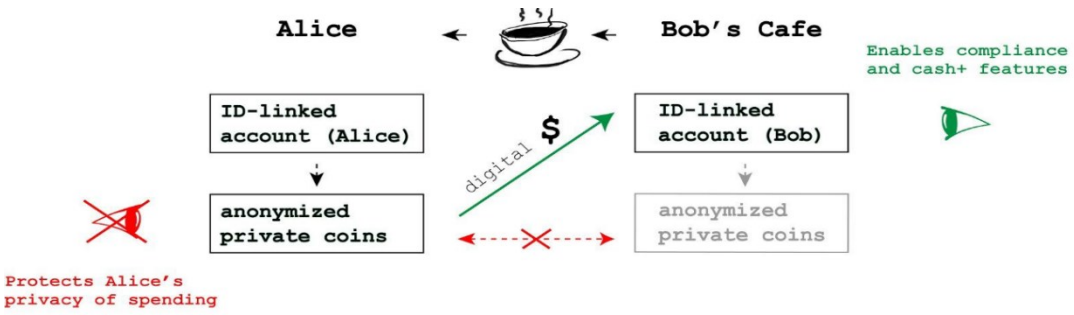
Source: IMF staff in Mancini-Grifolli et al. (2018), p. 8

Figure 10: Elements of decentralisation on account-based and token-based CBDC



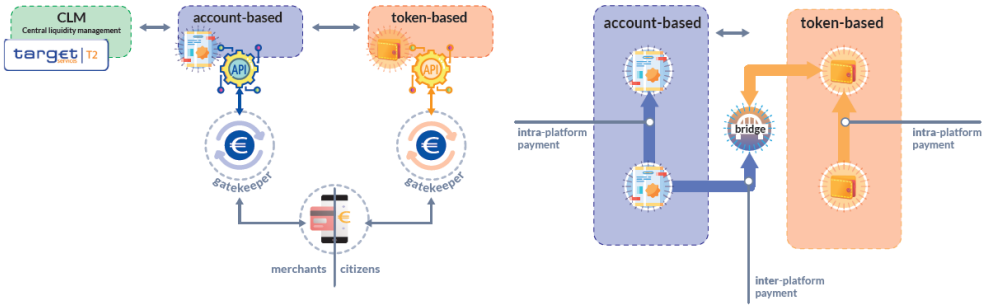
Source: Auer, R / Boehme, R. (2020), p. 92

Figure 11: Hybrid CBDC



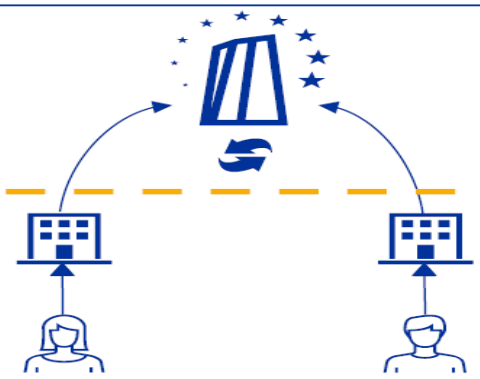
Source: Tinn / Dubach (2021), p. 2

Figure 12: Graphical representation of an integrated model



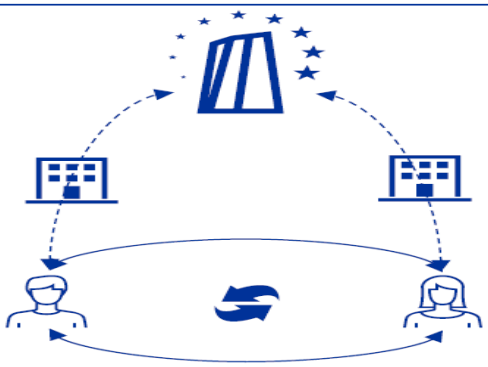
Source: Urbinati, et al. (2021), p. 19

Figure 13: Centralised infrastructure with intermediated access by end-users to central bank accounts



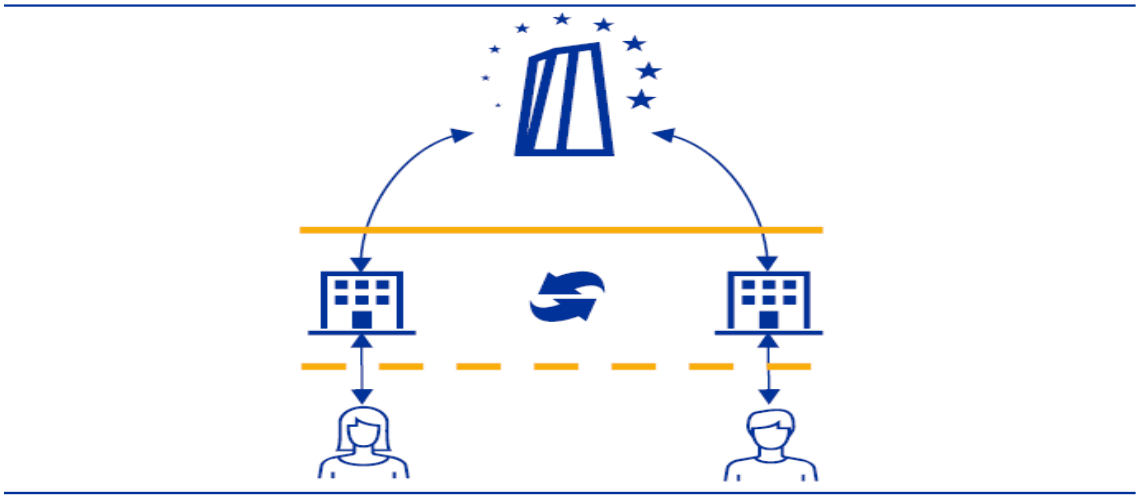
Source: ECB (2020), p. 39

Figure 14: Decentralised infrastructure with direct end-user access to a bearer digital euro



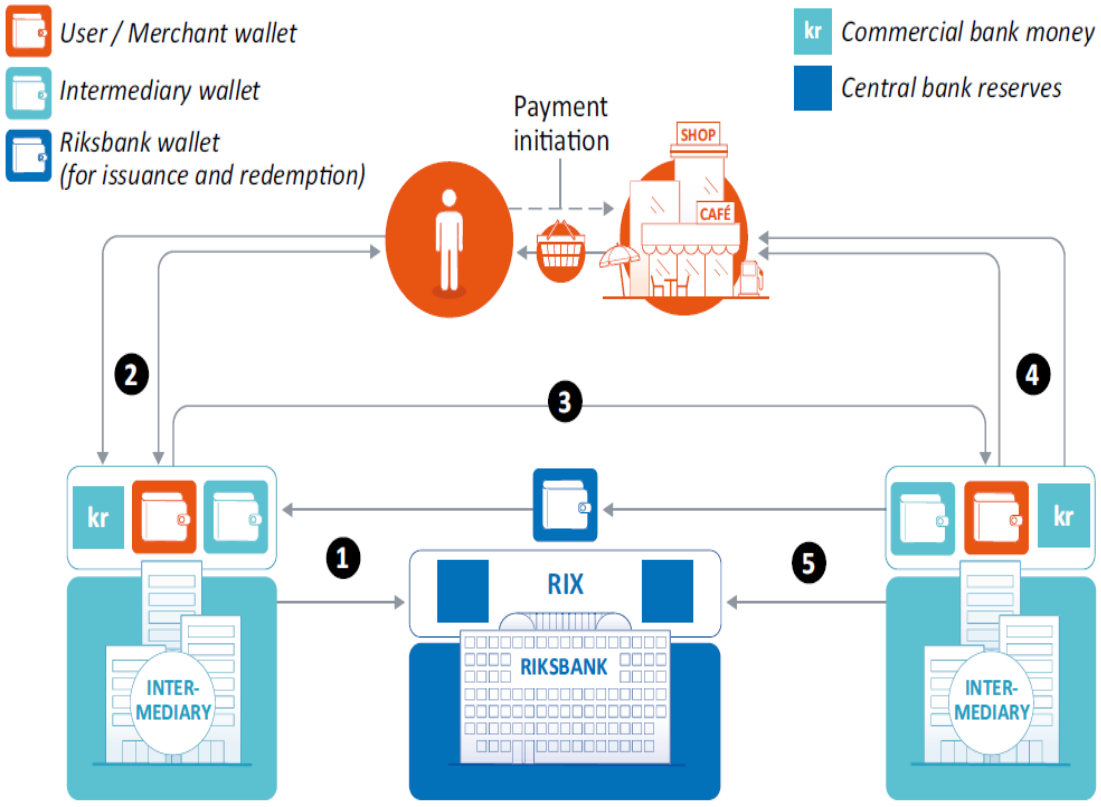
Source: ECB (2020), p. 40

Figure 15: Decentralised account-based and hybrid bearer infrastructure



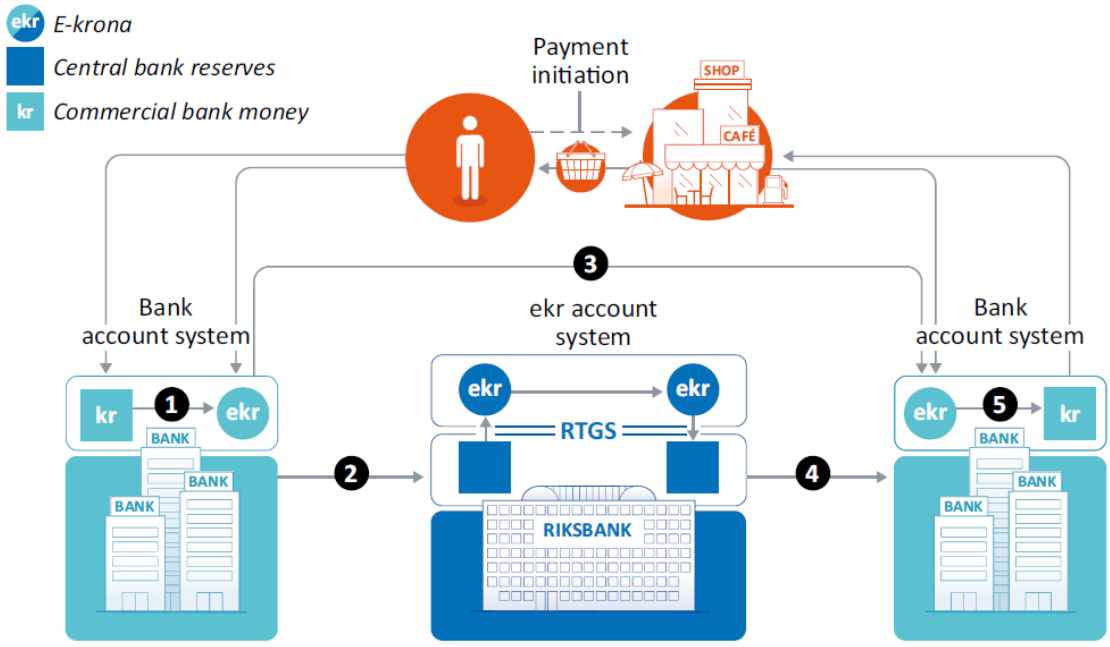
Source: ECB (2020), p. 41

Figure 16: Flow of e-kronor in a decentralized ledger system



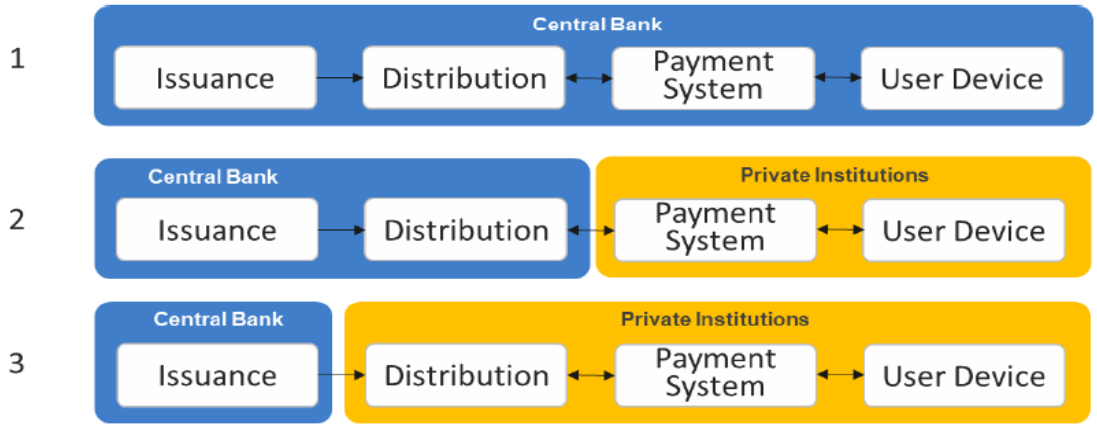
Source: Armelius (2020), p. 88

Figure 17: Synthetic e-krona



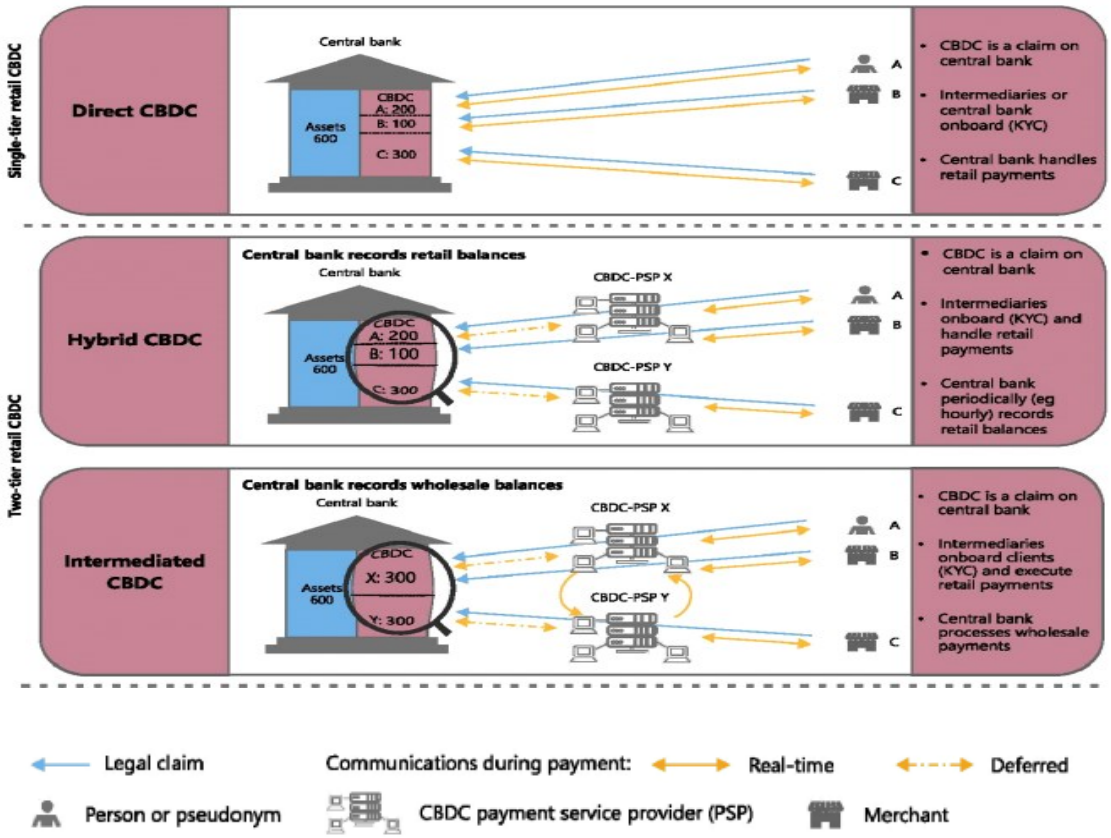
Source: Armelius (2020), p. 88

Figure 18: Different degrees of responsibility that can be adopted by Central Banks



