SUERF
The European Money and Finance Forum

SUERF Policy Note
Issue No 279, May 2022

Who comes after us? The correct mindset for designing a Central Bank Digital Currency






By Antoine d'Aligny, Emmanuel Benoist, Florian Dold, Christian Grothoff, Özgür Kesim and Martin Schanzenbach[1]

JEL codes: E42, E58.

Keywords: Retail CBDC, privacy, trust.

In December 2021 the European Central Bank (ECB) published a report on "Central Bank Digital Currency: functional scope, pricing and controls" in its Occasional Paper Series [BPT21], detailing various challenges for the Digital Euro. While the authors peripherally acknowledge the existence of token-based payment systems, the notion that a Digital Euro will somehow require citizens to have some kind of central bank account is pervasive in the paper. We argue that an account-based design cannot meet the ECB's stated design goals and that the ECB needs to fundamentally change its mindset when thinking about its role in the context of the Digital Euro if it wants the project to succeed. Along the same lines, the French National Council for Digitalization published a report on "Notes and Tokens, The New Competition of Currencies" [DGTV21]. Here, the authors make related incorrect claims about inevitable properties of Central Bank Digital Currencies (CBDCs), going as far as stating that a CBDC is not possible without an eID system. Our paper sets the record straight.

[1] **Antoine d'Aligny**, Bern University of Applied Sciences and EFREI Paris; **Emmanuel Benoist**, Bern University of Applied Sciences; **Florian Dold**, Taler Systems SA and The GNU Project; **Christian Grothoff**, Bern University of Applied Sciences, Taler Systems SA and The GNU Project; **Özgür Kesim**, Freie Universität Berlin; **Martin Schanzenbach**, Fraunhofer Institute for Applied and Integrated Security and The GNU Project.

Introduction

This article presents our comments regarding two papers that have been written by the European Central Bank (ECB) (Bindseil, Panetta, and Terol 2021) and the French National Council for Digitalization[2] (CNNum) (Dowek et al. 2021). As the French report is using some rather unclear definitions of currency, we will begin with a brief introduction of terms and technologies.

We will then explain why the ECB should not be the only guardian of the privacy of the European citizen and why coupling of a Central Bank Digital Currency (CBDC) with an identity system is a bad idea. We address a question raised in the ECB's report on the risks of a retail CBDCs promoting disintermediation to a degree that might threaten traditional banks.

Currency and payment systems

Currency is "something that is used as a medium of exchange; money."(Currency, n.d.). From the French dictionary, currency (i.e. la monnaie) is an "Instrument of measurement and conservation of value, legal means of exchanging goods"[3], or "Unit of value accepted and used in a country, a group of countries."[4] (Monnaie, n.d.) The main desired properties of a currency are therefore: conservation of value and availability for exchange.

For more than a hundred years, most currencies have been issued by central banks, while with the exception of cash, retail payment systems have typically been implemented by the private sector. In general, any payment system enables participants to make financial transactions, but does not in itself establish a new currency. Additionally, payment systems can provide credit, make transactions faster, cheaper, more private or more usable. Payment systems may require their users to trust payment system providers, as these intermediaries may introduce new failure modes into the system. As a result, payment service providers are generally regulated entities, at least when they deal with traditional fiat currencies.

There are two types of CBDCs, retail CBDCs and wholesale CBDCs. Wholesale CBDC is expected to be primarily used to trade between banks and between the central bank and banks. An example of wholesale CBDC can be found in the description of the project Helvetia of the Swiss National Bank (BIS 2020).[5] In contrast, a retail CBDC is intended to be used by citizens and businesses in their daily lives for their ordinary expenses, basically providing a form of digital cash that is, like physical cash, a liability of the central bank. This paper is about retail CBDCs. Our discussion will assume that the currency for the CBDC already exists, and thus focus on the requirements for the payment system that facilitates ordinary people to make digital transactions with such a currency.

[2] Conseil national du numérique

[3] "Instrument de mesure et de conservation de la valeur, moyen légal d'échange des biens."

