International Working Group
on Data Protection in Technology

Working Paper on Central Bank Digital Currency - CBDC

Published 13th June 2024[1]

Table of Contents

[1] *This paper was discussed at the 71st IWGDTP Meeting on 7th – 8th June 2023 and adopted, after final discussion, at the 72nd IWGDPT Meeting on 7th-8th December 2023. The written procedure followed after the latter meeting.*

Executive summary

A Central Bank Digital Currency (CBDC) is a ”fiat”[2] digital currency issued and backed by a central bank. The majority of central banks around the world have at least researched CBDC, with several moving on to pilot programs or even deployment. Reasons put forward for a CBDC include reinforcing central banks role, strengthening monetary policy, enhancing financial supervision and stability and promoting own currency.

CBDCs are issued by a central authority and are, as the traditional currency, subject to laws and other applicable regulations. CBDCs are designed to be used as a digital version of traditional currency, typically for both offline (cash) and online transactions, and may support new use cases that might impact individuals and society.

If sufficient privacy protections, controls and security safeguards are not put in place, CBDCs may provide financial entities involved, such as central and commercial banks, with unprecedented access to their citizens' financial information. This would imply deep insights into consumers' lives, both online and offline, allowing for profiling and surveillance of individuals. This paper takes those design choices into account and identifies the main privacy risks and challenges associated with CBDCs, drawing from a sample of use-cases; isolates and highlights the main elements of those risks; and proposes some high-level advice to mitigate those risks. Target audience are stakeholders such as policy makers, central banks, and other financial actors and organizations.

Establishing a CBDC is a critical decision that must consider both benefits and costs, taking into account not only financial aspects, but also any harmful consequences to society and individuals rights. It requires careful assessment to avoid unnecessary and disproportionate interference with fundamental rights, including privacy and personal data protection, but also individual and community related discrimination and financial exclusion. Deploying a CBDC should not be driven solely by the desire to keep up with technological trends or compete with other digital currencies. Unless there is a clear and demonstrated need for the CBDC, the privacy and data protection risks will outweigh the benefits of creating a CBDC.

The design of the CBDC should be driven by a privacy and data protection by design and by default approach. A privacy and data protection impact assessment considering also broader fundamental rights impacts should be carried out during the planning phases and monitored during deployment and operation. Data protection roles, in particular in use cases where many stakeholders intervene, should be clearly assigned to grant privacy and data protection rights.

The possible design options for a CBDC deeply affect the resulting privacy and data protection risks and thus require careful planning and assessment from the outset. In theory, it is possible to develop disintermediated, secure, confidential digital payments, while providing accountability of the payer

[2] A fiat money is a type of currency that is declared legal tender by a country but has no intrinsic or fixed value and is not backed by any tangible asset, such as gold or silver.

towards the payee. Yet anonymous payments would be incompatible with existing legal provisions addressing risks to individuals and society such as for preventing money laundering, fighting terrorism financing and stopping tax evasion. This is why privacy enhancing technologies can be used to provide for accountability while minimising personal data disclosure. Together with a proper design based on specific risk profiles, it is possible to minimise the visibility of transactions relying on CBDCs and focus instead on those transactions bearing significant risks.

Other design choices can contribute to mitigate risks. Peer-to-peer and offline transactions would enhance privacy protection by avoiding intermediation, where possible, by design. The need for programmable money should be carefully evaluated against possible adverse financial impact for individuals. The rationale for the use of Distributed Ledger Technologies should be assessed against relevant risks and, if confirmed, mitigating measures should be put in place. A targeted cybersecurity framework, ranging from offline use cases to interoperability requirements, can help avoid or mitigate the impact of compromises to such a critical function for individuals and society.

1. Introduction

1. The emergence of central bank digital currencies (CBDCs) represents a ground-breaking shift for the global financial system. Private cryptocurrencies have already impacted the way people engage in financial transactions. Proponents argue that private cryptocurrencies increase inclusion and transparency, speed up transactions, and reduce costs, although the majority of these benefits have failed to materialize.[3] Meanwhile, current cryptocurrencies impose a negative impact on the environment as well as greater risks, such as those linked to the nature of usually unregulated currencies, including high volatility, vulnerability to scams and value loss. CBDCs have the potential to transform how digital currency is issued, distributed, and used on a global scale. The majority of central banks around the world[4] have at least researched central bank digital currency, with several moving on to pilot programs or launching CBDCs. This comes in response to the increased adoption of digital, contactless payments, cryptocurrencies, and e-commerce,[5] further accelerated by Covid-19. The growth is also spurred by the possibilities offered by these digital currencies as a more flexible monetary tool compared to existing non-digital currency.

2. A CBDC is a ”fiat” digital currency issued and backed by a central bank. Unlike cryptocurrencies such as Bitcoin, CBDCs are issued by a central authority and are, as the traditional currency, subject to laws and other applicable regulations. CBDCs are designed to be used as a digital version of

[3] U.S. Dep’t of Treasury, Crypto-Assets: Implications for Consumers, Investors, and Businesses at 44 (Sept. 2022). Available at: https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.
[4] https://www.atlanticcouncil.org/cbdctracker and https://cbdctracker.org
[5] European Central Bank: Study on the payment attitudes of consumers in the euro area (SPACE) – 2022. Available at: https://www.ecb.europa.eu/stats/ecb_surveys/space/shared/pdf/ecb.spacereport202212~783ffdf46e.en.pdf

traditional currency, typically for both offline and online transactions, and may support new use cases[6] that might impact individuals and society.

3. The design of a CBDC can vary significantly depending on each jurisdiction's assessment of how a CBDC could support public policy objectives. While a few CBDCs are already in operation, many others are still in the research phase, in planning, development, or testing, and a few have already been discontinued. Future and existing CBDCs could be subject to change as the technology and regulatory landscape evolves.

4. Central banks have put forward many reasons to deploy their CBDC.[7] First is the reinforced role of central banks in the global financial system. CBDCs could impact this in several ways.[8] Firstly, CBDCs could strengthen monetary policy by providing central banks with additional tools to implement policy more precisely and efficiently. Secondly, CBDCs could promote financial stability by providing a safer and more secure means of payment and reducing the risk of value loss for users in case of bank runs.[9] Additionally, CBDCs could help inform economic policy design as well enhance financial supervision capabilities by providing central banks with a better understanding of how money is being used and where it is being held. Lastly, CBDCs could promote national sovereignty by allowing governments to maintain control of their monetary policy over private entities or foreign governments.

5. Another reason for a central bank to issue a CBDC is to aid in reinforcement of its own currency. Creating a CBDC could increase market confidence in the currency issued in that jurisdiction, as it would represent a tangible commitment from the central bank to safeguard financial stability. Additionally, issuing a CBDC would provide a new means for the central bank to promote the use of the national currency, potentially reducing the reliance on other currencies and strengthening the position of the national currency in the global financial system.