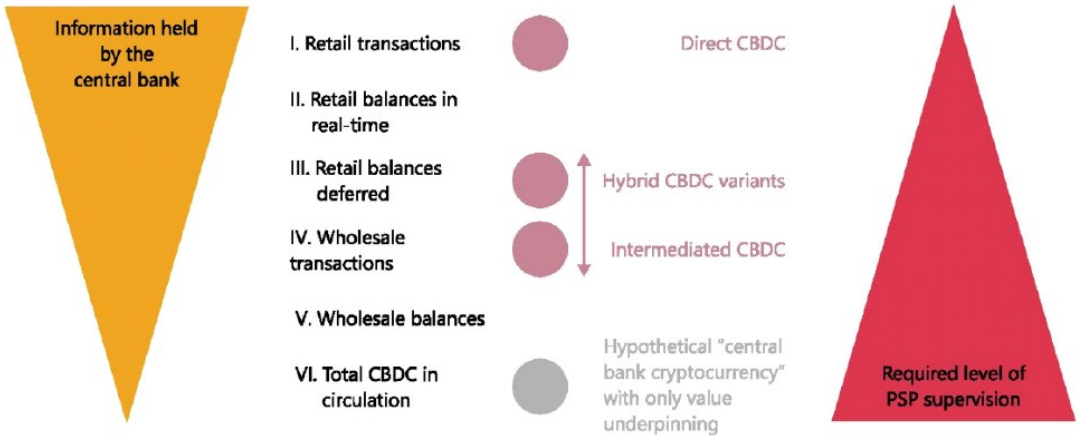
Source: Kiff, J. et al. (2020)

Figure 19: Potential retail CBDC architectures which differ in terms of the structure of legal claims and the record kept by the central bank (the division of tasks between central bank and intermediaries)



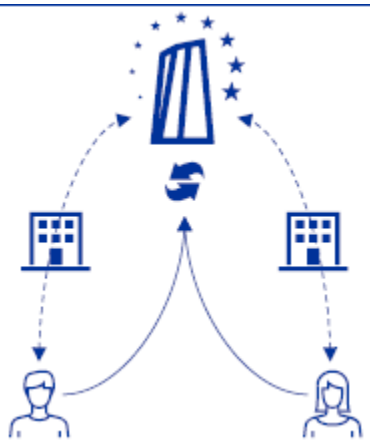
Source: Auer / Böhme (2021), p. 10 (adaptation of the figure in Auer / Böhme (2020), p. 89)

Figure 20: A new trade-off for the central bank of the future



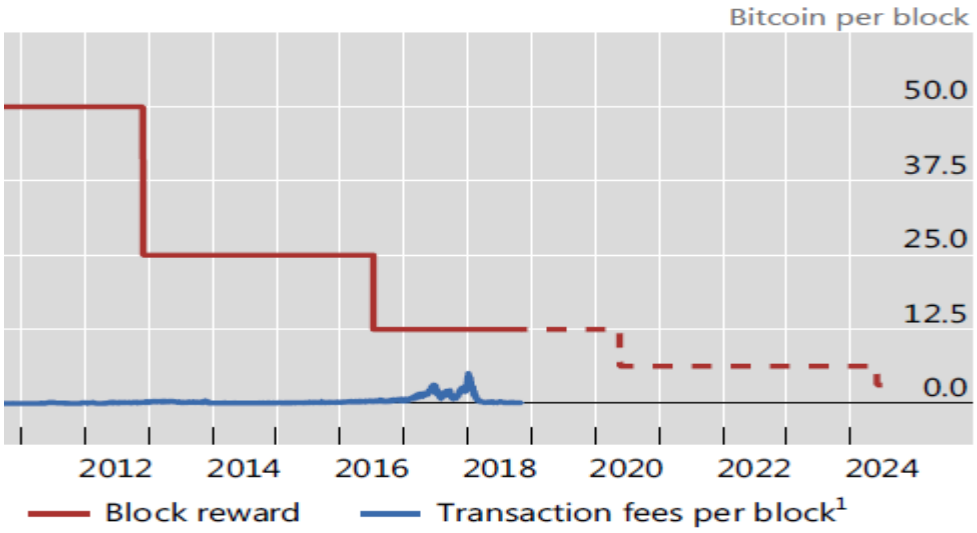
Source: Auer / Böhme (2021), p. 13

Figure 21: Centralised infrastructure with direct access by end-users to central bank accounts



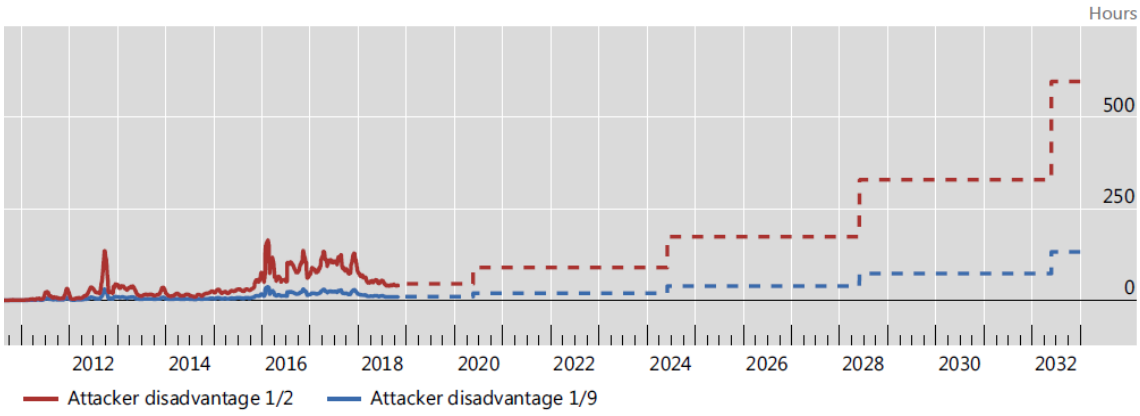
Source: ECB (2020), p. 38

Figure 22: Miners' income is made up of block rewards and transaction fees



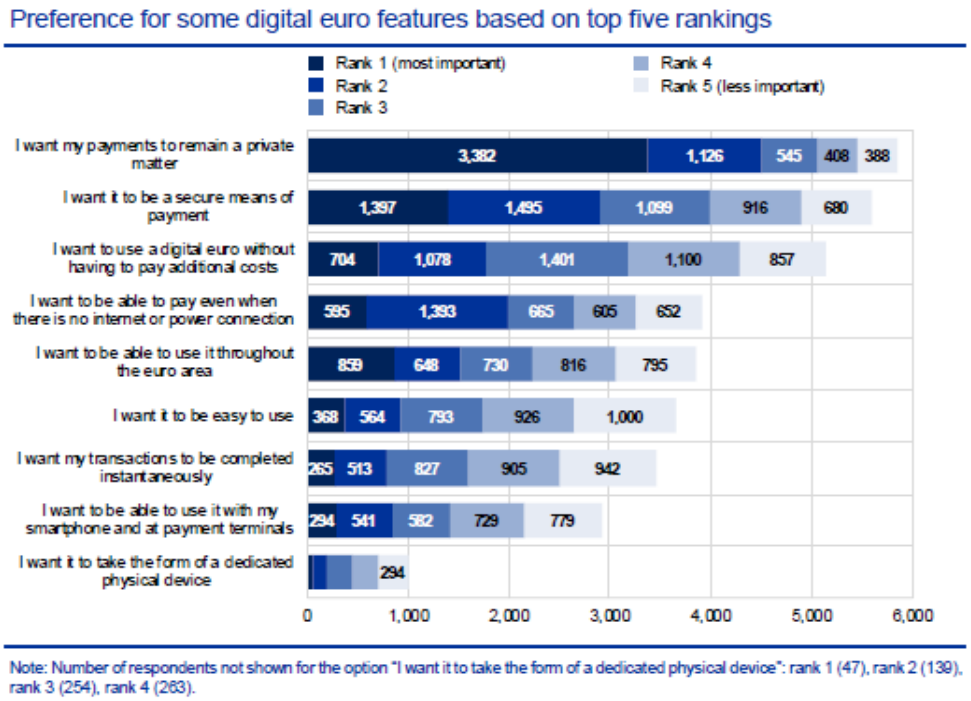
Source: Auer (2019), p. 9

Figure 23: Longer waiting times result when Bitcoin block rewards decline



Source: Auer (2019), p. 19

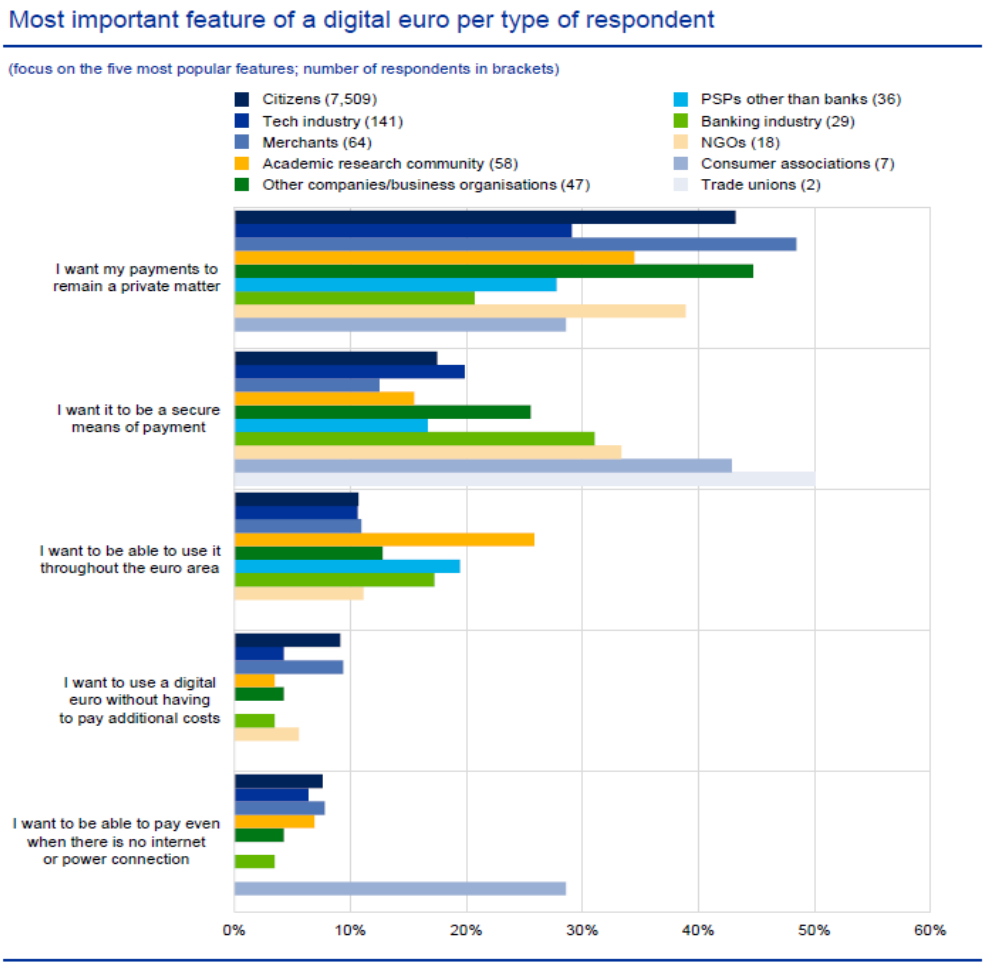
Figure 24: Preference for some digital euro feature based on top five rankings



Note: Number of respondents not shown for the option "I want it to take the form of a dedicated physical device": rank 1 (47), rank 2 (139), rank 3 (254), rank 4 (263).

