DISCUSSION PAPER SERIES

DP13728

WELFARE AND POLITICAL ECONOMY ASPECTS OF A CENTRAL BANK DIGITAL CURRENCY

Alex Cukierman

INTERNATIONAL MACROECONOMICS AND FINANCE AND MONETARY ECONOMICS AND FLUCTUATIONS

ISSN 0265-8003

WELFARE AND POLITICAL ECONOMY ASPECTS OF A CENTRAL BANK DIGITAL CURRENCY

Alex Cukierman

Discussion Paper DP13728
Published 12 May 2019
Submitted 10 May 2019

Centre for Economic Policy Research
33 Great Sutton Street, London EC1V 0DX, UK
Tel: +44 (0)20 7183 8801
www.cepr.org

WELFARE AND POLITICAL ECONOMY ASPECTS OF A CENTRAL BANK DIGITAL CURRENCY

Abstract

The point of departure of this paper is that, in order to preserve the effectiveness of monetary policy in a world increasingly flooded by private digital currencies, central banks will eventually have to issue their own digital currencies. Although a non-negligible number of central banks (CBs) are actively considering the pros and cons of a central bank digital currency (CBDC) there is yet no CB that has issued such a currency on a full scale. Following a brief survey of current CBs positions on the issuance of a CBDC the paper presents two proposals for the implementation of such a currency: A moderate proposal in which only the banking sector continues to have access to deposits at the CB and a radical one in which the entire private sector is allowed to hold digital currency deposits at the CB. The paper compares and contrasts the implications of those two polar paths to a CBDC for the funding of banks, the allocation of credit to the economy and their implications for welfare as well as for political feasibility. One section of the paper shows that the radical implementation may pave the way toward a narrow banking system and dramatically reduce the need for deposit insurance in the long run. The paper evaluates the relative merits of issuing a currency on a blockchain using a permissionless distributed ledger technology in comparison to a centralized (permissioned) blockchain ledger operated by the CB and concludes that the latter dominates the former in more than one dimension. But it does acknowledge that distributed ledger technologies have many actual and potential cost savings benefits in other segments of the financial and real sectors.

JEL Classification: E5, E4, H41

Keywords: Central bank digital currency, blockchain technology, permissioned, permissionless, centralized versus decentralized currencies, narrow banking

Alex Cukierman - alexcuk@tauex.tau.ac.il
Tel-Aviv University and Interdisciplinary Center and CEPR

Welfare and Political Economy Aspects of a Central Bank Digital Currency

Alex Cukierman[1]

April 9 2019

ABSTRACT

The point of departure of this paper is that, in order to preserve the effectiveness of monetary policy in a world increasingly flooded by private digital currencies, central banks will eventually have to issue their own digital currencies. Although a non-negligible number of central banks (CBs) are actively considering the pros and cons of a central bank digital currency (CBDC) there is yet no CB that has issued such a currency on a full scale. Following a brief survey of current CBs positions on the issuance of a CBDC the paper presents two proposals for the implementation of such a currency: A moderate proposal in which only the banking sector continues to have access to deposits at the CB and a radical one in which the entire private sector is allowed to hold digital currency deposits at the CB. The paper compares and contrasts the implications of those two polar paths to a CBDC for the funding of banks, the allocation of credit to the economy and their implications for welfare as well as for political feasibility. One section of the paper shows that the radical implementation may pave the way toward a narrow banking system and dramatically reduce the need for deposit insurance in the long run.

The paper evaluates the relative merits of issuing a currency on a blockchain using a permissionless distributed ledger technology in comparison to a centralized (permissioned) blockchain ledger operated by the CB and concludes that the latter dominates the former in more than one dimension. But it does acknowledge that distributed ledger technologies have many actual and potential cost savings benefits in other segments of the financial and real sectors.

JEL Classifications: E5, E4, H41

Keywords: Central bank digital currency, blockchain technology, permissioned, permissionless, centralized versus decentralized currencies, narrow banking.

---

[1]Tel-Aviv University and Interdisciplinary Center, Herzeliya. Email: alexcuk@tauex.tau.ac.il. This paper was presented at the April 2019 meeting of the European Public Choice Society at the Hebrew University in Jerusalem. Etienne Farvaque made useful comments

1. Introduction

The emergence of blockchain and related technologies for the production of cryptocurrencies like Bitcoin has the potential to fundamentally alter the ways the macroeconomic system, the money supply process, and the financial system operate. While it opens up a whole range of welfare enhancing opportunities due to reduction in transaction costs, it also introduces new risks and problems. To this point the financial press focused mainly on the risks associated with large fluctuations in the price of a bitcoin, the lack of transparency about the producers of cryptocurrencies and their motives, the problems of security and potential hacking, the ease with which a digital currency like bitcoin can be used to finance illegal transactions, and the potential benefits of blockchain technology for the efficiency of the financial system.