6. From the privacy and data protection perspective, as already outlined by the EDPS in recent work,[10] CBDCs may provide governments, central banks and financial entities involved with unprecedented access to their citizens' financial information, posing significant risks to privacy,

[6] Such as programmable payments and money, as illustrated later on in the text.
[7] For a comprehensive analysis on goals and reasons, see 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
[8] For more information, see https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2713~91ddff9e7c.en.pdf
[9] A bank run is a situation where many customers simultaneously withdraw their deposits from a bank due to concerns about the bank's solvency or stability. This can lead to a liquidity crisis for the bank, making it difficult for it to meet the demands of its depositors and potentially leading to the bank's failure. For more info, see Allen, F. & Gale, D. (2000). Financial contagion. Journal of Political Economy, 108(1), 1-33. https://doi.org/10.1086/262109
[10]https://edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-03-29-techdispatch-12023-central-bank-digital-currency_en

security, and individuals' rights. Given the ongoing trend in many countries to progressively abandon the use of cash, which is intrinsically far less traceable than digital transactions, CBDCs would then be the natural candidates to replace it. Therefore, CBDC features and designs must be carefully assessed when planning its feasibility.[11] Privacy and safeguards for rights and freedoms must be built into the design from the outset to create a trustworthy CBDC.

2. Main objective of this paper

7. In the last few years, experts have written extensively on how privacy requirements would affect the plans for CBDCs. A few solutions have been proposed, which must be adapted to the complex policy, operational, and technology options. Several considerations have also been put forward by central banks and stakeholders on how to design a privacy-protective CBDC. The goals of this paper are (i) to identify the main privacy risks and challenges associated with CBDCs, drawing from a sample of use-cases identified in our research, (ii) to isolate and highlight the main elements of those risks, and (iii) to propose some high-level advice to mitigate the risks, ensuring that CBDCs are designed and implemented in a way that respects citizens' privacy and rights.

3. Scope, terminology, and target

8. CBDCs can be broadly divided into two categories: retail and wholesale. Retail CBDCs are designed for general public use and usually aim to complement or replace current means of retail payments, such as cash, checks, debit cards, etc. Wholesale CBDCs, on the other hand, are designed for use by central banks and financial institutions and aim to facilitate interbank payments and settlement.

9. This paper focuses on retail CBDCs, due to their direct impact on the privacy of individuals. Wholesale CBDCs are outside the scope of this paper.

10. This paper addresses mainly stakeholders as policy makers, central banks, and other financial actors and organizations, to urge them to take into account privacy considerations and individual rights when crafting CBDCs. The general public, who will use the CBDC for payments, and civil society organisations defending people's rights and freedoms may also benefit from it to understand the challenges and be able to properly evaluate the risks of CBDCs on offer.

[11] The International Monetary Fund has issued a paper proposing "a dynamic decision-making framework under which the central bank can make decisions under uncertainty" with a view to a CBDC. G. Soderberg et al., How Should Central Banks Explore Central Bank Digital Currency?, 8 September 2023. Available at: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504 . Privacy is among elements take into consideration, at page 21.

4. CBDC main components and design choices

11. For a factual analysis of risks, we must first clearly identify the main functional building blocks (which we will call “components”) expected in a CBDC. While CBDC structure may vary, this paper will focus on a few main components that are most consistently seen in CBDC projects from central banks around the world and at the same time feature noticeable privacy challenges. This will help gain insight into the different ways they could be designed and implemented and the impact this has on privacy risks and their mitigation.

12. Based on our observation, a list of the main components of CBDC projects follow. Some of them are functional to others, some may be considered sub-components or horizontal processes. Not all of these components are strictly necessary for a CBDC system, but governments generally look to implement all of them. As a rule, we will not go through each component in this paper, but having them listed can be useful for further, more specific analysis.

- Identity management: a system for verifying and managing user identities, typically involving digital identification methods and authentication and authorisation protocols.
- On-boarding: the process of registering and integrating new users into the CBDC system, including Know Your Customer (KYC)[12] checks and the creation of digital wallets[13] or accounts.
- Value storage: a digital representation of the currency's value, which can be held as digital tokens or accounts managed by financial institutions or the central bank.
- Value transfer (payments): mechanisms and protocols for transferring value between parties, which can involve peer-to-peer transactions or intermediaries such as banks.
    - Transaction management: a system for processing, validating, and recording transactions, which can be based on centralized or decentralized ledger technologies.
    - Offline payments: the ability of the digital currency to be transacted and used for payments without the use of an Internet connection.
    - Peer-to-peer payments: a feature enabling direct transactions between users without the need for intermediaries, leveraging the CBDC's transaction management and value transfer components.

[12] KYC procedures are a critical component of effectively managing money laundering and terrorist financing risks. KYC measures assist firms in understanding their customers and their financial dealings, and in detecting suspicious activities. For more info, see https://en.wikipedia.org/wiki/Know_your_customer
[13] This term may include devices such as smart cards to be used also in offline payments or mobile apps for online payments.

- Settlement process: the process of finalizing transactions, ensuring the value transfer is completed and irrevocable, and updating the balances of the involved parties.

- Interoperability in payments: the possibility to interact with CBDCs system under other jurisdictions to enable trans-border payments.

- Programmability of payments and money: system for automating the payment processes at certain times and the development of new financial products and services through smart contracts[14] and other programmable features.

- Anti-money laundering (AML) and general fraud management: systems and tools for detecting, preventing, and responding to potentially fraudulent activities, such as unauthorized transactions, identity theft, and other malicious behaviours.

- Account recovery: systems allowing individuals to reclaim funds or related digital identities in scenarios when the individual changes electronic devices, becomes a victim of fraud, loses account information, or to transfer accounts when the individual dies.

- Monetary policy related tools and mechanisms: these may include tools or mechanisms used for managing holding limits and related emergency mechanisms (such as switching).

13. The possible design choices for a CBDC deeply affect the resulting privacy and data protection risks. Despite the many possible CBDC design dimensions, we can identify three as the most impactful: the choice of the CBDC operational model, the underlying IT infrastructure model, and the way the user authorisation to perform CBDC operations is verified. These design choices have important implications for the functionality, security, and privacy of the CBDC.[15] The way they are categorised below helps clarify the issues at stakes and the breadth of options.

14. A CBDC model type may be **direct, indirect, or a hybrid** of the two (also called, respectively, one-tier, two-tier, or a hybrid approach). In a direct model, the central bank fully operates the overall CBDC, holding user accounts and managing all functional components of the CBDC. This option is usually discarded since it would completely revolutionise the current system, putting burdens and responsibilities on central banks while drastically reducing the role of intermediaries. In an indirect model, the central bank would delegate to the financial intermediaries most operational tasks, such as user on-boarding, user account management, and anti-money laundering/combating the

[14] A smart contract is a self-executing digital contract that contains the terms of an agreement between parties written directly into lines of code. The code is stored on a blockchain network, which ensures its execution and enforceability without the need for intermediaries. For more information, see Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.