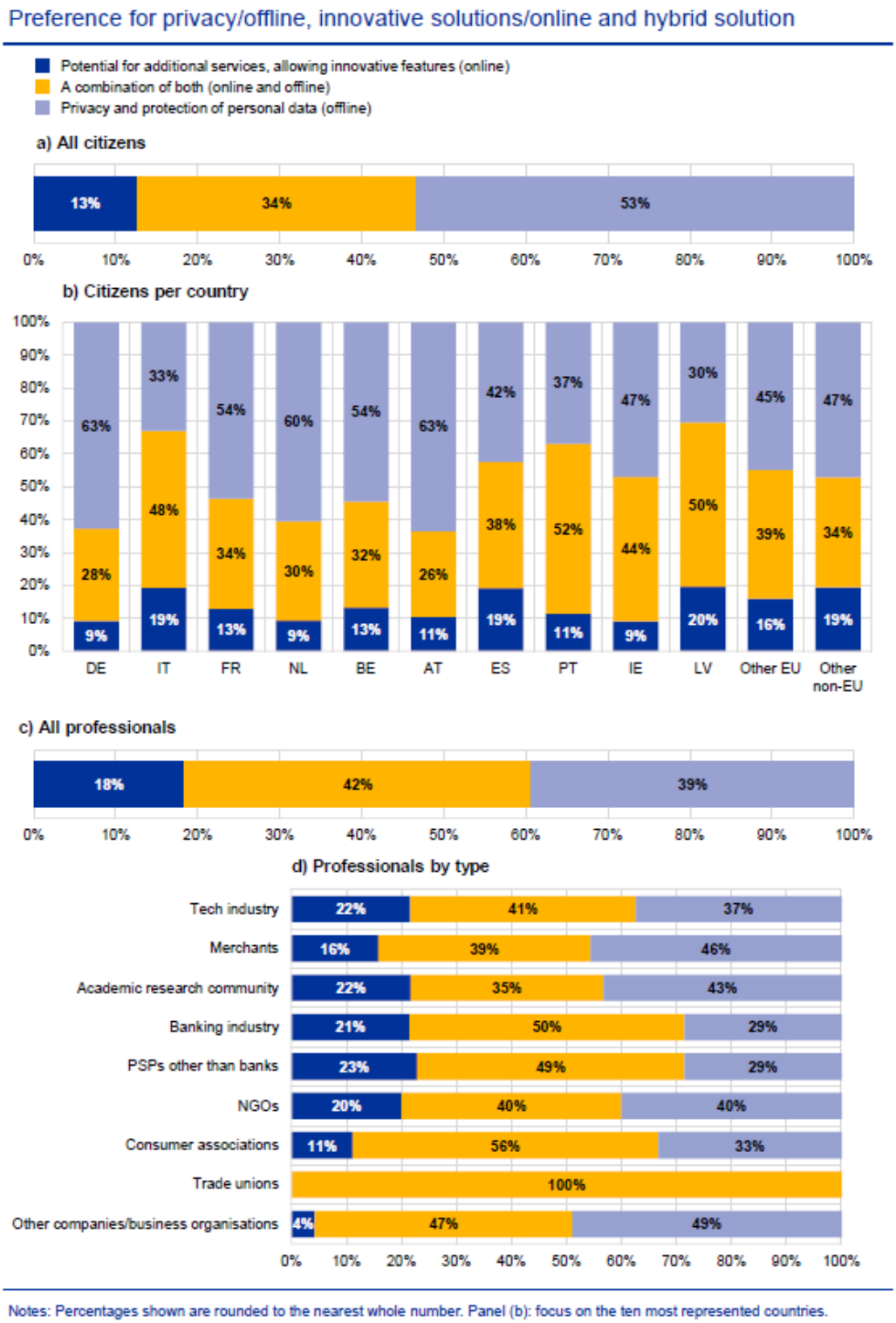
Source: ECB (2021a)

Figure 25: Most important feature of a digital euro per type of respondent



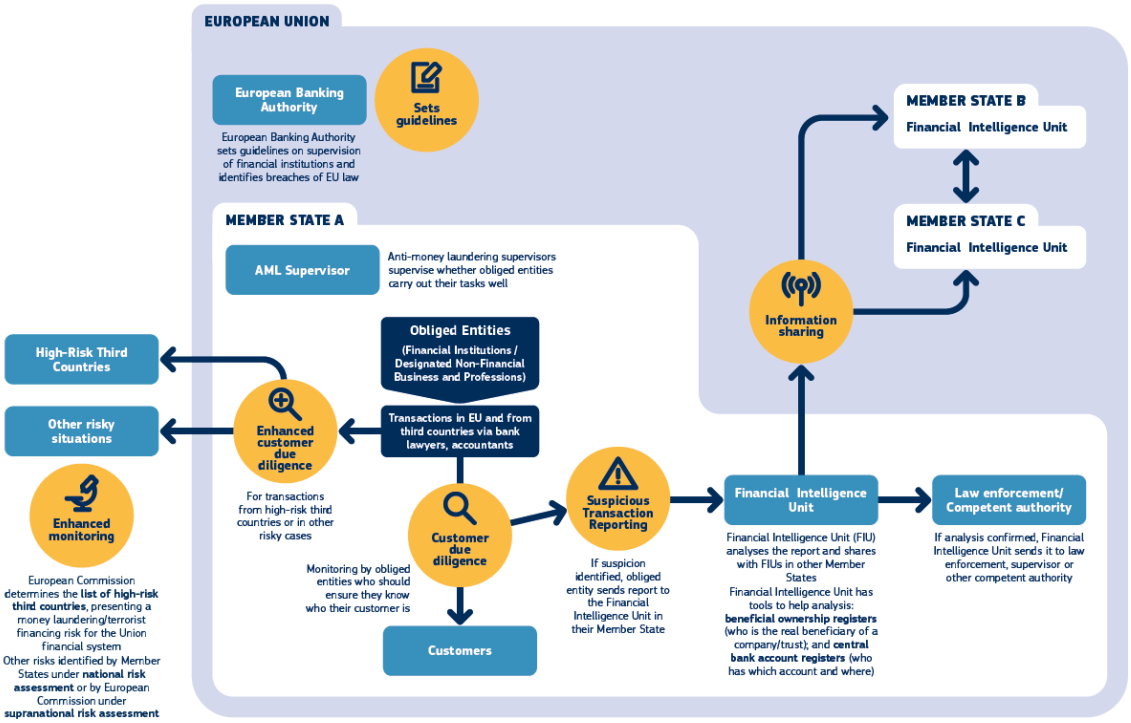
Source: ECB (2021a)

Figure 26: Preference for privacy/offline, innovative solutions/online and hybrid solution



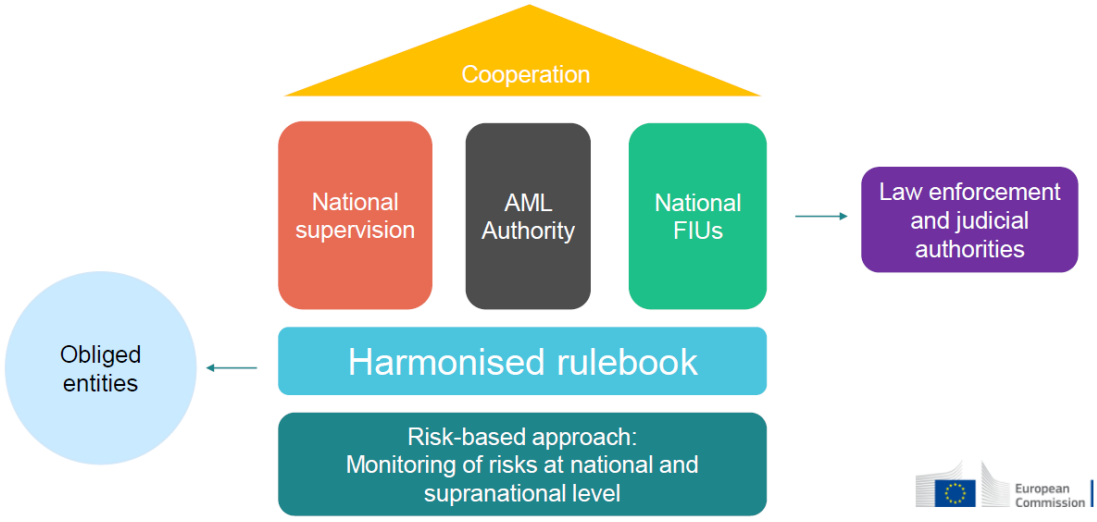
Source: ECB (2021a)

Figure 27: How does work in practice preventing money laundering and terrorist financing across the EU



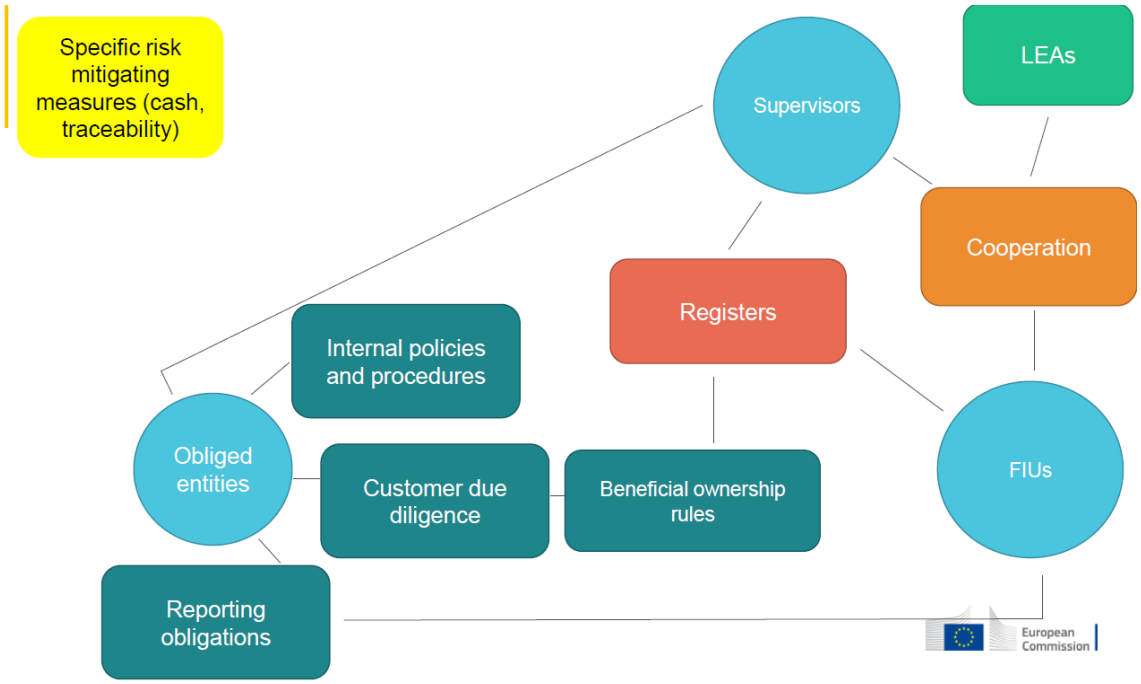
Source: https://ec.europa.eu/info/sites/default/files/diagram_aml_2018.07_ok.pdf

Figure 28: The future preventive framework in EU AML/CFT



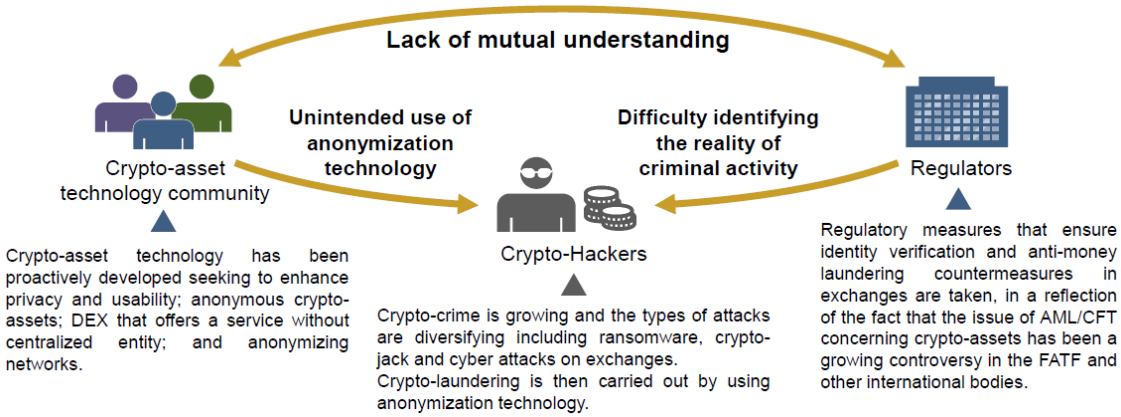
Source: Bacci (2021a), p. 15

Figure 29: The future preventive framework AML/CFT interconnexions



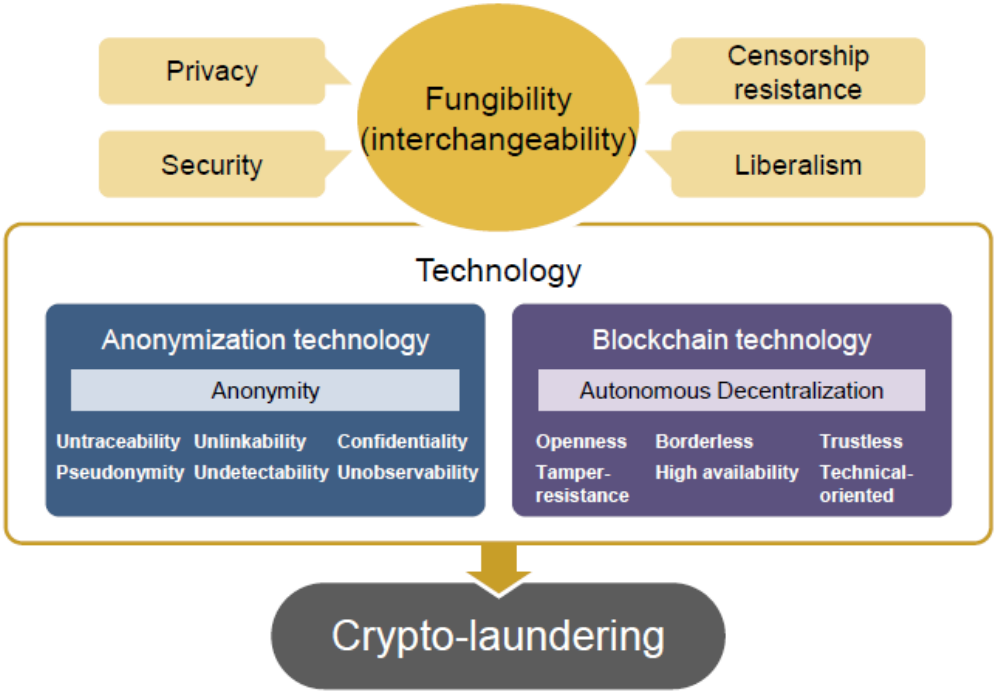
Source: Bacci (2021a), p16

Figure 30: Major stakeholders surrounding the current status of AML/CFT concerning crypto-assets



