Cental Bank Accounts are Dangerous and Unnecessary
A critique of two papers*

Antoine d'Aligny[△£], Emmanuel Benoist[△], Florian Dold[†♡], Christian Grothoff[△†♡], Özgür Kesim[§], and Martin Schanzenbach[‡♡]

[△]Bern University of Applied Sciences
[£]École d'Ingénieurs Généraliste du Numérique
[†]Taler Systems SA
[§]Freie Universität Berlin
[‡]Fraunhofer Institute for Applied and Integrated Security
[♡]The GNU Project

March 4, 2022

Abstract

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.

JEL Classification Codes: E42, E58
Keywords: retail CBDC, privacy, crypto-currency, trust

*We thank Martin Summer for encouraging us to put our critique of the ECB's report in writing. We thank central bankers for their good aspirations, which they should keep up even if we question their universal realization.

1 Introduction

This article presents our comments regarding two papers that have been written by the European Central Bank (ECB) [BPT21] and the French National Council for Digitalization[1] (CNNum) [DGTV21]. As the French report is using some rather unclear definitions of currency and crypto-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.

The second part of this paper proposes a set of design principles that any retail CBDC must integrate. We then argue that a retail CBDC based on GNU Taler would not only satisfy these principles, but also could provide an added value over existing commercial solutions for a retail CBDC. Finally, we explain how tokenization can help to build an eGold payment system or a system allowing micropayments in Bitcoins and Ethereum.

2 Currency, crypto-currency and payment systems

Currency is "something that is used as a medium of exchange; money."[Cur]. From the French dictionary, currency (i.e. la monnaie) is an "Instrument of measurement and conservation of value, legal means of exchanging goods"[2], or "Unit of value accepted and used in a country, a group of countries."[3] [Mon] The main desired properties of a currency are therefore: conservation of value and availability for exchange.

For more than a hundred years, most currencies were issued by central banks. Over the last decade a large number of new crypto-currencies have appeared, and these currencies are not tied to any central bank. The first and best known of them is Bitcoin [Nak08]. The various crypto-currencies are very heterogeneous and based on different principles. Some use accounts with balances with a blockchain used to establish a consensus on the account balances (Bitcoin was the first currency to use it), while others allow the transfer of fungible tokens that are disassociated from any transaction history (Zcash [HBHW16]). Among those using a blockchain, some use proof of work (Bitcoin, Ethereum), others use proof of stake (Ethereum, expected in Q2 2022 [mer22, Nel21]) or most recently proof of wasted human lifetime (Play to Earn [But21]). Some are rather transparent (Bitcoin, Ethereum), while others allow private transactions (Monero [Noe15]).

[1] Conseil national du numérique

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

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

Crypto-currencies do not have a central bank controlling the rules governing the currency. Instead, software developers program rules into algorithms. New rules are adopted if they find the consensus of the "miners" (for crypto-currencies using proof of work) or "stakeholders" (for crypto-currencies using proof of stake). In general, the rules are written to produce some artificial scarcity of the currency minted according to the rules, so as to convince hoarders of the value of their limited-edition bitstrings. A key design challenge is thus to provide ample rewards to "miners" and "stakeholders" that facilitate transactions while maintaining a limited supply.

Crypto-currencies are beginning to gain functionalities through the addition of payment systems on top of these basic currency mechanisms. In general, any payment system enables participants to make financial transactions, but does not in itself establish a new currency. Compared to the transaction mechanisms offered by the underlying currency, 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. Examples for payment systems used with crypto-currencies include the various proprietary crypto-trading platforms as well as distributed layer-2 solutions like the Lightning network [LPS+20].

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 [BIS20].[4] 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.

3 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,

[4] We note that the French report confuses project Helvetia (which implements a wholesale CBDC) with an entirely different proposal [CGM21a] for a retail CBDC.

one of the central banks of the Eurosystem, is dominantly privately held and listed on the Athen's stock exchange [oG16]. Similar constructions with privately owned central banks exist outside of the Eurozone, for example with the Swiss National Bank [Ban20]. That all central banks are independent and operate in the public interest is sometimes questioned in the popular press [Tec20]. 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, implementors and main operators themselves, could be malicious.

