Central Bank Digital Currencies and Distributed Ledger Technology

Santiago Fernández de Lis and Javier Sebastián[1]

1. Introduction

The debate on Central Bank Digital Currencies (CBDCs) was triggered by the emergence of cryptocurrencies like Bitcoin on the one hand, which may compete with traditional central bank money, and the trend towards the disappearance of cash in some countries on the other hand. These trends led to a reflection on the possibility of issuing a digital form of central bank money. Several modalities were explored, distinguishing between a wholesale only versus a retail approach, and among the latter a token versus and account variant.

In most of the literature addressing this topic it is assumed that the infrastructure of any such scheme would be based on Distributed Ledger Technology (DLT), by analogy with cryptocurrencies. But there is little discussion on whether this is necessarily the case or there are other options. This depends crucially on the modality chosen, in particular on whether it is wholesale or retail. In the case of wholesale payment systems it is unclear to what extent DLT may improve the efficiency of present Real Time Gross Settlement systems (RTGS). There is a certain degree of consensus that this is not the case at present, but this may change in the future as DLT improves over time. A key question in this regard is the extent to which a DLT-based wholesale payments system may help improve the efficiency in the use of collateral, a question that is far from clear at this stage.

In the case of retail payment systems DLT is probably the best option. A retail CBDC based on a permissioned DLT would not be subject to the scalability problems of public DLT schemes. Like in the case of the wholesale modality, there are practical questions on how to reconcile the decentralized nature of DLT and the need to have the central bank at the core (and with adequate capacity of control) of any CBDC variant. In addition, there is the question of whether it is appropriate for a retail CBDC to be anonymous or not, a debate that is currently clearly moving towards an identified option due to the potential problems that the anonymous option would produce.

As if that weren't enough, the recent announcement of the stablecoin Libra supported by a technology giant like Facebook is causing some concern among policymakers and regulators that it may have a direct impact not only on payments but on issues related to monetary policy and financial stability. This movement has brought back to the table, perhaps with greater urgency, the appropriateness of the issuance of CBDCs.

In this paper we explore the current landscape of ideas and uncertainties about the use of DLT in the different CBDC options. The first part of the document is dedicated to explain the basics of Distributed Ledger Technologies (DLT), including blockchain and cryptocurrencies. In the second part, we explain the fundamental concepts underlying the idea of Central Bank Digital Currencies and the different design options for this kind of instruments. The third part is dedicated to explore the advantages, disadvantages and

[1] BBVA Regulation

implications of the different types of potential CBDCs showing the current state of reflection about the topic.

Finally, we extract the main conclusions derived from the analysis of the current conditions and environment, including the existence of initiatives from Big Tech companies and the position of regulators.

2. DLT Fundamentals

Distributed Ledger Technologies include a set of concepts related to the use of distributed ledgers, a type of databases characterized by not being managed by a central administrator but by a variable number of parties that use some kind of consensus mechanism to decide what information is inserted in the database. DLTs usually are complemented with some kind of cryptographic scheme that ensures the immutability of the registered information.

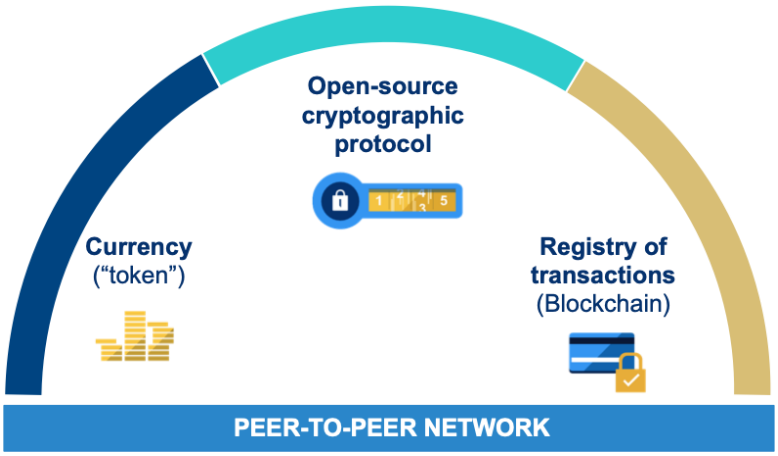
There are distributed ledgers in which the information is registered in a particular way: it is grouped in blocks of information, and each new block registered include a hash (a kind of "cryptographic summary") of the previous block, linking both. That is the reason why this kind of distributed ledgers are called "blockchains".

Nevertheless, it is common in the literature on this topic to use the terms "blockchain" and "DLT" as synonymous. In the context of this paper, we will refer - unless explicitly stated - to blockchain-like distributed ledgers.

2.1. Blockchain and DLT: basic concepts

The origin of the blockchain concept dates back to the birth of Bitcoin in October 2008[2]. It is not within the purposes of this paper to enter into details about how Bitcoin works, but it is worth to explain some basic concepts related to the different technological components that underlie Bitcoin-like protocols, with the aim to help understand the advantages and disadvantages of the use of blockchain.

Bitcoin is basically a set of four components: a peer-to-peer network, tokens, cryptographic protocols and a registry of transactions (the blockchain.)



[2] https://bitcoin.org/bitcoin.pdf

As Bitcoin was designed to be a peer-to-peer electronic cash payment system, the first essential component is a peer-to-peer network on the Internet. By 2008, this kind of networks were already well known, and used to share files (think of initial file sharing networks like Napster, or the current *torrent* networks as an example.) In Bitcoin, this network is public, meaning that everybody can freely take part in it, without the need to identificate or ask for permission, just by downloading a piece of software - a wallet identified by an address - and becoming a node of the network.

Participants in the network are able to send and receive tokens between them. Tokens in this case are meant to be a currency - bitcoin - in the sense that it is a transfer of something that arguably has a value.