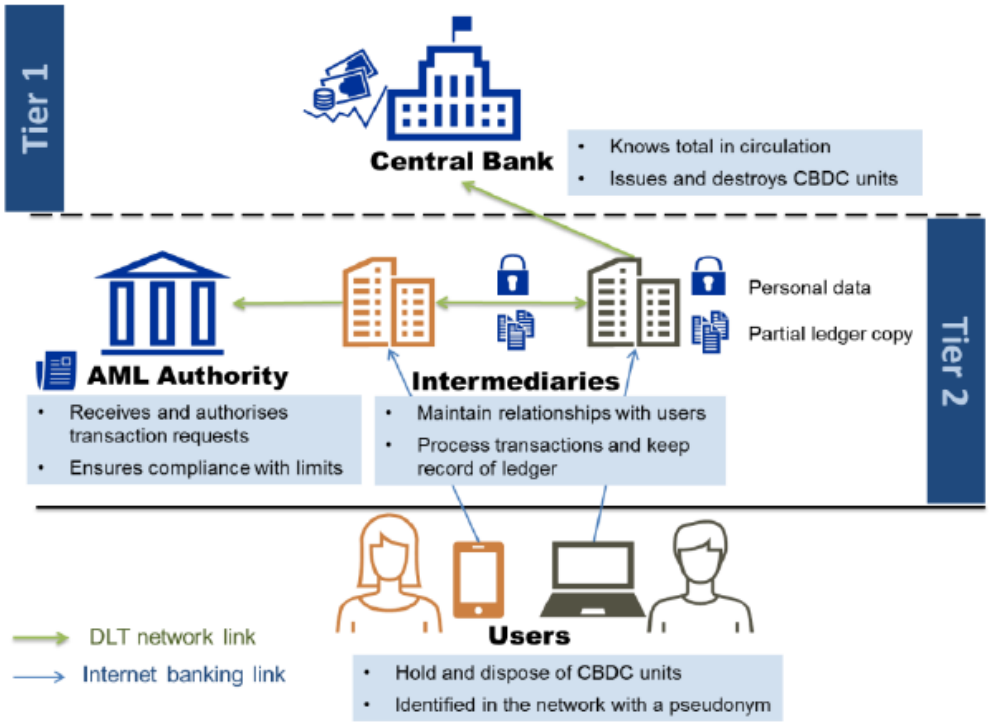
Source: Mitsubishi Research Institute, Inc. (2019)

Figure 31: Relationship between fungibility of crypto-assets and crypto-laundering



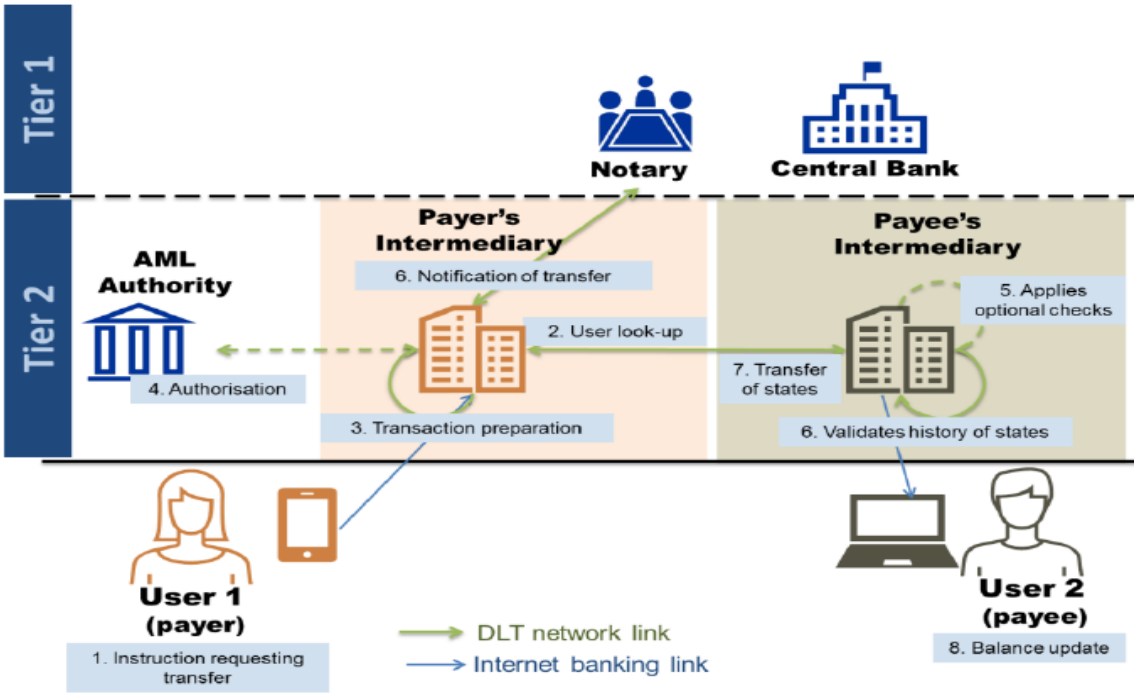
Source: Mitsubishi Research Institute, Inc. (2019)

Figure 32: Two tier model of Retail CBDC and relationship between entities



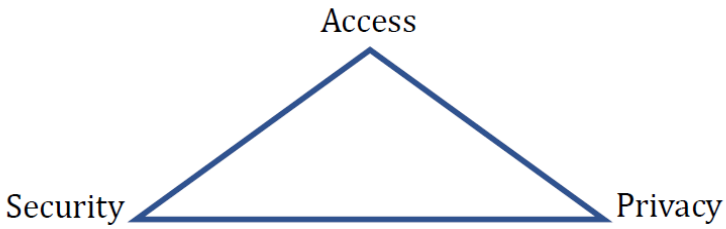
Source: ECB (2019), p. 5

Figure 33: Transfer with AML checks



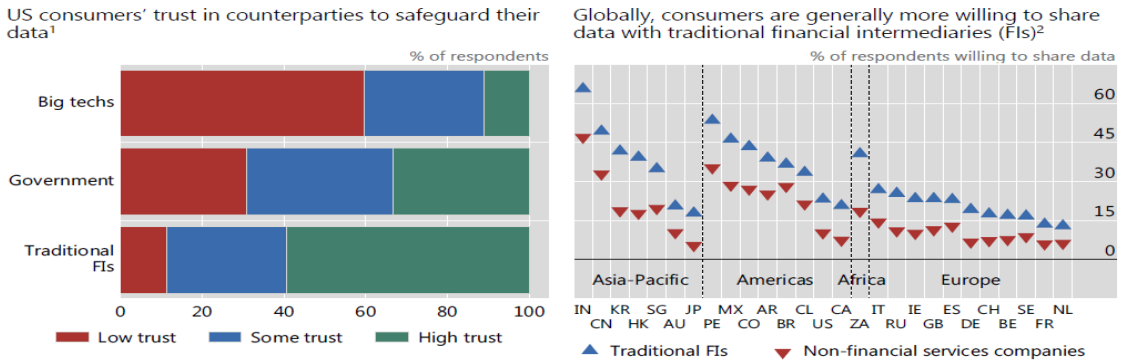
Source: ECB (2019), p. 8

Figure 34: Three-way trade-off between access, privacy and security



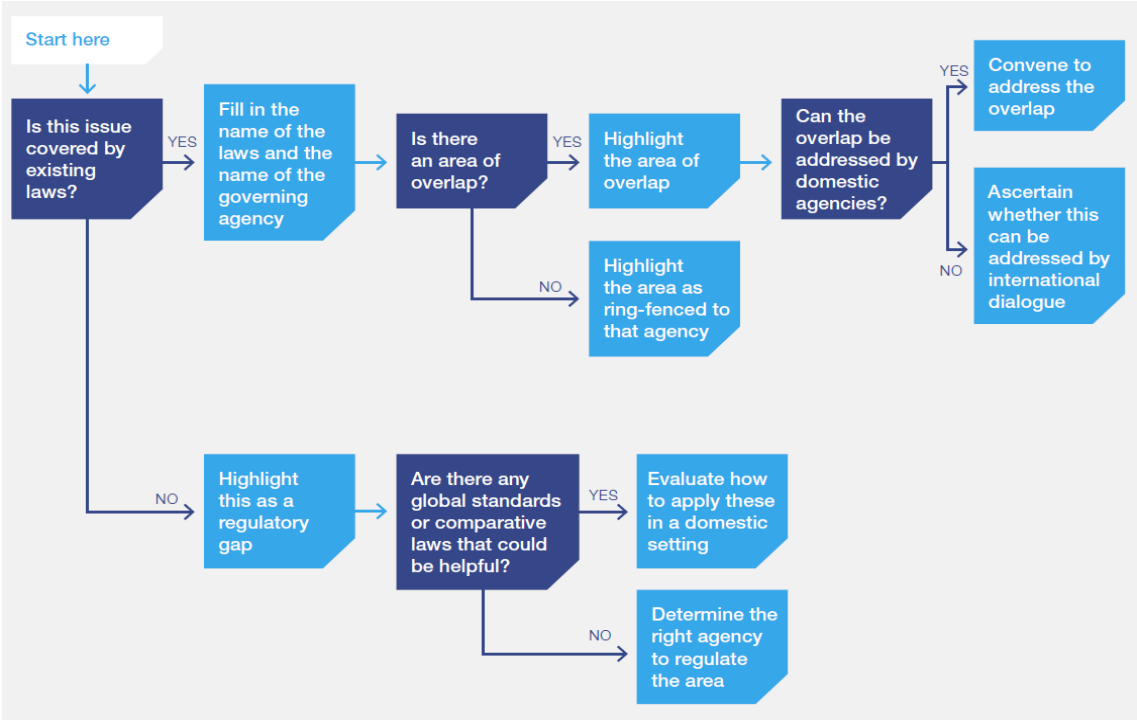
Source: Kahn / Rivadeneyra / Wong (2018), p. 10

Figure 35: Consumers' trust in big techs, government and traditional FI to safeguard their data



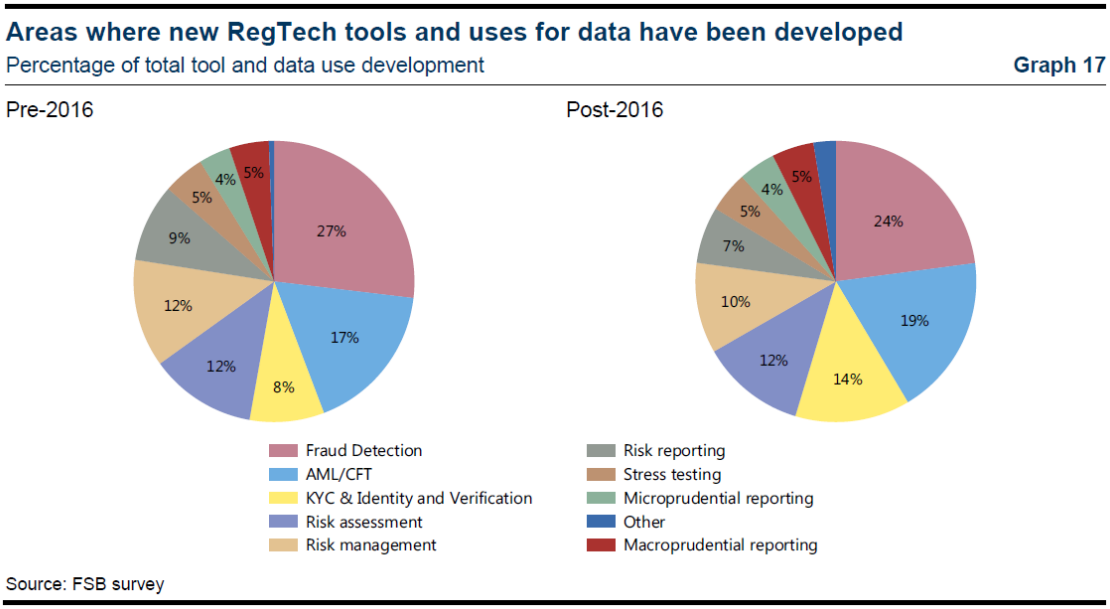
Source: Carstens et al. (2021), p. 6

Figure 36: Regulatory and standards mapping: Decision tree



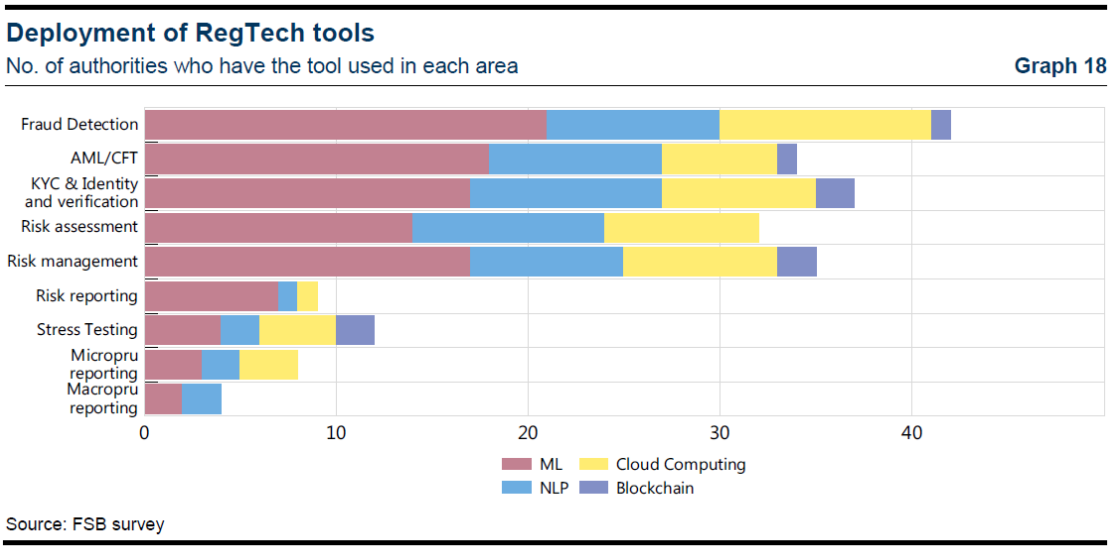
Source: World Economic Forum (2021), p. 60