[15] See for example: Tsang, Cheng-Yun (CY) and Yang, Alex Yueh-Ping and Chen, Ping-Kuei, Disciplining CBDCs: Addressing the Privacy Aspects and Central Bank Independence (October 20, 2022), available at SSRN: https://ssrn.com/abstract=4253888 or http://dx.doi.org/10.2139/ssrn.4253888, and Pocher, Nadia and Veneris, Andreas, Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme (January 3, 2021). Available at SSRN: https://ssrn.com/abstract=3759144 or http://dx.doi.org/10.2139/ssrn.3759144.

finance of terrorism (AML/CFT) activities. A hybrid CBDC would combine elements of both approaches. For example, central banks might either keep a copy of all retail transactions or just manage wholesale balances with intermediaries. Furthermore, they might continue delegating retail payments' settlement to intermediaries or perform direct settlement of all transactions.

15. CBDC IT infrastructure models may rely on either a **centralised** ledger/repository or a **distributed** ledger (DLT). In the centralised model, all user transactions are recorded in a central ledger under central bank control. In the distributed model, central banks authorise a limited number of other entities to update the ledger. Whatever the choice, the very nature of the CBDC requires that the central bank maintain the role of a central authority and a high level of control over the ledger, including on the amount of the CBDC issued, who can update the ledger, and other elements.

16. Finally, the CBDC may be either **token or account-based**. A token-based CBDC uses a digital token (such as a digital signature) under users' control to access and use the currency they own, without the need to provide any identity information, like a digital version of bank notes or coins. A payee receiving a digital token would not need to verify the customer's identity - only the validity of the token itself. Conversely, an account-based CBDC requires the intermediary with whom the user holds their account to identify the user, manage the account, and track related transactions and balances, as occurs when using private bank money held in bank accounts.

5. General privacy risks and relevant advice

17. CBDCs entail several privacy and data protection challenges. A survey of the European Central Bank[16] showed that privacy and security are the most compelling concerns for European citizens. These concerns are particularly relevant given the increasing use of digital technologies, the growing importance of personal data in the modern economy, and the potential surveillance risks from governments and private financial organisations that the implementation of a CBDC might entail if payments are pervasively monitored.

18. Potential privacy impacts would first depend on the policy objectives and features[17] of the CBDC. A clear specification of those objectives and planned functionalities, as well as of the possible interplay with other digital and financial elements and policy initiatives, is essential to be able to assess those impacts. Furthermore, ensuring privacy requires appropriate design choices by carefully considering the planned CBDC design choices for its components such as identity management, the transaction and settlement management system, and the value storage and

[16] European Central Bank. ECB publishes the results of the public consultation on a digital euro. 2021. Available at https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html

[17] For example, a policy might limit the amount of CBDC per user, where other policies might not. Another choice could be to allow only one CBDC account per user, whereas another option is to allow many. Or programmable money could be a feature of a CBDC, but not of others.

transfer mechanisms. Those choices should be the outcome of a proper assessment of privacy risks leading to the identification of adequate mitigating measures.

19. In theory, it is possible to develop disintermediated, secure, confidential digital payments, providing accountability of the payer towards the payee. However, anonymous payments would be incompatible with existing legal provisions addressing risks to individuals and society and imposing certain data processing activities in the financial sector. For instance, laws aimed at preventing money laundering, fighting terrorism financing and stopping tax evasion impose specific requirements that necessitate personal data processing (such as payer/payee identity, payment history, balances) by competent authorities with access to data. The design and features of a CBDC might consider specific risk profiles regarding anti-money laundering and counter-terrorism financing, to avoid full visibility of transactions relying on CBDCs and to focus instead on the ones representing significant risks.

5.1. Profiling and surveillance

20. Cash is the only form of confidentially exchanged public money that operates within regulated domains. The increased adoption of digital payments and reduced cash use,[18] identifies a trend towards a full digital payment landscape, which might result in increasing exploitation of financial transactions data.

21. If sufficient privacy protections, controls and security safeguards are not put in place, pervasive transaction tracking can provide deep insights into consumers' lives, both online and offline, allowing for profiling and surveillance of individuals by parties involved in payment systems or any other entity given access to the data. A CBDC may enable real-time financial transaction monitoring, potentially revealing sensitive personal information about individuals, even beyond their spending habits, income, and financial obligations. Payment data can reveal a full picture of users' personal life, including health status, sexual orientation, religious and philosophical beliefs, and political opinions. The accumulation and availability of such a vast amount of data poses a severe risk to the rights and freedoms of data subjects because of possible mass surveillance, discrimination, unlawful repurposing, and data breaches.

22. Issuing a CBDC raises specific concerns as to access by central banks, governments, and other public authorities to financial information linked to individuals, which introduces the risk of systemic surveillance violating democratic rules and citizens' privacy and fundamental rights. This risk can vary depending on the country's institutional and democratic setup and level of independence of central banks.[19] The risk of physical or virtual access to data could potentially be exploited if the political and institutional context changes.

[18] See footnote 5.

[19] Tsang, Cheng-Yun (CY) and Yang, Alex Yueh-Ping and Chen, Ping-Kuei, Disciplining CBDCs: Addressing the Privacy Aspects and Central Bank Independence (October 20, 2022). 2022 DC Fintech Week Winning Papers, Available at SSRN: https://ssrn.com/abstract=4253888 or http://dx.doi.org/10.2139/ssrn.4253888.

23. In the current payment framework, AML/CFT operations are delegated to financial intermediaries. Direct or hybrid CBDCs would add a central AML/CFT service performed directly or indirectly by central banks. In direct CBDCs, central banks would almost completely take over from intermediaries and hybrid CBDCs could have different possible service configurations, with either central banks providing strategic consultancy leveraging aggregated data for pattern identification or performing real time AML/CFT checks based on real time visibility of CBDC transactions

Advice

24. A CBDC design that restricts the access from central banks, government and other stakeholders to personal information and prioritizes data minimization can help reduce privacy risks. In contrast, a configuration that enables unnecessary collection and allows to identify and store personal information and payments data, or to link payment data to customer profiles would amplify privacy risks.

25. From a privacy and data protection perspective, direct or hybrid CBDCs enabling central banks to view all transactions adds a new, specific risk with respect to an indirect CBDC where a central bank can only see wholesale transactions with financial intermediaries. In an indirect CBDC modality, payment data would be visible only to financial intermediaries, posing a privacy risk comparable to the one resulting from the usage of debit and credit cards in account-based digital payment systems, where private banks might unlawfully process an account holder's personal data.

26. Where the design allows central banks to view transactions, privacy enhancing technologies (PETs) can offer tools to mitigate risks. For example, pseudonymisation techniques would not reveal the real identity of users to central banks but would still provide them with the opportunity to perform assessments over transactions based on the pseudonym. This safeguard would require other legal and organisational measures to ensure a reasonable level of protection to avoid unlawful central banks access to identification data held by intermediaries and set limits on re-identification.