The way in which this network works, that is, the "rules of the game" are codified within the cryptographic protocols, which in the case of Bitcoin are open-source. The protocols set how new bitcoins are issued (in a decentralized way and at a predetermined rate), how are transactions initiated and validated, who are the validators, what kind of consensus mechanism is used in the validation, how transactions are registered in the blockchain, etc.

Finally, the blockchain is a registry of all the transactions (token movements) between participants in the network. It is important that all the history of transactions is compiled in the blockchain, that each block is linked to the next, and that information in the blocks, due to the insertion mechanism, cannot be modified once it is registered.

Validator nodes, called "miners" have the task of verifying that a transaction is correct before entering the blockchain, among other things ensuring that there is not "double spending", that is, that a user does not spend the same bitcoins more than once. These miners are rewarded with the new minted bitcoins following a competition mechanism based on the consumption of computer power. Any participant in the network can choose to be a miner.

As mentioned before, in Bitcoin anybody can be a member of the network, both in user and validator mode. This kind of schemes are called "permissionless" ledgers. But there are other types of blockchains in which participants are identified and have to ask for permission to become a member of the network. This kind of schemes are called "permissioned" ledgers. There is even a third option in which participant can be anonymous but validators have to be identified: these are the "hybrid" ledgers.

2.2. DLT as payment rails

The fact that the design of bitcoin was focused on the use of the scheme as a peer-to-peer payment network without intermediaries led to the generalized idea that the underlying technology pieces could be used as a mechanism for digital payments without the need of using the bitcoin token. Thus, the first use case to be explored by banks was to use blockchain-based infrastructures as "payment rails" in substitution of the current rails being used, e.g. card schemes like Visa and Mastercard, SWIFT, etc.

Main advantages of blockchain-based payments is the fact that clearing and settlement are simultaneous, the network is intrinsically global, there is no need of intermediation, the price of the transaction is relatively low - although growing -, and the system works 24/7/365.

Regarding the time to complete a transaction, in the case of Bitcoin is around 10 minutes, which could be considered too high for retail payments compared with any other means of payments, but can be also seen as an advantage when we think of cross-border payments. Anyway, this time can vary depending on the protocol.

2.3. Cryptocurrencies: basics and types

Since 2008 and the surge of bitcoin, considered the first cryptocurrency, the landscape has radically evolved.

As mentioned above, the bitcoin tokens were designed to be used in peer-to-peer payments, that is, they were born with the aim to become an alternative currency. But, as tokens can be a representation of anything, since then the typology of tokens has diversified, so that today there are about 2.000 different tokens, of which only a small percentage have been created with the vocation of actually become money.

Although there is not a common taxonomy of crypto-tokens officially accepted, there is a certain consensus among the blockchain community - and also in regulatory and supervisory authorities - in classifying crypto-tokens in three basic types. In its latest report[3], the EBA define this types as follows:

- **Investment tokens**

  Typically provide rights (e.g. in the form of ownership rights and/or entitlements similar to dividends). For example, in the context of capital raising, asset tokens may be issued in the context of an ICO which allows businesses to raise capital for their projects by issuing digital tokens in exchange for fiat money or other crypto-assets.

- **Utility tokens**

  Typically enable access to a specific product or service often provided using a DLT platform but are not accepted as a means of payment for other products or services. For example, in the context of cloud services, a token may be issued to facilitate access.

- **Payment/exchange/currency tokens**

  Often referred to as VCs or cryptocurrencies. Typically do not provide rights (as is the case for investment or utility tokens) but are used as a means of exchange (e.g. to enable the buying or selling of a good provided by someone other than the issuer of the token) or for investment purposes or for the storage of value.

However, there is a wide variety of crypto-assets some of which have features spanning more than one of the categories identified above (hybrid crypto-assets). For example, Ether has the features of an asset token but is also accepted by some persons as a means of exchange for goods external to the Ethereum blockchain, and as a utility in granting holders access to the computation power of the Ethereum Virtual Machine.

[3] https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf

For the purposes of this paper, we will focus only on the payment/exchange/currency tokens, in which bitcoin-like ones would be included.

Being open-source, Bitcoin allows the reuse of its code for the creation of other cryptocurrencies with similar characteristics, and that was the mechanism for the design of the first denominated “altcoins”, like Litecoin. These new cryptocurrencies were aimed to improve or add certain features to those of bitcoin. Thus, as en example, in the case of Litecoin the time of validation of transactions is shorter than in Bitcoin. Others, like Zcash or Monero, were designed to be more anonymous than Bitcoin.

Anyway, the common issue to all this cryptocurrencies to be considered money is that they currently do not fulfill the three traditional basic functions of money, that is, to be accepted as a **medium of exchange**, to be a **unit of account** so that cost of goods and services can be compared over time and between merchants, and to be a **store of value** that stays stable or increases as a remuneration of saving over time.

The main reason why cryptocurrencies do not fulfill these three functions is their high volatility in price, which makes it difficult to use them as a stable store of value, a unit of account and a medium of exchange (in this case scalability problems also play a role). The volatility in turn is caused by the dynamics of price setting in the markets for this type of currencies.

The analysis of these dynamics is the object of academic research and exceeds the scope of this document, but in summary it could be said that of the various factors that affect price variations the fundamental one is the fact that it is established by a pure mechanism of supply and demand and the high concentration of the market - for example, most bitcoins are found in very few wallets, the so-called "whales" - which facilitates manipulation.

In order to reduce this volatility and facilitate the adoption of cryptocurrencies as alternatives to fiat money, a new type of cryptocurrencies called stablecoins are being created, which try to keep their price stable through the use of various mechanisms. There are mainly two types of stablecoins:

- Asset-backed stablecoins stabilize their price by being collateralized with some kind of asset, which can in essence be of three types: a fiat currency, a commodity or other cryptocurrency.

- Algorithmic stablecoins try to replicate the functioning of a central bank by using algorithms to issue or “retire” the amount of currency in the market depending on price increases or decreases.