Figure 37: Areas where new RegTech tools and uses for data have been developed



Source: Financial Stability Board (2020), p. 30

Figure 38: Deployment of RegTech tools



Source: Financial Stability Board. (2020), p. 31

Figure 39: Explainable AI, Human-in-the-loop technology, and NLP will be critical elements of future AML systems, addressing a number of challenges arising from ever-changing policies

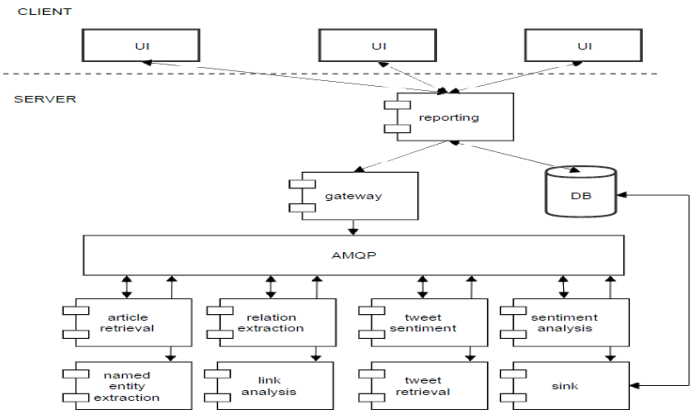
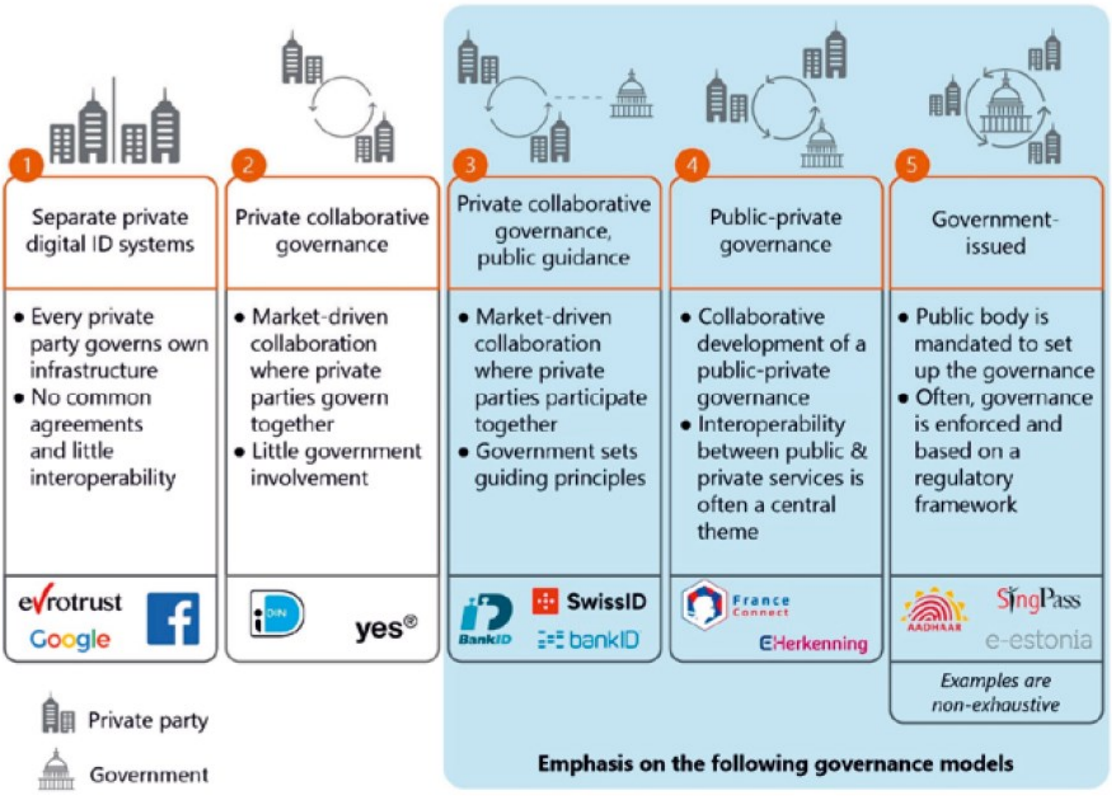


Figure 2: *Explainable AI, Human-in-the-loop technology, and NLP will be critical elements of future AML systems, addressing a number of challenges arising from ever-changing policies.*

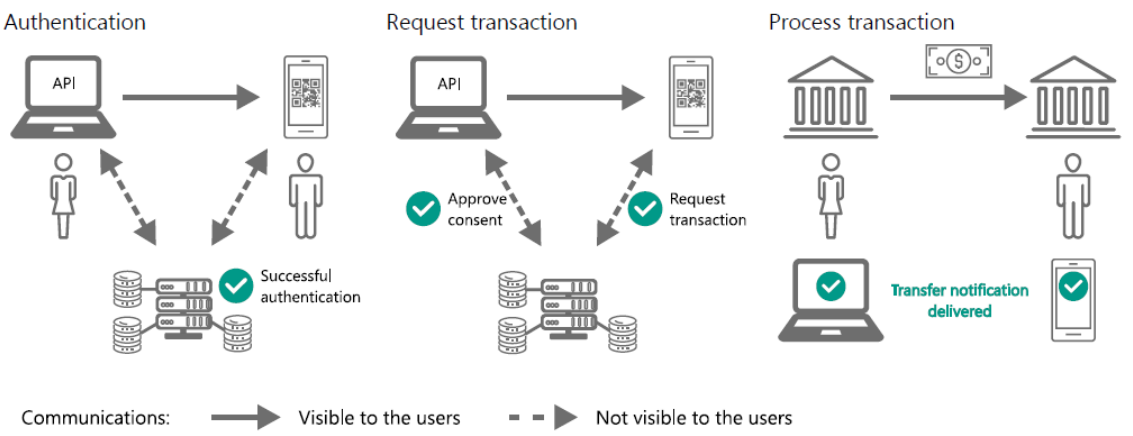
Source: Han / Huang / Liu / Towey (2020)

Figure 40: A broad range of public and private solutions for digital identification



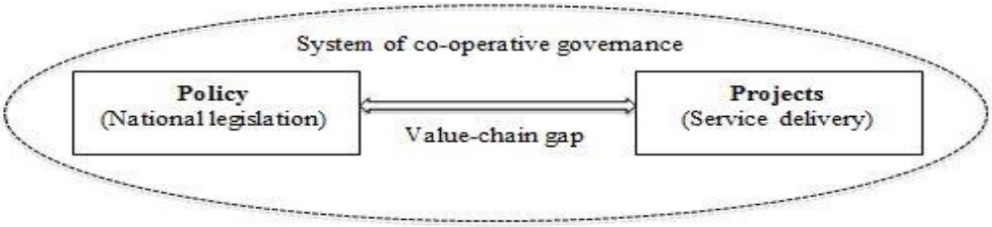
Source: BIS (2021), p. 83

Figure 41: Using an application programming interface for a transaction



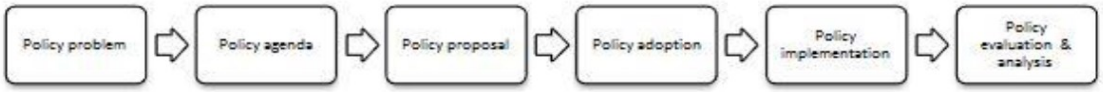
Source: BIS (2021), p. 74

Figure 42: Conceptual map for value-chain analyses



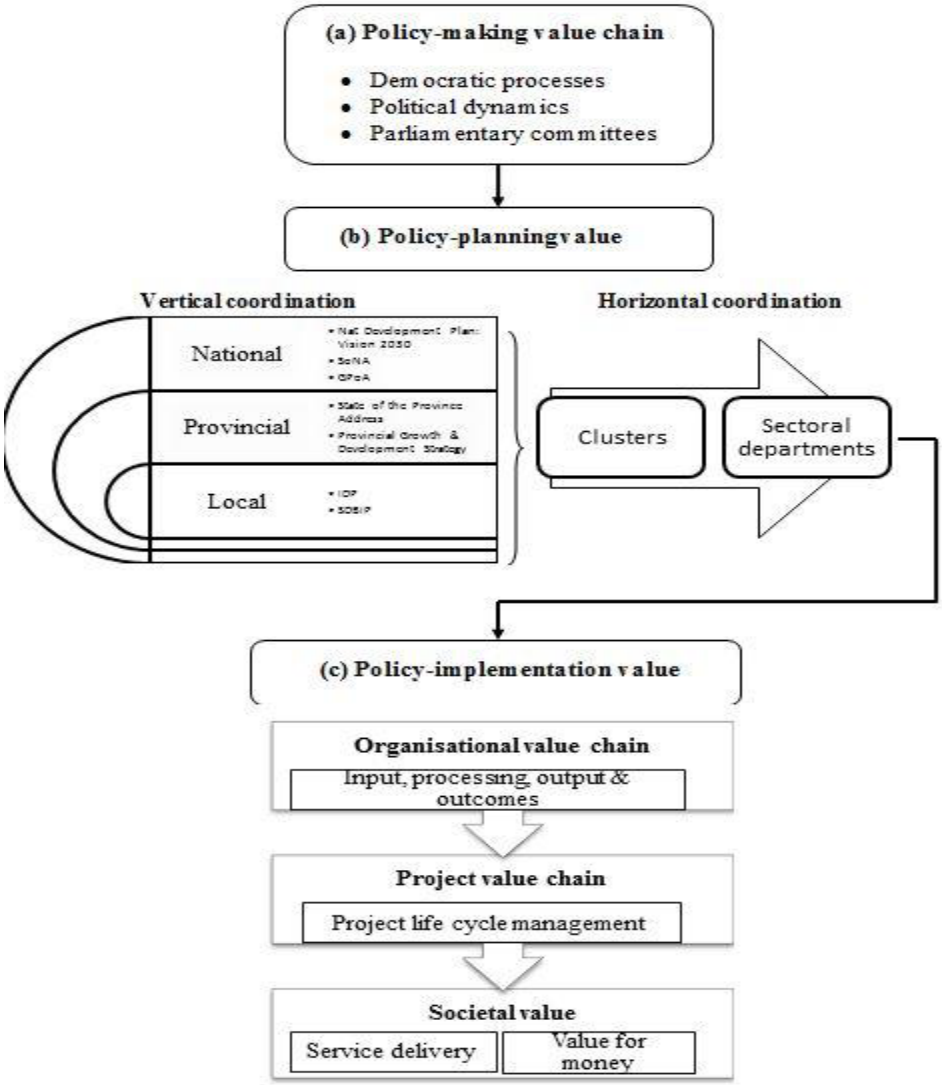
Source: Walt, 2016, p. 2

Figure 43: Policy-making process's value chain



Source: Walt, 2016, p. 7

Figure 44: Public Service Value-chain Network Model



Source: Walt, 2016, p. 17

Appendix 2: Tables

Table 1: CBDC Legal Framework Analysis

Question	Examples	Comments
What are the relevant **domestic laws** and regulations?	Constitution, Central Bank Law (and central bank by-laws, and/or regulations), Banking Law, Criminal Law, Budget Law, Tax Law, financial integrity regulation, etc.	Ensure a complete overview of relevant legislation, including possible pending amendments.
What are specific **legal requirements** and limitations to CBDC?	Monetary policy instruments, payment system aspects, cash currency management requirements, financial supervision instruments, accounting requirements, government consultation requirements, as well as internal organization requirements (such as procurement, data security, external audit).	Ensure a complete overview of specific legal requirements and limitations, their interactions, as well as possible judicial interpretations.
What are **potential needs** to be captured in legal considerations?	Input/comments from government and public sector at large (finance, economics, telecom, taxation, police, financial intelligence unit, as well as the attorney-general), industry consultation: commercial sector (bank, insurance, pension fund, money exchangers' representatives, chamber of commerce, telco operators, other fintech companies).	Ensure a near-to complete overview of input and views from relevant stakeholders regarding legal considerations to a possible CBDC.
What could be the limitations **of CBDC** within the current legal framework?	Provide a gap analysis of the scope, nature and intent of CBDC as is possible within the existing legal framework, and identify, if any, what kind of legal changes are necessary.	Conduct a feasibility analysis for issuing CBDC within the current legal framework.