27. To provide accountability and cooperate while minimising personal data disclosure to central banks and intermediaries, more advanced PETs,[20] such as zero-knowledge proofs[21] including Pedersen commitments,[22] one-time addresses,[23] homomorphic encryption, multi-party

[20] ENISA calls them « advanced pseudonymisation techniques ». See ENISA, January 2001, Data pseudonymisation advanced techniques and use cases. Available at: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/

[21] Gross, Jonas and Sedlmeir, Johannes and Babel, Matthias and Babel, Matthias and Bechtel, Alexander and Schellinger, Benjamin, Designing a Central Bank Digital Currency with Support for Cash-Like Privacy (July 22, 2021). Available at SSRN: https://ssrn.com/abstract=3891121 or http://dx.doi.org/10.2139/ssrn.3891121.

[22] Id.

[23] European Central Bank, Bank of Japan, February 2020, STELLA – joint research project of the European Central Bank and the Bank of Japan, Balancing confidentiality and auditability in a distributed ledger

computation[24] etc., can be implemented. Research projects and pilot implementations[25] are well-established, reportedly providing for definitive anonymity in payments[26] to partial/revocable anonymity,[27] taking into consideration various levels of accountability and auditability needs. The use of these PETs must co-exist with other requirements such as performance, scalability, usability, and available resources as well as integration with existing payment infrastructure,[28] which represents one of the main design challenges.

28. Payment confidentiality under a certain payment threshold (taking into account AML/CFT risks) could also be an unprecedented privacy-focused feature for CBDC solutions, differentiating it from other private digital payment methods used by citizens, where anonymous cashless payments are not an option. Transaction caps can be placed that make it possible to un-blind or de-anonymize a transaction above a certain threshold. Such caps may be a more privacy-protective approach to anti-money laundering controls than widespread transaction reporting requirements, pattern-analysis of small transactions, or other real-time monitoring capabilities[29]. Peer-to-peer payments and offline payments (see below for more focus) are also privileged design choices to minimise data sharing.

29. Personal data relating to CBDC operations should be processed only during the time necessary to perform identified necessary and lawful operations. After this period, they should be deleted or anonymised, and no longer available to stakeholders other than the payer and the payee. Legislators should define specific retention periods for personal data based on the purpose of data processing. This would reduce the amount of data available and the risk of profiling, surveillance, and breaches.

5.2. Cybersecurity risks

30. To establish the trust that citizens must have in order to be comfortable adopting and using CBDCs, high security must be in place. CBDCs rely on complex digital infrastructure and data storage

environment. Available at: https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf.

[24] See section 3.1.2 of Bank of Japan, Central Bank Digital Currency Experiments Results and Findings from Proof of Concept Phase 2, May 2003. Available at: https://www.boj.or.jp/en/paym/digital/dig230529a.pdf

[25] Id.

[26] D. Chaum. Blind signatures for untraceable payments. In Crypto'82, Plenum Press N.Y., 1983.

[27] J. Claessens, B. Preneel, J.Vanderwalle. Anonymity controlled electronic payment systems,1999. Available at: https://www.esat.kuleuven.be/cosic/publications/article-360.pdf.

[28] Auer, Raphael and Böhme, Rainer, The Technology of Retail Central Bank Digital Currency (March 1, 2020). BIS Quarterly Review, March 2020, Available at SSRN: https://ssrn.com/abstract=3561198.

[29] David Chaum, Christian Grothoff, & Thomas Moser, How to Issue a Central Bank Digital Currency, SNB Working Papers (Mar. 2021), https://www.snb.ch/en/publications/research/working-papers/2021/working_paper_2021_03.

systems and could be vulnerable to cyber-attacks[30] that could compromise users' financial security and privacy and the economy at large scale. Security concerns in the CBDC infrastructure may turn into severe consequences among stakeholders and a significant loss of trust from users, leading them to dismiss the CBDC as a viable payment option, thus resulting in the failure of the project. Recently, the need to ensure CBDC cybersecurity has attracted more focus[31] and targeted cybersecurity frameworks are being developed.[32]

31. Certain risks common in existing payment systems are also worth noting for CBDCs. Unauthorized access to credentials can compromise user accounts and personal data processed for a CBDC. Cyber attackers employ sophisticated techniques like social engineering, side-channel attacks, and malware to extract credentials from users' devices, leading to potentially disruptive consequences.

32. Moreover, the exponential increase in computing power due to the emergence of quantum computing poses a potential threat to financial services security. Quantum computers are able to compromise some existing data encryption methodologies and cryptographic primitives that currently protect the access, confidentiality, and integrity of stored and transmitted data.

33. Another critical security risk is the concentration of payment data, commonly referred to as "data concentration." If all CBDC user payment data were stored in a central bank's databases, it would create attractive incentives for cyberattacks and pose a high systemic risk. Data breaches or unlawful access to this concentrated data could result in individual or general widespread surveillance, loss of funds, fraud, and other harms to privacy and individual rights. Additionally, the possibility of denial-of-service attacks targeting a centralised database could disrupt all payment operations.

34. Alternatively, where a distributed architecture/technology is implemented, and in particular where data is stored on user devices, it becomes crucial to effectively minimize the risks associated with "double-spending" attacks, particularly in the offline, bearer-based configuration of a CBDC. These attacks involve illegitimately spending the CBDC multiple times, a form of counterfeiting.

35. Furthermore, while CBDCs are usually linked to a specific jurisdiction, risks due to interoperability and cross-border dimensions[33] can arise. Since central banks primarily focus on domestic CBDC applications, insufficient attention may be given to cross-border regulation, interoperability, and

[30] The Guardian. (2021). New Zealand's central bank says its systems have been hacked. Available at: https://www.theguardian.com/world/2021/jan/11/new-zealands-central-bank-says-its-systems-have-been-hacked

[31] 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/.

[32] BIS Innovation HUB, Project Polaris: a security and resilience framework for CBDC systems. Available at: https://www.bis.org/publ/othp70.htm.

[33] Ongoing pilots can contribute to raising awareness also on interoperability related privacy issues. E.g. see BIS Innovation HUB, Project Icebreaker: breaking new paths in cross-border retail CBDC payments, in particular section 6.6. Available at: https://www.bis.org/publ/othp61.htm

standardization. Transferring personal and transaction data across multiple jurisdictions may also amplify the scale, scope, and speed of potential data breaches.

Advice

36. Since CBDCs would be critical for people and economies, they must have well-defined and strong security governance and risk management processes, including adopting robust security measures to safeguard the CBDC infrastructure, protect user assets and data, and ensure resilience against cyber-attacks. In general, bank and payments services cybersecurity is already highly regulated and legally mandatory in some jurisdictions.

37. Collaborative efforts among cybersecurity constituencies are crucial to mitigate relevant risks and harmonize cybersecurity frameworks. This enables a level playing field and ensures safer interoperability without weak links. International standards must be established considering the minimum security measures CBDCs should comply with.

38. Specific and continuous care should be devoted to assessing technologies and algorithms. Open source solutions would be particularly helpful, to enable transparency and peer review, provided that an adequate open source governance and management is adopted and implemented within the CBDC project. Open source adoption would also foster inclusion and public buy-in.