Relatively less attention has been paid to the implications of a future world dominated by privately produced cryptocurrencies for the conduct of national monetary policies. In particular, the effectiveness of monetary policy instruments in stabilizing shocks to the economy during both normal and abnormal times (such as those experienced during the recent financial crisis) will be greatly reduced or even destroyed. Relatedly, the consequences of economic shocks to a single country will be harsher because mitigation of such shocks by means of exchange rates adjustment through monetary policy actions will become infeasible in the presence of a world dominated by privately produced, profit seeking, issuers. Finally, the sovereign will lose the seigniorage income from issuing its own currency and will have to replace this lost income by taxes which have welfare-reducing consequences.

Sceptics may argue that the above drawbacks are more than compensated by the efficiency gains made possible in a world dominated by private digital currencies. This spectisism is misplaced for the following basic reason: Governments and central banks aim at the maximization of national social welfare while, profit motivated, private issuers of a world currency do not internalize the impact of their actions for the rest of society. In a world dominated by political considerations the attempts of public institutions to cater to the public interest may not be totally successful. However, being subject to public scrutiny and periodic elections, public officials are more likely to be closer to the

maximization of social welfare than private producers of a digital currency whose only objective is the maximization of profits.

One way to preserve the potency of monetary policy while appropriating the substantial transaction costs savings associated with the new fintech technologies is to issue central bank digital currencies (CBDCs).[2] By offering a legal tender digital currency a national central bank (CB) can maintain a sufficiently large share of publicly produced world currency to maintain the potency of its monetary policy in the national area. Although a non-negligible number of central banks (CBs) are actively considering the pros and cons of a CBDC there is yet no CB that has issued such a currency on a full scale.

The issuance of a CBDC on a broad scale raises both purely economic as well as political economy problems. By competing with private bank deposits the issuance of such a currency will strip banks from a major source of funds possibly endangering the stability of the financial system. Since, in addition to anticyclical monetary policy, CBs are also in charge of financial stability this creates a tension between anticyclical policy and financial stability. One extreme position on this dilemma is to abstract from this problem and let the chips fall where they may - - possibly moving a large chunk of current private banks' activities into the CB. This may force CBs into the process of credit allocation to the economy. This is undesirable since private banks are better equipped to evaluate the risks associated with various types of loans than the CB.

Furthermore, a cold turkey implementation of the CBDC proposal is likely be politically infeasible because politically powerful banking interest are very likely to vigorously oppose an extreme institutional implementation. Last but not least, centralized allocation of credit through the CB is very likely to invite political meddling on the part of governments blurring the line between fiscal and monetary policies and endangering CB autonomy. It is therefore important to devise a more balanced approach to the institutional implementation of CBDCs.

The organization of the paper follows. Section 2 discusses current positions of CBs on the issuance of a CBDC. Section 3 describes two proposals for the implementation of a CBDC – a radical one in which the general public is allowed to hold

[2] Private digital currencies have already largely replaced cash in Sweden and China.

deposits at the central bank, and a moderate one in which only banks have deposits at the CB (as is the case today) and evaluates their relative merits. Section 4 discusses political economy problems originating in the private banking system that are likely to arise with the issuance of a CBDC.

Motivated by Roubini (2018) testimony to the US congress section 5 describes and analyzes the synergy between such a move and a potential revival of the old narrow banking system proposal. Section 6 evaluates the relative merits of issuing a currency on a blockchain using a permissionless distributed ledger technology in comparison to a centralized (permissioned) blockchain ledger operated by the CB and concludes that the latter dominates the former in more than one dimension. Nonetheless distributed ledger technologies have many actual and potential cost savings benefits in other segments of the financial sector and the real sector. This is acknowledged in section 7 by briefly discussing the numerous applications of (mostly permissioned) distributed ledger technologies. A brief conclusion follows.

2. Current positions of CBs on the issuance of CBDCs

To date the views of major central bank on the desirability of issuing a CBDC are mixed. On one hand they are attracted by the efficiency gains that can be obtained through the incorporation of the new technology. On the other hand some are worried that it may interfere with the functioning of the private banking system particulary if the public is allowed to hold deposits at the central bank. There are two types of concerns. One is that such a move will drastically reduce demand deposits in the banking system stripping private banks from an important source of funds. The other (expressed, among others, by Bank of England governor Mark Carney) is that during crisis times all funds will swiftly flow into the central bank forcing it to assume the role of a major financial intermediary.

But abstaining from providing a public alternative to privately produced digital currencies carries the risk that sooner or later those currencies will largely replace legal tender. Recognizing this risk most central banks currently research the various options for eventually adopting some form of CBDC. Some like the Dutch central bank and the

central bank of Uruguay have even experimented on a limited basis with such a currency and, the Federal Reserve Bank is considering the issue of a Fedcoin. [3]

3. Two proposals for the implementation of a CBDC: Radical and moderate

Central banks can appropriate some of the benefits of the new technology of a digital currency without abandoning the monetary policy instrument by issuing their own publicly provided digital currencies that would be freely convertible at a fixed one-to-one exchange rate into cash and paper currencies. Unlike privately produced digital currencies a central bank digital currency (CBDC) would have the status of legal tender so that the traditional definition of narrow money (M1) would now include, in addition to demand deposits and cash held by the public, also the CBDC. As is the case with cash and demand deposits the distribution of the three components of the wider M1 concept would be determined by the public's relative demand for them. Digital currency held by banks at the CB would, as is the case today, be considered as reserves and the monetary base would include, in addition to bank reserves and cash, also the CBDC. This extended, three components base, would provide the financial depth needed to determine the desired policy rate through appropriate open market operations in the same manner as is the case today with the two components base.