Source: Kiff, John et al. (2020), p. 39

Table 2: CBDC Central Bank Internal Organization Analysis

Question	Examples	Comments
What central bank **objectives** and/or functions will the CBDC serve?	For instance, payment system stability, price stability, financial stability (macro prudential oversight, micro prudential supervision, ELA/LOLR, resolution), financial integrity, financial inclusion, consumer protection, economic growth. Possible links / interaction with the central bank's strategy plan.	CBDC can serve multiple central bank objectives. However, like existing central bank instruments, the central bank needs to be aware of and balance potential conflicts between objectives and therefore the use of CBDC.
What are the **technical requirements** for CBDC?	For instance, a gap analysis of existing infrastructural and technological requirements for and limitations to setting-up and issuing CBDC. See previous subsection on technological infrastructure, and cyber-security.	Identified technological limitations should be assessed from a risk perspective and a financial perspective (see next point), to ensure a realistic overview of what CBDC possibilities the central bank could explore.
What are the **internal organization requirements**?	For instance, building up of expertise and training of staff, risk management (third-party involvement / procurement and outsourcing risk, contractual arrangements, cyber security, and other operational, legal and reputational risks for the central bank), budget requirements and restrictions, data collection and data management requirements.	A complete overview of internal organization requirements (which could also be in part based on internal and external audit findings, and internal and external organization assessments) would help to identify the relevant contextual issues for setting-up and issuing CBDC.
How will **transparency and accountability** over the CBDC be shaped?	For instance, internal audit findings, accounting mechanisms, and internal and external communication.	Transparency by the central bank on CBDC developments will allow for proper accountability to its stakeholders (parliament / society), which on its turn could lead to strengthening / clarifying the central bank's mandate and legal framework (see previous subsection).

Source: Kiff, John et al. (2020), p. 42

Table 3: Summary of Retail CBDC Implementation Considerations

	Considerations	Description	Technical Assistance Components
1.	**Objectives**	Central bank identifies the needs and problem(s) that a retail CBDC would address, and the full array of possible (other) solutions. Central bank assesses cash and non-cash use and trends	Policy frameworks Central bank law Payments and Financial Market Infrastructures
2.	**Implementation & Infrastructure**	Central bank identifies project management approach and involves key stakeholders. Central bank assesses CBDC design features based on policy objectives (point 1) and country circumstances, including aspects of cybersecurity, user-centricity, flexibility, and financial integrity.	Central bank project management Central bank cyber-security Payments and Financial Market Infrastructures
3.	**Legal Framework**	Central bank identifies constraints posed by legal framework, including legal tender definition.	Central bank law
4.	**Governance, Organization, Risk Management**	Central bank identifies decision-making structure relevant for CBDC, organization structure (including innovation hub and/or sandbox), and operational risks (including outsourcing/cloud computing).	Central bank governance, organization, risk management, accounting. internal audit

Source: Kiff, John et al. (2020), p. 48

Table 4: Potential Features of CBDC

Feature	Cash	CBDC popular	CBDC wholesale	Central bank account
Wide usage (public)	Yes	Yes	No	Yes
Constant availability 24/7	Yes	Yes	Possible	Likely
Anonymity (from the central bank)	Yes	Unlikely	No	No
Anonymity (from revenue services, law)	Yes	Possible	Yes	Possible
Limits and caps on transactions	No	Possible	Unlikely	Possible
Peer-to-peer transfers	Yes	Possible	Possible	No
Micropayments	No	Yes	Yes	Yes
Permissioned central ledger	No	Yes	Yes	Yes
Integration of smart contracts	No	Yes	Yes	No
Coexistence with other payment methods	Yes	Possible	Unlikely	Possible
Interest-bearing	No	Possible	Possible	Possible

Source: Dupuis, D. / Gleason, K. / Wang, Z. (2021)

Table 5: Costs associated with developing and operating CBDC

Cost Category	Examples
Labor	IT consulting firm; developers; user experience specialist; wallet maintenance costs, etc.
Infrastructure	Cloud or on-premise servers
Software	Licenses; service fees
Cyber Security	Threat modeling; protection; identification; response management; penetration tests. Etc.
Support	Help desk; training; communication

Source: Kiff, John et al. (2020)

Table 6: Potential improvements of different CBDC arrangements to frictions in correspondent bank arrangements for cross-border payments

Frictions cross-border payments	Model 1–mCBDC arrangement based on compatible CBDC systems	Model 2–mCBDC arrangement based on interlinked CBDC systems	Model 3–single mCBDC multi-currency system
Legacy technology platforms	Compatible systems allow for efficiency gains in existing banking relations	A common clearing mechanism could reduce the number of relationships and provide economies of scale	A single system does not require such relations (however, a single system may add to operational costs)
Limited operating hours	CBDCs can be open 24/7, eliminating any mismatch of operating hours		
Fragmented and truncated data formats	Compatible message standards allow payments to flow without data loss or manual intervention	The message standard (eg ISO 20022) adopted by the interlinkage would act to harmonise standards across systems	Single message standard across the system eliminates mismatches
Unclear FX rates and unclear incoming fees	Compatibility requirements for wallet providers could enable users to calculate fees and rates prior to a payment	Common calculation of rates and fees for transfers using any interlinkage would aid transparency	A single system would likely be designed to include options for FX conversion
Long transaction chains	CBDCs could settle instantly, reducing the need for status updates		
Complex processing of compliance checks	Compatible compliance regimes reduce uncertainty and costs	Interlinking systems do not impact multiple or conflicting compliance requirements	Single set of access requirements means compliance could be equivalent across the system

Source: BIS / CPMI / Innovation Hub / IMF / World Bank (2021), p. 14 (adaptation of table from Auer / Haene / Holden, 2021)

Table 7: Risk mapping checklist

	Issuer	Exchange	Custody/wallet provider	Digital currency holder	Other relevant players?
Issuance	– Capitalization risk – Liquidity risk – Counterparty risk – Run risk – Customer fund risk – Cybersecurity risk – AML/CFT – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Concentration risk – Tax evasion risk – Technical risk (e.g. insufficient smart contract audits) – Data privacy	Not applicable	Not applicable	Not applicable	
Circulation (distribution/ exchange)	– AML/CFT – Cybersecurity risk – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Concentration risk – Tax evasion risk – Data privacy	– Liquidity risk – Cybersecurity risk – Customer fund risk – AML/CFT – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Concentration risk – Tax evasion risk – Technical risk (e.g. insufficient smart contract audits) – Data privacy	– Cybersecurity risk – Capitalization risk – Customer fund risk – Run risk – AML/CFT – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Concentration risk – Tax evasion risk – Data privacy	– AML/CFT – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Tax evasion risk – Cybersecurity risk – Data privacy	
Storage	Not applicable	Not applicable	– Cybersecurity risk – Capitalization – Counterparty – Customer fund risk – Fraud – Monetary policy/ financial stability risk – Concentration risk – Data privacy	– Non-custodial wallet: property risk (theft, damage etc.) – Cybersecurity risk – Monetary policy/ financial stability risk – Data privacy	
Governance	– Redemption risk – Market risk – Fraud – Monetary policy/ financial stability risk – Risk of minority holders' interests being infringed by majority holders	Not applicable	Not applicable	Not applicable	

Source: World Economic Forum (2021), p. 55

Table 8: Comparison of current top-line consumer risks in existing systems and in digital currencies

	Value & backing risks	Depositor protection risks	Payment risks	Privacy risks	Security & technology risks	Accountability risks
Cash	Backed by central bank	N/A	Fraud and theft	High level of privacy from all parties except direct recipient (payee)	At risk of counterfeiting	Depends on issue; payee responsible for accepting legitimate cash
E-money	Reliant on depositor protection	Two-layer risks (wallet-provider and deposit-taking institution where wallet-providers deposit customer funds)	Typically protected from user error and by debit guarantees	Account-based: dependent on privacy laws of country	Relatively secure and tested	Bank and wallet-providers accountable
Commercial bank money	Same as e-money	High degree of standardized protections and regulation	Same as e-money	Same as e-money	Same as e-money	Bank accountable
Stablecoins	Variety of backing mechanisms which carry different risks[15]	Varied: typically no or limited depositor protections	Limited examples of protections equivalent to bank money or e-money	Varied: governance systems differ on privacy. Many institutions push privacy obligations to VASPs	Varied: audit standards still to be fully developed Varied: Counter-feiting risk in the form of double spend	Unclear - See Fig. 5
CBDC	Same as cash	N/A	Some risk depending on architecture (e.g. in "push" vs "pull" transactions)	Dependent on design & architecture (see Privacy white paper)	Dependent on design & architecture. Early pilots reveal focus on security standards and the prevention of hacking or breach[16] Varied: Counter-feiting risk in the form of double spend or illegitimate copying of CBDC	Central bank accountable

High consumer risk Medium consumer risk Low consumer risk

Source: World Economic Forum (2021), p. 74

Table 9: Agency mapping

	Domestic retail CBDCs	Foreign retail CBDCs*	Domestic stablecoins	Foreign stablecoins**	Issuer	Exchange	Wallet	Users	Other relevant players?
Central bank	Issuance Circulation Financial stability AML/CFT	Foreign exchange AML/CFT	Issuance Circulation AML/CFT	Issuance Circulation AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	N/A
Finance ministry	Issuance	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Banking/financial services regulators	Circulation	Circulation	Issuance Circulation	Issuance Circulation	Licensing Auditing	Licensing Auditing	Licensing	N/A	N/A
Securities commission	N/A	N/A	Issuance Circulation	Issuance Circulation	Licensing Auditing	Licensing Auditing	N/A	Market stability Insider trading	N/A
Commodity/derivatives	N/A	N/A	Issuance Circulation	Issuance Circulation	Licensing Auditing	Licensing Auditing	N/A	N/A	N/A
Consumer protection bureau	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	N/A
Tax authorities	Income tax calculation and collection	Income tax calculation and collection	Income tax or capital gain tax calculation and collection	Income tax or capital gain tax calculation and collection	Tax reporting	Tax reporting	N/A	Tax reporting Income tax or capital gain tax calculation and collection	N/A
Other relevant agencies	Data privacy	Data privacy	Data privacy	Data privacy	Data privacy	Data privacy	Data privacy	Data privacy	N/A
Standards organizations (e.g. FATF)	AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	N/A

*Refers to retail CBDCs issued by foreign country
**Refers to stablecoins issued by entities incorporated outside of the jurisdiction

Digital Currency Governance Consortium White Paper Series 56

Source: World Economic Forum (2021), p. 56

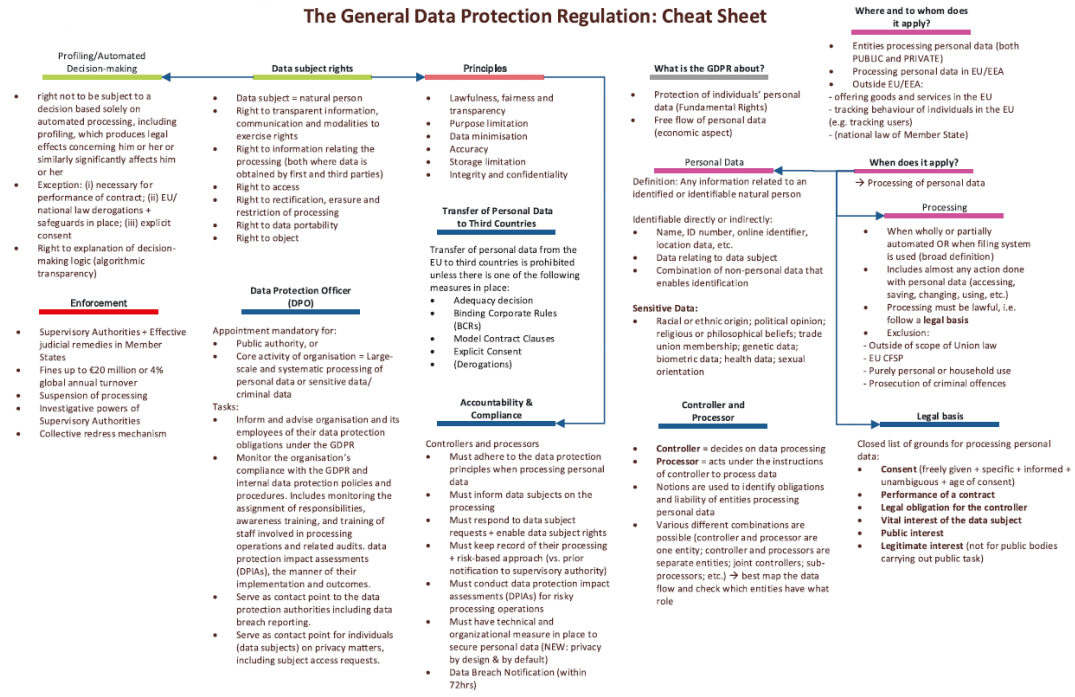
Table 10: Data subjects' rights as protected by GDPR, CCPA and PIPEDA

Data subjects' rights over their personal data	GDPR	CCPA	PIPEDA
Informed and expressed consent needed to process the data	Yes	No	No
Possibility of objecting to the processing of data	Yes	Yes	No
Special categories of personal information	Yes	Yes	Yes
Access to data	Yes	Yes	Yes
Correct incomplete or incorrect data	Yes	Limited	Yes
Right to be forgotten (data erasure)	Yes	Yes	No
Obligation to designate a data privacy officer	Yes	No	Yes
Obligation to provide transparency in data processing	Yes	Yes	Yes
Obligatory security measures	Yes	Yes	Yes
Breach notification	Yes	Yes	Yes
Privacy by design	Yes	No	No
Privacy by default	Yes	No	No
Employees' data protection	Yes	Limited	No

Source: Accenture

Source: WEF (2021), p. 169

Table 11: GDPR - Cheat Sheet



Source: Kubben et al. (2019), p. 66

References

Åberg, P. / Corsi, M. / Grossmann-Wirth, V. / Hudepohl, Tom / Mudde, Y. / Rosolin, T. / Schobert, F. (2021). "Demand for central bank reserves and monetary policy implementation frameworks: the case of the Eurosystem", *Occasional Paper Series*, n.o 282 (September)

Amstad, M. / Huang, B. / Morgan, P. J. / Shirai, S. (2019). *Central Bank Digital Currency and Fintech in Asia*. Asian Development Bank Institute.

