SUERF
The European Money and Finance Forum

SUERF Policy Briefs
No 114, June 2021

How to issue a privacy-preserving central bank digital currency


By Christian Grothoff and Thomas Moser[1]

JEL codes: E42, E51, E52, E58, G2.

Keywords: Central Bank Digital Currency, privacy, blind signatures.

Many central banks are currently investigating Central Bank Digital Currency (CBDC) and possible designs. A recent survey conducted by the European Central Bank has found that both citizens and professionals consider privacy the most important feature of a CBDC. We show how a central bank could issue a CBDC that would be easily scalable and allow the preservation of a key feature of physical cash: transaction privacy. At the same time the proposed design would meet regulatory requirements and thus offer an appropriate balance between privacy and legal compliance.

Introduction

A central bank digital currency (CBDC) for the general public would be a new type of money issued by central banks, alongside banknotes and reserve accounts for selected financial market participants. Despite initial skepticism, the number of central banks investigating CBDC has grown steadily over the past three years. However, there is currently no consensus on how a CBDC should be designed and what features it should have. These questions are being intensively debated and researched.

[1] Christian Grothoff, Bern University of Applied Sciences and Taler Systems SA.
Thomas Moser, Swiss National Bank.

A recent survey conducted by the European Central Bank has found that both citizens and professionals consider privacy the most important feature of a digital Euro (ECB 2021). This may be surprising, but the fact that citizens place a high value on privacy is a consistent finding of many surveys. Skeptics sometimes counter that citizens express just the opposite in their behavior; they consistently choose convenience, speed, and financial savings over privacy. However, in doing so they are often not fully aware of the extent to which technological advances have improved the ability to track, aggregate, and disseminate personal information. They also often do not expect their data to be shared and used in a context other than the one in which they disclose the data (Nissenbaum 2010).

Over the past decade, the public has become increasingly aware and concerned about the vast scale of data collected and stored by governments and corporations. Goldfarb and Tucker (2012) provide behavior-based evidence of increasing consumer privacy concerns. Payments data are particularly revealing, and a CBDC could potentially provide a great deal of data on citizens, making them vulnerable to malicious use for political or commercial purposes. We thus believe that a successful CBDC would need to provide credible transaction protections in order to gain broad public acceptance. Moreover, privacy is not just an individual value, it also has a social value. Privacy is essential for a free society and democracy.

At the same time, a CBDC should not provide protection for illegal transactions and tax evasion. A privacy-preserving CBDC must ensure legal compliance, particularly compliance with anti-money laundering (AML) and combating the financing of terrorism (CFT) regimes. It is thus crucial to find the right balance between privacy and legal compliance. We believe that our proposal recently published as a Swiss National Bank Working Paper promises to do just that (Chaum et al. 2021). It builds on and improves the eCash technology (Chaum, 1983, and Chaum et al. 1990) and uses GNU Taler (Dold, 2019). Taler is part of the GNU project, which is a collaborative project for the development of "Free/Libre and Open Source Software" (FLOSS).[2] With FLOSS, all interested parties have access to the source code and the right to tailor the software to their needs. The patent-free, open standard protocol improves interoperability and competition among service providers. Instead of using proprietary secrets or hardware security modules, Taler exclusively uses cryptographic software with public specifications to provide privacy and security.

Privacy in payments: accounts versus tokens

Payment systems can be account-based or token-based. In an account-based system, a payment is made by debiting the payer's account and crediting the payee's account. This implies that the transaction must be recorded and involved parties identified. In a token-based system, a payment is made by transferring a token that represents monetary value. The prime example is cash – coins or banknotes. Paying with cash means handing over a coin or banknote. There is no need to record the transfer or identify the parties involved, possession of the token is sufficient. However, the payee must be able to verify the token's authenticity.

It has been suggested that the distinction between account- and token-based systems is not applicable to digital currencies (Garratt et al. 2020). We believe that the distinction is also useful for digital currencies. The critical distinction is the information carried by the information asset. In an account-based system, the assets (accounts) are associated with transaction histories that include all of the credit and debit operations involving the accounts. In a token-based system, the assets (tokens) carry information about their value and the entity that issued the

[2] For more information about GNU, see https://www.gnu.org. GNU Taler is released free of charge under the GNU Affero General Public License by the GNU Project. GNU projects popular among economists are the software packages «R» and "GNU Regression, Econometrics and Time-series Library" (GRETL).

token. The only possibility of attaining the transaction privacy property of cash, therefore, lies in token-based systems.

