Staff memo

On the possibility of a cash-like CBDC

Hanna Armelius,

Carl Andreas Claussen and

Isaiah Hull

Payments Department and Research Division

February 2021

Contents

Summary[1]

We explain why all CBDCs will need a ledger that keeps track of CBDC ownership regardless of whether they are "token-based", "DLT-based" or "on a blockchain"; and regardless of how we define these terms. Consequently, token-based CBDCs appear not to have a greater capacity for providing payments that are peer-to-peer, offline or anonymous like cash than "account-based" CBDCs.

[1] We would like to thank colleagues at the Riksbank for comments and numerous discussions. Remaining mistakes are our own. The views expressed in this paper are those of the authors and do not necessarily coincide with the views of the Executive Board or the Staff of Sveriges Riksbank.

"A coin cannot be a simple file, and a transactions cannot be a transmission of the file from one user to another: Had it been done this way, the sender could have kept her copy, thus keeping the coin while also sending it." Allen S. et al. (2020, p. 14)

1 Introduction

Many central banks are exploring whether they should issue a digital complement to cash, a so called retail Central Bank Digital Currency (CBDC). Like physical cash, the CBDC will be central bank issued money that can be used for everyday payments, denominated in the national currency and exchangeable at par with commercial bank money.

A key question is which format the CBDC should take: should it be cash-like or more like money in deposit accounts? In CBDC discussions this question is often phrased as a question of whether the CBDC should be account-based or token-based. The latter term is then used as a shorthand for CBDC design choices that allow for offline, per-to-peer and anonymous payments.

In this paper we argue that the tokens versus accounts distinction appears irrelevant if we are interested in whether a CBDC has these cash-like properties. This irrelevance originates from the fact that all CBDC payments will involve reconciliation with one or more remote ledgers. This is the case regardless of whether the CBDC is account-based or token-based and regardless of what we mean by "token" and where this token is stored. For CBDCs involving balances on CBDC accounts, this is obvious. For token-based CBDCs it follows from two facts. First, token-based technologies for CBDCs are typically technologies where the tokens are not stored on local devices, but remotely. Second, if tokens are stored locally, payments with these tokens will still eventually have to reconcile with a ledger. This is due to the so called double-spending problem, which results from the ease with which locally stored digital tokens can be copied. This problem means that locally stored tokens cannot function as money unless the central bank takes a large risk or there is a remote ledger that keeps track of their transactions and/or ownership.

As all CBDC payments involve a remote ledger, no CBDC can be genuinely peer-to-peer, offline and anonymous like cash. CBDCs can still be somewhat peer-to-peer, somewhat offline and somewhat anonymous, but we see no major difference between a token- and account-based CBDCs in terms of the degree to which they can deliver these properties. This does not necessarily mean that a token-based system for supplying CBDCs is without benefits. New token-based technologies may offer new opportunities for efficiency or other advancements. Our point is simply that central banks should investigate and invest in these technologies for the right reason. That reason should not be to supply a digital cash-like CBDC.

In comparison to the existing discussion, our contribution (if any) is that we provide an easy-to-read and intuitive explanation of the following:[2] a CBDC-token – defined as sequences of bits – can be "stored" on a local device or remotely. If CBDC-tokens are stored remotely, it follows, by definition, that CBDC payments cannot be offline, peer-to-peer or anonymous like cash payments. If they are stored locally, they cannot function as money unless there is also a remote ledger that keeps track of their ownership. Thus, locally stored tokens cannot offer offline, peer-to-peer or anonymous payments like cash. We refer to relevant literature in the main text.

The paper is organized as follows: in section 2 we explain why all CBDC payments require reconciling a remote ledger. In section 3 we discuss the consequences of this fact for the peer-to-peer features, offline capability, anonymity and privacy features of a CBDC. Section 4 concludes.

2 All CBDC payments involve a remote ledger

In the following section we focus on token-based CBDC designs. CBDC solutions where users hold money balances (not tokens) on accounts will necessarily require a remote ledger that keeps record of balances and transactions. This is also the case if the central bank only provides the accounts, but is not responsible for user-facing and account-servicing functions on them.