Antunes, J. E. (2021). "As criptomoedas", *Revista da Ordem dos Advogados*, ano 81, vol. I/II, pp. 119-187

Aragão, M. (2021). "A Few Things You Wanted to Know about the Economics of CBDCs, but were Afraid to Model: a survey of what we can learn from who has done". Banco Central Brasil - *Working Paper Series*, no. 554

Armelius, H. / Guibourg, G. / Johansson, S. / Schmalholz, J. (2020). "E-krona design models: pros, cons and trade-offs", *Sveriges Riksbank Economic Review*, 2020(1), pp. 80-96

Armelius, H. / Claussen, C. A. / Hull, I. (2021). "On the possibility of a cash-like CBDC". Staff memo - Payments Department and Research Division of Sveriges Riskbank (February)

Arora, S. / Saadi, S. (2021). *CBDCs: The Time Has Come*. https://www.acamstoday.org/cbdcs-the-time-has-come/

Arvidson, N. (2018). "The future of cash", *The Rise and Development of FinTech - Accounts of Disruption from Sweden and Beyond*, Teigland, R. / Siri, S. / Larsson, A. / Puertas, A. M. / Bogusz, C. I. (eds.), London, Routledge, pp. 85-98

Assenmacher, K. / Bindseil, U. (2021). "The Eurosystem's digital euro project: Preparing for a digital future", *Central Bank Digital Currency: Considerations, Projects, Outlook*, D. Niepelt (editor), Centre for Economic Policy Research - CEPR Press, London, pp. 111-118

Auer, R. (2019). "Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies", *BIS Working Papers*, no 765

Auer, R. / Böhme, R. (2020). "The technology of retail central bank digital currency", *BIS Quarterly Review*, March, pp. 85-100

Auer, R. / Böhme, R. (2021). "Central bank digital currency: the quest for minimally invasive technology". *BIS Working Papers*, no 948

Auer, R. / Cornelli, G. / Frost, J. (2020) "Rise of the central bank digital currencies: drivers, approaches and technologies". *BIS Working Papers*, no 880

Auer, R. / Doerr, S. / Frost, J. / Gambacorta, L. / Shinin, H. S. (2021). "Central bank digital currencies and data in the digital age: A triple imperative", *Central Bank Digital Currency: Considerations, Projects, Outlook*, D. Niepelt (editor), Centre for Economic Policy Research - CEPR Press, London, pp. 23-32

Auer, R. / Frost, J. / Gambacorta, L. / Monnet, C. / Rice, T. / Shinin, H. S. (2021). "Central bank digital currencies: motives, economic implications and the research frontier". *BIS Working Papers*, no 976.

Auer, R. / Haene, P. / Holden, H. (2021). "Multi-CBDC arrangements and the future of cross-border payments", *BIS Papers*, no 115

Bacci, C. (2021a). "New legislative proposals to strengthen the EU's AML/CFT rules: overview". PPP presented in ERA conference 4-5 November 2021

Bacci, C. (2021b). "The proposed new AML/CFT Regulation (AMLR) and the proposed Sixth AML/CFT Directive (AMLD 6)". PPP presented in ERA conference 4-5 November 2021

Bacci, C. (2021c). "EU AML/CFT reform and the crypto sector". PPP presented in ERA conference 4-5 November 2021

Bank of England. (2020). *Discussion Paper – Central Bank Digital Currency: Opportunities, challenges and design.* Collection Future of Money.

Bank of England (2021) *Responses to the Bank of England's March 2020 Discussion Paper on CBDC*. https://www.bankofengland.co.uk/paper/2021/responses-to-the-bank-of-englands-march-2020-discussion-paper-on-cbdc

Bank for International Settlements (BIS) (2020). *Central bank digital currencies: Foundational principles and core features.* Report no 1 in a series of collaborations

from a group of central banks (Bank of Canada / European Central Bank / Bank of Japan / Sveriges Riksbank / Swiss National Bank / Bank of England / Board of Governors Federal Reserve System). Published by BIS

Bank for International Settlements (BIS). (2021). "CBDCs: An opportunity for the monetary system"*, BIS Annual Economic Report 2021*, pp. 65-95

Bank for International Settlements (BIS) / CPMI / Innovation Hub / IMF / World Bank (2021). *Central bank digital currencies for cross-border payments - Report to the G20*. https://www.bis.org/publ/othp38.pdf

Bates, Richard (2017). *Banking on the future: An exploration of FinTech and the consumer interest*. Consumers International

Barone, R. / Masciandaro, D. (2019). "Cryptocurrency or usury? Crime and alternative money laundering techniques". *European Journal of Law and Economics*, Springer, vol. 47(2), pp. 233-254

Barontini, C. / Holden, H. (2019). "Proceeding with caution – a survey on central bank digital currency". *BIS Working Papers*, no 101

Bashir, I. (2017). *Mastering Blockchain*. Packt Publishing.

Bech, M. / Garrat, R. (2017). "Central bank cryptocurrencies", *BIS Quarterly Review*, September, pp. 55-70

Bech, M. / Faruqui, U. / Shirakami, T. (2020). "Payments without borders", *BIS Quarterly Review*, March, pp. 53-66

Bech, M. / Hankock, J. (2020). "Innovations in payments", *BIS Quarterly Review*, March, pp. 21-36

Bech, M. / Hankock, J. / Rice, T. / Wadsworth, A. (2020). "On the future of securities settlement", *BIS Quarterly Review*, March, pp. 67-84

Berentsen, A. / Schär, F. (2018). "The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies", *Federal Reserve Bank of St. Louis Review*, Second Quarter 2018, 100(2), pp. 97-106

Bindseil, U. (2020). "Tiered CBDC and the financial system". *Working Paper Series*, No 2351

Bindseil, U. / Panetta, F. / Tero I. (2021). “Central Bank Digital Currency: functional scope, pricing and controls”. *ECB Occasional Paper Series*, No 286 / December

Board of Governors of the Federal Reserve System (2022). *Money and Payments: The U.S.Dollar in the Age of Digital Transformation*,

Bordo, M. (1989). “The contribution of a *Monetary History of the United States, 1867-1960* to Monetary History”. *Money, History, and International Finance: Essays in Honor of Anna J. Schwartz*, M. D. Bordo (editor), University of Chicago Press, 1989, pp. 15-78.

Bordo, M. (2021). “Central Bank Digital Currency in Historical Perspective: Another Crossroad in Monetary History”. *National Bureau of Economic Research Working Paper No. 29171*.

Bordo, M. / Levin, A. (2017). “Central bank digital currency and the future of monetary policy”, *NBER Working Papers*, no 23711

Bossu, W. / Itatani, M. / Margulis, C. / Rossi, A. / Weenink, H. / Yoshinaga, A. (2020) *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations*. IMF WP 20/254

Carstens, A. (2020). “Shaping the future of payments”. *BIS Quarterly Review*, March, pp. 17-20

Carstens, A (2021). “Digital currencies and the future of the monetary system”. Hoover Institution policy seminar. https://www.bis.org/speeches/sp210127.pdf

Carstens, A. / Claessens, S. / Restoy, F. / Shin, H. S. (2021). “Regulating big techs in finance”, *BIS Bulletin,* No 45.

CB Insights (2022). *State of Gintech Global 2021*

Cecchetti, S. G. / Schoenholtz, K. L. (2021). “Central bank digital currency: Is it really worth the risk?”in *Central Bank Digital Currency: Considerations, Projects, Outlook*, D. Niepelt (editor), Centre for Economic Policy Research - CEPR Press, London, pp. 57-63.

Chaum, D. / Grothoff, C. / Moser, T. (2021). *How to issue a central bank digital currency*. SNB Working Papers 3/2021.

Chavez, R. / Lester, J. (2017). *The State of the Financial Services Industry 2017*. Marsh & McLennan Companies.

Chavolla, M. G. (2018) "Cashless Societies and the Rise of the Independent Cryptocurrencies: How Governments Can Use Privacy Laws to Compete with Independent Cryptocurrencies", *Pace International Law Review*, 31(1), pp. 263-292

Chishti, S. / Barberis, J. (2016). *The FINTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries*, John Wiley & Sons Ltd, West Sussex (UK)

Committee on Payments and Market Infrastructures (CPMI) (2018). *Central bank digital currencies*, joint report with the Markets Committee, CPMI Papers, no 174.

Consumers International (2017). Banking on the Future: An Exploration of Fintech and the Consumer Interest. Consumers International MonographComing Together for Change July.

Conway, L. (2021). *Blockchain Explained*. Investopedia. https://www.investopedia.com/terms/b/blockchain.asp

Council of the European Union (2018). "Anti-Money Laundering Action Plan - Council Conclusions (4 December 2018)", 15164/18. https://www.consilium.europa.eu/media/37283/st15164-en18.pdf

Council of the European Union (2021a). "Council conclusions on the Commission Communication on a 'Retail Payments Strategy for the European Union'", https://data.consilium.europa.eu/doc/document/ST-6694-2021-REV-1/en/pdf

Council of the European Union (2021b). "Anti-money laundering: Council agrees its negotiating mandate on transparency of crypto-asset transfers". *Press Release*. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2021/12/01/anti-money-laundering-council-agrees-its-negotiating-mandate-on-transparency-of-crypto-asset-transfers/

Dent, H. (2020). "International Trade Law Concerns with China's Digital Currency: How Sovereign-Issued Stablecoin Can Destabilize International Trade", *George Journal of International Law*, 51/4, pp. 919-950

Deutsche Bundesbank (2021). “Eurosystem experimentation regarding a digital euro - Research workstream on hardware bearer instrument”.

Didenko, A. N. / Buckley, R. P. (2021). *Central Bank Digital Currencies — A Potential Response to the Financial Inclusion Challenges of the Pacific*. ASIAN DEVELOPMENT BANK

Duffie, D. (2021). “Building a stronger financial system: Opportunities for a digital dollar”, *Central Bank Digital Currency: Considerations, Projects, Outlook*, D. Niepelt (editor), Centre for Economic Policy Research - CEPR Press, London, pp. 137-145

Dupuis, D. / Gleason, K. (2021). “Money laundering with cryptocurrency: open doors and the regulatory dialectic”, *Journal of Financial Crime*, Volume 28, Issue 1, pp. 60-74

Dupuis, D. / Gleason, K. / Wang, Z. (2021). “Money laundering in a CBDC world: a game of cats and mice”, *Journal of Financial Crime*, DOI 10.1108/JFC-02-2021-0035

Elwell, C. K. (2011). “Brief History of the Gold Standard in the United States”. Congressional Research Service R41887

European Banking Authority (2019). “Opinion of the European Banking Authority on communications to supervised entities regarding money laundering and terrorist financing risks in prudential supervision”. EBA-Op-2019-08

European Banking Authority (2021). *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (‘The ML/TF Risk Factors Guidelines’) under Articles 17 and 18(4) of Directive (EU) 2015/849*. EBA/GL/2021/02

European Central Bank (ECB) (2012). *Virtual Currency Schemes* (Report October)

European Central Bank (ECB) (2019). “Exploring anonymity in central bank digital currencies*”*. *IN FOCUS*, Issue No 4

European Central Bank (ECB) (2020). *Report on a digital euro*.

European Central Bank (ECB) (2021a). *Eurosystem report on the public consultation on a digital euro*.

European Central Bank (ECB) (2021b). “Report: Digital euro experimentation scope and key learnings”, https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf

European Central Bank (ECB) (2021c). “Eurosystem launches digital euro project”, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html

European Central Bank (ECB) (2021d). “ECB announces members of Digital Euro Market Advisory Group”, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr211025~08af93ada7.en.html.

European Central Bank (ECB) / Bank of Japan (BOJ) (2017). “Stella project leaflet”.

European Central Bank (ECB) / Bank of Japan (BOJ) (2020). *Balancing confidentiality and auditability in a distributed ledger environment - Project stella report phase 4*.

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

European Commission (EC) (2021a). *Communication from the Commission to the European Parliament, The Council, The European Central Bank, The European Economic and Social Committee and the Committee of the Regions — The European economic and financial system: fostering openness, strength and resilience.*

European Commission (EC) (2021b). *Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism Rules*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

European Commission (EC) (2021c). *Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010*

European Commission (EC) (2021d). *Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*

European Commission (EC) (2021e). *Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*

European Commission (EC) (2021f). *Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast)*

European Parliament (2021). *European Parliament resolution of 10 February 2021 on the European Central Bank - annual report 2020 (2020/2123(INI)).*

European Union Agency for Cybersecurity (ENISA) (2022). *Data protection engineering*. ENISA, DOI 10.2824/09079

Europol (2015). "Why Cash Is King? A Strategic Report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering." https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering

Europol (2021). "European Money Mule Action leads to 1 803 arrests". https://www.europol.europa.eu/media-press/newsroom/news/european-money-mule-action-leads-to-1-803-arrests

Fanusie, Y. J. (2020). "Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them", *The Digital Social Contract: A Lawfare Paper Series*

Felländer, A. / Siri, S. / Teigland, R. (2018). "The three phases of FinTech", *The Rise and Development of FinTech - Accounts of Disruption from Sweden and Beyond*, Teigland, R. / Siri, S. / Larsson, A. / Puertas, A. M. / Bogusz, C. I. (eds.), London, Routledge, pp. 154-167

Federal Bureau of Investigation (FBI) (2019). "Money Mule Awareness", https://www.self-helpfcu.org/docs/default-source/pdfs/money-mule-awareness-booklet-july-2019.pdf?sfvrsn=2

Financial Action Task Force (2015). *FATF Report Money Laundering Through the Physical Transportation of Cash*, FATF, Paris

Financial Action Task Force (2017). *Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence* (2013-2017), FATF, Paris

Financial Action Task Force (FATF) (2020). *FATF Report to the G20*, FATF, Paris

Financial Action Task Force (FATF) (2021a). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris

Financial Action Task Force (FATF) (2021b). *Opportunities and Challenges of New Technologies for AML/CFT*, FATF, Paris

Financial Action Task Force (FATF) (2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012-2022), FATF, Paris

Financial Stability Board (2020). *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications*.

