TECHDISPATCH

CENTRAL BANK DIGITAL CURRENCY

EDPS
European Data Protection Supervisor

EDPS TechDispatch

HTML ISBN 978-92-9242-714-6 ISSN 2599-932X doi: 10.2804/382187 QT-AD-23-001-EN-Q
PDF ISBN 978-92-9242-711-5 ISSN 2599-932X doi: 10.2804/109194 QT-AD-23-001-EN-N

Central bank digital currency

Countries around the world are examining whether they should offer central bank money to the public not only as banknotes and coins, but also in digital form. The fact that the majority of central banks around the world have already started exploring the possibility of launching a state-owned digital currency comes as a response to the increased adoption of digital, contactless payments, cryptocurrencies and e-commerce, further accelerated by Covid-19, and also due to the possibilities offered by these digital currencies as a more flexible monetary tool compared to the existing non-digital currency.

Privacy, the protection of personal data and security are amongst the most important requirements, which impact the core design choices to be taken, as well as expected citizens' trust and acceptance.

1. What is a central bank digital currency?

Money can mainly exist in two forms[1]: central bank money and private money.

Money created by central banks is central bank money, and cash is currently the only kind of central bank money available to the public. In fact, cash is a physical token in the form of coins and banknotes that represent value. Just holding the token means that one legally possesses it. Transfers can be executed by exchanging it between two people, without the necessity to have a third party (as a bank) to validate the transaction. Cash **must be accepted if offered in payment within a jurisdiction** (concept defining the "legal tender status"[2]).

Private money is created by commercial banks[3] when receiving cash in deposit and reusing it by granting loans. This money appears in the bank account, and it can be used to pay by using a various set of instruments such as debit or credit cards. Money, then, can be withdrawn in the form of cash, back to its original form of central bank money. The relationship between holders and commercial banks is based on the trust that money will be held safely and with acceptable risks. Nowadays, there is no payment instrument apart from cash that has legal tender status.

A central bank digital currency (CBDC) is a **digital form of public money issued by a central bank**. Essentially, a CBDC system consists of individuals and companies having access to a digital currency put at their disposal for transactions and savings accounts by their home country's central bank. A distinction can be made between retail CBDC, available to citizens and companies, and wholesale CBDC, only available to financial actors. In this TechDispatch, we will mainly refer to the retail CBDC.

In other words, CBDC consists of a digital representation of coins and banknotes in the form of digital tokens. It is an electronic file that embodies a specific value **with a reference to its owner** attached to it. By just changing that reference, the value is transferred and a payment is made. CBDC is usually presented by central banks as a complement to cash, equipped with similar features (notably, having regard to the legal tender status), but adapted to some functional needs and to the 'digital' nature referred to above.

1. To know more about money, currency and value see European Central Bank, What is money?, 2017 - **https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.en.html**
2. "Legal tender" status is a key attribute of currency: it entitles a debtor to discharge monetary obligations by tendering currency to the creditor – International Monetary Fund, Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations, WP/20/254, pag. 8.
3. Hereinafter, referred also as private banks and financial intermediaries. For more information, please see Investopedia, How Banking Works, Types of Banks, and How To Choose the Best Bank for You, accessed on November 2022 - **https://www.investopedia.com/terms/b/bank.asp**

The key aspect of CBDC that differentiate it from any other means of electronic payment is its legal tender status. In other words, a CBDC **must be accepted if offered in payment within a jurisdiction**, while any other electronic means of payments can be refused.

Both physical and digital tokens are issued directly by central banks. This aspect - added to the legal tender status - is the main difference between CBDC on the one hand and, on the other hand, private money and the almost 22.000[4] different cryptocurrencies (including around 9000 top stablecoins[5]) issued by private actors existing in the last years, as of the latest developments in distributed ledger technology (DLT) and cryptography.

The actual digital payment landscape is driven by commercial banks and transfers are made using only private money. Moreover, customers have a claim to withdraw their money in the form of cash only to the commercial bank where this money is deposited. For this reason, risks related to the solvency of the bank where the person has deposited cash are present and the trust between holders and banks is a key element for the functioning of the whole system.