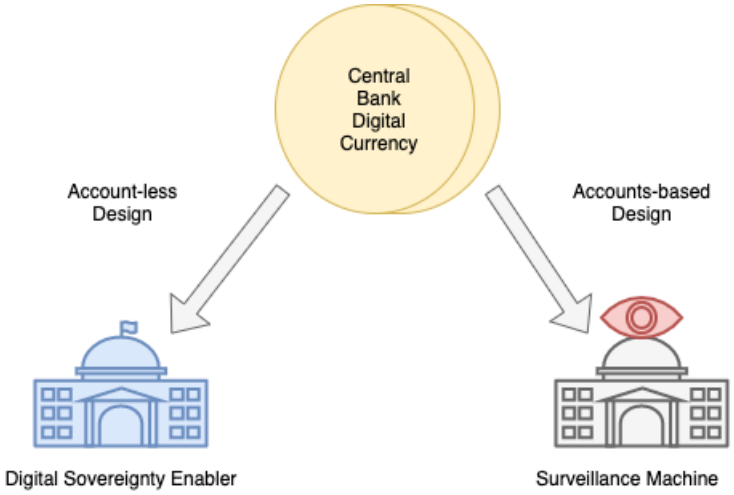
[4] "Unité de valeur admise et utilisée dans un pays, un ensemble de pays."

[5] We note that the French report confuses project Helvetia (which implements a wholesale CBDC) with an entirely different proposal (Chaum, Grothoff, and Moser 2021a) for a retail CBDC.

Central Banks cannot be the Guardian of Privacy

The ECB's report starts with a public interest-oriented self-image of central banks. For example, the authors claim that "central banks operate in the interest of society, setting goals in the public interest rather than private interest" and "as public and independent institutions, central banks have no interest in monetising users' payment data. They would only process such data to the extent necessary for performing their functions and in full compliance with public interest objectives and legislation." While this is a laudable aspiration, it is a false statement: The Bank of Greece, one of the central banks of the Eurosystem, is dominantly privately held and listed on the Athen's stock exchange (Greece 2016). Similar constructions with privately owned central banks exist outside of the Eurozone, for example with the Swiss National Bank (Bank 2020). That all central banks are independent and operate in the public interest is sometimes questioned in the popular press (Tecimer 2020). With counter-examples inside the European System of Central Banks (ECBS) itself and within Europe, it is clear one needs to be careful to avoid confusing the idealistic view of central banks as politically neutral and public-minded institutions with reality. To build secure systems, it is best to assume that all parties, including the system's designers, implementers and main operators themselves, could be malicious.

Central banks thus need to take a different mindset, and ideally picture themselves as malicious actors when working on the design of a CBDC. Only this way, they will avoid designs which would entrust them with information and decisions that they must not be entrusted with. For example, the ECB's report currently suggests that the ECB "may also prefer the (...) the ability to control the privacy of payments data". This is a fundamental misconception of the notion of privacy. Citizens will *only* have privacy with a Digital Euro if they themselves have control over their payment data. Privacy and the human right of informational self-determination requires that each (legally capable) citizen is in control of their personal data. A central bank asserting the "ability to control the privacy" is thus an oxymoron: once anyone else has control, citizens have no privacy. Public institutions that act in the public interest must acknowledge this to not patronize their sovereign: the citizens.



The French report (Dowek et al. 2021) correctly states that a Digital Euro based on accounts poses "democratic risks"[6] and could allow "state surveillance of all transactions of every individual"[7]. Subsequently the wording of the French report is misleading, as it turns the possibility of privacy-invasive monitoring into a mandatory

[6] "risques démocratiques"

[7] "surveillance de toutes les transactions de chaque individu par l'État"

feature of any CBDC, which is demonstrably false: There are many digital currencies and payment systems that do not allow comprehensive surveillance (Sun et al. 2017; Dold 2019). Thus, it is wrong for the authors of the French report to take a possible design choice of an account-based system as a necessity, for example when they write that "the centralization and data tracking of CBDC projects leads to a loss of privacy that coupled with the programmability of the currency can have serious consequences."[8] Using the indicative here is a serious mistake, as it is understood that any CBDC design would necessarily lead to a loss of privacy, when this is false.