39. When designing CBDC technologies, post-quantum cryptography must be considered, which can withstand the computing power of quantum systems and provide enhanced security measures. A common approach should be identified by central banks proposing CBDCs[34].

5.3. Unclear data protection roles and responsibilities

40. Based on the specific design choices made by the central bank, various actors (central banks, government, intermediaries, private companies acting as contractors) within the CBDC ecosystem may be involved in processing personal data. It is crucial to recognize the different data protection roles played by these actors to ensure compliance with applicable laws and ensure that individuals can effectively exercise their data protection rights. Particularly, when implementing a decentralized architecture, such as the ones based on Distributed Ledger Technology (DLT)[35], the governance structure and involvement of multiple actors in data processing can present specific challenges.

Advice

41. Identify responsibilities based on the applicable data protection law (e.g. controller(s) and processor(s) in the GDPR) to attribute accountability and obligations throughout the payment

[34] BIS Innovation HUB, Project Leap: quantum-proofing the financial system. Available at: https://www.bis.org/about/bisih/topics/cyber_security/leap.htm.
[35] See section 6.1

chain and other ancillary financial operations. Establishing clear governance and allocation of tasks between central banks and financial intermediaries is crucial in determining data protection obligations in a decentralized and multiparty environment, for example which entity is responsible for notification regarding a potential personal data breach or for addressing data subjects' rights, such as the right to information, access, or withdrawal of consent.

42. Establish clear communication channels and cooperation and coordination mechanisms. This includes data sharing agreements and implementing measures to ensure data subjects' rights are respected throughout the CBDC functioning, from the on-boarding forward. Collaborative efforts are vital to address the challenges associated with data protection in such a complex context.

5.4. Financial exclusion for specific individuals and vulnerable groups

43. 40. A CBDC will not increase financial inclusion by default. Whether a digital currency provides people on the margins of society with more access to the financial system or worsens existing divides is a question of CBDC design, implementation, and the social support provided to onboard more marginalized users.[36] A poorly designed CBDC risks leaving out people with less technical literacy, people without reliable internet access, poor communities, and undocumented/migrant communities. If CBDC is paired with the reduction or elimination of physical cash, the consequences for already marginalized populations could be severe. Financial exclusion falls into two categories that should be treated separately: accidental exclusion and intentional exclusion through state repression.

44. Accidental exclusion encompasses poor design choices that make a CBDC inaccessible to the average user or marginalized populations. For example, a CBDC that is fully intermediated by the existing banking system is unlikely to increase financial inclusion for individuals who do not currently trust the banks and refuse or are denied access to banking. In contrast, a tokenized CBDC holdable in any digital wallet might increase financial inclusion by facilitating online transactions for unbanked individuals.

45. Accidental exclusion may also result from poor policy around CBDCs. Less technically literate populations like older individuals and potentially individuals in rural communities may not automatically adopt a CBDC without social support and inclusive design. The same is true for individuals with disabilities who interact differently with their smartphones.

46. Intentional financial exclusion may result from specific decisions by governments to deny certain individuals or even certain groups and populations access to CBDCs, with a strong impact on individual’s rights and freedoms, as well from restriction for specific uses cases. Such exclusion may also be couched in terms of counter-terrorism or anti-money laundering efforts that fall

[36] Ashley Lanquist and Brandon Tan, Central Bank Digital Currency’s Role in Promoting Financial Inclusion, International Monetary Fund Fintech Notes (Sept. 2023), https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/22/Central-Bank-Digital-Currency-s-Role-in-Promoting-Financial-Inclusion-538728 .

disproportionately on minority populations, or be more explicitly targeted at ethnic/religious minorities or immigrants [37]. Systems that provide governments with the ability to cut off access to a CBDC for individuals or populations create greater risks of financial exclusion than systems that treat a CBDC as a cash-equivalent.

Advice

47. Governments considering implementing a CBDC should design systems from the ground up with financial inclusion in mind. This means meaningful disability accommodations from the outset and careful consideration of the special circumstances of all populations. Certain design choices are likely to increase adoption of CBDCs and also increase inclusion. These include offline and peer-to-peer payment capabilities, irrevocable confidentiality for retail-sized transactions, transparent and inter-operable design, and accessible privacy-protecting digital wallets.

48. Governments should also address inclusivity from the outset with policy. Specific outreach to marginalized populations can speed adoption, and governments should be diligent in providing accessible support services to onboard individuals to the system and troubleshoot problems.

49. Better anti-money laundering controls could focus on reduced confidentiality for transactions above a certain threshold limit and other targeted interventions. CBDC systems should be designed to limit governments' power to fully exclude individuals from access to a digital currency. Technical and organizational measures may be considered to share the power for critical actions among multiple entities. As an example, a cryptographic key needed for carrying out a critical operation could be split up and distributed among several entities ("secret sharing"). This measure could be useful more in general to implement joint governance for critical actions that have a strong impact on individuals rights and freedom.

5.5 Overall adoption and use of a CBDC: necessity and proportionality

50. When protecting privacy and fundamental rights, determining the necessity of processing certain personal data and operational proportionality balancing interference in the personal sphere compared to the objectives pursued, are two essential criteria.

51. Bearing these two criteria in mind, establishing a CBDC is a critical decision that must consider both benefits and costs, taking into account not only financial aspects, but also any harmful consequences to society and individuals rights, including privacy and personal data protection.

[37] In the United States, for example, some Members of Congress and Senate have considered that anti-money laundering policies have disproportionately targeted Arab and Muslim Americans and immigrants, resulting in denial of banking access for Americans with no connection to terrorism or financial crimes. See letter Elizabeth Warren, Ilhan Omar et al. to U.S. Banking Regulators on modernizing sanctioning and anti-money laundering/financial crimes compliance policies, U.S. Congress (Dec. 2, 2022), https://files.constantcontact.com/d51f5406801/55723f25-4c19-4c8c-ad57-943dbd461b2f.pdf.

52. If necessity and proportionality are not carefully considered throughout the CBDC creation process, the CBDC system could exercise unnecessary and disproportionate interference with fundamental rights, including privacy and personal data protection, contrary to what is expected in a democratic society. The CBDC's policy objectives, roles and responsibilities identified, features to implement, architectural and design choices planned, and the possible use of new technologies bearing specific risks all must be evaluated through the lens of necessity and proportionality.

Advice

53. CBDC project deployment should be driven by a clear and demonstrated necessity for a digital currency. This means that policymakers and central banks should carefully consider whether a CBDC is necessary to achieve their objectives, such as enhancing financial inclusion, reducing transaction costs, or improving monetary policy transmission. Deploying a CBDC should not be driven solely by the desire to keep up with technological trends or compete with other digital currencies. Unless there is a clear and demonstrated need for the CBDC, the privacy and data protection risks are likely to outweigh the benefits of creating a CBDC. By ensuring that the CBDC deployment is driven by a clear and demonstrated need, policymakers and central banks can better weigh the privacy and data protection risks associated with CBDCs against those needs when deciding whether to move forward.[38]

54. Once those needs are identified, the design of the CBDC should be driven by a privacy and data protection by design and by default approach[39]. A privacy and data protection impact assessment considering broader fundamental rights impacts should be carried out during the planning phases to evaluate the impact of the planned functionalities and use cases on individuals' rights and freedoms. Regular assessments should also be carried out throughout deployment, as some risks and impacts may not be apparent until the technology is in use.