With CBDC, the situation will be more similar to cash. In fact, due to the legal tender status of the CBDC, the parties involved in the transaction will have **a direct claim to the central bank** issuing the CBDC, even in scenarios where transactions remain intermediated by commercial banks. In other words, in case of bankruptcy, the sum owned by a holder in a private bank in form of CBDC will not be lost. For this reason, solvency risk is very low. This change in the payment mechanisms has been considered by some authors as a change in the "soul" of the payment system[6], allowing a safer and more solid financial system to grow under this perspective. At the same time, the decrease in bank deposits due to CBDC calls for a limitation (and possibly a threshold per-citizen on the maximum amount of CBDC individuals can hold) to avoid a lack of deposits at banks, and, consequently, a lack of investments by banks via (decreased) deposited money. Under this viewpoint, CBDC presents risks to the financial system that need to be addressed.

Overall, the decision to issue a CBDC is not only a technical, but also, if not mainly, a political choice, which might have an important impact on the economy, as well as on the rights and freedoms of citizens and on society as a whole.

4. Source: **https://www.forbes.com/advisor/investing/cryptocurrency/different-types-of-cryptocurrencies/**
5. CoinMarketCap - **https://coinmarketcap.com/view/stablecoin/ (accessed in October 2023).**
6. VoxEU CEPR, Central bank digital currency: the battle for the soul of the financial system, 2021 - **https://cepr.org/voxeu/columns/central-bank-digital-currency-battle-soul-financial-system**

1.1 What is the possible design of CBDC?

The design and implementation of CBDC requires technical and organisational choices. The specific design choices are not pure technological elements but have profound implication in the underlying economic paradigm and in many other policy-related issues, including privacy of payments. The most important design choices concern: 1) the underlying architecture; 2) the centralization level; and 3) the access modality.

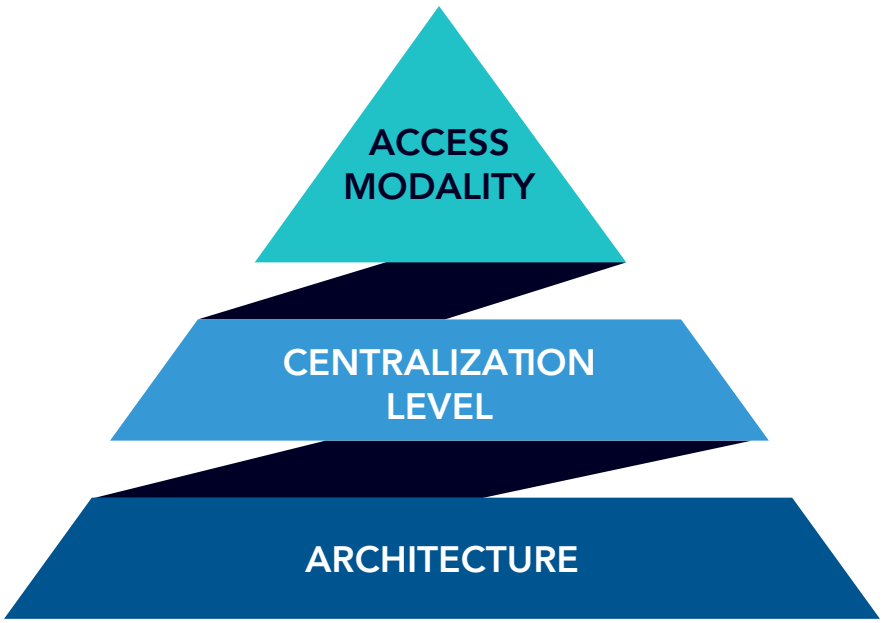
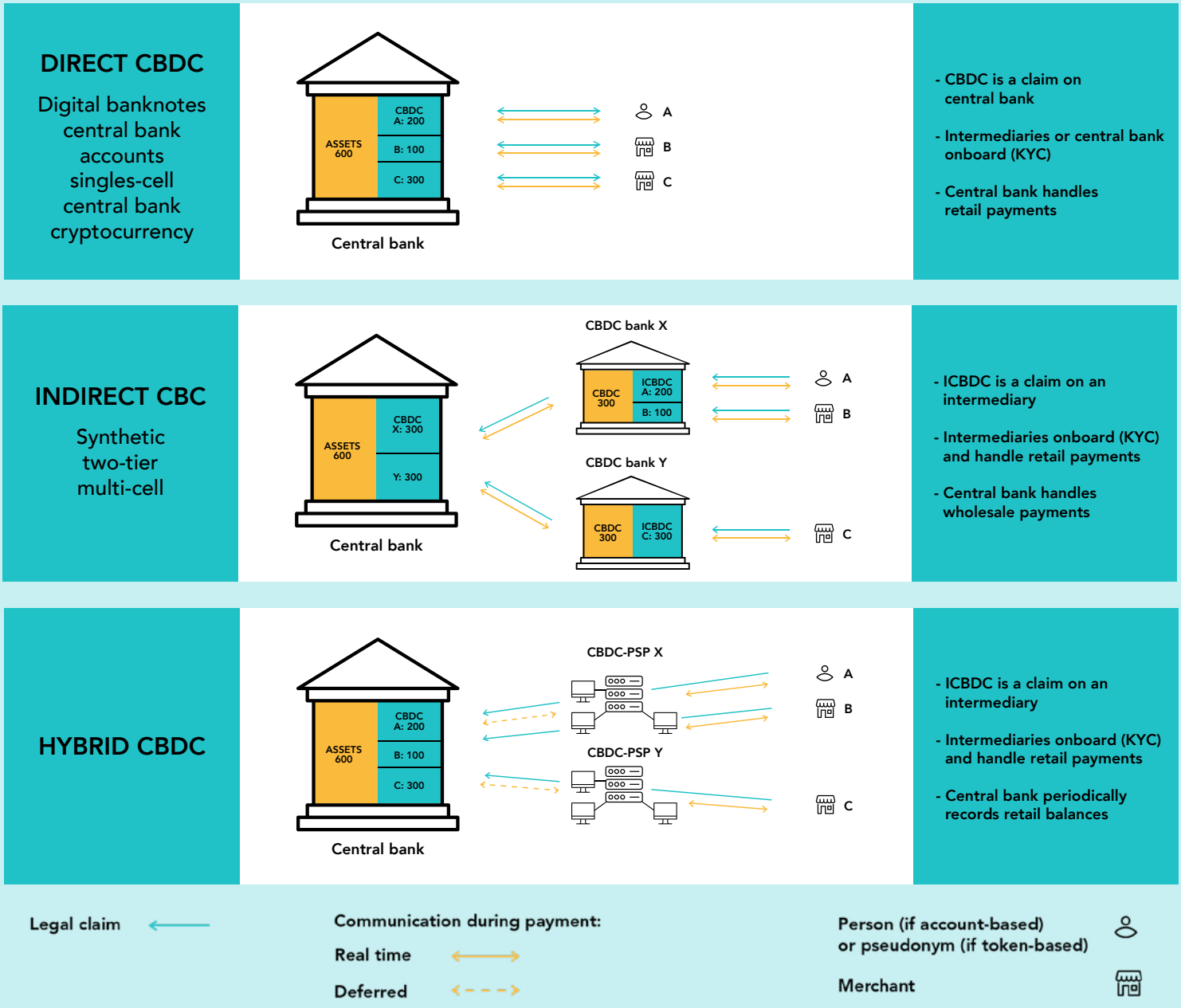