Central banks thus need to take a different mindset, and idally picture themeselves 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 [DGTV21] correctly states that a Digital Euro based on accounts poses "democratic risks"[5] and could allow "state surveillance of all transactions of every individual"[6]. Subsequently the wording of the French report is misleading, as it turns the possibility of privacy-invasive monitoring into a mandatory feature of any CBDC, which is demonstrably false: There are many digital currencies and payment systems that do not allow comprehensive surveillance [SALY17, Dol19]. 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."[7] 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

[5] risques démocratiques

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

[7] 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.

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"[8] 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 Agustin Carstens of the Bank of International Settlement[9]) are dangerous if the central bank can choose to void privacy assurances. Carsten's reasons include that the central bank should have the ability to know about every payment. As he states that the central bank would be able to strictly enforce its rules and regulations, this 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.

4 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.[10] 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.

Consequently, the question should be if central banks should limit CBDC issuance within the scope of their current mission instead of modifying their rulebooks. Wisely, the US Federal Reserve is currently barred from maintaining digital account balances for individuals [Boa22]. 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.

[8] "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."

[9] See speech given on October 19th 2020 on "Cross-Border Payment – A vision for the future"

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

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"[11]. From a technical perspective, the statement is hard to defend since current cryptocurrencies 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.[12] 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." [Sch16] Despite this well-established insight, the ECB report is insinuating to link identities with payments which consequently and inevitably produces highly sensitive[13] 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.

Citizens themselves are well aware of this aspect and it consequently would have a significant impact on acceptance of a CDBC: The Swiss population recently rejected a proposal for a national eID [Eid21], and the newly elected German government is promising a reversal of ubiquitous data retention (without cause) [SGF21]. The European Parlia-

[11] 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

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

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

ment has members proposing to ban the use of facial recognition in public spaces [Com20]. 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 [Fin22]. 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.

5 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. [Coe12] 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 [CGM21b], 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). Owners of cryptocurrencies are very familiar with the fact that self-custody is risky [Cim20, Gus21]. 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.

6 Design principles for CBDCs

We think that any CBDC must be based on the following design principles inspired by [Dol19], given in order of priority:

1. **A CBDC must be implemented as Free Software.**

   Free refers to "free as in free speech", as opposed to "free as in free beer". More specifically, the four essential freedoms of free software [Sta02] must be respected, namely users must have the freedom to (1) run the software, (2) study and modify it, (3) redistribute copies, and (4) distribute copies of the modified version.

   This prevents vendor lock-in, as another software provider can take over, should the current one provide inadequate quality of service. Only Free Software can be seen as truly respecting the sovereignty of citizens using the software, as well as countries relying on it. As the ECB report states, international or even cross-border use of a CBDC may be desireable, but this excludes solutions that would be under the control of one nation unless we presume that nations will be willing to subject critical infrastructure to the whims of other nations. Recent attacks by the US government against Huawei effectively limited Huawei's ability to use US software [Smi20]. Such political games can cause significant suffering for the population when they impact critical infrastructure. It is thus clear that only domestic or Free Software is acceptable for critical infrastructure of sovereign countries. Cross-border payments using the same payment system require at least one country to use non-domestic software. Thus, only with Free Software all countries and organizations can run the payment system without the risk of being controlled by foreign entities. Customers benefit from this freedom, as the wallet software can be made to run on a variety of platforms, and user-hostile features such as tracking or telemetry could easily be removed from wallet software.

   This rules out the mandatory usage of specialized hardware such as smart cards or other hardware security modules, as the software they run cannot be modified by the user. These components can, however, be voluntarily used by merchants, customers or payment processors to increase their operational security.