2.1 What is a CBDC token?

Although there is much talk about token-based CBDCs, the term "token" itself is often not defined. In some cases, "token-based CBDC" is used as shorthand for an idealized CBDC design – rather than a specific technical instantiation – where it is assumed that payments can be made without the involvement of a trusted third party or reconciliation with a ledger (e.g. Bordo and Levin, 2017; and Bouchaud et al., 2020).[3] Such work is often concerned with exploring the theoretical implications of such idealized CBDCs, irrespective of whether they are technically feasible to implement. Others define token-based CBDCs as CBDC systems that rely on the ability of the payee to verify the validity of the payment object rather than ownership of the object (e.g. CPMI, 2018).[4] In this case, a "token" can simply be a balance on an account. Finally, and often intertwined in these definitions, many think of a token-based CBDC as building on "new

[2] Similar conclusions can be found in, for instance, Bank of England (2020, p. 47).

[3] Bordo and Levin (2017) puts it this way: "Should CBDC payments involve transfers between accounts held at the central bank, or digital "tokens" that can be transferred directly from payer to payee?" Bouchaud et al. (2020) writes the following: "The transfer of a token from one party to another does not require reconciling two databases, but is rather the near-immediate transfer of ownership, very much like handing over banknotes from one person to another." Similar statements appears in many CBDC-papers.

[4] This also appears many places, see for instance Securities and Markets Stakeholder Group, (2018) p. 4, paragraph 12: "The term 'token' is more neutral as it does not carry the implicit legitimacy of 'currency'. It is a broad term that encompasses many virtual assets and can be defined by opposing it to account-based assets. An account-based system relies on the ability to verify the identity of the owner, while a token-based one relies on the ability to verify the validity of the token itself."

technology" like blockchain or a distributed ledger (e.g. Bordo and Levin, 2017; Yao, 2018).

In this paper we use a general definition of CBDC token which is consistent with any of the three uses of the term balance-based CBDC above:

Definition: A *CBDC token* is a digital object that (i) has a given value expressed in the national unit of account and (ii) is a claim on the respective central bank.

This definition simplifies the discussion and fosters intuition; however, our conclusions are robust to reasonable modifications of it. Some might, for instance, argue that there is no such thing as a digital token (Grym, 2018), or a digital object (see Milne, 2020), or central bank issued fiat money representing a claim on the central bank (Allen J. et al., 2020). These readers can replace CBDC token with "a sequence of bits".

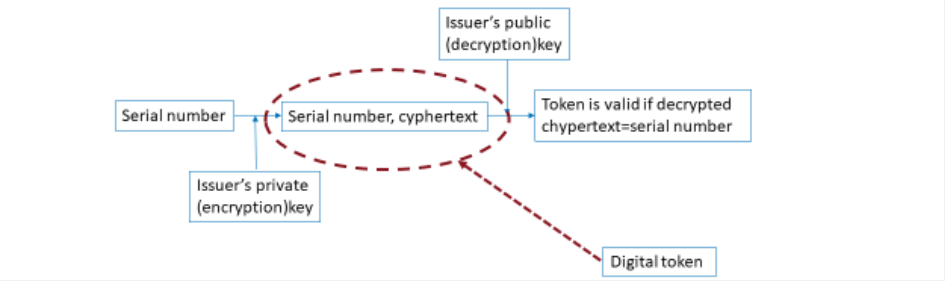
The example in Box 1 may further enhance the intuition of what a CBDC token is. There the CBDC token is a data file containing a serial number with a digital central bank signature. Many other forms of tokens are possible. In many cryptocurrencies, for instance, the (block)chain of previous transactions (or UTXO) may be thought of as a token. Our conclusions are not dependent on the particular example in Box 1.

Box 1. CBDC token – an example

Let the "private key of the central bank" be an encryption method/algorithm that turns the serial number like CB0000001 (*plaintext*) into a jumble/gobbledegook (*cyphertext*). Let the "public key of the central bank" be a decryption algorithm that decrypts the cyphertext created by the central bank's private key into the original plaintext. Only the central bank has the private key, but anyone can have the public key. The private key can be used to produce the cyphertext that the central bank's public key can decrypt. A CBDC token could then be a digital object consisting of the serial number and the cyphertext based on this serial number.

To check whether the token is an authentic central bank token, the receiver decrypts the cyphertext in the particular token using the central bank's public key into plaintext and compares it with the serial number in the token. If they are the same, the token is an authentic central bank digital token. The terms and the process are illustrated below. The process can be used for any issuer of digital tokens.