Figure 1 - Different layers of design choices to be taken in the process of implementing a CBDC

1) The **architecture** relates to the operational roles of the central bank and private institutions in transaction management. A direct, indirect or hybrid approach is considered. An **indirect** CBDC is very similar to the actual payment system, where commercial banks manage transactions backed by central bank money. In this case, the central bank keeps no record of transactions and individuals only have claim against commercial banks. Instead, in a **direct** CBDC architecture, accounts are managed directly by the central bank that is the only institution handling payments. This scenario is a fundamental shift from today's payment system and could entail a dramatic increase of the operations of the central bank. Finally, **hybrid** models can be considered. Here, individuals hold money in the central bank, but the payment chain continues to be managed by commercial banks. Some of the possible benefits of this solution include easier portability of a CBDC account from one commercial bank to another, reducing impacts of technical faults or bankruptcy on individuals.

Figure 2 - Data flows in the diverse configuration of the architecture of a CBDC



2) **The centralisation level** of the CBDC transaction management is another important design choice. The CBDC can be based on a conventional centrally-controlled database or a novel DLT. Both technologies often store data in physically separate locations. The main difference lies in how data is updated. In conventional databases, data is stored over one or multiple physical nodes under the control of one authoritative entity, usually the controlling bank, that validates transactions. In DLT solutions, the ledger is jointly managed by different entities in a decentralised manner and without a single authoritative entity. Blockchain is a possible distributed ledger technology where new entries are first bundled into "blocks" and then sequentially linked to each other, forming a chain. Because each block incorporates a cryptographic coded summary of the previous one[7] , the blockchain is hard to be tampered with.