Furthermore, the use of the term "surveillance" in the French report actually understates the negative impact of an account-based CBDC, as with an account-based CBDC the central bank would likely also be in a position to prevent individuals from spending money and to manipulate their balances, thereby gaining comprehensive power over the economic activities of individuals going far beyond mere analytical capabilities. The use of permissioned blockchains does not inherently prevent such manipulations as long as the participating operators are colluding. Thus, if European democratic ideals and personal freedoms are to prevail, we clearly cannot ignore this danger and must reestablish the principles of personal responsibility, personal independence and subsidiarity in the design processes for critical infrastructure created by European institutions.

Since this conjecture is taken as fact while counterexamples exists, the conclusion of the first part of the French report follows a logical fallacy. The authors assert that "the new properties of CBDC raise political questions"[9] which implies that the deployment of a CBDC would be impossible in the current state. But adaptations of central bank missions to include "absolute control over the rules and regulations of the use" of money via the issuance of a CBDC (as envisioned by Agustín Carstens of the Bank for International Settlements[10]) are dangerous if the central bank can choose to void privacy assurances. Carstens correctly states that with the proposed CBDC design the central bank would have the ability to know about every payment. Consequently, the central bank would be able to strictly enforce its rules and regulations, which implies the bank could arbitrarily block payments by private citizens. The repressive potential of a government with such a capability is so large that it must be firmly rejected.

Harmful coupling with identity

The risk is not theoretical. The Emergencies Act of February 2022 granted the Canadian executive the right to freeze bank accounts without judicial oversight. The Canadian minister of justice David Lametti promptly used this to threaten people on CTV News with extrajudicial asset freezes if they were making significant financial contributions to a political cause he strongly disagrees with.[11] If this is possible in Canada today, we do not want to imagine what might happen in less established democracies if an account-based CBDC were to largely displace cash.

[8] "Toutefois, la centralisation et la traçabilité des données des projets de monnaie numérique de banque centrale conduit à une perte de vie privée qui, associée à la programmabilité de la monnaie, peut avoir de lourdes conséquences."

[9] "Dans un contexte où les nombreux projets d'émettre des monnaies numériques viennent étendre le rôle des banques centrales se pose la question des enjeux démocratiques et politiques de ces nouveaux attributs."

[10] See speech given on October 19th 2020 on "Cross-Border Payment – A vision for the future", https://meetings.imf.org/en/2020/Annual/Schedule/2020/10/19/imf-cross-border-payments-a-vision-for-the-future at 00:24:30

[11] https://www.youtube.com/watch?v=xoTCxWSQW30

Consequently, the question should be if central banks should limit CBDC issuance within the scope of their current mission instead of modifying their rulebooks. The US Federal Reserve is currently barred from maintaining digital account balances for individuals (Board of Governers of the Federal Reserve System 2022). We consider this law wise, as we argue that tightly coupling payments with identity is harmful. While the law prevents the Federal Reserve's from issuing an account-based retail CBDC, it does not seem to prevent the Federal Reserve from issuing a token-based privacy-respecting CBDC. This is crucial, as the technology behind token-based privacy-respecting CBDCs would fundamentally not support the kind of asset freezes enabled by the Canadian Emergencies Act.

In contrast, ECB report suggests that "combining use of digital identity and CBDC" might be beneficial. The same idea is echoed in the French report which quotes an unpublished report from Catenae (2020) to say that "it is difficult to envisage the creation of a retail CBDC, and more specifically a Digital Euro without first creating a reliable, secure digital identity offering the necessary guarantees"[12]. From a technical perspective, the statement is hard to defend since payment systems exist that work perfectly well without depending on a "trusted digital identity".