3. CBDC Fundamentals

An alternative to cryptocurrencies that is receiving increasing attention is the possibility of a similar issuance by central banks, the so-called Central Bank Digital Currencies (CBDCs). A CBDC is a central bank-issued instruments combining cryptography and digital ledger technology to offer an electronic variant of central bank money. It is therefore a central bank liability, which may emulate the features of cash (if held by the general public) or central bank reserves (if held only by banks and other financial intermediaries that have access to the wholesale payments system, normally organized around the central bank).

3.1. The problems of cash

The debate on CBDCs was triggered by the emergence of Bitcoin and other cryptocurrencies that may in theory compete with cash, with the background of a certain traditional insatisfaction with cash. Indeed, cash is costly. Its issuance, circulation and retirement requires an expensive infrastructure. Furthermore, it generates crime (theft) and falsifications. And it is the main vehicle of money laundering, tax evasion and the financing of terrorism[4]. A digital variant would in principle be more efficient, cleaner and safer. As we will discuss later, whether or not CBDCs retain the anonymity feature inherent to cash is a key decision on the design of CBDCs, with very important implications in terms of AML/CFT.

3.2. Current wholesale and retail payment systems

Wholesale payments

Central banks play a fundamental role in wholesale payment systems. They do it by acting as the bank of commercial banks, that is, taking deposits from them and providing credit to them. In the case of banks, deposits in the central bank are referred as reserves or central bank money. These relationships between central and commercial banks allow the efficient operation of the financial system, because they ease both the monetary policy implementation and the settlement of transactions between banks.

On a daily basis, there are a lot of transfer of funds to be made between banks, resulting basically from large value wholesale transactions resulting both from pure payments and from financial market - exchange-for-value - operations. The processing of these transfers involves two key elements: clearing, which is the transfer of information between the payer and payee banks, and settlement, which is the actual transfer of funds between the payer's bank and the payee's bank. The delay between clearing and settlement of transactions causes the surge of different types of settlement risk, notably credit and liquidity risk, related to the possibility that the transaction may not be completed at the time of settlement due to different causes.

Starting in the mid 1980s, a new type of interbank settlement systems appeared that since then have been increasingly deployed in different countries. These so-called real-time gross settlement (RTGS) systems[5] are becoming the standard for interbank settlement, and have as their main feature the fact that each operation is cleared and settled individually in real-time. This automatically lowers settlement risks.

Settlement is usually achieved through a transfer of funds between the central bank accounts of the banks, using their reserves in central bank money, which provides certainty of settlement finality. When there is a lack of funds to settle an operation, there are different alternatives: the operation can be rejected and passed to a queue until the account has been refunded or, more usually, the central bank gives credit to banks in order to supply enough intra-day liquidity to keep the machine running and eliminate friction in the system. This credit is guaranteed by the central bank normally against a certain amount of adequate collateral that banks have to deposit as a guarantee. Typically, collateral refers to

[4] See Rogoff (2016). An alternative view can be find in Schneider (2019).

[5] *Real-time gross settlement systems*. Bank for International Settlements, May 1997.

marketable financial securities, such as bonds, or other types of assets, such as non-marketable assets or cash, but is defined by each central bank.

Retail payments

Non-cash retail payment systems are currently concentrated on a few number of card payment networks providers who control the market in an oligopolistic model, while the connection between these systems and wholesale schemes is currently based on infrastructures organized by banks. In fact, evolution of instant payments through direct account-to-account transfers is already challenging the card networks.

New fintech companies entering the payments space have tried to disrupt the market but, in the end, have been limited to those existing payment rails. Different initiatives based on telco networks or diverse types of e-money are in some cases trying to workaround card networks - but in some cases have ended up by collaborating with them - and, in all cases, the link through the banking system to access settlement systems is unavoidable. The surge of DLT-based schemes, starting with Bitcoin, was theoretically trying to circumvent these schemes as well and leave the financial system apart, something that so far has had little success.

The recent announcement of the Facebook-backed Libra - a DLT-like network with an associated stablecoin aimed to be used for payments - and other similar schemes that may come soon led by major digital players - eg. Telegram - may represent a significant change in the status quo of the payments sector, especially in the field of international remittances. Nevertheless, the connection with the fiat world, according to the information known to date about Libra, will take place through “authorized resellers” that will be regulated entities.

3.3. CBDCs: basics and types

Cash is a very special type of asset that combines four features: (i) it is exchanged peer to peer (without knowledge of the issuer), (ii) it is universal (anybody can hold it); (iii) it is anonymous and (iv) it does not yield any interest. CBDC is an alternative to cash that is also peer to peer (P2P), but it opens the possibility of introducing changes in the other three features:

• They can be universal or restricted to a particular set of users. Likewise, DLTs can be open or closed (for instance, limited to banks or financial institutions).

• They can be anonymous (like cash) or identified (like current accounts). The first corresponds to the idea of token-based CBDCs, and the second to account-based CBDCs.

• They can pay interest or not. The delinking of cash from paper-money opens the possibility of including interest-bearing as a feature, either in the account based or in the token based variant. Interest can be positive or negative (see below).

These options can be combined in several ways to generate different modalities of CBDCs. The choice depends crucially on the objectives pursued with the introduction of CBDCs. There are basically four possible objectives: (i) to improve the working of wholesale payment systems; (ii) to replace cash with a more efficient alternative; (iii) to enhance the instruments available for monetary policy, especially when confronted with the zero lower

bound and (iv) to reduce the frequency and cost of banking crises. How do these objectives match with the different options that CBDCs open as compared to cash?[6]

(i) If the objective is to improve the functioning of wholesale payment systems, you may introduce CBDCs that are only accessible to banks and other financial institutions that participate in the wholesale payment system. The resulting CBDC would be restricted, identified and non-interest bearing: restricted because the general public will not have access to it; identified because participants will be known by the rest (although not all transactions of all the players need to be known by the rest, it is a possibility that they are only known by the central bank); and non-interest bearing because payment systems rely on fixed nominal amount accounts, although they are normally accompanied by yield-bearing (positive or negative) accounts in the central bank to and from which these institutions move funds in the context of their liquidity policy. The central bank, which in traditional RTGS is at the center of the system, would be in this scheme just another player, although it may play a special role as overseer and retain control over certain features of the system, like for instance admission and membership, as will be explained later

(ii) If the aim is to replace cash with a more efficient means of payment you would introduce a CBDC that is universal, anonymous and non-interest bearing: universal like cash, which can be used by anyone who holds it; anonymous because this is an essential feature of cash; and non-interest-bearing to emulate cash[7].