We propose a token-based, software-only CBDC, where the CBDC token is issued and distributed just like banknotes. Consequently, we will simply refer to these CBDC tokens as "coins." Customers withdraw coins by withdrawing money from their bank account; that is, they load coins onto their smartphone or computer and their bank debits their account for the corresponding amount. The proposed CBDC is genuine digital bearer instrument; it is stored locally on the computer or smartphone; there is no account or ledger involved. There is also no record linking the CBDC and the owner.

Privacy is achieved with a cryptographic technique called blind signatures. Before the user interacts with the central bank to obtain a digitally signed coin, a blinding operation performed locally on the user's device hides the numeric value representing a coin from the central bank before requesting the signature. In GNU Taler, this numeric value is a public key, with the associated private key only being known to the owner of the coin. The coin derives its value from the central bank's signature on the coin's public key. The central bank makes the signature with its own private key. A merchant or payee can use the central bank's corresponding "public key" to verify the central bank's signature and thereby the authenticity of the CBDC.

Because the blind signatures are carried out under the control of the users themselves, users do not have to trust the central bank or the commercial bank to safeguard their private spending history. The central bank only learns the total amounts of digital cash withdrawn and the total amount spent. Commercial banks learn how much digital cash their customers withdraw, but not how much an individual customer has spent or where they are spending it. Privacy in this design is thus not a question of confidentiality; it is cryptographically guaranteed.

The benefits of NOT using Distributed Ledger Technology (DLT) for CBDC

Most central banks experiment with distributed ledger technology (DLT). DLT is an interesting design if no central party is available or desired: the purpose of a blockchain or DLT is to establish an immutable consensus across multiple parties. However, this is not required in the case for a retail CBDC issued by a trusted central bank. Distributing the central bank's ledger merely increases transaction costs; it does not provide tangible benefits in a central bank deployment.

A critical benefit of not using DLT is improved scalability. Our proposed scheme would be easily scalable and as cost-effective as modern RTGS systems currently used by central banks. GNU Taler can easily handle tens of thousands of transactions per second. The main cost of the system would be the secure storage of 1-10 kilobytes per transaction. Using Amazon Web Services pricing, experiments with an earlier prototype of GNU Taler showed that the cost of the system (memory, bandwidth, and computation) at scale would be less than USD 0.0001 per transaction.

Furthermore, achieving privacy with DLT is a challenge, because DLT is essentially an account-based system. The only difference to a traditional account-based system is that the accounts are not kept in a central database but in a decentralized append-only database.

Cryptographic privacy-enhancing technologies such as zero-knowledge proofs are possible but computationally demanding in a DLT-context, so that the high resource requirements make their use on mobile devices impractical. This does not apply to the Chaum-style blind signature protocol used in GNU Taler, which can be executed efficiently and quickly.

How to prevent double-spending in a token-based system

Money has value only when it is scarce, which means, among other things, that double-spending of a monetary asset is prevented. In a token-based system, one way to prevent double spending is to make it difficult to copy the token. This is the approach that central banks take with banknotes. With digital currencies, however, preventing copying is a challenge. Two potential technologies to prevent digital copying are unclonable functions and secure zones in hardware. However, physically unclonable functions cannot be exchanged over the Internet (eliminating the main use case of CBDCs), and security features in copy-prevention hardware have been repeatedly compromised.

Our proposal, which consists only of software, does not even attempt to prevent token copying. Rather, double spending is prevented by the fact that each coin can be spent exactly once only. Once a coin has been spent, the number of the corresponding coin goes on a list of spent coins managed by the central bank. This list contains only the number of the spent coin but no transaction history. The coins also cannot be linked to the payers because they blinded the coins when the CBDC was withdrawn. When a payee receives a coin, the payee consults this list to see if the coin has already been spent before. If it has, the payment is rejected as invalid.

Because our proposal requires online checks to prevent double-spending it does not enable offline payments. While this could be considered a disadvantage, Grothoff and Dold (2021) point out that any offline payment system has inherent and severe risks and thus its own drawbacks. Given that central banks do not intend to replace physical cash with CBDC, but rather to issue CBDC in addition to physical cash, physical cash can be used as the secure offline fallback in the event of power outages or cyber attacks.

Regulatory and policy consideration

In the proposed scheme, central banks do not learn the identities of consumers or merchants or transaction amounts. Central banks only see when electronic coins are withdrawn and when they are redeemed. Commercial banks continue to provide crucial customer and merchant authentication and, in particular, remain the guardians of know-your customer information. Commercial banks observe when merchants receive funds and can limit the amount of CBDC per transaction that an individual merchant may receive, if required. Additionally, transactions are associated with the relevant customer contracts. The resulting income transparency enables the system to be compliant with the AML/CFT regulations.