2. **A CBDC must protect the privacy of buyers.** Where possible, privacy should be guaranteed via technical measures as opposed to mere organizational policies. Especially with micropayments for online content, a disproportionate amount of rather private data about buyers would be revealed, if the payment system does not have privacy protections.

In legislations with data protection regulations (such as the recently introduced GDPR in Europe [VVdB17]), merchants benefit from this as well, as no data breach of customers can happen if this information is, by design, not collected in the first place. Obviously some private data, such as the shipping address for a physical delivery, must still be collected according to business needs.

The security of the payment systems also benefits from this, as the model shifts from authentication of customers to mere authorization of payments. This approach rules out whole classes of attacks such as phishing [GPCR07] or credit card fraud [SD10].

3. **A CBDC must enable the state to tax income and crack down on illegal business activities.**

   Naturally, a central bank cannot deploy a payment system that does not meet broadly accepted rules and regulations for payment systems. While it is conceivable that specific rules and regulations may be modified to accomodate a CBDC, it is inconceivable that states would relax the rules to the point where businesses receiving income are not held accountable for their actions, especially as there seems to be a broad consensus that levying of taxes based on economic activity is beneficial to society.

4. **A CBDC must prevent payment fraud.**

   This imposes requirements on the security of the system, as well as on the general design, as payment fraud can also happen through misleading user interface design or the lack of cryptographic evidence for certain processes.

5. **A CBDC must only disclose the minimal amount of information necessary.**

   The reason behind this goal is similar to (2). The privacy of buyers is given priority, but other parties such as merchants still benefit from it, for example, by keeping details about the merchant's financials hidden from competitors. Similarly, the central bank should not know all the details of say the contract between a merchant and a consumer, and only learn the amount transacted. Other state agencies, such as the tax office during a tax audit, may be able to compell merchants to disclose additional information, but again always only the minimal amount necessary for the specific function.

6. **A CBDC must be usable.**

   Specifically it must be usable for non-expert customers, such as children. We note that account-based payments are generally not accessible to children, as they are often unable to open a regular bank account under current rules. This alone is a good reason for a CBDC to not be account-based! Usability also applies to the integration with merchants, and informs choices about the architecture, such as encapsulating procedures that require cryptographic operations into an isolated component with a simple API.

7. **A CBDC must be efficient.**

   Approaches such as proof of work are ruled out by this requirement. Efficiency is necessary for a CBDC to scale to the hundreds

of thousands of transactions required to support larger economic areas. Efficient payments can also open up new use-cases by enabling micropayments.

8. **A CBDC must avoid single points of failure.**
   While a central bank is itself kind-of a single point of failure and inherent in a CBDC, the technical deployment should avoid single points of failure. This manifests in architectural choices such as the isolation of certain components, and auditing procedures.

9. **A CBDC must foster competition.**
   It must be relatively easy for various commercial businesses to operate components of the overall payment system. While the barriers for this in traditional financial systems are rather high, the technical burden for new operators to join must be minimized. Operators may incluce licensed entities such as banks (for operations that are closely related to the payment processing), but also unlicensed entities can partake in activities such as enabling backups or integrating payment services at retailers. A design choice that supports this is to split the whole system into smaller components with well-defined protocols between them, such that the various components can be operated, developed and improved upon independently, instead of having one completely monolithic system.

In our opinion, any candidate for CBDC must follow at least those principles to be trustworthy and successful.

A cross-cutting concern here is that when achieving the security goals, the CBDC must never rely on the central bank being trustworthy. Good security designs always strive to avoid trusted parties. This implies that neither the correctness nor the privacy assurances must rely on an honest central bank. This false sense of security also became evident when the former director of the NSA (DIRNSA) revealed his belief that with respect to control over the toxic data assets accumulated by the NSA "nobody comes after us" [App22, page 6f], suggesting that the (by the DIRNSA clearly presumed trustworthy) US government would never fall. The assumption turned deadly when the Taliban took over personal profiles including biometric data of Afgahnis that had collaborated with NATO forces after the retreat of NATO in 2021 [Hu21]. We must not make the same mistake, that is believing that our institutions are good and eternal, when it comes to our private payment data. Thus, it is necessary that technical protections for our privacy are put in place that even the central bank cannot break:

Privacy is most meaningful when it is guaranteed via technical measures, as opposed to mere policies. Without a technical layer providing privacy-by-default, financial transactions reveal unnecessary levels of personal or private data. This would be especially true if a CBDC became a ubiquitous payment method. Thus, a CBDC must protect the privacy of buyers and avoid the use of accounts to avoid facilitating totalitarian control over the population. Limited private data, such as the shipping address for a physical delivery, may need to be collected by merchants (but not the central bank) according to business needs and protected ac-

cording to local laws. In this case, the CBDC must enable deletion of such data as soon as it is no longer required.

A possible trap for the design of a privacy-respecting CBDC is central banks merely delegating responsibility for privacy-sensitive data to commercial banks. Such a delegation does not provide adequate protection against state overreach, as commercial banks still could too easily be compelled to sanction opposition against the ruling party. Nevertheless, Auer's proposal [AB21] to delegate the technical operation of a CBDC to tightly supervised commercial banks as an alternative to the central bank acquiring the technological prowess to centrally operate such a system has merit: such a delegation can eliminate a likely single point of failure, and might entice commercial banks to diversify the feature set. It would also give commercial banks a raison d'être, and thus mitigate the risks from CBDC disintermediation. In order for commercial banks to make a valuable contribution when operating the CBDC, we believe the central bank would still need to set an open standard to ensure interoperability. Strict cryptographically-enforced privacy-assurances for consumers must be baked into such a standard.

7 GNU Taler

We have implemented the GNU Taler token-based payment system based on the above principles [Dol19]. GNU Taler offers an alternative to ID/account-based systems, while still enabling the state to ensure business is legal (and tax-paying) without infringing on the sovereignty of private citizens.

In addition, CBDCs should also provide additional benefits compared to existing digital payment systems. One of the key questions the ECB report raises is what it might take for a CBDC to be successful in the market, as the authors realize that even if a central bank offers a payment system, this does not assure that the population will adopt it to a meaningful extend.

So far, we have already given several reasons for adoption, including the use of Free Software, the protection of privacy, usability and cost-effectiveness. Furthermore, we believe that a CBDC should also strongly consider the issue of inclusion, from children to illiterate or innumerate users which are underserved by contemporary commercial payment solutions. When it comes to serving children, age-verification for Websites is a related domain where digital identity-based solutions are inappropriately pursued today: With Taler, we can cryptographically extend the principle of strictly protected privacy also into the domain of age restrictions in e-commerce [Kes21]. By integrating age restrictions with privacy-preserving payments, we can enable legal guardians to protect their wards without contributing to the conversion of sovereign citizens to digital subjects. This extension offers benefits for society in multiple ways: Buyers remain anonymous during payment, yet efficacy of age restriction is guaranteed. Anonmyous age restriction during payment simplifies processees for merchants significantly. It is based on the principle of subsidiarity and gives control over age restriction to closest responsible persons (gen-

erally the parents). And finally, for more than 5 million children in the European Union between 10 and 18 [Eur] this would allow participation in e-commerce more freely.

Assuming that owners of bank-accounts are mature adults, it allows them to withdraw age-restricted coins for their wards. The wards can then anonymously spend the coins, but transactions will fail at merchants that sell goods with an age restriction exceeding the age-limit of the coins as specified by the bank account holder, acting as a guardian. This design guarantees that the only information disclosed is that the age-restriction imposed by the merchant is satisfied - but not the age itself. The payment service provider does not even learn that age-restrictions are being used, and merchants cannot distinguish successful purchases by adults from successful purchases by wards with a sufficiently high age-limit. Thus, this design offers a clear alternative to identity-based age-verification that is better aligned with the principle of subsidiarity which requires that we solve problems at the smallest unit that can solve them. And protecting the children should be the task of their parents. We argue that the ECB should merely give the parents the technical means to protect their children as they see fit, instead of taking control.