Foley, S. / Karlsen, J. R. / Putnins, T. J. (2019). "Sex, drugs and bitcoin: How much illegal activity is financed through cryptocurrencies?". *The Review of Financial Studies*, Volume 32(5), pp. 1798–1853

Fong, Dick (2021). *Central Bank Digital Currencies (CBDC) - Introduction and updates*. McKinsey & Company.

Freij, Å (2018). "A regulatory innovation framework - How regulatory change leads to innovation outcomes for FinTechs", *The Rise and Development of FinTech - Accounts of Disruption from Sweden and Beyond*, Teigland, R. / Siri, S. / Larsson, A. / Puertas, A. M. / Bogusz, C. I. (eds.), London, Routledge, pp. 21-42

G7 United Kingdom (2021). *Public Policy Principles for Retail Central Bank Digital Currencies*
https://www.mof.go.jp/english/policy/international_policy/convention/g7/g7_20211013_2.pdf

Garratt, R. / Lee, M. / Malone, B. / Martin, A. (2020). “Token- or Account-Based? A Digital Currency Can Be Both”. https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/

Garratt, R. / Lee, M. (2021) “Monetizing Privacy with Central Bank Digital Currencies”. https://ssrn.com/abstract=3767028

Gera, P. / McIntyre, A. / Sandquist, E. (2019). *Global Financial Services Consumer Study: Discover the patterns in personality*. Accenture.

Giancarlo, C. H. / Giancarlo, J. C. / Gorfine, D. / Treat, D. B. (2020). *The Digital Dollar Project - Exploring a US CBDC*. Digital Dollar Foundation / Accenture.

Goldstein, I. / Jiang, W. / Karolyi, G. A. (2019). “To FinTech and Beyond”. *Review of Financial Studies*, 32(5), pp. 1647–1661.

Gross, J. / Schiller, J. (2020). “A model for central bank digital currencies: Do CBDCs disrupt the financial sector?” https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721965

Grothoff, C. / Moser, T. (2021). “How to issue a privacy-preserving central bank digital currency”. *SUERF Policy Briefs* No 114.

Grym, A. (2018). “The great illusion of digital currencies”, *BoF Economics Review*, N.º 1/2018

Guindos, L. (2021). “Interview with Luis de Guindos, Vice-President of the ECB, conducted by Frank Wiebe and Jan Mallien”, https://www.ecb.europa.eu/press/inter/date/2021/html/ecb.in210729_1~fb3aa571cc.en.html

Gürtler, K. / Nielsen, S. T. / Rasmussen, K. / Spange, M. (2017). “Central bank digital currency in Denmark?”. *Analysis Danmarks National Bank*, n.º 28/2017

Han, J. / Huang, Y. / Liu, S. / Towey, K. (2020). “Artificial intelligence for anti-money laundering: A review and extension”. *Digital Finance*, 2(3–4), pp. 211–239. https://doi.org/10.1007/s42521-020-00023-1

Heintzman, R. / Marson, B. (2005). “People, service and trust: is there a public sector service value chain?”, *International Review of Administrative Sciences*, Vol 71(4), pp. 549–575

Herlin-Karnell, E. / Ryder, N. (2017). “The robustness of EU financial crimes legislation: A critical review of the EU and UK anti-fraud and money laundering scheme”. *European Business Law Review*, 27(4), pp. 427-446

Houben, R. / Snyers, A. (2018). *Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion*. Policy Department for Economic, Scientific and Quality of Life Policies. Directorate-General for Internal Policies

Jones, C. (2016). European Central Bank scraps €500 note. *Financial Times*. https://www.ft.com/content/e13cec74-120e-11e6-839f-2922947098f0

Kahn, C. M. / Rivadeneyra, F. / Wong, T. (2108). “Should the Central Bank Issue E-money?”. *Staff Working Paper*, 2018-58. Bank of Canada

Keister, T. / Monnet, C. (2021). “Information, privacy and central bank digital currency” in *Central Bank Digital Currency: Considerations, Projects, Outlook*, Centre for Economic Policy Research, pp. 17-22

Kiff, J. / Alwazir, J. / Davidovic, S. / Farias, A. / Khan, A. / Khiaonarong, T. / Malaika, M. / Monroe, H. / Sugimoto, N. / Tourpe, H. / Zhou, P. (2020). “A Survey of Research on Retail Central Bank Digital Currency”. *IMF Working Paper WP/20/104*

KPMG (2020). *Creating a leading central bank*. Fifth edition. Central Bank network.

Koning, J. P. (2020). “The Big Problems with Big Denomination Bills”. https://www.cato-unbound.org/2018/08/07/j-p-koning/big-problems-big-denomination-bills/

Kryparos, G. (2018). “Information security in the realm of FinTech”, *The Rise and Development of FinTech - Accounts of Disruption from Sweden and Beyond*, Teigland, R. / Siri, S. / Larsson, A. / Puertas, A. M. / Bogusz, C. I. (eds.), London, Routledge, pp. 43-65

Kubben, P. / Dumontier, M. / Dekker, A. (2019). *Fundamentals of Clinical Data Science*, Springer, Cham Switzerland

Labonte, M. / Nelson, R (2022). “Central Bank Digital Currencies: Policy Issues”. Updated February 7, 2022. Congressional Research Service (CRS) R46850.

Lagarde, C. (2021). “Interview with Christine Lagarde, President of the ECB, conducted by David Rubenstein, Bloomberg, on 13 September”. https://www.ecb.europa.eu/press/inter/date/2021/html/ecb.in210916~5b06e18ebc.en.html

Ledger Insights (2021). “China catches fraudsters using central bank digital currency for money laundering”, November 15, 2021. https://www.ledgerinsights.com/china-catches-fraudsters-central-bank-digital-currency-cbdc-for-money-laundering/

Lee, A. / Malone, B. / Wong, P. (2020). "Tokens and accounts in the context of digital currencies," FEDS Notes. Washington: Board of Governors of the Federal Reserve System, December, https://doi.org/10.17016/2380-7172.2822

Longchamp, Y. / Deshpande, S. / Mehra, U. (2020). “A Beginner’s Guide to Blockchain Accounting Standards”. SEBA Bank AG

Mancini-Griffoli, T. / Peria, M. S. M. / Agur, I. / Ari, A. / Kiff, J. / Popescu, A. / Rochon, C. (2018). “Casting Light on Central Bank Digital Currency”, *IMF Staff Discussion Note,* 18/08.

Mandeng, O. J. / Velissarios, J. (2019). *The Revolution of Money II - Blockchain Empowered Central Bank Digital Currencies*. Accenture.

MarketLine Case Study (2021a). *Payments & Transactions – Companies investing in the 10 key themes will dominate the payments industry.*

MarketLine Case Study (2021b). *Retail Banking Industry is having to adapt to ultra-low interest rates.*

Mersch, Y. (2017): “Digital base money: an assessment from the ECB’s perspective”, https://www.ecb.europa.eu/press/key/date/2017/html/sp170116.en.html.

Mitsubishi Research Institute Inc. (2019). “Research on privacy and traceability of emerging blockchain based financial transactions”. Financial Services Agency.

Mookerjee, A. S. (2021). *What If Central Banks Issued Digital Currency?* Harvard Business Review. https://hbr.org/2021/10/what-if-central-banks-issued-digital-currency

Nabilou, H. (2020). “Testing the waters of the Rubicon: the European Central Bank and central bank digital currencies”. Journal of Banking Regulation, Palgrave Macmillan, vol. 21(4), pages 299-314, December.

Niepelt, D. (2021). «Introduction», *Central Bank Digital Currency: Considerations, Projects, Outlook*, D. Niepelt (editor), Centre for Economic Policy Research - CEPR Press, London, pp. 1-8

Norges Bank (2021). *Central bank digital currencies - Third Report of Working Group*. *Norges Bank Papers* No 1

Omarova, Saule T. (2020). “Dealing with Disruption: Emerging Approaches to Fintech Regulation”. *Washington University Journal of Law & Policy*, 61(1), pp. 25-54

Organisation for Economic Co-operation and Development (OECD). (2019). *OECD AI Principles overview.* https://oecd.ai/en/ai-principles

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

Panetta, F. (2021b). “Preparing for the Euro’s Digital Future”. www.ecb.europa.eu/press/blog/date/2021/html/ecb.blog210714%7E6bfc156386.en.html

Panetta, F. (2021c). *“*Hic sunt leones” – open research questions on the international dimension of central bank digital currencies*”.* https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211019_1~b91b5f9595.en.html

Panetta, F. (2021d). “Central bank digital currencies: a monetary anchor for digital innovation”. Speech at the Elcano Royal Institute, Madrid (5 November 2021). https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211105~08781cb638.en.html

Panetta, F. (2022). “Central bank digital currencies: defining the problems, designing the solutions”. https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220218_1~938e881b13.en.html

Piechocki, M. / Leslie-Bini, A. (2017). *Data as a critical factor for central banques*. IFC Bulletin chapter 44-06.

PWC (2020). *Central Bank Digital Currency PwC Overview*.

Quiroz-Gutierrez, M. (2022). "Crypto is fully banned in China and 8 other countries", *Fortune*, https://fortune.com/2022/01/04/crypto-banned-china-other-countries

Rice, T. / Peter, G. von / Boar, C. (2020). "On the global retreat of correspondent banks", *BIS Quarterly Review*, March, pp. 37-52

Riechmann, J. M. (2020). *Blockchain takes to the skies* [Master's thesis].

Rogoff, K. S. (2016). *The Curse of Cash*. Princeton University Press, Princeton, New Jersey

Rogoff, K. S. / Scazzero, J. (2021). "Covid Cash". *Cato Journal*, Vol. 41, No. 3, pp. 571-593

Rosalino, H. "Crypto Currency & CBDC", https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/intervpub20211019.pdf

Sackheim, M. S. / Howell, N. A. / Biery, J. B. / Blake, A. P. / Gallego, D. / Harmon, T. W. / Munsell, J. C. / Teitelbaum, D. E / Tessler, L. / Stromberg, A. R. / Engoren D. / Teager, K. S. (2021). *The Virtual Currency Regulation Review: USA*. https://thelawreviews.co.uk/title/the-virtual-currency-regulation-review/usa

Schnabel, I / Shin, H. S. (2018). "Money and trust: lessons from the 1620s for money in the digital age". *BIS Working Papers*, No 698

Setiawan, K / Maulisa, N. (2019). "The Evolution of Fintech: A Regulatory Approach Perspective", *Advances in Economics, Business and Management Research*, volume 130, pp. 218-225

Silva, E. C. / Silva, M. M. (2022). "Research contributions and challenges in DLT-based cryptocurrency regulation: a systematic mapping study", *Journal of Banking and Financial Technology*, https://doi.org/10.1007/s42786-021-00037-2

Smith-Meyer, B. (2022). "Digital euro bill due early 2023", https://www.politico.eu/article/digital-euro-bill-due-early-2023/

Söderberg, G. (2018). "Are Bitcoin and other crypto-assets money?", *Sveriges Riksbank - Economic Commentaries*, n. 5

Söderberg, G. (2019). "The e-krona – now and for the future", *Sveriges Riksbank - Economic Commentaries*, No 8

Sveriges Riksbank (2020). “The Riksbank’s e-krona pilot”. Reg. no 2019-00291.

Sveriges Riksbank (2021). “Report: E-krona pilot phase 1”.

Thakor, A. V. (2020). “Fintech and banking: What do we know?”. *Journal of Financial Intermediation*, 41, 1–13. doi: 10.1016/j.jfi.2019.100833

Tien, P. P. / Quddus, A. / Asad, I. S. / Popesko, B. / Hussain, S. (2021). “The factors of fintech: A literary review”, *17th International Bata Conference for Ph.D. Students and Young Researchers*, DOI: 10.7441/dokbat.2021.34, pp. 395-405

Tinn, K. / Dubach, C. (2021). “Central Bank Digital Currency with Asymmetric Privacy http://dx.doi.org/10.2139/ssrn.3787088

Todd, R. / Rogers, M. (2020). *A Global Look at Central Bank Digital Currencies - From Iteration to Implementation*, The Block Research / KPMG / BRD / HashKey Capital

Urbinati, E. / Belsito, A. / Cani, D. / Caporrini, A. / Capotosto, M. / Folino, S. / Galano, G. / Goretti, G. / Marcelli, G. / Tiberi, P. / Vita, A. (2021). “A digital euro: a contribution to the discussion on technical design choices”. *Mercati, infrastrutture, sistemi di pagamento* (*Markets, Infrastructures, Payment Systems*), n.º 10/2021.

Van der Waldt, G. (2016). “From policy to projects: A Public Service Value-Chain Network Model”. *Journal of Social Sciences: Interdisciplinary Reflection of Contemporary Society* 49(1,2), pp.145-157

Wadsworth, A. (2018). “The pros and cons of issuing a central bank digital currency”. *Bulletin*, *81*(7). Williamson, Stephen. (2019). *Central Bank Digital Currency: Welfare and Policy Implications*. University of Western Ontario.

Wahl, T. (2021a). “AML Package III: 6th AML Directive Proposed”, https://eucrim.eu/news/aml-package-iii-6th-aml-directive-proposed/

Wahl, T. (2021b). “AML Package IV: EU Traceability of Funds Legislation to Be Extended to Crypto-Assets”, https://eucrim.eu/news/aml-package-iv-eu-traceability-of-funds-legislation-to-be-extended-to-crypto-assets/

Williamson, S. (2019). “Central Bank Digital Currency: Welfare and Policy Implications”. University of Western Ontario. *2019 Meeting Papers 386,* Society for Economic Dynamics.

World Bank (2021). *Central Bank Digital Currency: Background Technical Note*. International Bank for Reconstruction and Development / The World Bank.

World Economic Forum (WEF) (2021). *Digital Currency Governance Consortium White Paper Series - Compendium Report*.

Zellweger-Gutknecht, C. (2021). “The right and duty of central banks to issue retail digital currency”, *Central Bank Digital Currency: Considerations, Projects, Outlook*, D. Niepelt (editor), Centre for Economic Policy Research - CEPR Press, London, pp. 31-37.