7. For more information on blockchain technologies, see **https://www.oreilly.com/library/view/masteringbitcoin/9781491902639/ch07.html**

Consequently, each update of the ledger has to be harmonised amongst the nodes of all entities. The resulting reduced speed of operation can limit direct CBDC to small jurisdictions. On the other hand, DLTs can be more easily used in indirect CBDC architecture, as the number of transactions to be managed by the central bank is limited, since most of the overall payments will be handled by commercial banks.

3) The **access modality** relates to how and to whom the banks should give access to tokens to end-users ('citizens'). A first option is to follow the conventional **bank account model** and tie ownership to a proven identity. A "bearer-based", also referred as **"token-based"** options is also a possible access modality. Here, the holder needs to demonstrate knowledge of a certain information, like a private key (or digital signature).

An important aspect connected to the access modality is indeed also the offline usability of a CBDC. While online transactions can be made through websites and apps, offline payments could be made through smart cards, mobile devices and payment terminals that are pre-funded with an amount of digital tokens deducted from the balance that a user has online (in her/his bank account) before they are used offline. The trusted device would contain the current balance and adjust it upon payment by the user made via contact or contactless modalities (for instance, NFC capabilities[8] or Bluetooth). Offline functionality (with peer-to-peer validation of transactions) avoids the sharing of transaction details with parties other than the payer and payee, enabling the CBDC to become an equivalent to cash.

Programmability[9] of CBDC is also an important design choice. **Programmable payments** are different from **programmable money**. Programmable money consists of a CBDC with built-in rules, imposing restrictions on the usage of that money. With this feature, a government could also define a positive or negative interest rate to incentivise or disincentive the use of money for the purchase of a particular good; limit its use to a certain category of services; set an expiry date.

Programmable payments enable automatic transfers of money when pre-determined conditions are met. For example, a person can instruct their bank account to send a certain amount of money at the end of every month to another account. In a machine-to-machine payment scenario, payments can be automated and money can be sent when a parcel is checked as delivered at a certain store room. At the same time, CBDC could be used as payments programmed as automatic transfers by a State actor (e.g. for welfare payments). While **programmability of money** needs to be wired in the core design features of a CBDC, and it is something that has been rarely natively implemented in the current payment system, the case for **programmable payments** is different.

8. For more information about NFC protocol, see Wikipedia - **https://en.wikipedia.org/wiki/Near-field_communication** (accessed in October 2022).
9. For more information about programmable money, see Federal Reserve, FED Notes, What is programmable money?, June 2021, available at **https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.html**

We can already program our payments throughout bank accounts. In a similar way, in case of CBDC, the programmability of money would be provided, as value-added services, by financial institutions to their customers (notably businesses and citizens), on top of the CBDC infrastructure[10].

The different design choices described so far can result in very different user experiences. For example, in case of a decentralised, indirect, account-based solution, the users might indeed not feel major changes from the actual payment means in terms of user experience (exception made for the possible cap per-user).

In the opposite scenario of a **centralised, direct, token-based solution** a major change in payment experiences will be faced by users that will have to differentiate their expenditure between a CBDC wallet and the classic payment instruments offered by commercial banks.

1.2 Why issuing a CBDC?

Technology solutions and design choices are triggered by the main rationale for developing CBDCs pursued at political level. Reinforcement of monetary sovereignty, strategic autonomy and monetary policy implementation are the most relevant ones. The CBDC development can be also seen as a response to the broader trend of the creation of new form of private money by private actors that bypass the existing bank-based payment systems.

Besides, CBDCs can be designed with other important functions[11]. First of all, to stimulate competition and innovation in payments, removing barriers and avoiding closed payment systems created by platforms (e.g. the attempt of Meta of deploying its crypto-token, called "Diem"). Second, to foster financial inclusion, rendering the process easier for people that currently do not have a bank account. Third, to improve cross-border retail payments. While the European Union is reducing barriers[12], domestic payment systems are often not interoperable between countries all over the world. The current system architecture tends to be slow, expensive and difficult to automate. Moreover, risks related to money laundering, tax evasion and terrorist financing are typically high while the CBDC features of identifiability of the end-user and traceability of their transactions can render this tool more effective to prevent ML/FT, as well as frauds.