From a regulatory perspective, it is understood that institutions working with a Digital Euro will at times be legally required to establish the identity of actors. However, when a Digital Euro needs a digital identity for some of the actors in the digital currency production chain, one can use existing Know-Your-Customer (KYC) processes of commercial banks or use certificates based on the already widely used X.509 standard, which are both already in common use on the Internet.[13] While we can imagine a world in which a new "trusted digital identity" exists, and develop new protocols for this world, this is by no means a prerequisite to any work on a Digital Euro. Waiting for the creation of a new trusted digital identity at the European level before creating a CBDC may be equivalent to postponing the decision indefinitely, and the necessity of first deploying a new electronic identity scheme is not shown by the authors.

What neither report appreciates is that combining payments with such a digital identity system would create a serious liability. Even if central banks were neutral custodians of citizens' privacy (see Section 3), the problem is the data itself. As Bruce Schneier has concisely argued already in 2016: "Data is a toxic asset. We need to start thinking about it as such, and treat it as we would any other source of toxicity. To do anything else is to risk our security and privacy." (Schneier 2016) Despite this well-established insight, the ECB report is insinuating to link identities with payments which consequently and inevitably produces highly sensitive[14] metadata. Referring to the toxicity of this metadata, Edward Snowden famously said at IETF 93 in 2019 that

> "(...) we need to get away from true-name payments on the Internet. The credit card payment system is one of the worst things that happened for the user, in terms of being able to divorce their access from their identity."

If the European Union wants to avoid a dystopia of the transparent citizen and catastrophic cases of personal data theft, it must enable citizens to put a firewall between their identity and their payments.

---

[12] "il est difficile d'envisager la création d'une monnaie numérique de banque centrale de détail, et plus particulièrement d'un "euro numérique", sans création préalable d'une identité numérique fiable, sécurisée et offrant les garanties nécessaires."

[13] They correspond to the "s" in "https", for example.

[14] Or to stick with Schneier's analogy, "super-toxic"

Citizens themselves are well aware of this aspect and it consequently would have a significant impact on acceptance of a CBDC: The Swiss population recently rejected a proposal for a national eID (Eidgenössische Justiz- und Polizeidepartement EJPD 2021), and the newly elected German government is promising a reversal of ubiquitous data retention (without cause) (SPD, Grünen, and FDP 2021). The European Parliament has members proposing to ban the use of facial recognition in public spaces (Commitee for Civil Liberties, Justice and Home Affairs 2020). The ECB's proposal seemingly ignores the popular rejection of treating every citizen as a criminal suspect by doubling down. The missing link in the ECB proposal that would reveal the dystopic reality they would invoke would be a statement that facial recognition could be used to conveniently establish the payer's identity – or "pay with your smile", as contemporary account-based digital payment offerings already put it. We stress that CBDC payment data, like other payment data, can be expected to be retained for 6 or more years (Financial Conduct Authority 2022). If CBDC payment data is additionally strongly coupled with our identities, those who dislike living in a panopticon could only hope for such a CBDC to be rarely used.

Addressing Balance Sheet Disintermediation via Self-Custody

The ECB report describes the risk of (commercial) bank balance sheet disintermediation as one of the major risks to consider from the introduction of a CBDC. Basically, the risk is that consumers losing faith in a commercial bank may shift funds into CBDC, thereby exacerbating the situation by creating a "bank run". The ECB report discusses various strategies, but primarily focuses on limiting "hoarding" of CBDC by imposing a balance limit. They then realize that this can be quite difficult, as businesses may have varying needs for CBDC, so a fixed low limit would strangle the utility of the CBDC, while a fixed high limit may not be effective. They then propose a dynamic limit which they would "calculate in accordance to (...) presumed cash needs".