There obviously is more than one way to implement the institutional details of such a CBDC. I will focus on the following two alternatives: [4] (i) A radical version in which the CB (taking advantage of the transaction cost savings afforded by the new technology) allows the general public to keep digital currency accounts directly at the CB. As a consequence individual private transactions can be cleared directly at the CB. (ii) A moderate version in which the CB maintains the long institutional tradition that only banks can keep deposits at the CB. In both cases the public has access to CBDC but in the moderate version this access is implemented via the private banking system rather than directly. Thus, if a private individual desires to buy CBDC she can do that only through a private bank in exchange for funds from either a checking deposit or cash. The

[3] A number of CBs have issued reports on this question (Lober and Houben (2018). Barontini and Holden (2019) report limited experiments with CBDC by the central bank of Uruguay and the Riksbank.
[4] Bordo and Levin (2017) investigate various options for the implementation of such a system.

bank can then replenish its stock of CBDC at the CB by running down its reserve balance.

By contrast, in the radical version the individual can obtain CBDC from other private individuals with accounts at the CB without the mediation of the private banking system. The difference between the radical and the extreme versions from the point of view the private banking system is fundamental. In the first case banks stand to lose a large chunk of their traditional business. Similar elements may operate in the moderate case albeit in a substantially attenuated fashion. Those differences raise important welfare and political economy questions that are briefly discussed in the next section.

4. Political economy problems raised by the issuance of CBDC

A radical implementation of CBDC appears risky on both economic efficiency grounds as well as impractical in the foreseeable future even if the CB and the financial system finally adopt such a system in the long run. The radical implementation would lead to a wholesale migration of checking deposits from private banks to the CB stripping the former from a relatively abundant and cheap sources of funds. At least in the short run this would reduce banking credit to the economy, force the banks to look for alternative sources of funds and may lead to an increase in bank failures. In parallel there would be pressures on the CB to make up for the lost credit pushing it to get involved in the allocation of credit to the economy.

Due to both welfare and efficiency considerations this is undesirable for several reasons. One of the main functions of banks is to evaluate the credit worthiness of different borrowers and to monitor them in order to channel funds mainly to viable projects. Clearly private banks have a comparative advantage in doing that relatively to CBs. The upshot is that, on purely welfare grounds, it is better to leave the allocation of credit to private financial institutions. Involving the CB in the allocation of credit to the economy is also undesirable since it is likely to draw CBs into the political arena, open the door for crony capitalism and ultimately jeopardize their autonomy as relatively non-political professional bureaucratic institutions. Those considerations imply that, as long

as substantial private substitutes for banking credit do not emerge, stability of the banking system is a public good worthy of safeguarding.

Due to the political clout of banks there also are serious practical impediments to the implementation of a radical version of a CBDC. Although this statement applies to many countries it is particularly true for developed economies with well-developed financial sectors like the US in which banks provide a large chunk of political contributions to candidates seeking election to Congress, the white house and numerous other state legislative bodies.[5] Hence, even legislation seeking to empower the CB with a relatively modest ability to issue its own digital currency is likely to encounter lobbying and political opposition. This is a fortiori true for any initiative based on the radical version of such a currency. Such an initiative is highly unlikely to be seriously considered by legislators. Hence, in the foreseeable future, the moderate proposal for implementation of a CBDC that gives a non-negligible weight to the interests of a private banking system is preferable on economic welfare grounds and more practical due to political economy considerations.

Last but not least a modest start on the issuance of a CBDC mitigates the substantial uncertainties involved in the introduction of this institutional change against the background of existing and forthcoming adoption of fintech innovations by the private financial system.[6] Both developments are likely to eventually radically alter the character of the private financial system as well as that of the CB. Although, this process may eventually converge toward a system that is nearer to the radical than to the moderate version the second version, by opening opportunities for learning along the way, is likely to be less bumpy.

Having said that, it important to keep in mind that CBs have to maintain sufficient ammunition for effective conduct of monetary policy for the public good through the various phases of the upcoming transformation. Abstaining from issuing a CBDC in a financial world that is in the process of adopting fintech innovations on a wide scale is likely to seriously dent the effectiveness of monetary policy. But both the seriousness of

[5] Igan and Mishra (2014) provide detailed evidence for this phenomenon in the US.
[6] A recent survey of the impact of blockchain technology on finance and some of its implications for the future appears in Casey et. al. (2018). A brief summary appears in section 7 of this paper.

this threat and its timing are hard to predict in advance. Under the moderate proposal the CB can maintain the effectiveness of monetary policy by adjusting the stock of CBDC in line with changing circumstances without forcing it into the role of a major credit supplier to the private sector.