Figure: Digital signatures and digital tokens



This token can be stored locally on devices. It is also possible to transfer these tokens directly (peer-to-peer) without being online as it is essentially about moving numbers. However, as explained in the main text, this is problematic because of the double spending problem.

2.2 Remotely stored CBDC tokens

Generally, we can think of essentially three alternative forms of remote storage of CBDC tokens. The first is the storage of CBDC tokens in accounts or wallets at some provider of such services. An example is the solution tested by the Riksbank in its e-krona pilot where so-called participants in the private DLT e-krona network run nodes that store e-kronor and receive, validate and forward e-krona transactions for their connected end users. The second alternative is a system where the tokens are stored in a network of computers or servers. In contrast to the first solution, the tokens are not at some specific provider, but rather exist on the ledger which is on the network. The network can be operated by trusted parties or by anyone. Bitcoin is an ideal example of the latter.

In both of these alternatives there is some type of ledger that keeps track of ownership of the tokens. Thus, any CBDC payment requires that we reconcile the relevant (remote) ledger.

A third alternative is to have the tokens stored remotely on some device in a known physical location. This option is analogous to storing cash in a bank box or at a friend's house. We include this alternative for completeness, but it can just as well be seen as a local storage alternative.

2.3 Locally stored CBDC tokens

Let us now look at systems where the tokens are stored locally on mobile phones or some other local device, and only there. This includes, for instance, our third alternative above. Such tokens can be moved from device to device without reconciling any remote ledger, without a third party, and even offline. However, as we explain below, such tokens need a remote ledger to function as money.

The double spending problem

We can start by observing that locally stored tokens (digital or not) can only function as money if the payee can control the authenticity of the tokens; who would accept tokens as payment if they could not be sufficiently certain that they were authentic? Similarly, if it were easy to copy central bank tokens, "why would anyone care to work to earn such money? It is easier just to make copies of existing tokens. Money would cease to function, and the economy would grind to a halt, unless it switched to a different, more difficult to copy, currency" (Halaburda & Sarvary, 2016, ss. 100 - 101).

For physical banknotes and coins it is possible to exert sufficient control over their validity. This is self-evident, as otherwise banknotes and coins (physical central bank tokens) would not function as money. Notice that banknotes and coins function as money even though there is no ledger recording who owns which token. They work as money even though they are ledger free.

For digital tokens, it is more difficult to prevent counterfeiting. To see why, we first note that a-priori there are two ways to counterfeit CBDC tokens: (i) make copies of existing tokens or (ii) make genuinely fake ones.[5] For the intuition behind this we can think of CBDC tokens as serial numbers. Any such token can easily be copied (counterfeit method (i)) and someone can invent a new number (counterfeit method (ii)). The latter would be a "copy" if the central bank already has issued one with this number and genuinely fake if the central bank has not. This distinction may seem subtle and somewhat pedantic, but has important implications, as we will see below.

In the case of locally-stored digital tokens, it is possible to set up a system where we can quite easily detect genuinely fake tokens with the help of an (offline) local device. The underlying technology, which is based on sets of encryption and decryption keys,

[5] For physical tokens examples are (i) copying a valid US dollar note on a copy machine and (ii) creating "new dollar notes" by drawing notes on a piece of paper.

is illustrated in Box 1. Essentially, it is a system where the central bank digitally signs each token and where the payee by herself can check the authenticity of the signature without conferring with a third party. This means that counterfeit method (ii) is not a problem for central bank digital tokens even if there is no ledger keeping track of validity and/or ownership.

However, it is possible to make exact copies of digital tokens, as shown in counterfeit method (i).[6] This is because a "digital token is essentially a string of zeros and ones, perhaps encoded on a magnetic strip, on a chip, or stored somewhere in the cloud. Regardless of where it sits, this piece of data is imminently copyable. We can reproduce it exactly, in as many copies as we wish, without harming the original."[7] (Halaburda & Sarvary, 2016, s. 101) This challenge -- that you can copy an original token and spend it many times -- is called *the double-spending problem*. Chohan (2017) defines this problem as "…a potential flaw in a … digital cash scheme whereby the same single digital token can be spent more than once … because a digital token consists of a digital file that can be duplicated or falsified." The double spending problem was recognized, for instance, in the whitepaper that introduced Bitcoin (Nakamoto, 2008).