Here, the authors might want to review some of the hard lessons from the introduction of CO_2 emissions certificates, where initial allocations were calculated based on "presumed emission needs" of certain industries, resulting in windfalls for shifty polluters that managed to rig the calculations, giving them excess certificates that they could then resell. (Coelho 2012) If CBDC holdings are limited and financially attractive, there will clearly again be businesses profiting from organizing their business data to obtain high account limits. This kind of socially unproductive optimization will happen regardless of the specific rules that the ECB will design. Thus, this is a fundamentally flawed design.

The ECB's focus on account-based solutions seems to have caused it to ignore a better solution that was proposed in (Chaum, Grothoff, and Moser 2021b), even though it was clearly on the table: When justifying the need to control hoarding of CBDC, the authors write that "risk-free assets have a negative yield (apart from banknotes, which are costly and risky to store in large amounts)". Here, they presume that hoarding CBDC must be risk-free. However, with Digital Euros represented as tokens that citizens hold in self-custody, the CBDC would not be risk-free: citizens would have to safeguard their digital devices (both physically and against malware). Thus, a CBDC design using digital tokens under the control of citizens indirectly provides a good solution for hoarding, as self-custody of the digital assets entails a risk, quite comparable to the risk of hoarding cash. By analyzing this risk, citizens and businesses would themselves determine appropriate individual limits for their CBDC holdings based on their actual cash needs.

Conclusion

There are no trusted third parties. That does not prevent people from designing and deploying systems that rely on the assumption that a trusted third party exists. Central banks must not follow the former DIRNSA's hubris (Appelbaum 2022, 6f) and assert that they are an eternally trusted third party.

The dominance of accounts on the Internet and the resulting delegation of economic and political power to big Internet service providers sets a dangerous precedent for the design of CBDCs. It is time for central banks to abandon this account-centric mindset, which will help them address privacy issues and help the Internet transcend surveillance capitalism.

More specifically, the ECB needs to review its design approach for the Digital Euro and commit to granting financial sovereignty to its constituents. Instead of controlling the citizen's privacy and forcing a particular ECB App onto CBDC user's phones, the ECB needs to design a Digital Euro based on respect for the citizen's sovereignty and self-responsibility. A digital cash system can be build using privacy-preserving open protocols with Free Software reference implementations. The resulting self-responsibility of citizens will address various key design challenges inherent to account-based designs, including the biggest challenge of all: creating a product citizens would actually like to use. ■

References

Appelbaum, J. 2022. "Communication in a World of Pervasive Surveillance." PhD thesis, TU Eindhoven.

Bank, Swiss National. 2020. "Breakdown of Share Ownership." https://www.snb.ch/en/mmr/reference/shares_structure/source/shares_structure.en.pdf.

Bindseil, Ulrich, Fabio Panetta, and Ignacio Terol. 2021. "Central Bank Digital Currency: Functional Scope, Pricing and Controls." *ECB Occasional Paper*, no. 2021/286.

BIS. 2020. "Project Helvetia Phase I: Settling Tokenised Assets in Central Bank Money." https://www.bis.org/publ/othp35.pdf.

Board of Governers of the Federal Reserve System. 2022. "Money and Payments: The U.S. Digital Dollar in the Age of Digital Transformation." United States Federal Reserve.

Chaum, David, Christian Grothoff, and Thomas Moser. 2021a. "How to Issue a Central Bank Digital Currency." In *SNB Working Papers*. 2021-3. Swiss National Bank.

———. 2021b. "How to issue a central bank digital currency." *SNB Working Paper Series*. https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03.

Coelho, Ricardo. 2012. *Green Is the Color of Money: The Eu Ets Failure as a Model for the "Green Economy"*. Edited by Joanna Cabello and Tamra Gilbertson. Carbon Trade Watch.

Commitee for Civil Liberties, Justice and Home Affairs. 2020. "Motion for a European Parliament resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters." https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html.

Currency. n.d. "Dictionary.com." {https://www.dictionary.com/browse/currency}.

Dold, Florian. 2019. "The Gnu Taler System." PhD thesis, L'university de Rennes 1.