The upshot is that CBs better start to experiment with, at least initially, a moderate version of a CBDC sooner rather than later in order not to leave the continuity of monetary policy "behind the curve".

5. Central bank digital currency as a catalyst for revival of the old narrow banking system idea

In a recent testimony for the hearings of the US Senate Banking, Housing and Urban Committee Roubini (2018) convincingly argues in favor of using the new fintech technology along with centralized ledgers (CL) rather than using the blockchain technology to implement distributed ledger technologies (DLT- also called a shared ledger). A DLT is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple internet sites, in different countries and institutions with no central administrator or centralized data storage. In a similar vein Aizenman (2019) and Auer (2019) argue that, since they suffer from the tragedy of the commons, privately administered DLT are unlikely to provide the stability and scalability required to efficiently perform the medium of exchange function.

A centralized ledger could be administered by sufficiently large and reliable institutions within either the private or the public sector. For advanced economies with well-developed financial systems centralization within the public sector appears to be a first best. Given this assessment the CB is a choice institution for appropriating the cost savings provided by the existing fintech technology. The CB already possesses the infrastructure for issuing a currency and is backed by the tax collection apparatus of governments. [7]

[7] In emerging markets like China or Africa in which large chunks of the population have no bank accounts a private entity may be more desirable. Two prominent examples are the Alipay payment system administered by Alibaba in China and the Empera system in some African countries.

Following the great depression Irving Fisher became a strong supporter of the "Chicago plan" that advocates the establishment of a 100% percent reserve requirement on banks. Both Fisher as well as the University of Chicago economists behind the Chicago plan proposal believed that, by increasing the CB's control of credit, this institutional change will greatly reduce the likelihood of financial crises. But, as is well known, this idea was never implemented.

Following the global financial crisis a modern reincarnation of the idea, adapted to the much deeper current financial markets, was proposed by Cochrane (2014). Cochrane proposes that banks should be funded by equity and that their fixed-value debt should be 100% backed by Treasury or Fed obligations.[8] But this idea did not take into consideration the potential longer term natural interaction between the issuance of a CBDC and the replacement of a fractional reserve banking system by a fully backed system. The likely reason is that even Cochrane (2014) version of a fully backed private banking system arose before the potential emergence of a private digital currency prompted the world central banks to seriously consider the issuance of a CBDC.

At a keynote address on CBDC at the January 2019 World Economic Forum in Davos Roubini envisaged three possible options for the issuance of such a currency. The first is basically the moderate proposal discussed in section 3. The CB adds a digital CB currency to the money supply but private individuals have access to the CBDC only through the banking system so that the existing fractional banking system remains in place. The other two options considered by Roubini are basically two variants of the radical proposal discussed in section 3 in which all individuals in the economy have direct digital accounts at the CB. In both cases the private banking system will, most likely, lose deposits as a source of funding for credit operations transforming it into a De facto narrow banking system. The two variants considered by Roubini differ in the potential way the private banking system will be compensated for the loss of this source of funds. In a somewhat middle of the way proposal the CB could make up for this loss

[8] During 2015 a Swiss group collected the 100,000 signatures necessary to require a national referendum on requiring banks to hold 100% reserves but the proposal was rejected.

by raising the level of banking reserves or rely on the ability of banks to find other long term sources of funds like equity, long term loans, certificates of deposits and other shorter term market based liquidity instruments like repos to replenish temporary liquidity deficiencies. In line with the terminology of section 3 I will refer to the first variant as radical proposal 1 and to the second as radical proposal 2. As pointed out by the advocates of a fully backed narrow banking system the main advantage of the (two variants) of such a system is that it will greatly reduce the risk of banking panics and financial crises possibly eliminating the need for deposit insurance and the associated regulatory apparatus.

Making predictions about the distant future is a hazardous business. Given our current state of knowledge I would still venture the following educated guess about the likelihood of a CBDC cum narrow banking system emerging in developed economies within the next twenty or more years. Sooner or later the potential disruptions to the conduct of monetary policy and the risks associated with private digital currencies will force CBs to issue a CBDC. Due to the substantial cost savings afforded by having direct clearing of daily transactions at the CB it is likely that after a period of experimentation with the moderate version some CBs will allow all individuals to hold accounts at the CB forcing the private banking system to ultimately find alternative sources of funds within the private sector as in radical version 2. For reasons discussed in section 4 the process may be a lengthy and tortuous one due to the strong opposition of banks and their political clout. But if and when the advantages of an institutional arrangement made possible by the new fintech technology become clear to the general public and legislators the emergence of a system in which banks do not rely on checking deposits for the funding of credit operations may become a reality.