The proposed scheme thus offers one-sided privacy, allowing the buyer to remain anonymous while making the seller's incoming transactions and underlying contractual obligations available upon request by competent authorities. If unusual patterns of merchant income are detected, the commercial bank, tax authorities, or law enforcement can obtain and inspect the business contracts underlying the payments to determine whether the suspicious activity is nefarious. Overall, the system implements privacy-by-design and privacy-by default approaches (as required by the EU’s General Data Protection Regulation). Merchants do not inherently learn the identity of their customers, banks have only necessary insights into their own customers’ activities, and central banks are blissfully divorced from detailed knowledge of citizens’ activities.

A potential financial stability concern often raised with retail CBDCs is banking sector disintermediation. While this would be a serious concern with an account-based CBDC, it should be less of a concern with a token-based CBDC. Hoarding a token-based CBDC entails risks of theft or loss similar to those of hoarding cash. However, should hoarding or massive conversions of money from bank deposits to CBDC become a problem, the proposed

design would give central banks several options, including imposing per-account withdrawal limits or negative interest rates.

Imposing limits could also be a requirement of the AML/CFT regime. While GNU Taler by design allows its users to transact any amount in any currency, legislation could impose an enforceable ceiling on individual transactions, requiring merchants that receive transactions exceeding the transaction limit to determine the identity of the buyer. However, since there are no accounts, it would not be possible to impose holding limits. But this is a good thing. Technologically enforced restrictions on holding or receiving CBDC should be avoided anyway, as such restrictions would result in failures where users are unable to execute transactions despite sufficient liquidity.

With the proposed design, central banks, commerce and citizens could reap the full benefits of the digital economy. The efficiency and cost effectiveness, along with the improved consumer usability that comes from shifting from authentication to authorization, make this system likely the first to support the long-envisioned goal of online micropayments. In addition, the use of coins to cryptographically sign electronic contracts would enable the use of smart contracts. This could lead to the emergence of entirely new applications for payment systems.

A recently designed extension for GNU Taler integrates privacy-preserving age verification that allows legal guardians to impose age restrictions on digital purchases made with coins given to wards. Merchants would only learn that the buyer meets the age requirement for the goods sold, while the identity and exact age of the child would remain private. This is just one example of how central banks could use this system to issue programmable money.

References

Chaum, David (1983). “Blind signatures for untraceable payments.” Advances in Cryptology: Proceedings of Crypto ‘82, Vol. 82, No. 3, pp. 199–203.

Chaum, David, Amos Fiat, and Moni Naor (1990). “Untraceable electronic cash.” Advances in Cryptology: Proceedings of CRYPTO '88, pp. 319–327.

Chaum, David, Christian Grothoff, and Thomas Moser (2021). How to issue a central bank digital currency. SNB Working Papers 3/2021.

Dold, Florian (2019). The GNU Taler System: Practical and Provably Secure Electronic Payments. PhD Thesis, University of Rennes 1.

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

Garratt, Rod, Michael Lee, Brendan Malone, and Antoine Martin (2020). “Token- or Account-Based? A Digital Currency Can Be Both.” Liberty Street Economics, Federal Reserve Bank of New York.

Goldfarb, Avi, and Catherine Tucker (2012). "Shifts in Privacy Concerns." American Economic Review, 102 (3): 349-53.

Grothoff, Christian and Florian Dold (2021). Why a Digital Euro should be Online-first and Bearer-based. https://taler.net/papers/euro-bearer-online-2021.pdf

Nissenbaum, Helen (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

About the authors

Christian Grothoff *is a 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. Before, he was leading the Décentralisé research team at INRIA and an Emmy Noeter research group leader at TU Munich. He earned his PhD in computer science from UCLA, an M.S. in computer science from Purdue University, and a Diplom in mathematics from the University of Wuppertal. He is an Ashoka Fellow and co-founder of Taler Systems SA and Anastasis SARL. He also served as an expert court witness, and has reported on technology and national security as a freelance journalist.*

Thomas Moser *is an Alternate Member of the Governing Board of the Swiss National Bank. Before joining the Swiss National Bank, he was an Executive Director at the International Monetary Fund (IMF), and earlier in his career an Economist at the Swiss Institute for Business Cycle Research (KOF) at the Swiss Federal Institute of Technology (ETH), Zurich. Thomas Moser is also a member of the Managing Committee of the Swiss Institute of Banking and Finance at the University of St. Gallen, a Member of the Board of Directors of Orell Füssli Ltd., and a Member of the Advisory Board of the NZZ Swiss International Finance Forum. Thomas Moser holds a Master and a Doctorate in Economics from the University of Zurich.*

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