8 Tokenization beyond CBDC

With electronic tokens it is possible to implement payment systems that are not CBDCs. For example, a Swiss group around Claudio Zanetti [14] is considering launching an electronic payment system based on gold. Direct payments with physical gold are problematic, as giving change is impractical with gold as is the validation that the gold is pure. With eGold, Zanetti plans to "establish a private competitor to the Swiss National Bank, that is not able to deflate economic crises by inflating the currency at the expense of the working class".[15] It remains to be seen if this effective limitation on central bank policy making is ultimately beneficial, given the ecological cost of mining gold and the detrimental effect of rampant economic crises on the poor. Regardless, the idea is interesting as it may require governments to take a more preventative stance against economic crises — and economists (naturally ignoring the global environmental impact of mining gold) have previously claimed that a competing gold-backed payment system might be inherently beneficial to the (Swiss) economy [Ber12].

Systems like Bitcoin and Ethereum that are based on distributed ledger technology (DLT) are often confused with true token-based systems. In Bitcoin and Ethereum funds are still stored in accounts that have a value because of an incoming transaction, and not because some issuer backs the token. With the Depolymerizer [16] we have created an adapter that allows the tokenization of blockchain-based cryptocurrencies. Here, the cryptocurrency would be held in escrow by a trusted third party that backs the tokens representing Bitcoin or Ether. By reducing the need for

[14] `https://www.zanetti.ch/`
[15] Personal communication.
[16] `https://git.taler.net/depolymerization.git`

on-chain transactions, we expect that a Depolymerized DLT can in theory scale linearly with the available computational resources, primarily limited by the much slower transaction rate of the underlying DLT for inbound and outbound on-chain transactions. The resulting system would also provide durable transactions within milliseconds, making cryptocurrency payments significantly more practical. However, like with e-gold it would do nothing to mitigate the environmental cost of (cryptocurrency) mining, so fiat currency remains an environmentally preferable choice.

For the conversion between fiat currency, e-gold and Depolymerizer-tokenized cryptocurrencies it is likely that regulated payment service providers will be required to perform some kind of KYC procedure to identify their customers. However, this is no different from identification procedures required by banks today, and hence hardly predicated on the creation of a national or even global electronic identity platform with its associated dangers for individual freedom and democracy [Hel19, DGTV21].

An interesting aspect that all these electronic payment systems based on a tokenization system would share is that they require some trust into the issuer of the currency, as in all cases the issuer could renegotiate on its promise to redeem the electronic tokens for the underlying asset. For such systems it should be possible for third parties to audit the issuer of tokens [Dol19], which in the absence of fractional reserve banking reduces the risk from the issuer to that of the underlying asset class.

We note that issuer risk always exists and this mitigation is crucial. With cryptocurrencies, an issuer (like a cryptocurrency exchange) defaulting is a type of exit scam commonly called a "rug pull" for cryptocurrency "investments". [Phe21] For (largely historic) currencies tied to gold such a "default" was legalized by calling it "abandoning the gold standard" or "currency reform". We note that even modern fiat currencies usually have some limited backing in the form of assets held by the central bank that the central bank is expected to wisely use these assets to stabilize the value of its currency. Here, the equivalent of an exit scam is hyperinflation from quickly balooning central bank liabilities. The effect is equivalent to an exit scam, as it again effectively disowns the holders of the central-bank backed tokens. Hence, even central bank liabilities are hardly "risk-free assets", a final questionable claim repatedly made in the ECB's report. The same assumption of the Euro not requiring trust into the ECB is made in the French report. In their section on trust, the authors try to contrast "natural" trust in fiat currencies with "abnormal" trust for cryptocurrencies. The authors write that "While trust in money has long relied on a mechanical guarantee in gold or the role of the state, neither of these guarantees of trust exist for cryptocurrencies."[17]. Here, the authors pretend to be unaware that the Euro is neither based on a mechanical guarantee in gold (first abandoned in France during the First World War and then definitively under the Popular Front almost a century ago), nor on the role of a state since the Eurozone has none of the prerogatives of a state (army, tax, foreign policy, or even government).