10. For more information about programmability of money and payment, see P. G. Sandner, The Digital Programmable Euro, Libra and CBDC: Implications for European Banks, Conference: EBA Policy Research Workshop: New technologies in the banking sector – impacts, risks, and opportunities, 2020.
11. Bank for International Settlements, BIS Papers No 125, Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies, by Anneke Kosse and Ilaria Mattei, May 2022
12. For more information about the work of the European Union on Intra-EU cross-border payments please see European Commission, Frequently asked questions: Intra-EU cross-border payments, February 2019, available at **https://ec.europa.eu/commission/presscorner/detail/sv/MEMO_19_1170**

Cross-border CBDCs, where one or more systems automatically handle cross-border payments between multiple domestic CBDCs, could significantly improve cross-border financial transactions [13].

Finally, an additional argument in favour of central bank money is that it is of superior quality than other form of money created by commercial banks because it does not depend on the solvency of a private issuer. This however could have a profound adverse impact on the current banking system. In fact, the availability of such safe asset might encourage savers to withdraw their bank deposit and move the funds to their digital currency wallet or accounts at the central bank, causing a major disruption of the liquidity present in commercial banks.

For these reasons, as highlighted above, limits might be imposed by the central bank issuing the CBDC in form of caps/ceilings to account holders, where only a limited amount of digital currency can be owned by each person.

Diversely, with a "tiering approach" no hard limit exists, but holdings above certain threshold would be dissuaded by fees or negative interest rate. The hard limit might coexist with the "tiering" (that is, money above a certain threshold would receive a negative interest rate, and there however will be a maximum threshold for all CBDC, including the one with negative interest rate). At the same time, doubts have been expressed on the added-value of CBDCs compared to existing retail solutions for payments [14].

To conclude, a CBDC is a policy project based on complex technical and organisational design choices that are strictly interconnected with the policy aims pursued by central banks/ state actors. In any case, regardless of the specific policy objectives pursued via the CBDC project, a complex and robust regulatory framework needs to be adopted in order to tackle many challenges, including privacy and data protection.

13. The need for intermediaries would be reduced or eliminated by allowing banks to directly hold foreign CBDCs; and correspondent banking would be sped up through automated or integrated compliance and validity checks on an interoperable digital platform; both leading to reduced latency and fees for end users. - **https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privacy_in_cross-border_digital_currency-_A_transatlantic_approach__-.pdf**
14. See, among others, the Analysis by the Danish Central Bank, New types of digital money, 23 June 2002, at page 28: "At present, and with the associated costs and possible risks, it is not clear how retail CBDCs will create significant added value relative to the existing solutions in Denmark." The Study is available at: **https://www.nationalbanken.dk/en/publications/Documents/2022/06/ANALYSIS_no%208_New%20types%20of%20digital%20money.pdf**

2. What are the privacy and data protection issues?

Depending on the technical design choices made for a CBDC, different privacy and data protection challenges might emerge. A **recent survey of the European Central Bank (ECB)** showed that privacy is amongst the most compelling issues for European citizens. If implemented without proper security protocols and an adequate architecture, privacy and security issues of a CBDC could have a major impact due to the scale of such projects. Much would also depend on the policy objectives and use-cases of the CBDC. So, it is key to wire data protection and privacy requirements within the core concept of a CBDC and to maintain a data protection impact assessment over time to be able to take the necessary measures. At the same time, a clear specification of the policy objectives and use-cases, as well as of the possible interplay with other aspects and digital policy initiatives, is key.

2.1 Privacy and data protection issues in payments can be exacerbated by certain design choices

Design choices have strong impacts on the way privacy is ensured, managed and preserved. On the one hand an **account-based** CBDC solution may require verified identities for all account holders to **map each individual to one identifier across the entire payment system** for both the functioning and security/compliance reasons, representing challenges in terms of privacy and data protection. On the other hand, whilst a **token-based** approach can in principle offer a more universal access and better data protection, there are downsides such as the risk of losing money if end users fail to keep their key secure.

Moreover, some design choices in the underlying technological infrastructure might exacerbate the privacy and data protection issues that already exist in the current digital payment landscape. For example, the unlawful use of transactional data for creditworthiness assessment and abusive marketing initiatives can become even easier according to the level of data accessibility agreed to each actor in the payment process (and facilitated, as possibility for user's profiling, by the single and persistent CBDC user-identifier).

The technological choices of a new CBDC project potentially impact all citizens living in the jurisdiction of a central bank, resulting in large-scale processing operations with high risks for rights and freedoms of data subjects.