It is important to stress, however, that CBs should limit their activities to the area in which they have a comparative advantage. That is; the provision of a stable, scalable and secure mean of payments. Provision of credit to the private economy should be left to private banks and other private financial institutions since they have a comparative advantage in evaluating the risk involved in granting loans to various projects and individuals. Furthermore, involvement of CBs in the allocation of credit is dangerous for their hardly won independence since it opens the door for political pressures concerning

the allocation of credit and the associated crony capitalism prevailing in countries such as China. Hence potential future temptations to have the CB engage in the allocation of credit to the economy should be strongly avoided.

6. Building and maintaining trust in a currency: centralized vs decentralized systems

As is well known an essential attribute of a good currency is widespread acceptability by economic agents against the supply of goods and services. A precondition for this attribute is trust in the currency. Individuals must trust that the currency has a stable purchasing power, will not be debased by the issuer(s) of the currency and that private ownership of currency is fraud proof. Under current monetary arrangements this trust is achieved through centralized ledgers administered by national central banks that are granted a monopoly on the issuance of fiat money. In practically all developed economies and many developing countries two important layers underlying this trust are inflation targeting and the willingness of governments to accept settlements of tax obligations in fiat currency. [9] Like cash or checking deposits denominated in fiat currency a CBDC would rely on the trust created by means of the centralized ledger administered by the bank.

At the other extreme are fully decentralized contender currencies like bitcoin in which trust is achieved by using the blockchain technology. Blockchains are built upon a well-known problem in computer science called "distributed consensus". Distributed consensus is the problem of how multiple, independently run computers can reliably agree on the validity of a common data set where there is a risk that one or more computers are intentionally or unintentionally programmed to introduce false information.[10]

A blockchain is a computerized (distributed) ledger that relies on cryptographic techniques and is designed to be read by a computer, rather than by the human eye. A blockchain is characterized by the following features:

[9] Stable coins backed by USD are appropriating some of the trust built into that fiat currency by fully collateralizing those coins with USD. One example) is ether.

[10] This problem arises in large distributed networks like the internet, and many software companies employ distributed consensus algorithms to protect access to critical data. A succinct overview of blockchain technology appears in chapter 1 of Casey et. al. (2018).

(i) The ledger is shared among and worked on by multiple, possibly distrusting, participants, none of which has a single point of control over it.

(ii) An ever-growing chain of ledger entries links the entire history in such a way as to prevent tampering with or rewriting past records.

(iii) Digitally signed transactions or instructions indicate intent to record or modify data, or to transfer digital assets across electronic purses.

(iv) Joining the ledger is open to anybody that has sufficient computing hardware and knowledge. The ledger is therefore "permissionless" as opposed, for example, to a "permissioned" ledger that can be accessed only by one or a limited group of members.

Trust in the ledger of a fully decentralized currency is achieved by making it extremely hard for one, or a small group, of computers to tamper with the transaction ledger. This is achieved by a built in requirement that any new transaction must be approved by a majority of computer nodes. In addition the protocol that governs the ledger of a fully decentralized currency must include a built in provision that limits the creation of new money in order to preserve its purchasing power. Cryptography is the computer technique used to secure transactions and to control the creation of new currency units.

The bitcoin blockchain protocol was first proposed in a white paper by the mysterious Nakamoto (2008).[11] The paper argues it is possible to replace centralized authorities that verify currency – commercial and central banks. – with a decentralized public blockchain of transactions. People trust that the existing fiat currency issued by a centralized authority has stable value because of stable monetary policies, because the currency can be used to pay taxes to government, and because it is impossible for anyone to spend the same dollar more than once. The blockchain protocol can offer trust in a decentralized currency system and solve the double-spending problem, without a central bank by devising a system in which the owners of the computer nodes have a private interest in approving only legitimate past and current transfers of coins from one electronic purse to another one.

A coin on a blockchain refers to the "chain of digital signatures" that makes up the history of a transaction, where an exchange is a transfer of control of coins from the

[11] Further details on some computer aspects of this protocol appear in the appendix.

sender's wallet to the recipient's wallet. The money transfer protocol for user X to transfer coins to user Y is as follows: User X's coin client arranges a set of prior transfers to X which, when added together, are of equal or greater value than the intended value to be sent to Y. If the value of prior transfers is greater than the amount to be sent, then X transfers the "change" value back to a new address of his own. Note that an address is a hashed form of a public key. X proves these transfers are genuine by signing them with his private key, affirming in a publicly verifiable way (via public key) that X and only X chose to execute the transaction. Accordingly, any transfer of currency contains the evidence that the transferor has the funds to back up the transaction. A wallet is a cryptocurrency analogue to a conventional bank account. Wallets allow users to receive, store, and send digital money relying on public key cryptography. Wallets can generate new public-private key-pairs anytime, and reveal no information a priori on the identity of the user operating it.