(iii) If the authorities want to enhance the instruments of monetary policy, in particular in the proximity of the zero-lower bound, they would introduce a CBDC that is universal, anonymous and yield-bearing. It should be universal because you want to reach the public (and ultimately replace the banknotes in the hands of the population); yield-bearing because you want to exploit the opportunity digital money provides of carrying interest rates, either positive or negative; and anonymous also for similarity with cash, although it could be identified too (but for reasons of clarity of the different models this option is reserved to the next variant). As mentioned above, interest rates may be positive or negative. Historically the former is much more frequent than the latter, but the objective of this proposal being overcoming the problems of the zero-lower bound, the proponents are rather thinking on negative interest rates situations.

(iv) If the aim of introducing CBDCs is opening accounts for the population in the central bank then the modality would be universal, identified and non-interest bearing. Those in favour of this modality have normally in mind the final objective of reducing or eliminating the likelihood and destabilizing impact of banking crisis and/or offering to the population an alternative that competes at the same time with banks' deposits and private e-money schemes.It would be universal because it is addressed to the population; identified like in the case of bank deposits; non-interest bearing because, like in the previous variant, we

[6] See Gouveia et. al (2017)

[7] When this article was in the finalization process we learned that the Chinese authorities announced more details of their CBDC project, according to which they will launch a combination of options (i) and (ii). It will consist on a two-tier system, with banks operating with the central bank in the wholesale level with a DLT-based system and the banks operating with the public in a Token-based system. It is unclear whether the later will use DLT. See Binance Research (2019) https://info.binance.com/en/research/marketresearch/CBDC.html

want to differentiate option (iv) from option (iii), although the possibility of combining both features (identified and interest bearing) is always an option. The logic behind this proposal is that banking crises are the result of fractional reserves, which implies that sight deposits with fixed nominal value on the liability side of banks are backed in the asset side by longer-term credit whose value is uncertain. Following this logic, if the central bank provides deposits to the population the provision of payments would be delinked from the provision of credit and most banking crises would be avoided[8].

3.4. Central Banks and Monetary Policy Management in a digital world

It is unclear how digitalization trends may affect monetary policy. The substitution of cash by e-money is a trend in some countries (in particular in Nordic countries), but is far from being a generalized trend. Quite the opposite, the use of cash has even increased in many countries since the Great Financial Crisis[9]. The increase in the use of electronic wallets as compared to cash may weaken the connection between retail means of payments and the balance sheet of the central bank. This may introduce some volatility in the monetary multiplier and complicate the monetary policy transmission mechanism, but to the extent that central banks tend to rely on interest rates rather than monetary aggregates as instrumental variables for monetary policy it is not clear whether this would really be the case.

It is interesting to note that countries where cash is disappearing are reacting very differently to this trend. Whereas Sweden is seriously considering introducing a CBDC Denmark does not consider it as a problem. The reasons for this different reaction may be related to different sensitivities to the oligopoly power of foreign credit card suppliers, or different importance attached to potential financial exclusion problems in population with less access to private electronic means of payments.

The recently announced emergence of Libra, the stablecoin sponsored by Facebook, has triggered a reaction in some central banking quarters in favour of CBDCs, including in the BIS[10]. This may be explained by the uneasiness among central banks of the possibility of a reduction in the degree of control central banks have on the domestic payments system (and of a weaker connection between monetary policy variables and nominal expenditure and therefore inflation). This debate is very incipient and it is therefore too early to set a position. But central banks' reaction to Libra certainly indicates that there is considerable concern on this potential effects.

4. DLT as an infrastructure for CBDCs

It is a reality that the conversations around CBDCs have been fuelled by the surge of Distributed Ledger Technologies, and in particular by the fact that the primal cryptocurrency bitcoin is based on an underlying technological infrastructure like

---

[8] A different variant is the so-called "synthetic CBDC", in which the central bank does not issue cash but provides full backing of privately-issued e-money. This variant, which seems to present certain advantages as compared to fully fledged CBDC, is not analyzed here. Seee Adrian and Mancini Griffoli (2019).

[9] *Payments are a-changin' but cash still rules.* Bank for International Settlements, March 2018.

[10] "[I]t might be that it is sooner than we think that there is a market and we need to be able to provide central bank digital currencies.", A. Carstens, BIS General Manager

blockchain. However, digital currencies are not necessarily synonymous of cryptographic currencies, that is, the concept of digital currency is previous to the birth of bitcoin and the blockchain. The current impulse towards DLT-based CBDCs has its explanation in the differential advantages that a DLT infrastructure can add to the definition of a digital currency, specially if this currency is meant to be considered as legal tender.

4.1. DLT-based vs non-DLT-based CBDCs: alternatives and advantages

It is usual to identify the concept of CBDC with the notion of a cryptography-based type of token issued by a central bank, transacted and settled on a DLT infrastructure. Nevertheless, in a general way, a Central Bank Digital Currency could be any kind of non physical token issued by a central bank with the aim to substitute or complement an equivalent physical currency, namely cash.

From this perspective, there are several alternatives for the issuance of a CBDC, apart from the DLT-based approach. In fact, of all money issued by central banks, only cash remains physical, therefore alternatives to DLT already are in place except for the cash issue. Let's explore the digital alternatives to the issuance of banknotes and coins not using a DLT infrastructure.

It is true that in certain countries the use of cash is diminishing, but the reason is that there are electronic alternatives for payments that are substituting the use of cash, mainly plastic cards or mobile wallets, or even mobile instant payment schemes. Even immediate transfers lead to a decrease in the use of cash.