For this reason, privacy and data protection requirements should be wired within the regulatory framework and in the core technological decisions on the design of the project, and all decisions regarding features, configurations and risk-acceptance should be duly evaluated and documented. A data protection impact assessment needs to be conducted and maintained in time and over different phases of the CBDC project[15]. From the very beginning, the CBDC design research and development process should be built with a clear data protection by design and by default approach. Retrofitting a CBDC due to a wrong design choice, if ever possible, in addition to the economic costs, would result in higher direct and indirect costs and further uncertainties that can lead to a loss of acceptance of the project itself by citizens and companies.

Complexities would emerge in case distributed ledger technologies are involved in the development of a CBDC, especially for what concerns data minimization and storage limitation principles due to the add-only and ever-growing nature of a blockchain.[2]
Moreover, the design of a CBDC entails privacy and data protection risks with regard to cross-border payments.[3] Payment operations must comply with domestic rules, and despite international standards, there can be significant differences in the implementation and controversial cross-border interplays. This will likely further complicate the implementation and design of cross-border CBDCs due to incompatibilities including among privacy, data protection and anti-money laundering (AML) rules.

These potential issues could be remedied through proper design, as well as multilateral coordination, to align technical, regulatory and supervisory frameworks. Standardization and harmonization efforts, translating into consistent privacy and transparency standards could also be implemented ensuring interoperability across jurisdictions and over time[16].

2.2 Privacy in payments risks to be diminished

Nowadays, **cash** is the only form of money exchanged in an **anonymous way** – under certain thresholds[17] – that operates within regulated domains. Due to the increased adoption of digital means of payments and reduced use of cash as a means of payment[18], cash may be marginalised in a few years. In fact, anonymity can be ensured for payments in cash, which can be exchanged between two peers without a third party that validates the transaction.

15. For a more extensive explanation on data protection impact assessment in the EU, see Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, as last Revised and Adopted on 4 October 2017.
16. For more information about privacy issues in cross-border payments see Atlantic Council - Geoeconomics Center, Privacy in Cross-border Digital Currency - A Transatlantic Approach, 2022 - available at **https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privacy_in_cross-border_digital_currency-_A_transatlantic_approach__-.pdf**
17. Different sectorial legislation have already balanced the privacy of payees against other competing values. In fact, the anti-money laundering directive prohibit credit and financial institutions from keeping anonymous accounts or anonymous passbook, defining also thresholds of amounts where to apply due diligence processes. For more information, see Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
18. For more information, see European Central Bank - Study on the payment attitudes of consumers in the euro area (SPACE) – 2022.

On the other hand, the private digital payment solutions available in the market enable an increasing data exploitation, leading to a reduction of anonymous payments. **Anonymity under a certain threshold can become a clear unique feature for the token- based CBDC solution** (which is a bearer-instrument like banknotes), **differentiating it from all the other private digital payment methods used by citizens.** This would be a unique opportunity for citizens, as secure, stable and anonymous cashless payments are inexistant currently.

Offline solutions (e.g. the token-based CBDC that would have offline transaction capability) can potentially offer the most in terms of privacy and data protection, since only minimal processing operations are required to realize the transaction.

Moreover, offline payments are processed locally without the need of any third party to validate the transaction. Offline payments are also a secure back-up in cases of major internet outages. The token-based CBDC that would have offline transaction capability could become functionally equivalent to cash or an endorsed check.

Due to the digital nature of CBDC, it is inherently more transparent. Fully anonymous CBDC solutions might be difficult to reconcile with the need to hinder illegal activities such as drug trafficking, money laundering and terrorism financing that rely on anonymous cash transactions or alternative remittance systems. Here, the legislator can define the correct balance and the necessary use-cases, which could be implemented through advanced pseudonymisation techniques mixed with other privacy enhancing technologies[19].

Finally, a proper solution for identifying and allowing access and use of offline digital tokens shall be defined. **Account-based** identification can lead to identifying and potentially tracking of all end-user's transactions and profiling thereof (see section 2.5), while an offline token-based CBDC system would enable anonymous payments.

19. For more information, see World Economic Forum, The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value, September 2019 and Future of Financial Intelligence Sharing (FFIS), Innovation and discussion paper: case studies of the use of privacy preserving analysis to tackle financial crime, January 2021

2.3 The resulting interference of the adoption and use of CBDC on people's private life might not fulfil the requirements of necessity and proportionality

Any design choices resulting in an interference with people's private life should be proven necessary for the social need or policy objective pursued by the CBDC project. In addition, each design option needs to be considered under the necessity and proportionality principle in order to determine if alternative technologies and processes could deliver safer options.