Dowek, Gilles, Elisabeth Grosdhomme, Joëlle Toledano, and Jean-Marc Vittori. 2021. "Billets et Jetons — La Nouvelle Concurrence Des Monnaies." *Counseil National Du Numerique*, 44.

Eidgenössische Justiz- und Polizeidepartement EJPD. 2021. "Elektronische Identität: das E-ID-Gesetz." https://www.ejpd.admin.ch/ejpd/de/home/themen/abstimmungen/bgeid.html.

Financial Conduct Authority. 2022. "FCA Retention Schedule." https://www.fca.org.uk/publication/systems-information/retention-schedule.pdf.

continued

Greece, Bank of. 2016. “Statute of the Bank of Greece, Tenth Edition.” https://www.bankofgreece.gr/en/the-bank/legal-framework/statute.

Monnaie. n.d. “Dictionnaire Le Robert.” https://dictionnaire.lerobert.com/definition/monnaie.

Schneier, Bruce. 2016. “Data Is a Toxic Asset, so Why Not Throw It Out?” https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html.

SPD, Bündnis 90/Die Grünen, and FDP. 2021. “Mehr Fortschritt Wagen - Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit.” *Koalitionsvertrag Zwischen SPD, Bündnis 90/Die Grünen Und FDP*. https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

Sun, Shi-Feng, Man Ho Au, Joseph K Liu, and Tsz Hon Yuen. 2017. “RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero.” In *European Symposium on Research in Computer Security*, 456–74. Springer.

Tecimer, Cem. 2020. “‘Is the Turkish Central Bank Independent?’ as an Uninteresting Question.” https://dx.doi.org/10.17176/20201118-161945-0. https://doi.org/10.17176/20201118-161945-0.

About the authors

Antoine d’Aligny is a postgraduate student at EFREI Paris, he worked as an intern at the Bern University of Applied Sciences for the project “Depolymerizer” where he developed a solution for using Taler for off-chain payments using Bitcoin and Ethereum.

Emmanuel Benoist is professor for computer science at the Bern University of Applied Sciences, his research is aimed at privacy protection for the Internet. The two main areas of research are e-health and Darknet markets since for both topics, privacy protection is a central asset.

Florian Dold is co-founder and CTO of Taler S.A. He works as a board member in the GNUNet project. He received a PhD from the University of Rennes for research done at INRIA Rennes.

Özgür Kesim is a PhD condidate at the work-group 'Internet Technologies' at the FU Berlin with advisor Prof. Dr. Matthias Wählisch. He is also CEO of Code Blau GmbH, a IT security consulting firm from Berlin, Germany, for the last 20 years.

Christian Grothoff is professor for computer network security at the Bern University of Applied Sciences, researching future Internet architectures. His research interests include compilers, programming languages, software engineering, networking, security and privacy.

Dr. Martin Schanzenbach is head of the research group "Applied Privacy Technologies" at the Fraunhofer Institute for Applied and Integrated Security (AISEC). His areas of expertise include identity management, privacy-enhancing technologies and secure distributed systems. In the context of various research activities and projects he is researching self-sovereign identity management systems, peer-to-peer technologies and secure name systems.

SUERF Publications

Find more **SUERF Policy Notes** and **Policy Briefs** at www.suerf.org/policynotes

SUERF
The European Money and Finance Forum

SUERF is a network association of central bankers and regulators, academics, and practitioners in the financial sector. The focus of the association is on the analysis, discussion and understanding of financial markets and institutions, the monetary economy, the conduct of regulation, supervision and monetary policy. SUERF's events and publications provide a unique European network for the analysis and discussion of these and related issues.

SUERF Policy Notes focus on current financial, monetary or economic issues, designed for policy makers and financial practitioners, authored by renowned experts.

The views expressed are those of the author(s) and not necessarily those of the institution(s) the author(s) is/are affiliated with.

SUERF Secretariat
c/o OeNB
Otto-Wagner-Platz 3
A-1090 Vienna, Austria
Phone: +43-1-40420-7206
www.suerf.org • suerf@oenb.at