But all these means of payment do not really mimic the characteristics of cash, in particular the lack of intermediation when paying, and the anonymity.

Neither e-money as defined in the EMD2 is equivalent to cash, because the issuer is not the central bank. A central-bank issued e-money would get closer to cash, but it would lack anonymity.

Prepaid cards are a way to substitute money by means of "tokenizing" cash, but some kind of party managing the card balance is needed, so it is not pure peer-to-peer, there is intermediation.

Therefore, the question is if there is really an alternative to DLT-based CBDC, at least in an scheme where CBDC tries to act as a form of "digital cash". For identified schemes, central bank issued e-money could be an alternative. And, of course, for wholesale payments, current systems already use electronic money, so there is not advantages beyond the still-to-be-proven in efficiency and cost, as we will show afterwards.

4.2. DLT models for CBDCs: public, permissioned, hybrid? Scalability and other issues

One of the main unknowns when planning to deploy some kind of CBDC from the point of view of central banks is the infrastructure model that better fits with the desired functioning of the CBDC scheme.

First, the proper infrastructure depends, of course, on the type of CBDC to be implemented: wholesale or retail. And, within the retail option, it depends on whether the CBDC is anonymous or not. These options will be discussed in more detail below.[11]

DLT for wholesale CBDC

In this scenario, nodes of the distributed network would be the entities with granted access to the RTGS system - in principle, banks and probably other authorized financial intermediaries - plus one node for the central bank. This means that the DLT infrastructure would follow a permissioned model in which all nodes are identified. The main question would be who would act as validator(s) of the transactions, and what kind of consensus mechanism should be implemented, and who would be able to access the transaction information.

If we assume that the management of the system would remain the responsibility of the central bank - which, on the other hand, goes against the fundamental idea of using a distributed ledger - then its node would have special powers as all transactions should be validated by this node. In this case, there would be only one validator and, although the scheme could be set up to allow all nodes to access information of all transactions, the most probable option would be that only the two parties implied on each transaction - plus the central bank - would have access to the information. The reason is that banks and financial intermediaries would not be inclined to disclose the detail of their liquidity strategy to competitors. This is a particular way to run a distributed ledger scheme, and in fact it is not really a blockchain, it is exactly the model that R3 chose for its platform Corda. Actually, a pilot of Italian banks for interbank settlement is being run on Corda following this model.

Other options appear as less likely to be implemented. One of them would be the definition of a consensus mechanism that allows other nodes different than the central bank to act as a network of validators. Any flavour of this scheme presents important issues. To begin with, it is unthinkable that the central bank does not have veto power, because in other case banks could reach a consensus on transactions without the agreement of the central bank. This loss of supervision power is completely off the radar. To continue, even if that option were possible, the definition of the group of validators would be problematic too: if only some banks have the right to validate transactions together with the central bank, they would enjoy and advantage vis-à-vis competitors and we would be mimicking the current "tiered" model of most RTGS systems, while in theory one of the benefits of the use of a DLT would be to facilitate the access to central bank money of more entities than today, including non-bank financial intermediaries.

DLT for retail CBDC

[11] It is worth mentioning that known details about the CBDC initiative in China describe a two-tiered hybrid model, in which the relationship between the Central Bank and the "distributors" of the currency is based on a DLT infrastructure, while the relationship between this "distributors" and consumers is not specifically designed to be managed through a DLT, although "blockchain is an option", according to the People's Bank of China. Therefore, the CBDC is at the same time wholesale and retail, and supports both anonymous and identified models. Technical details have not been disclosed yet. See Binance Research (2019) https://info.binance.com/en/research/marketresearch/CBDC.html

In the scenario in which access to the CBDC is universal, there are a number of options depending on the characteristics of the issued currency. First of all, we would have a public network that allows individuals to join in order to have a wallet and use the CBDC. Joining to the network could require some kind of identification or not, depending on whether we are in an account-based model or in a token-based model of CBDC.

A different thing is the definition of the nodes that would act as validators of the transactions. In a pure public network any node can act as a validator, something that presents multiple difficulties: a) if validators are not identified parties, potential "51% attacks"[12] can happen, b) the consensus mechanism in principle decreases in efficiency and scalability when the number of participants increases, and c) we still have the issue of the loss of power of the central bank.

Therefore, it seems that the best model could be one in which validators are identified - and probably selected to be trusted parties, maybe banks could be good candidates - and the rest of nodes can be anonymous if we are in a token-based CBDC, and identified if we are in an account-based CBDC. Validation should be carried on by the group of selected validators, but with a final approval by the central bank. Limiting the number of validators, together with some other technical improvements, would diminish the scalability problem that is usually associated to public DLT networks, because consensus mechanisms are simpler and faster the smaller the number of parties that have to come to an agreement. In addition, working with identified validators difficult some types of potential attacks.

Regarding the rest of nodes that are only users of the network, in an anonymous scheme they could join the network simply by downloading the needed app to manage their wallet(s) to a device. This requires users to be confident that data about their device or other identifying data would not be used by the central bank to monitor their transactions, a commitment that is unlikely to be credible in the presence of for instance AML-related incidents. In an identified scheme, there must be some kind of service acting as a gateway to enter the network and managing the process of identification of the consumer: it is unlikely that the central bank itself provides this services, and banks are already doing it, so they seem good candidates to act as these "gatekeepers".

4.3. Wholesale CBDC models: managing collateral

DLT-based RTGS systems

In a DLT-based RTGS system, reserve accounts are substituted by reserve "wallets" and transfer of funds are made through the rails of the DLT scheme. This is an important difference, but the main one is that the central bank, which in traditional RTGS systems is located at the center of the scheme and centralises operations, while in a DLT scheme the central bank is one of the nodes of the network, although probably it should be a "super-node" with special voting and overseeing power.