55. The identified risks and impacts should lead to identifying adequate mitigating measures. A CBDC project should be designed in a way that minimizes the collection and use of personal information by ensuring that only the necessary information is collected and processed. Furthermore, the least intrusive processes and technologies should be identified and adopted. If, notwithstanding the efforts in this direction, the level of intrusiveness is still not acceptable from a proportionality standpoint, creators must reconsider the planned design, functionalities, information processing

[38] For an example of assessment (no endorsement): Bank of England. Central Bank Digital Currency: opportunities, challenges and design. (2020). Available at https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper.

[39] See for example the EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Despite they are based on the European Union GDPR, they convey useful recommendations and suggestions for all constituencies. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

architecture, and protocols necessary to reduce the impact, up to abandoning the project, if necessary.[40]Collaboration between policy makers, central banks, financial services regulators and data protection authorities is an important element of understanding and anticipating privacy harms. In addition, engagement between policy makers, central banks, financial services regulators and data protection authorities is an effective way to achieve the public trust needed for widespread adoption. These authorities should make use of (or develop) avenues for dialogue and co-operation, such as memoranda of understanding, digital regulatory co-operation fora, regulatory sandboxes, and ad hoc measures of consultation[41].

6. Privacy risks on some specific choices or components

56. In this section, we highlight a short selection of some privacy risks and relevant advice on specific choices for CBDC design or components. The below considerations are not exhaustive but a sample that might be helpful for policy makers and (if applicable) central banks when enacting frameworks and technical features for CBDCs.

6.1. The use of Distributed Ledger Technology (DLT)

Description

57. A distributed ledger is "a database that is consensually shared and synchronized across networks, spread across multiple sites, institutions, or geographies, allowing transactions to have [multiple private or] public 'witnesses'". [42] Blockchain is one example of a DLT.

58. DLT-based systems use a distributed ledger to record and verify transactions. Each participant on the network has a copy of the ledger, and any changes made to the ledger must be verified by a consensus mechanism before they are definitively added. Usually, participants are a range of different actors, such as banks, payment service providers, and other financial institutions.[43]

[40] Grimm, R., & Böhme, R. (2021). "Central Bank Digital Currencies: A Privacy Perspective." In Proceedings of the 17th International Conference on Privacy, Security and Trust (PST).

[41] Data protection authorities can provide expertise on the risks and measures for mitigating them and address data protection requirements, such as the principles of necessity, proportionality, and data minimization; the data governance and risk assessment process, including data protection impact assessments; issues with data sharing agreements; and any other requirements under applicable data protection laws.

[42] WORLD ECONOMIC FORUM, INNOVATION-DRIVEN CYBER-RISK TO CUSTOMER DATA IN FINANCIAL SERVICES – WHITE PAPER 6 (2017), https://www.weforum.org/whitepapers/innovation-driven-cyber-risk-to-customer-data-infinancial-service.

[43] As for the Riksbank e-Krona project. For more information see https://www.riksbank.se/en-gb/payments--cash/e-krona/technical-solution-for-the-e-krona-pilot/.

59. Once a transaction is added to the ledger, it is irreversible, providing a high degree of immutability and security. The use of cryptography ensures that only authorized parties can access the ledger and that transactions are authenticated and encrypted for confidentiality.[44]

60. While many DLT-based applications do not limit the participation of users in the system, a DLT-based CBDC system is usually configured to allow only authorized nodes to participate in the network. Here, the central bank oversees the system governance and settlement operations, ensuring that it functions efficiently, securely, and in accordance with regulatory and legal requirements. Moreover, it administrates the network nodes, updating the software and ensuring the system's scalability and resilience.[45]

61. Historically, central banks have experimented extensively with DLTs, somewhat influenced by private actors' efforts issuing and managing private digital money such as Bitcoin. The reportedly identified benefits in terms of integrity and transparency and potential use of smart contracts for programmable money also influence DLT use. Its distributed nodes infrastructure and consensus based operation implies that DLT architecture is frequently considered for operations such as wholesale payments among central banks and relevant intermediaries[46] as well as cross-border payments.[47]

62. CBDC projects around the world that use DLT-based settlement systems include:

    - China's Digital Currency Electronic Payment (DCEP). Developed by the People's Bank of China, the Digital Yuan is a digital version of China's fiat currency, the Renminbi.[48]

    - Sweden's e-Krona. The Riksbank, the central bank of Sweden, is exploring the development of the e-Krona, a proposed CBDC that would use DLT-based technology.[49]

[44] Swan, M. (2015). "Blockchain: blueprint for a new economy." O'Reilly Media, Inc – available at https://www.oreilly.com/library/view/blockchain/9781491920480/.

[45] BIS Working Papers – No 1015, DLT-Based Enhancement of Cross-Border Payment Efficiency – a Legal and Regulatory Perspective, May 2002. Available at: https://www.bis.org/publ/work1015.pdf.

[46] Demystifying wholesale central bank digital currency, Speech by Fabio Panetta, Member of the Executive Board of the ECB, at the Symposium on "Payments and Securities Settlement in Europe – today and tomorrow", 26 September 2002.

[47]World Bank Group, Central Bank digital currencies for cross-border payments, A review of current experiments and ideas, November 2021, available at: https://documents1.worldbank.org/curated/en/369001638871862939/pdf/Central-Bank-Digital-Currencies-for-Cross-border-Payments-A-Review-of-Current-Experiments-and-Ideas.pdf.

[48] For more information, see People's Bank of China. "Digital Currency (DC/EP)." https://www.pbc.gov.cn/en/3688110/index.html.

[49] For more information, see Riksbank. "The e-Krona Project." https://www.riksbank.se/en-gb/payments--cash/e-krona/.

- Digital Euro: For the back-end prototype, the Eurosystem developed a centralised settlement engine (N€XT), based on unspent transaction output (UTXO).[50]

Risks

63. Relying on a DLT architecture does not necessary entail a more privacy friendly solution. Lack of confidentiality is a risk to consider when implementing a DLT-based settlement system. In fact, data stored in distributed ledgers are natively visible to all participants on the network. This creates a high degree of transparency and auditability, which can be useful for preventing fraud and money laundering. However, it also raises concerns about privacy and confidentiality, as personal information such as transaction amounts and account balances may be visible to other parties on the network if adequate controls are not in place, in a way that deteriorates privacy protection even with respect to the current payments schema. This lack of confidentiality could deter some users from using CBDCs.[51]

64. Immutability of DLT solutions, such as blockchain, must also be considered. In a DLT, once data has been written to the ledger, it cannot be changed or deleted. While immutability provides significant benefits in terms of integrity, it also poses potential privacy risks. In particular, when personal data is written to the blockchain, it cannot be removed or corrected. This poses significant challenges for compliance with data protection rights such as the right to rectification, the 'right to erasure', or 'right to be forgotten'.