Secure hardware does not solve the double spending problem

A-priori it seems that a simple solution to the double spending problem would be to use local devices that cannot be tampered with and program them such that a token cannot be spent more than once. Unfortunately, such 100 per cent tamper-proof devices do not exist. Furthermore, the economic incentives for tampering with the devices are strong, and the system would not support "graceful degradation" (Allen S. et al, 2020). The latter means, essentially, that that it is sufficient for one device or one vendor to be malicious for the whole system to break down. These challenges might be mitigated by a sufficiently large chance and cost of being caught in double spending CBDC tokens. But, that would require that it is possible to trace down where the double spending has taken place, something that again reintroduces the need for a remote ledger.

Thus, we can conclude that currently, the only solution to the double spending problem is to institute one or more trusted central parties or a DLT that keep ledger(s) to record ownership.

[6] While this is true for any classical digital token, it is not true for "quantum money," which encodes money states in quantum physical systems. We do not, however, discuss quantum money, since it has only been partially implemented in an experimental setting and is not yet technically feasible (Hull, Sattath, Diamanti, and Wendin, 2020).

[7] This also shows the subtleness of it all: It is not possible to make fake digital tokens, but it is possible to make copies. Arguably, it boils down to the same problem, but we often encounter the argument that digital signatures make it impossible to counterfeit digital tokens. Yes, that is true, but copies can still be made. Are they not counterfeits? We have also heard the argument that notes and coins cannot be double spent because they are "handed" over to the receiver. But this is obviously not the case. The point is rather that it is sufficiently hard/expensive to make copies that are completely indistinguishable from the original (as in the case of digital tokens).

A remote ledger fixes the double spending problem

To summarize this section we can conclude that for CBDC tokens to work as money and the central bank not to take a large risk, the tokens need a remote ledger that records their ownership regardless of whether they only exist on this ledger or whether they also exist outside of this ledger on local devices.[8]

3 The irrelevance of the tokens/accounts distinction for cash-likeness

3.1 Peer-to-peer and offline payments

Cash provides for payment features that are often described as "peer-to-peer": they are instant, person-to-person and do not involve any third party.

We do not need tokens for instant payments. It is technically feasible to design a CBDC that allows for instant, person-to-person payments, and to do so without using a token-based system. A simple example is a scheme where users hold CBDC balances in deposit accounts at the central bank. Adding appropriate applications for local devices, such a CBDC could allow for instant person-to-person payments. Indeed, the technology for these kinds of services already exist and are in use for commercial bank money.

As explained in Section 2, all CBDC payments will involve a remote ledger, i.e. a third party. Thus, in this sense, CBDC payments will still require a third party. However, if we allow for some offline payments, CBDC payments can be done without a third party "for a while".

For remote storage systems, opening for offline payments will be the same as allowing for deferred settlement; the payee gives the payer a credit expecting settlement to take place later when one of the parties is online and can inform the ledger to settle the payment. These kinds of offline payments introduce credit risk for the payee but are common for payments with commercial bank money as a consequence of appropriate regulation and technology. The simplest example is the offline credit allowed on payment cards.

For local storage systems, the basic offline risk is rather the risk that the central bank will lose control of money creation. This risk is not borne by the payee, but rather the central bank. Appropriate technology and regulation in addition to limits on amounts and how many times a token can change hands before reconciling the ledges might reduce this risk to tolerable levels. Currently, many payment service providers and central banks are working to develop such solutions and several have applied for new patents. It remains to be seen how well these systems will work and how well they

[8] Having a ledger of transactions built into the token (e.g. in the form of a block-chain of transactions) will not change this.

fare compared with the current offline payment solutions for money balances on deposit accounts.

3.2 Anonymity and privacy

Cash payments are anonymous in that they need not reveal the identity of the payer and the payee to anyone. Cash payments leave no traces.

A similar degree of anonymity is not possible with a CBDC, for three reasons.

First, CBDC payments are digital. Digital payments are generally traceable as they leave digital footprints that enable a transaction to be followed, at least to some extent. If tokens are stored locally and there is no remote ledger, payments will still be traceable for someone who has access to the device. If the CBDC payment is made by handing over the device where the CBDCs are stored, such a payment will not be traceable, just as cash payments are not traceable. However, such a payment is not digital.

Second, all CBDC payments involve a remote ledger (Section 2). This ledger will record transactions. Even if the identities of the payer and payee are not known, the ledger will still record things like the time of the payment, encryption keys and digital wallets.