[12] A type of attack derived from the fact that in a network governed by consensus mechanisms, if one player have the majority of the "votes" can act in malicious ways. In a "proof of work" consensus mechanism like the one in Bitcoin, this means to have a 51% of the computing power of the network.

There has been some debate about the advantages of a wholesale CBDC in terms of collateral management in wholesale payment systems, in particular arguing that the management of that collateral would be more efficient and part of it could be freed up.

However, a distinction should first be made between wholesale payment systems in countries that have already adopted an RTGS scheme and those that have not. Modern RTGS systems in particular were designed to reduce both the credit risk and liquidity risk that existed in the interbank settlement environment and are therefore already making efficient use of collateral. From this point of view, there is no evidence that the replacement of the technology underlying one of these modern RTGS systems - think of Target2 - by a DLT-based technology represents a significant improvement in collateral management.

Voices in the DLT space point to the unique characteristic of a DLT-based payment system - the coincidence in time of clearing and settlement - as a clear advantage. As settlement is instantaneous, collateral is not needed. But this is true if we assume that each transaction in the system is prefunded. Recent studies[13] state that the savings in collateral would be minimal compared to the increased costs of prefunding.

On the other hand, we could think of a way to implement an equivalent to the mechanism of intra-day credit transfer from the central bank to the participants in the DLT system so that they can face the corresponding payments without the need of prefunding, with the only difference that the funds would be given in CBDC. But, in this case, the collateral would also be needed to cover that credit and we will replicate the current model without any savings.

As of today, pilots performed on this type of DLT systems have not showed a significant improvement in efficiency over the current RTGS systems. However, there is still uncertainty about the possibility that in the future more mature forms of DLT allow even faster processing and reduced reconciliation work[14], which may lead to more transactions occurring in real-time or near real-time in certain markets. The impact on the reduction on credit exposures and, consequently, a higher demand on liquidity, could deserve in this case a further analysis, because faster processes could mean a quicker release of liquidity that could be tied up in collateral as is the case in today's systems.

A different question, which would be worth analyzing, is whether there would be an improvement in efficiency through the use of "tokenized" collateral, so that the entire credit-guarantee-payment cycle would be supported by the same infrastructure. A first approach to this models is already being analyzed in relation with the investigation of DLT-based delivery-versus-payment (DvP) in financial markets, in which the "assets leg" is already being tokenized in several proof-of-concepts, while the problem of embedding of the "cash leg" into the DLT infrastructure is not solved yet, and the simultaneity of both transactions has to be managed through a relatively complex mechanism, that could perhaps be simplified with the use of a CBDC. A notable example of this kind of proofs-of-concept is Project Stella, carried out jointly by the ECB and the Bank of Japan, the results of which

---

[13] Steampunk Settlement. Deploying Futuristic Technology to Achieve an Anachronistic Result. Greenwich Associates. June 2019

[14] *Distributed ledger technology in payment, clearing and settlement. An analytical framework.* Bank for International Settlements, February 2017

have been published in an interesting report that explains certain mechanisms to solve this DvP problem.[15]

4.4. Retail CBDC models: dealing with anonymity

In retail CBDC models, individuals are able to access the network and use a wallet to carry on transactions through the payment rails provided by the underlying DLT infrastructure. Bearing in mind the previous reflection on the selection of validators, which in any case should be a group of identified entities plus the supervisory authority, the final users can be either anonymous or identified.

Anonymous (token-based) models

Anonymous universal CBDCs present clear challenges, both in non-interest-bearing and interest bearing models. First, anonymity makes the CBDC not only a good substitute of cash, but also an appealing alternative for people that prefer to manage their own funds outside the formal financial system and without a tight surveillance, specially in in an environment of very low or zero remuneration in the form of interest on bank accounts. Therefore, a shift of deposits towards the CBDC and an increase in informality is to be expected in this scenarios.

On the other hand, in emerging countries where informality is already high and managing cash is costly and burdensome for the financial system - cash transport alone can be a major problem in countries with complicated orography, security problems and poor infrastructure - a digital alternative could be helpful to solve some problems of financial inclusion, at least with regard to access to payments instruments. Of course, this would require a wide deployment of the mobile connectivity infrastructure and the individual devices needed to use the CBDC system.

In schemes in which the anonymous CBDC bears interest, the currency is not exactly a type of "digital cash" - which by definition is non-interest bearing - but becomes in theory an efficient transmission tool of the central bank's monetary policy. This kind of CBDC could allow avoiding the “zero lower bound” associated to cash and pose interests significantly lower than zero; it could also allow the distribution of “helicopter money”. There are legitimacy concerns of both situations, since we are talking about financial repression and monetary policy interfering with fiscal policy, which implies that these proposals are hardly compatible with central bank independence. Furthermore, this kind of CBDC could only be effectively used for the purpose of monetary policy if it does not coexist with cash. Otherwise, when the CBDC bears positive interest, people will fly away from cash, and when the CBDC bears negative interest, people will stay with cash, so the objectives of the central bank could not be achieved.

The impact on informality and on deposits of this type of CBDC would be more unpredictable than in the previous case, because it would depend on the sign of the interest rate, but could become much more pronounced in the case of a positive interest.

Identified (account-based) models

[15] Securities settlement systems: delivery-versus-payment in a distributed ledger environment. European Central Bank, March 2018

A universal identified CBDC leads to much more disruptive scenarios than the previous ones. In essence, this kind of model will be equivalent for individuals to having an account directly in the central bank, with the only difference that the account would have the form of a crypto-wallet.

In this account-based model the currency can bear or not interest. The considerations in case of an interest-bearing model would be the same as in the case of an anonymous currency regarding financial repression and helicopter money, and the potential movements between the CBDC and cash depending on the direction of the interest rate variation.