Advice

65. Limit personal data on-chain: data written directly to the chain should be limited, possibly only to non-personal data. Other personal data can be 'off-chain' and only the information strictly necessary to link to and account for the payer and the payee will be stored on the chain.

66. Give users more control over their personal information, such as the ability to selectively disclose certain transaction details to specific parties (be them central banks or intermediaries), or the ability to use pseudonyms to mask their identities. This could help to balance the need for transparency with the need for privacy and confidentiality.[52]

[50] For more information, see European Central Bank (2023), Digital euro – Prototype summary and lessons learned, available at https://www.ecb.europa.eu/pub/pdf/other/ecb.prototype_summary20230526~71d0b26d55.en.pdf.

[51] Cocco, L., Pinna, A., & Marchesi, M. (2017). "Banking on blockchain: costs savings thanks to the blockchain technology." Journal of Financial Perspectives, 5(3), 18-31.

[52] European Central Bank, IN FOCUS - Issue n°4, December 2019, Exploring anonymity in central bank digital currencies. Available at: https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

67. Design the DLT-based system to include privacy-enhancing features, such as zero-knowledge proofs, which could help to preserve the confidentiality of transaction information while still maintaining the integrity and security of the ledger.[53]

68. Verify whether it is possible to obtain equivalent (or better) features and performances by using non-DLT technology.[54] For example, smart contracts or PETs could be designed without necessarily using DLT.[55]

6.2. CBDC programmability

69. CBDC programmability means certain financial events can be programmed to take place as triggered by other events. In general, the literature distinguishes between programmability of payments and programmability of money.[56]

Description

Programmable payments

70. Programmable payments are payments that are executed automatically when certain conditions are met, based on pre-set rules. This is not a new feature that CBDCs might introduce, since programmable payments exist already in current bank payments systems (for example, standing orders or direct debits). In current CBDC plans, programmable payments are related to the use of smart contracts[57] based on DLT technology.

71. Programmable payments in a CBDC allow for the execution of time-bound transactions. This feature can be useful in scenarios such as payroll systems, where salaries can be automatically paid on predetermined dates. It also facilitates the automation of recurring payments, subscriptions, and contractual obligations. In a supply chain scenario, payment for goods can be automatically triggered once delivery confirmation is received. This feature ensures secure and transparent payments while reducing the risk of fraud or non-compliance with contractual terms. Finally, programmable payments in a CBDC can facilitate multi-party escrow arrangements so that funds

[53] Gross, Jonas and Sedlmeir, Johannes and Seiter, Simon, How to Design a Compliant, Privacy-Preserving Fiat Stablecoin Via Zero-Knowledge Proofs (December 15, 2022). Available at SSRN: https://ssrn.com/abstract=4331465 or http://dx.doi.org/10.2139/ssrn.4331465

[54] See footnote 46.

[55] Olaf Owe, Elahe Fazeldehkordi, A lightweight approach to smart contracts supporting safety, security, and privacy, Journal of Logical and Algebraic Methods in Programming, Volume 127, 2022, 100772. Available at: https://doi.org/10.1016/j.jlamp.2022.100772 .

[56] A.Bechtel, J.Gross, P.Sandner, V. von Wachter, Programmable Money and Programmable Payments, 29 September 2020. Available at: https://jonasgross.medium.com/programmable-money-and-programmable-payments-c0f06bbcd569.

[57] Singh, Jaskaran, Programmable Payments & Smart Contracts (July 15, 2022). Available at SSRN: https://ssrn.com/abstract=4215442 or http://dx.doi.org/10.2139/ssrn.4215442

are not transferred until all parties involved fulfil their obligations. This use case could be beneficial for complex transactions, such as real estate purchases or crowdfunding campaigns, where the release of funds is contingent upon the satisfaction of predefined conditions by multiple parties. Programmable payments enhance trust and security by automating the escrow process, reducing the need for intermediaries and minimizing the risk of disputes.

- Examples of CBDC projects around the world that consider the use of programmable payments are: the Digital Baht project by the Bank of Thailand[58], South Korea's Digital Won[59], and the European Central Bank Digital Euro.[60]

Programmable money

72. Programmable money refers to the ability to incorporate predefined rules and conditions into the digital currency itself. This means that the CBDC can be designed with the capability of automatically execute transactions based on predefined criteria. Again, smart contracts are the most explored example of this type of technology.

73. One example of programmable money's capabilities would be where a government decides to distribute a specific amount of money to certain citizens for cultural purposes, with the stipulation that these funds cannot be used for any other purpose. The government can encode the rules and conditions into the CBDC itself, ensuring that the funds are allocated solely for cultural activities. The payment can be automatically blocked if it is not directed towards those intended purposes. In this way, programmable money provides a powerful tool for governments, central banks, and other authorities to exert control over the use of funds, ensuring that they are utilized for specific purposes or within predefined parameters.

74. Programmable money could allow for real-time monitoring and auditing of specific transactions, enhancing regulatory oversight. By integrating programmable features into a CBDC, authorities could track the flow of funds, identify suspicious patterns or activities, and enforce transaction reporting requirements.

75. Moreover, programmable money could be used to automate compliance with regulatory frameworks. By incorporating the relevant rules and conditions within the CBDC infrastructure, the need for manual intervention and compliance checks can be reduced. In this way, the CBDC can automatically enforce regulatory requirements, such as limiting the size of transactions, implementing trading restrictions, or ensuring adherence to tax obligations.

[58] See https://www.bot.or.th/en/financial-innovation/digital-finance/central-bank-digital-currency.html
[59] https://www.bok.or.kr/eng/main/contents.do?menuNo=400411
[60] See ECB document: https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221110_item32programmablepayments.en.pdf

76. Examples of CBDC projects around the world that consider programmable money include:

- China's Digital Currency Electronic Payment (DCEP). The Digital Yuan is designed to allow programmable functionalities such as restrictions on usage, expiration dates, and smart contract capabilities.[61]
- Sweden's e-Krona.[62] The e-Krona project by Sveriges Riksbank, the central bank of Sweden, is considering programmable money features. The e-krona aims to enable programmable functionalities such as time-limited payments and transaction conditions through smart contracts.

Risks

77. Programmability features in CBDC inherently involve automated decision-making provisions, where algorithms and smart contracts execute transactions and enforce predefined rules. These automated processes analyse data and apply predefined algorithms to make decisions in real-time, such as verifying transaction validity, enforcing contractual terms, or determining eligibility for specific financial services. However, it is crucial to ensure that such automated decision-making processes adhere to legal and ethical standards, particularly in relation to data protection principles and individual rights, such as transparency and the rights to object, obtain human review and contest automated decisions.

78. Different programmable features of a CBDC present different privacy and civil rights risks that may outweigh the potential benefits. For example, restrictions on where money can be spent creates substantial risks of censorship and marginalisation of activities or even populations that governments consider undesirable. Time limits on spending a currency on the other hand can create many of the same policy benefits such as preventing currency hoarding and providing economic stimulus without involving the government in deciding which businesses are "worthy".