As elaborated in the appendix a node that gets to seal a pending set of transactions by creating a new block on the chain is remunerated by the protocol through the creation of a predetermined amount of bitcoins leading to an increase in the aggregate stock of bitcoins. By analogy to gold this activity is called "mining" and the computer nodes that compete for closing the next block are called "miners". Thus, on average, bitcoin seignorage accrues to the miners that have faster and deeper computing power. The protocol only recognizes the longest chain in the system. The parameters of the bitcoin protocol are adjusted periodically in line with improvements in computing power so as to make the transfer of the same coin twice by creating a new chain prohibitive for a single or a non-majoritarian group of nodes.[12]

As a single shared ledger, blockchain has the potential to reduce the fragmented reconciliation of ledgers across and within existing financial institutions such as banks, brokerage houses, mutual funds, and pension funds. With a single source of truth, transactions enjoy instant settlement instead of taking days, because payment is settlement -- which means improvements in transaction time, cost, transparency, and security. Recording, clearing, settlement, and reconciliation across multiple organizations

[12] To date the blockchain created since the inception of bitcoin about ten years ago has been impervious to hackers attacks.

or different units within the same organization are collapsed into one step. There is little doubt that those fintech advantages hold great potential for cost reduction in private financial institutions, maintenance of shared medical records, trade and forex transactions. Some of those benefits have already been internalized and are surveyed in section 7. Those advantages along with the anonymity made possible through the provision of a private currency led blockchain enthusiasts to support the decentralization of money creation.[13]

On the other hand a fully decentralized, blockchain private currency a la Nakamato such as bitcoin is most likely to be dominated by a CBDC for the following reasons:

(i) As stressed by Budish (2018) establishment of trust in a decentralized private digital currency on a blockchain requires that a majority attack on the system in order to double spend be prohibitively costly and that each of the self-interested miners that compete for adding the next block to the chain be small in comparison to the total mass of miners. As a consequence the electricity costs of running the decentralized system are substantial. One might hope that those costs would decrease over time, along with advances in hardware technology.

But this is not the case for the following reason: In order to assure that pending transactions are executed every ten minutes on average subject to the first condition above, the level of difficulty of the hash puzzle that has to be solved by miners is periodically adjusted upward in parallel with technological improvements.[14] Thus, the large electricity costs incurred by miners are, inherently, a necessary condition for the establishment of trust in permissionless decentralized systems. Since no such expenditures are needed to maintain trust in existing centralized systems administered by central banks this is a deadweight loss.[15] This view is also backed by Computer Scientists that are more familiar with the technical aspects of a blockchain decentralized currency.

---

[13] Although the final verdict on the alternative centralized CBDC is not in yet, some policymakers expressed doubts about its desirability on the ground that such an action could stifle fintech innovations in the private sector (Lagarde (2018)).

[14] The definition of a hash appears in the appendix.

[15] It should be stressed that this drawback does not apply to blockchains in permissioned partially decentralized applications in which trust is achieved by other means. More on this in section 7

In particular Gupta et. al. (2017) conclude their case in favor of issuing a digital currency by the Fed as follows:

"One of Fedcoin's main advantages over Bitcoin is the fact that it dramatically mitigates the risk of 51% attacks.. .. Fedcoin's threat model is based on the assumptions that the central bank is honest, the protocol's cryptography is secure, and that each transaction is processed by a set of Nodes with an honest majority. Should these hold true, double-spending will not be possible and commits issued by Nodes will be non-repudiable. …the Fed has total and complete auditability of Nodes, the low-level blocks they issue, and the logs they print, in order to cement the system's integrity. Moreover, Nodes have the incentive to provide honest service from the fee paid to them by the central bank for their performance in transaction".

(ii) One element of trust in a digital currency is the belief by individuals that in case of hacking individuals that suffer losses will be compensated. Compensatory schemes are more likely to be implemented by a centralized authority such as the CB that operates a verifiable ledger than within an anonymous decentralized private system.

(iii) One argument against a centralized ledger administered by a private institution opens the door for the extraction of monopolistic rents. This obviously could be regulated but it is more efficient to prevent that by a radical version of a CBDC since central banks are subject to public scrutiny and oversight.

(iv) In 2014 the Ethereum Foundation launched a new decentralized coin called "Ether". To avoid the large costs for establishment of trust via "proof of work" in the bitcoin ecsoystem the Foundation is developing an alternative system based on "proof of stake". Proof of stake is based on the idea that a miner would have to demonstrate that he has a sufficiently large stake in the Ether ecosystem. Although it avoids some of the large electricity costs associated with bitcoin the new system is conducive to the emergence of market power opening the door for collusion and price manipulations.

As a matter of fact Gandal et. al. (2018) report evidence of price manipulation even on a bitcoin exchange during periods of relatively strong price increases. This should not be too surprising since the inability to identify the individuals or companies behind impersonal electronic wallets opens the door for collusion neutralizing the competition between miners required by the Nakamoto protocol for a clean operation of

the system. In particular, the same company can own numerous anonymous accounts (or nodes) covering up the fact that they all belong to one large interested party.