However, there are other important consequences in these scenarios. In a crisis, the flight of deposits from commercial banks towards the perceived security of central bank accounts - in which funds would be fully guaranteed without the need of a deposit insurance scheme - could be dramatic. Banks would have serious difficulties to prevent that leakage of deposits, basically they could compete by offering better interest rates than the central bank, but the public sensitivity to interest rates would be very low in a crisis. In a normal situation, banks can try to compete with the central bank by offering a better remuneration and/or providing services associated to the accounts - eg. direct debits - that the central bank probably would not provide. Alternatively, banks would be forced to or change their business model by trying not to get funds through deposits, which would mean that banks would not be banks anymore as we know them.

The problem is not only for commercial banks, of course. There is a big question around this type of central bank accounts, related to the credit flow. If deposits fly towards the central banks, who is going to give credit?

Different alternatives have been considered to resolve this issue, all of them with intrinsic complexities to be analyzed[16]. The more direct way would be the central bank itself giving credit to individuals and companies: this would suppose a huge effort for the central bank in developing the capacities, processes and tools needed to manage the credit lifecycle, something that as of today cannot do and that would require a tremendous increase in budget with the aim to perform activities that are not within the reach of a central bank' objectives. More relevant, the nationalization of credit that this solution implies is hardly compatible with the democratic societies as we know them. In addition, the central bank should not be able to credit for an amount higher than the sum of all the deposits in its balance, so we would be in a kind of "narrow banking" scenario, and the end of fractional banking.

A second option would imply the return of the deposits from the central bank to the commercial banks through some kind of scheme. The "delegation" of the credit function in banks is a decoupling in the deposit-credit mechanism and makes more complex the functioning of the financial system, introducing more friction. Furthermore, it implies that banks funding would be largely dependent on the central bank, and that the later would be backing private banks' risk assumption, with the ensuing moral hazard.

The third option would imply an increased participation of other players - that already exist - as credit providers in the market. Alternative mechanisms like crowdfunding - in all its

[16] See Fernández de Lis and Gouveia (2019)

variants, equity and non equity, ICOs, STOs, IEOs, etc. - would probably increase filling part of the void, but with dynamics much more volatile than today.

A fourth option would be that the central bank uses the proceedings of the CBDC lo lend to the government. This scenario raises issues of fiscal dominance and is probably incompatible with central bank independence.

Another aspect to bear into mind related to this scenario of an account-based CBDC is related to the surveillance powers that it provides to the central bank. Although this could be precisely the main objective - together with diminishing the probability of bank runs - of a central bank when thinking about this kind of solution, in practice the people that would prefer to have their money fully covered at the price of renouncing anonymity in transactions is not the people that are currently using that anonymity for illicit activities or tax avoidance. Therefore, the objective could only be partially fulfilled, unless cash were completely eliminated.

Regarding the control of bank runs rationale, as we mentioned before, it could be at the cost of eliminating banks themselves. Even though some of them could survive, in times of tough economic conditions consumers would search for security, and banks would lose their remaining deposits in favor of the central bank.

4.5. The first-mover effect

Putting money on global ledgers

When thinking about putting central bank money on a distributed ledger, as in the case of CBDCs, making access universal - not restricted to a group of players - it is important not to lose the notion of who is able to access to the network. Retail CBDCs, regardless of who is validating the transactions, are open to users that want to operate a wallet, and it is by principle very difficult, not to say impossible, controlling the location of the user to impede access to foreign citizens. In identified, account-based schemes, it could be feasible to "filter" users by means of the appropriate KYC process. But in anonymous, token-based schemes, it works in the same way that currently cash does, everybody can have those CBDCs in their wallets. Control of borders in the digital world is futile, although IP addresses could be analyzed and located, a user could mask her IP address in a quite easy way.

The first central bank in issuing retail CDBCs, if it comes from a country with enough credibility, will have a market as big as the whole world, excluding only countries with strong capital controls and internet access limitations, and capacity to enforce both. Consumers attracted by the potential advantages of a "digital cash" will have a single option to use it, so they will be willing to exchange their money - cash, deposits, and even cryptocurrencies like bitcoin - for this CBDC and manage their own wallets. The number of users will grow as the network effect attracts more consumers, and the demand for the pioneer CBDC will increase, with the consequence of a) a rise in price and b) a higher issuance rate to control the price. The growth in demand translates into higher seigniorage income for the central bank issuing the CBDC, replicating the current problem of dollarisation. An important difference with the present situation is that the competition for seigniorage will have no limits, it will affect not only what is now external seigniorage (i.e.

dollars or euros circulating abroad), but could potentially reach the whole domestic cash circulation (again, with the exception of countries having capital controls).

This effect on the facilitation of dollarization has been recently mentioned by Tobias Adrian from the IMF[17]. In some countries - a clear example is the LatAm region - dollarization is commonplace, specially for large value transactions. The current national currencies in those countries are generally weak and cannot compete with dollars. In addition, given that banks in those countries do not usually offer foreign currency accounts, and transactions are limited, people tend to use physical dollars, which are difficult to transport and store, mainly compared with an electronic alternative. if there was a hypothetical crypto-dollar - or other cryptocurrency issued by a credible, strong country - dollarization would probably skyrocket. As Adrian states, storage would be easier, safer, and cheaper. Transactions in foreign currency would be facilitated, and costs of remittances could drastically fall, which would increase foreign currency inflows. In those circumstances, as mentioned above, countries would not be competing only for external, but for internal seigniorage, and those with weak institutions and policy frameworks would be under pressure. Alternatively, these countries would have strong incentives to set capital controls.

What this means for other central banks is quite obvious. Current competitive market between currencies would be seriously disrupted, and other central banks should react by issuing their own CBDC. The "knock-on effect" will be unavoidable, which means that every relevant central bank in the world will have to be at least prepared to issue a retail anonymous CBDC in a short period of time.

An alternative to this would be a co-operative solution, in which central banks provide a universal CBDC for cross-border payments, which will connect present national payment systems[18]. Although this seems a promising area of work, it is important to note that the cooperation would be limited to cross-border payments, but the problem of the cross-border impact of national CBDCs still persists, lacking a restriction to the access of non-residents to national CBDCs which will be very difficult to implement, especially in anonymous retail CBDCs, for the reasons mentioned above.