Advice

79. Transparency and accountability are essential requirements in a CBDC, and particularly programmable money systems. Organizations must provide individuals with clear information about how their data is processed, the logic behind automated decision-making, and the safeguards in place to ensure fairness and accuracy. Privacy policies should outline the data processing practices and individuals' rights, enabling users to exercise their rights when participating in programmable money systems.

80. When automated decision-making significantly affects individuals, a meaningful human intervention needs to be ensured, allowing individuals to contest decisions made solely by algorithms, and the right to obtain meaningful information about the logic involved in the

[61] See footnote 48
[62] See footnote 46

automated decision-making process and effective remedy when needed. Organizations operating programmable money systems need to implement mechanisms to enable this.

81. Legislators should consider whether certain programmable money features possibly having a severe impact on individuals' freedoms and democracy (e.g., preventing individuals or a category of individuals from spending money in a certain context) should ever be planned, to avoid that these could be unlawfully leveraged.

7. The case for peer-to-peer online and offline payments

82. Peer-to-peer on-line payments are typical payment schemes for cryptocurrencies, where money can be directly transferred without the need for intermediaries, such as a central bank, commercial banks, or payment processors, which can streamline the payment process and reduce financial costs as well as promote financial inclusion of unbanked people. Peer-to-peer online payments can also be components of a CBDC, in use cases where it has been established that there is no need for intermediation or immediate settlement of the single transaction. Peer-to-peer payments, including in the context of a CBDC scheme, can also take place between two offline devices (tokens) storing currency.

83. Peer-to-peer payments are not traced by central banks and intermediaries, thus ensuring privacy by design. As transactions occur directly between parties, users have more control over their personal information and can enjoy increased privacy compared to traditional, intermediated, and account-based payment systems. The peer-to-peer nature of CBDC transactions eliminates or reduces the reliance on centralized intermediaries, thereby excluding or minimizing their collection and storage of personal data. This can help mitigate concerns related to the potential misuse of personal information by intermediaries or the risk of data breaches.

84. Peer-to-peer payments have usually been considered only under certain circumstances, since their structure may hinder accountability and auditability, as well as necessary AML/CFT checks. Usually, if any, they are allowed for transactions under a certain amount or considering a transactions amount limit within a certain timeframe.

85. The decision to implement a peer-to-peer feature in a CBDC hinges on various factors, including the desired level of financial intermediation, the need for regulatory oversight, and the overarching goals of financial inclusion (for unbanked people) and efficiency. Therefore, the presence or absence of a peer-to-peer component in a CBDC is ultimately determined by the specific policy objectives of the central bank and the governing authorities.

86. Furthermore, online peer-to-peer payments still present some data protection risks. In general, whilst allowed in limited circumstances, they might share the same basic infrastructure and protocols as with intermediated payments. This entails that specific techniques have to be used in order to keep the needed confidentiality in the transactions.

87. Therefore, the CBDC system should collect and retain only necessary metadata while minimizing the disclosure of personally identifiable information. Mechanisms have to be considered that provide transactional validation while preserving user privacy. Techniques like zero-knowledge proofs can be explored to allow verification without revealing specific transaction details, thereby enhancing privacy in peer-to-peer CBDC transactions.[63]

88. Offline payments in the context of a CBDC present their own specific risks, due to their offline nature and because they are enabled by bearable devices such as smartphones, smartcards, and wearable devices. Challenges include the possibility of device loss or theft, device counterfeiting, the possible need to update their software when usually offline, and the need to keep secure the cryptographic key used for confidentiality and secure authentication. The use of devices such as smartphones, which are multi-purpose online devices, increases the attack surface.

89. Related risks include value loss, fraud (often due to instant payment and settlement), or double-spending (the possibility to spend multiple times the values stored in the device). It is essential to establish a specific risk-based approach tackling offline payments[64] . This is necessary to create a CBDC that aims to replace cash and keeps the promises for a privacy-preserving solution,[65] both offline and online.

90. CBDC projects around the world that are considering a peer-to-peer component include:

- The Bahamas' Sand Dollar,[66] a CBDC designed for the archipelago nation. The Sand Dollar includes a peer-to-peer component, allowing residents to transact directly with each other using the digital currency. This feature aims to promote financial inclusion and reduce reliance on cash transactions in remote areas, fostering economic efficiency and accessibility.

- Uruguay's e-Peso.[67] The Central Bank of Uruguay is developing the e-Peso, a CBDC project that includes a peer-to-peer component. The e-Peso aims to improve financial inclusion, reduce costs, and enhance the efficiency of payments within the country. With the peer-to-peer functionality, individuals and businesses can conduct direct transactions using the e-Peso, enabling secure and seamless digital payments.

- Sweden's e-Krona.[68] Sveriges Riksbank, the central bank of Sweden, is exploring the development of an e-Krona CBDC. The e-Krona project includes a peer-to-peer component

[63] See footnote 21.
[64] BIS Project Polaris: Part 1: A handbook for offline payments with CBDC, May 2023. Available at: https://www.bis.org/publ/othp64.htm
[65] Introductory statement by Fabio Panetta, Member of the Executive Board of the ECB, at the Committee on Economic and Monetary Affairs of the European Parliament, 4 September 2023. Available at: https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230904~8f5dff1e57.en.html
[66] For more information, see https://www.sanddollar.bs
[67] For more information, see https://www.bis.org/events/eopix_1810/licandro_pres.pdf
[68] See footnote 46

that allows individuals and businesses to make direct transactions using the digital currency. The aim is to create a secure and efficient payment infrastructure that can coexist alongside existing payment systems, enabling seamless peer-to-peer transfers.

- Digital Euro: the Proposal for a Regulation establishing a digital euro includes an offline modality for proximity (P2P) payments.[69]

8. Further reading

In addition to the references above, we would like to point out the following useful reading material.

- EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, 18 October 2023. Available at: https://edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/2023-10-18-edps-edpb-joint-opinion-digital-euro_en
- Bank of Canada report: “A Digital Canadian Dollar: What we heard 2020–23 and what comes next”. Available at: https://www.bankofcanada.ca/digitaldollar/a-digital-canadian-dollar-what-we-heard-2020-23-and-what-comes-next/
- AEPD blog post on “Digital Currencies”. Available at: https://www.aepd.es/en/prensa-y-comunicacion/blog/digital-currencies
- Reserve Bank of Australia, “Australian CBDC Pilot for Digital Finance Innovation”, project report, August 2023. Available at: https://www.rba.gov.au/payments-and-infrastructure/central-bank-digital-currency/pdf/australian-cbdc-pilot-for-digital-finance-innovation-project-report.pdf
- BIS Project Aurora, “The power of data, technology and collaboration to combat money laundering across institutions and borders”, May 2023. Available at: https://www.bis.org/about/bisih/topics/fmis/aurora.htm

[69] Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro COM/2023/369 final.