Confidence in fiat currencies is much more complex than what is de-

[17] Si la confiance en la monnaie a longtemps reposé sur une garantie mécanique en or ou sur le rôle de l'État, aucun de ces gages de confiance existent pour les cryptomonnaies.

scribed in the French report, and one must at least include the following elements:

- confidence in the non-inflationary nature of the currency (it can be hoarded without significant risk)
- confidence in the stability of the exchange rate (it is safe to trade with other assets)
- confidence in the banking system (that assets will not disappear overnight)

All these properties are currently those of the major European currencies, even if this has not always been the case. From this perspective, we can see that some of the large crypto-currencies also more or less respect these criteria (with some problems on the side of price stability).

9 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 hybris [App22, page 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

[AB21] Raphael Auer and Rainer Böhme. Central bank digital currency: the quest for minimally invasive technology. BIS Working Papers 948, Bank of International Settlement, June 2021.

[App22] J. Appelbaum. *Communication in a world of pervasive surveillance*. PhD thesis, TU Eindhoven, February 2022.

[Ban20] Swiss National Bank. Breakdown of share ownership. `https://www.snb.ch/en/mmr/reference/shares_structure/source/shares_structure.en.pdf`, 2020.

[Ber12] Peter Bernholz. Eine franken-gold-kombination brächte mehr sicherheit. *Neue Zürcher Zeitung*, (113):31, May 2012.

[BIS20] BIS. Project helvetia phase i: Settling tokenised assets in central bank money. `https://www.bis.org/publ/othp35.pdf`, December 2020.

[Boa22] Board of Governers of the Federal Reserve System. Money and Payments: The U.S. Digital Dollar in the Age of Digital Transformation. Technical report, United States Federal Reserve, January 2022. `https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf`.

[BPT21] Ulrich Bindseil, Fabio Panetta, and Ignacio Terol. Central bank digital currency: functional scope, pricing and controls. *ECB Occasional Paper*, (2021/286), 2021.

[But21] Paul Butler. "play-to-earn" and bullshit jobs. `https://paulbutler.org/2021/play-to-earn-and-bullshit-jobs/`, December 2021.

[CGM21a] David Chaum, Christian Grothoff, and Thomas Moser. How to issue a central bank digital currency. In *SNB Working Papers*, number 2021-3. Swiss National Bank, February 2021.

[CGM21b] David Chaum, Christian Grothoff, and Thomas Moser. How to issue a central bank digital currency. *SNB working paper series*, 2021.

[Cim20] Catalin Cimpanu. Bitcoin wallet update trick has netted criminals more than $22 million. `https://www.zdnet.com/article/bitcoin-wallet-trick-has-netted-criminals-more-than-22-million/`, 2020.

[Coe12] Ricardo Coelho. *Green is the Color of Money: The EU ETS failure as a model for the "green economy"*. Carbon Trade Watch, June 2012.

[Com20] (European) Commitee for Civil Liberties, Justice and Home Affairs. 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`, 2020.

[Cur] Currency. Dictionary.com. `{https://www.dictionary.com/browse/currency}`.

[DGTV21] Gilles Dowek, Elisabeth Grosdhomme, Joëlle Toledano, and Jean-Marc Vittori. Billets et jetons — la nouvelle concurrence des monnaies. *Counseil National Du Numerique*, page 44, November 2021. `https://cnnumerique.fr/nos-travaux/billets-et-jetons-la-nouvelle-concurrence-des-monnaies`.

[Dol19] Florian Dold. *The GNU Taler System*. PhD thesis, L'university de Rennes 1, 2019.

[Eid21] Eidgenössische Justiz- und Polizeidepartement EJPD. Elektronische Identität: das E-ID-Gesetz. https://www.ejpd.admin.ch/ejpd/de/home/themen/abstimmungen/bgeid.html, 2021.