In particular, risks for individuals might emerge when privacy and data protection need to be balanced with other values and rights to be protected. As of any other means of payments, CBDCs need to be developed in compliance with other applicable laws and regulations in a sector that results to be one of the most regulated in the data processing landscape.

For example, as is the case for non-CBDC use, anti-money laundering, anti-terrorism financing and anti-tax evasion laws require specific processing of personal data. The particular design and features of a CBDC can result in a specific risk profile in the anti-money laundering and anti-terrorism financing context, different from the one existing for other means of payments and cash. For this reason, these aspects should also be addressed in a forward-looking manner before the launch of any CBDC project[20].

Moreover, the privacy impact needs to be assessed carefully in order to find the right balance with specific and competing interests in CBDC as usability and auditability.
Depending on the chosen technical solution, for instance a fully centralized CBDC with clear and persistent user identification and full transparency on all online transactions of a user, the risk of generalized surveillance might emerge (see section 2.5).

20. Financial Action Task Force (FATF), Updated guidance for a risk-based approach, Virtual assets and virtual asset service providers, 2021

2.4 Roles and responsibilities are complex to identify

According to the specific design choices adopted by the central bank, diverse actors within the payment ecosystem could process personal data (see Figure 2). Recognising data protection roles is of outmost importance for a correct application of obligations and responsibilities under the applicable data protection law. The decentralised governance and the multiplicity of actors involved in the processing of data could lead to difficulties if a DLT-based architecture is implemented. Albeit difficult, the identification of the data controller(s) is the first element necessary to distribute data protection responsibilities across the payment chain.

For example, the **relationship between central banks and the financial intermediaries** is essential to determine who will have to notify a possible personal data breach or whom data subjects should contact to exercise their right to information, access or to withdraw their consent.

2.5 Systemic risks of profiling and surveillance are present

As already reported in our TechDispatch #2/2021 on card-based payments, tracking payments of a person can describe the consumers' life in great detail, understanding people's online and offline spending habits. The amount of personal information that actors involved in transactions' management learn about each individual when a payment system operates is significant. This generates a systemic risk of profiling and surveillance by the parties operating the payment system. Specifically, in the CBDC domain, this risk is connected to design choices. For example, a design that does not allow central banks to process personal data or that implements strict data minimisation might avoid or reduce the risks for privacy involved in the current payment systems.

On the contrary, a configuration that permits the central bank to identify and store personal information of the payments or where merchants[21] can collect and link payment data to customer profiles might amplify these risks compared to the currently existing payment methods.

21. A merchant represents a person or company that sells goods or services – for more info, please see Stax Payments, Explained Simply: What is a Merchant Services Provider?, available at **https://staxpayments.com/blog/merchant-services-provider/**

Furthermore, issuing a CBDC increases the central bank's – and by extension other public authorities' – possibility to access financial information directly linked to an identity, entailing the risk of systemic public surveillance. In any event, whether repurposed in the future, transmitted to another public authority or leaked by accident, such a huge data collection presents a general risk of mass surveillance and unintended use.

For these reasons, privacy enhancing technologies, including advanced pseudonymisation techniques and zero-knowledge proof, should be used in order to limit information shared between transaction partners to the minimum necessary to prove that the payment has been made successfully.

Moreover, defining and imposing by law specific personal data retention periods in relation to each purpose of the data processing is a key requirement, also to reduce risks in case of data breaches or unlawful access to the CBDC technological infrastructure.

2.6 Data concentration can increase security risks

Until recently, little work has been done publicly in the cybersecurity and central banking world to actually understand the risks which are specific to CBDC[22]. Similarly to other means of payment, **security** is a key component of a CBDC. Security is also key to build the necessary trust that citizens need to have in order to be comfortable in adopting and using CBDC. Access credentials are needed for accessing and transferring funds. The most significant risk, credential's theft or loss, is common to most of the other means of payment. In fact, credentials' theft and loss could result in compromising accounts and data. Modern attack techniques such as social engineering, side-channel attacks and malware could be used to extract credentials from a CBDC user's device. The impact of such an attack can be disruptive, with some mitigation if the architecture is implemented to process low amounts of digital currency.