5. Conclusions

The debate on the potential issuance of Digital Currencies by Central Banks has been ignited by the surge of Distributed Ledger Technologies and the potential competition of cryptocurrencies with cash. However, the implications of a CBDC on consumers, commercial banks, central banks and economy as a whole can be so profoundly transformative that central banks have to analyse them in detail before taking the decision to undertake such an initiative.

Those implications depend on the specific design of the CBDC. Wholesale models do not seem to present major problems because they ultimately do not propose a significant

---

[17] *Stablecoins, Central Bank Digital Currencies, and Cross-Border Payments: A New Look at the International Monetary System.* May, 2019

[18] See the report by the International Communications Union (2019), which also contains very useful information on the stage of progress of different CBDCs modalities and proofs of concept developed in several countries.

operational change beyond a replacement of technological infrastructure. On the other hand, there is also no evidence that a CBDC of this type presents significant advantages for the functioning of wholesale payments compared to modern RTGS systems, although there is a growing consensus that this may the case in the future, as DLT improves over time.

Retail CBDCs are much more complex to analyze, because you have to take into account a much greater set of potential derivatives. On the one hand, there is the dilemma between anonymous models and those identified. From a central bank's point of view, and given the AML problems arising from an anonymous model, the most viable alternative would be an identified CBDC. However, since the demand for an anonymous means of payment will be maintained in most countries, this identified CBDC would necessarily have to coexist with cash, never replace it. The countries where cash is most likely to disappear are those, such as Sweden, where it is already doing so, regardless of whether or not there is an alternative in the form of CBDC.

The identified CBDC, on the other hand, represents a potential disruption to the commercial banking business model by fundamentally "attacking" the main source of funding that customers' deposits represent. It is difficult to foresee an environment of competition between private banks and the central bank in the provision of deposits. The mechanism by which deposits in central banks could be transformed into credit in such a model, a function traditionally performed by commercial banks, is still an open question. This decoupling of deposit and credit introduces friction that does not currently exist within the financial system and could cause a stranglehold on the credit cycle.

In short, there are compelling reasons why central banks, and other supranational bodies such as BIS, have so far been extremely cautious in their analysis and movements regarding CBDCs.

In fact, although in its 2018/2019 annual report the BIS[19] includes the results of a survey among central banks according to which the issuance of a CBDC is unlikely, both in a wholesale and a retail model, in the short and medium term - ie, in the next six years - the truth is that after the official announcement of Libra, central banking officials have stated that central banks could adopt digital currencies sooner than expected, in response to fears that Bigtechs could establish a dominant position in global finance and represent a potential threat to competition, financial stability and social welfare.

This confirms that first mover issues are crucial in this debate, both between cryptocurrencies (or stablecoins) and CBDCs and among the latter. CBDCs open a channel for dollarization far more efficient than traditional cash circulation, with potentially huge impact on the competition for seigniorage and the incentives to introduce capital controls.

6. References

Adrian (2019): Stablecoins, Central Bank Digital Currencies, and Cross-Border Payments: A New Look at the International Monetary System.

[19] *Annual Report 2018/2019*. Bank for International Settlements, May 2019

https://www.imf.org/en/News/Articles/2019/05/13/sp051419-stablecoins-central-bank-digital-currencies-and-cross-border-payments

Adrian, T. and T. Mancini Griffoli (2019): The Rise of Digital Money, IMF FinTech Notes No. 19/001, https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097

Bech et al (2018): Payments are a-changin' but cash still rules. https://www.bis.org/publ/qtrpdf/r_qt1803g.htm

Binance Research (2019): First Look: China's Central Bank Digital Currency

https://info.binance.com/en/research/marketresearch/CBDC.html

BIS (1997): Real-time Gross Settlement Systems. https://www.bis.org/cpmi/publ/d22.pdf

BIS (2017): Distributed ledger technology in payment, clearing and settlement. An analytical framework. https://www.bis.org/cpmi/publ/d157.pdf

BIS (2019): Annual Report 2018/2019. https://www.bis.org/about/areport/areport2019.pdf

EBA (2019): Report on crypto-assets with advice to the European Commission. https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf

ECB (2018): Securities settlement systems: delivery-versus-payment in a distributed ledger environment. https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf

Fernández de Lis and Gouveia (2019): Central Bank digital currencies: features, options, pros and cons. https://www.bbvaresearch.com/en/publicaciones/central-bank-digital-currencies-features-options-pros-and-cons/

Gouveia et al (2017): Central Bank Digital Currencies: assessing implementation possibilities and impacts. https://www.bbvaresearch.com/en/publicaciones/central-bank-digital-currencies-assessing-implementation-possibilities-and-impacts/

Greenwich Associates (2019): Steampunk Settlement. Deploying Futuristic Technology to Achieve an Anachronistic Result. https://www.greenwich.com/sites/default/files/files/reports/Steampunk-Settlement.19-2018.pdf

International Telecommunications Union (2019): ITU-T Focus Group Digital Currency including Digital Fiat Currency -- Reference Architecture and Use Cases Report, https://www.itu.int/en/ITU-T/focusgroups/dfc/Documents/DFC-O-014_RA%20Delivrable_Reference%20Architecture%20and%20Use%20Cases%20Report.pdf

Libra Association (2019): Libra White Paper.
https://libra.org/en-US/white-paper

Nakamoto (2008): Bitcoin: A Peer-to-Peer Electronic Cash System.
https://bitcoin.org/bitcoin.pdf

Rogoff, K. (2016): The curse of cash, Princeton University Press
https://press.princeton.edu/titles/10798.html

Schneider, F (2019): Restricting or Abolishing Cash: An Effective Instrument for Eliminating the Shadow Economy, Corruption and Terrorism? SUERF Policy Note, Issue No 90
https://www.suerf.org/policynotes/6951/restricting-or-abolishing-cash-an-effective-instrument-for-eliminating-the-shadow-economy-corruption-and-terrorism/html