(v) Last but not least, displacement of traditional fiat or digital central bank currency by a decentralized permissionless currency operated by rent seeking miners neutralizes the ability to conduct monetary policy for the public interest. A brief discussion appears in the introduction.[16]

7. Can private digital instruments coexist along with a CBDC and should they be tolerated?

In my view once a clear boundary is established between the provision of a stable, scalable and secure mean of payments by the central bank and all other forms of financial investments vehicles the answer to this question is a resounding yes. This view actually underlies recent rulings by tax authorities and central banks that consider bitcoin, initial coins offerings as well as various versions of so called “stable currencies” backed by fiat dollars, gold, silver, real estate, diamonds and other forms of collateral as additional private investment vehicles rather than digital currencies. [17]

The emergence of such additional financial assets is likely to increase aggregate welfare by introducing more variety into the menu of financial assets offered to pension funds, insurance companies, hedge funds, private individuals and other thrift institutions. There is little doubt that the current proliferation of such ventures is exaggerated and that many of the newly born private digital versions of such assets will disappear after being tested by market preferences. But those that will survive are likely to increase public welfare provided the minimal adequate regulations are ultimately established.

At the very least private digital instruments possess the following two advantages: First, by swiftly introducing the fintech technology to reduce the costs of transacting across different fiat currencies, they compete with the grossly inflated commission of banks in this area inducing further substantial future decreases in forex transaction commissions. Second, in (mainly agrarian) countries with underdeveloped financial

[16] A broader discussion appears in Amihud and Cukierman (2018) and a model oriented analysis in Benigno (2019).
[17] Lagarde (2018) expresses guarded support for issuance of CBDC provided it does not stifle the application of fintech innovations in the private sector. See also Mancini-Griffoli et.al. (2018).

systems in which large chunks of the population have no access to bank accounts, nor to credit, private digital currencies are already filling some of this gap and have the potential to further broaden the access of the currently excluded individuals to financial services. In parallel with the banning of bitcoins Chinese authorities are considering the issuance of a CBDC. Since such private systems already exist (Alipay and WeChat) it would be a relatively easy matter for Bejing to pressure those institutions to adopt the digital Yuan.[18] The downside of such a move in a totalitarian country like China is that it would facilitate surveillance of the citizens by the central government.

As argued at length in the previous section the provision of a stable trust-worthy digital currency by the central bank dominates the provision of such a currency through a permissionless decentralized blockchain technology in more than one dimension. But the blockchain technology has numerous other cost reduction advantages in a variety of areas. Some of those are already operational and others are in various stages of development. The bulk of those applications are embedded in permissioned systems with a limited number of participating nodes in which mutual trust does not rely on the costly proof of work device. Those versions of the blockchain technology are already being used within both the financial and the real sector and have great potential for further efficiency and cost reduction gains.

Within the financial sector permissioned blockchain systems are used for the swift reconciliation of post trade processes in banks, brokerage houses, custodians and clearing houses. Efforts are being made to develop platforms in which the issuance of bonds and loans would be placed on a blockchain so that all parties concerned would possess a shared record of transactions and updates replacing the manual methods used currently. Posting transactions records on distributed ledgers facilitates the tracking of trade finance operations as well as the work of regulators. Examples of blockchain applications beyond the financial sector are the tracking of inventories and supply chains within and across interconnected firms, the automatic sharing of medical records produced by different suppliers and the swift identification of individuals through the network. A detailed

[18] See for example: https://medium.com/altcoin-magazine/chinas-push-to-issue-digital-currency-may-have-an-unintended-boost-for-cryptocurrency-86ccc983b8c3

discussion of existing and prospective applications of permissioned DLT appears in chapters 3 and 5 of Casey et. al (2018).

8. Concluding remarks

Although DLT on blockchains have many useful existing and prospective applications within both the financial and the real sectors this is not the case for supplying a stable and trustworthy currency to the economy. A centralized ledger operated by the CB clearly dominates private permissionless distributed ledgers in more than one dimension. Furthermore, unlike bitcoin that relies on permissionless DLT in which trust is established by proof of work, most useful applications for other purposes are permissioned blockchains that establish trust by other means.

To date practically all CBs did not introduce digital currencies leaving this area widely open to the private sector. In countries with prior limited access to bank accounts like China and many African countries this function has been filled by centralized private networks. All over the world various private digital coins are being circulated competing for the potential rewards to be reaped by establishing themselves as currencies. CBs better introduce their own digital currency sooner rather than later in order to provide a dependable currency and preserve the ability to conduct monetary policy. By competing directly with the numerous aspiring private currencies such a move will also potentially reduce the burden of additional regulation of such coins.

In the long run issuance of a CBDC is likely to provide immediate clearing of transactions across individuals dramatically reducing the costs of clearing. This may substantially reduce the funding of private banks through checking deposits and open the door for a narrow banking system. Such a radical implementation of a CBDC is likely to encounter political opposition from the financial sector and may take a long time to materialize. On the other hand a radical version of a CBDC in which the public is allowed to hold checking deposits at the CB has a number of advantages. First, it shortens the channels of transmission of monetary policy to the economy. Second, by replacing cash a CBDC makes it possible to bypass the zero lower bound restriction. Finally, provided a radical version of a CBDC is ultimately implemented leading to the replacement of the existing fractional reserve system by a 100% reserve requirement the

likelihood of runs on banks runs would be greatly reduced along with the need for deposit insurance.