Third, legal regulations require digital payments to be non-anonymous. According to current regulations in the EU, account-based systems must have registers that make it possible to establish the identity of the owner of each account (Sveriges Riksbank, 2018). We suspect that any system where CBDCs are stored remotely will fall under this regulation, regardless of whether they involve tokens or not. In the case of locally stored tokens, anti-money laundering regulations at present allow for the payer to make a payment of up to EUR 150 without needing to identify themselves.

Since cash payments can be completely anonymous, they also allow for a weaker form of anonymity in that a payment can be made between two parties that know each other's identity but without revealing the identities to any third-party. This is sometimes referred to as "privacy" (Grym, 2018). As long as there is a ledger involved, privacy is not possible per definition as there is a third party involved (the ledger). Thus, there is no difference between a token- and an account-based CBDC in this respect.

4 Concluding remarks

The default CBDC technology approach among many central banks seems to be token-based. For instance, King and Rachel (2020) report that among the 46 central banks in their survey, 58 percent focus their research on "a token model". Furthermore, commentators and researchers – some affiliated with central banks – argue that CBDCs ought to be token-based (see e.g. Kahn and Rivadeneyra (2020)).

Our analysis shows that the perception that token-based technology can uniquely achieve cash-like features is misguided. A token-based CBDC appears to be no better in at achieving cash-like properties than an account-based CBDC.

There may be other advantages to token-based CBDC that fall outside of the scope of this paper. We hope our discussion can structure and spur further dialogue about when the choice of technology matters for a CBDC. More discussion and research will enable us to reach better conclusions.

References

Allen, Jason, Will Bateman, Simon Gleeson, Michael Kumhof, Rosa M. Lastra and Saule Omarova (2020), "Central Bank Money: Liability, Asset, or Equity of the Nation?," *CEPR Discussion Papers*, no. 15521

Allen, Sarah, Srđjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A. Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst and Fan Zhang (2020a), "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," *NBER Working Papers*, no. 27634, National Bureau of Economic Research, Inc.

Bank of England (2020), "Central Bank Digital Currency - Opportunities, challenges and design, " *Bank of England Discussion Paper*, March.

Bordo, Michael D. and Andrew T. Levin (2017), "Central Bank Digital Currency and the Future of Monetary Policy," *NBER Working Papers*, no. 23711, National Bureau of Economic Research, Inc.

Bouchaud, Matthieu, Tom Lyons, Matthieu Saint Olive and Ken Timsit (2020), "Central banks and the future of digital money Central banks and the future of digital money - An overview and proposal for central bank digital currency on the Ethereum blockchain," A ConsenSys Solutions White Paper

Chohan, Usman (2017), "The Double Spending Problem and Cryptocurrencies", *SSRN Electronic Journal*. Doi: 10.2139/ssrn.3090174

Grym, Aleksi (2018), "The great illusion of digital currencies," Bank of Finland Economics Review 1/2018

Halaburda, Hanna and Miklos Sarvary (2016), "Beyond Bitcoin - The Economics of Digital Currencies," Palgrave Macmillian

Hull, Isaiah, Or Sattath, Eleni Diamanti, Göran Wendin (2020), "Quantum Technology for Economists," *Sveriges Riksbank Working Paper Series,* no. 398

Kahn, Charles M. and Francisco Rivadeneyra (2020), "Security and convenience of a central bank digital currency," *Bank of Canada Staff Analytical Note*, 2020-21.

King, Rachael (2020). The Central Bank Digital Currency Survey 2020 -- debunking some myths. Central banking: https://www.centralbanking.com/7540951

Milne, Alistair (2020), "Argument by false analogy: the mistaken classification of Bitcoin as token money," Memo, Loughborough University

Nakamoto, Satoshi (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System", Memo, www.bitcoin.org

Securities and Markets Stakeholder Group (2018), “Advice to ESMSA - Own Initiative Report on Initial Coin-Offerings,” Electronic copy available at: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf

Sveriges Riksbank (2018), *E-krona project report 2*

Yao, Qian (2018). “A Systematic Framework to Understand Central Bank Digital Currency,” S*cience China Information Sciences*, Vol. 61(3):033101

SVERIGES RIKSBANK
Tel +46 8 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUCTION SVERIGES RIKSBANK