[Eur] Eurostat. Population on 1 January by age and sex (Europa, Altersgruppe 10). https://bit.ly/32iWEyV.

[Fin22] Financial Conduct Authority. Fca retention schedule. https://www.fca.org.uk/publication/systems-information/retention-schedule.pdf, February 2022.

[GPCR07] Sujata Garera, Niels Provos, Monica Chew, and Aviel D Rubin. A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM workshop on Recurring malcode*, pages 1–8. ACM, 2007.

[Gus21] Samuel Gush. How hackers hack crypto wallets, and how to protect yourself. https://www.makeuseof.com/how-hackers-hack-crypto-wallets/, 2021.

[HBHW16] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash protocol specification. https://raw.githubusercontent.com/zcash/zips/master/protocol/protocol.pdf, 2016.

[Hel19] Dirk Helbing. *Digital Fascism Rising?*, pages 99–102. Springer International Publishing, Cham, 2019.

[Hu21] Margaret Hu. The taliban reportedly have control of us biometric devices – a lesson in life-and-death consequences of data privacy. https://theconversation.com/the-taliban-reportedly-have-control-of-us-biometric-devices, 2021.

[Kes21] Özgür Kesim. Anonymous Age Restriction Extension for GNU Taler. https://docs.taler.net/design-documents/024-age-restriction.html, 2021.

[LPS+20] Jian-Hong Lin, Kevin Primicerio, Tiziano Squartini, Christian Decker, and Claudio J Tessone. Lightning network: a second path towards centralisation of the bitcoin economy. *New Journal of Physics*, 22(8):083022, aug 2020.

[mer22] The merge. https://ethereum.org/en/upgrades/merge, 2022.

[Mon] Monnaie. Dictionnaire Le Robert. https://dictionnaire.lerobert.com/definition/monnaie.

[Nak08] Satoshi Nakamoto. Re: Bitcoin p2p e-cash paper. *The Cryptography Mailing List*, 2008.

[Nel21] Matt Nelson. The state of the merge: An update on ethereum's merge to proof of stake in 2022. https://consensys.net/blog/news/the-state-of-the-merge-an-update-on-ethereums-merge-to-proof-of-stake-in-2022/, 2021.

[Noe15] Shen Noether. Ring signature confidential transactions for monero. *IACR Cryptol. ePrint Arch.*, 2015:1098, 2015.

[oG16] Bank of Greece. Statute of the bank of greece, tenth edition. `https://www.bankofgreece.gr/en/the-bank/legal-framework/statute`, 2016.

[Phe21] Phemex. What is a rug pull and how can you avoid one? `https://phemex.com/academy/what-is-a-rug-pull`, August 2021.

[SALY17] Shi-Feng Sun, Man Ho Au, Joseph K Liu, and Tsz Hon Yuen. Ringct 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In *European Symposium on Research in Computer Security*, pages 456–474. Springer, 2017.

[Sch16] Bruce Schneier. 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`, March 2016.

[SD10] Y Sahin and E Duman. An overview of business domains where fraud can take place, and a survey of various fraud detection techniques. In *Proceedings of the 1st international symposium on computing in science and engineering, Aydin, Turkey*, 2010.

[SGF21] SPD, Bündnis 90/Die Grünen, and FDP. Mehr Fortschritt Wagen - Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. `https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf`, 2021.

[Smi20] Adam Smith. Huawei ban: Trump extends executive order against china tech firms. *The Independent*, May 2020.

[Sta02] Richard Stallman. *Free software, free society: Selected essays of Richard M. Stallman*. Lulu.com, 2002.

[Tec20] Cem Tecimer. "Is the Turkish Central Bank Independent?" as an Uninteresting Question. `https://dx.doi.org/10.17176/20201118-161945-0`, November 2020.

[VVdB17] Paul Voigt and Axel Von dem Bussche. *The EU General Data Protection Regulation (GDPR)*, volume 18. Springer, 2017.