Appendix: A brief exposition of computer science concepts underlying the blockchain technology:[19]

A network protocol is a set of rules for crediting accounts and a blockchain is a data structure that serves as a public digital ledger and is shared across a distributed network of computers. As an immutable record, it stores transactions in the form of a time ordered series. The blockchain protocol describes a chain of blocks where a block is a group of transactions that have been sealed and added to the existing chain of blocks at the same point in time.

Any participant in the blockchain network can add a new block to the chain, as long as a majority of the other participants in the network ratifies the addition. When a computer node proposes the addition of a new block, the other nodes check the blockchain transaction history to ensure the new transactions proposed are valid. If a majority of the network approves the new block it is appended to the last block in the chain increasing the length of the chain. In addition to the new transactions included in the proposed new block this block also contains the output of a cryptographic hash function of the content of the block to which it is chained. A cryptographic hash function is a deterministic function that maps an input of any length into an output of fixed length. [20] This timestamps the block in the chain and guarantees that the chronological ordering of the blocks in the chain is known by all nodes.

The network only considers the longest chain of blocks at any given point to be the working blockchain, which is continually ratified by at least 50% of the network. This stipulation, along with "proof-of-work", consisting of finding solutions for computationally intensive hashing puzzles, makes it near impossible to double-spend a coin or modify a transaction once added to the ledger.[21] The first node to solve the hash puzzle is rewarded by the network with newly created currency, increasing the existing

[19] This appendix partially draws on section 2 of Gupta et.el. (2017).
[20] Independently of the size of the input, the output always has a fixed length of 256 bits.
[21] This involves using CPU intensive computer simulations to find a guess for the input of a hash given its output that is sufficiently near to a preassigned target value.

stock. In addition it also collects the commissions offered by the issuers of pending transaction that are executed and sealed at the time of the block closing.

References

Aizenman J. (2019), "On the built in instability of cryptocurrencies", Presented **at the Bitcoin Economic Forum in Davos,** January 24-25 2019.

Auer R. (2019), "The doomsday economics of 'proof-of-work' in cryptocurrencies", in Fatas A. (ed.), **The Economics of Fintech and Digital Currencies**, a VoxEU.org eBook, March.

Amihud Y. and A. Cukierman (2018), "The macroeconomic perils of a world with a private digital currency and how to address them**", CEPR VoxEU Blog**, October 9. https://voxeu.org/content/macroeconomic-perils-world-private-digital-currency-and-how-address-them

Barontini C. and H. Holden (2019), "Proceeding with caution – a survey on central bank digital currency", **BIS Papers 101**, January.

Benigno (2019), "Monetary policy in a world of cryptocurrencies", CEPR DP 13517, February.

Bordo M. and A, Levin (2017), "Central bank digital currency and the future of monetary policy", **NBER WP 23711**, August.

Budish E. (2018), "The economic limits of the blockchain", manuscript, Chicago Business School, May.

Casey M., J. Crane, G. Gensler, S. Johnson and N. Narula (2018), **The Impact of Blockchain Technology on Finance: A Catalyst for Change**, Geneva Reports on the World Economy, 21.

Cochrane J. (2014), "Toward a run free financial system", Manuscript, University of Chicago School of Business.

Gandal N., JT Hamrick, T. Moore and T. Oberman, (2018), "Price manipulation in the Bitcoin ecosystem", **Journal of Monetary Economics**, 95, 86-96, May.

Gupta S., P. Lauppe and S. Ravishankar (2017), "Fedcoin: A Blockchain Backed Central Bank Cryptocurrency", Manuscript, Department of Computer Science, Yale University.

Igan D. and P. Mishra (2014), “Wall Street, Capitol Hill, and K Street: Political Influence and Financial Regulation”, **Journal of Law and Economics**, 57(4), 1063-1084, November.

Lagarde C. (2018), “Winds of change: The case for new digital currency”, Speech to the Singapore Fintech Festival, November 14, 2018.

Lober K. and A. Houben (2018), “Central bank digital currencies”, **Working Group Report Committee on Payments and Market Infrastructures Markets, BIS**, March.

Mancini-Griffoli T., M.S. Martinez Peria, Agur I., A. Ari, J. Kiff, A. Popescu and C. Rochon (2018), “Casting Light on Central Bank Digital Currency”, **IMF SDN/18/08**, November.

Nakamoto, S. (2008), “Bitcoin: A Peer-to-Peer Electronic Cash System”,

Roubini N. (2018), “Exploring the cryptocurrency and blockchain ecosystem”, **Testimony for the Hearing of the US Senate Committee on Banking, Housing and Community Affairs**, October 11.