'Data concentration' is also an important security risk to consider. In fact, if payment data of all citizens were **concentrated in the database of a central bank**, this would generate incentives for cyberattacks and a high systemic risk of individual or generalised surveillance in case of data breaches or, more in general, of unlawful access, as well as for denial-of-service attacks jeopardising the possibility to carry out payments, in particular in case of "direct" approach.

22. For more information, see Atlantic Council, Missing key: the challenge of cybersecurity and central bank digital currency, June 2022 - available at **https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/**

On the other hand, where a distributed ledger technology is adopted (and data storage occurs on device), "double-spending"[23] attacks need to be adequately minimised, especially in the **offline, bearer-based** configuration of a CBDC. Those consists in a form of counterfeiting where the CBDC is spent multiple times illegitimately.

Quantum computing might ultimately impact all financial services as it could compromise major data encryption methodologies and cryptographic primitives used for protecting access, confidentiality and integrity of data stored and transmitted and the need for possible post-quantum cryptography should be taken into account during technology design[24].

Lastly, fragmented efforts to build CBDCs at national level are likely to result in cybersecurity risks stemming from difficulties in ensuring interoperability, notably in a cross-border dimension. Central banks have been focused so far on domestic uses of CBDC, with too little thought for cross-border regulation, interoperability and standard-setting. The multi-jurisdictional transfer of personal and transaction data may increase the scale, scope, and speed of data breaches.

In order to correctly handle the security risks, a technical governance should be an integral part of a CBDC system in order to monitor new developments and anticipate risks. Adopting open-source models may help foster transparency, innovation and trust. Security concerns in the CBDC infrastructure, whose relevant requirements and expectations are high, may turn into severe consequences among stakeholders and a significant loss of trust from users, with the consequent dismissal as a widely-used means of payment, thus resulting in the failure of the project.

23. Sveriges Riksbank, On the possibility of a cash-like CBDC, February 2021 - **https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf**
24. Many banks around the world are already developing and testing post-quantum security capabilities. On this, see Bank for International Settlements, BIS Innovation Hub announces new projects and expands cyber security and green finance experiments, June 2022 - **https://www.bis.org/press/p220617.htm** and Finextra, Banque de France tests 'post quantum' security tech, September 2022 - **https://www.finextra.com/newsarticle/41018/banque-de-france-tests-post-quantum-security-tech**

Recommended readings

European Parliament, The digital euro: policy implications and perspectives, January 2022 - **https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)703337**

Banca d'Italia, A digital euro: a contribution to the discussion on technical design choices, July 2021

R. Auer, R. Bohme, The technology of retail central bank digital currency, BIS Quarterly Review, March 2020

Digital Euro Association, Ahead of the digital euro, August 2022

Raskin et. al., Digital currencies, decentralized ledgers, and the future of central banking, National Bureau of Economic Research, 2016

Institute and Faculty of Actuaries, Understanding Central Bank Digital Currencies (CBDC), March 2019

International Monetary Fund, F&D Series, The Money Revolution – Crypto, CBDCs, and the future of finance, September 2022

Atlantic Council, Missing key: the challenge of cybersecurity and central bank digital currency, June 2022 - available at **https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/**

Bank of International Settlement, Central bank digital currencies: system design and interoperability, 2021 – available at **https://www.bis.org/publ/othp42_system_design.pdf**

This publication is a brief report produced by the Technology and Privacy Unit of the European Data Protection Supervisor (EDPS). It aims to provide a factual description of an emerging technology and discuss its possible impacts on privacy and the protection of personal data. The contents of this publication do not imply a policy position of the EDPS.

Issue Authors: Stefano LEUCCI, Massimo ATTORESI, Xabier LAREO
Editor: Massimo ATTORESI
All links cited and listed have been lastly accessed on the 10th March 2023.
Contact: **techdispatch@edps.europa.eu**

To subscribe or unsubscribe to TechDispatch publications, please send a mail to **techdispatch@edps.europa.eu**. The data protection notice is online on the **EDPS website**.

© European Union, 2023. Except otherwise noted, the reuse of this document is authorised under a **Creative Commons Attribution 4.0 International License (CC BY 4.0)**. This means that reuse is allowed provided appropriate credit is given and any changes made are indicated.

For any use or reproduction of photos or other material that is not owned by the European Union, permission must be sought directly from the copyright holders.

edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

@EDPS@social.network.europa.eu

@EDPS@tube.network.europa.eu