Indian Institute of Management Calcutta

Working Paper Series

WPS No 862 / April 2021

The Techno-Economics of Central Bank Digital Currency (CBDC): An Exploration

Debashis Saha*
Management Information Systems Group
Indian Institute of Management Calcutta
Joka, D H Road, Kolkata 700104, India
e-mail: ds@iimcal.ac.in

Partha Ray
Economics Group
Indian Institute of Management Calcutta
Joka, D H Road, Kolkata 700104, India
e-mail: pray@iimcal.ac.in / raypartha1@gmail.com

* Corresponding Author

Indian Institute of Management Calcutta, Joka, D.H. Road, Kolkata 700104

URL: http://facultylive.iimcal.ac.in/workingpapers

The Techno-Economics of Central Bank Digital Currency (CBDC): An Exploration

Debashis Saha[1] & Partha Ray[2]

Abstract

Ever increasing threat from cryptocurrencies has perhaps induced the central banks across the globe to explore the potential of central bank digital currency (CBDC). In this context, this paper gazes at the techno-economics of CBDC: the distributed ledger technology that powers any digital currencies vis-à-vis the current status and viability of CBDC as a financial medium of exchange. Specifically, the paper explores the genesis and implications of CBDC on national and international financial landscapes. We have used the lens of the basic criteria associated with any common tender in facilitating seamless exchange of goods and services to explore the techno-economic feasibility and potential of CBDC. While the path ahead seems to be marked with some haziness, in the days to come CBDC could emerge as a key component of the ever-evolving socio-economic construct called "money".

Keywords: Common tender, currency regulation, digital currency, cryptocurrency, central bank digital currency (CBDC), blockchain, distributed ledger, digital money.

[1] Professor, Management Information Systems Group, Indian Institute of Management Calcutta, e-mail: ds@iimcal.ac.in.

[2] Professor, Economics Group, Indian Institute off Management Calcutta, e-mail:pray@iimcal.ac.in.

The Techno-Economics of Central Bank Digital Currency (CBDC): An Exploration

1. Introduction

Despite its popularity and university of usage, money has been quite a vexed issue in social discourse. It is often felt, "*Evil (Distrust) Is the Root of All Money*" (Kiyotaki and Moore, 2002). But, by its very existence, ever since the concept of money came into being, money allows two strangers to transact without having to barter or bothering about counter-party risks and thereby solving double coincidence of wants. Thus, in some sense, money becomes a substitute for trust. Of course, concept of money has undergone a sea-change over the history of civilization – from commodity money of different forms – gold, silver, or copper to paper money to cheques – the list seems rather long. In this continuum of evolution of money, the latest kid in the block is Central Bank Digital Currency (CBDC), which is the focus of this paper.

Broadly speaking, the concept of CBDC may be located in terms of digital money or what is increasingly known as *cryptocurrency*. The advent of distributed ledger facilities and associated innovation of blockchain paved the way for various types of digital monies like bitcoin, which, unlike traditional money, is based on a decentralized registry. Thus, by their very existence digital currencies questioned the hegemony of state power over printing of fiat/paper currencies and thereby depriving the governments of the seigniorage revenue (loosely defined as the profit derived out of printing currency, i.e., the difference between the face value of paper money and their production cost). Naturally, to begin with, the monetary authorities were rather cagey about the existence of digital currencies like bitcoin. But, over the years central banks have joined the bandwagon of digital currencies, perhaps following the dictum, "*If you can't beat them, join them*". In fact, in recent times, many central banks have issued guidelines and have expressed their interest to take CBDCs seriously (Bech and Garratt, 2017).

What is the nature of these CBDCs? How did they emerge technologically? Where can we locate these CBDCs within the broad range of, what has come to be known as, digital money? Often the technological and economic aspects of CBDCs emanate from silos without appreciating the other half of the gamut of challenges underlying CBDCs. This paper seeks to resolve these issues by taking an integrated view at CBDC. Specifically, towards seeking answers to some of these questions, the present paper takes a look at the techno-economic

tenets of CBDCs. Since the CBDCs are still in the process of being and becoming, the paper tilts towards the broad conceptual issues without necessarily delving into country-specific experiences and is in the nature of a review and assessment. We have also tried to make the review in terms of first principles without assuming any prior background, as much as possible.

The rest of the paper is organized as follows. Sections 2 and 3 delve into the conceptual issues of (a) distributed ledger technology (DLT) and block chain; and (b) money and its measurement. The relationship between DLT and Digital Currency is explored in section 4. While section 5 is devoted to the conceptual issues on CBDCs, section 6 presents the concluding observations.

2 Distributed Ledger Technology (DLT) and Blockchain

To begin at the beginning, it is useful to start with the concept of Distributed Ledger Technology (DLT), that is being touted world-wide as "the" technology behind developing and implementing digital currencies - whether retail (B2C) or wholesale (B2B). The beauty of DLT is that it can easily enable basic payment functionalities, such as issuing, distributing, transferring, and destroying any digital currency, and other related functions; plus, it can also innovate ecosystem functionalities such as invoice tokenization and smart contracts to schedule conditional payments and multi-party trades, even cross-border.

2.1 Distributed Ledger

In our traditional way of exchanging of assets, a trusted intermediary (third party) always oversees the complete process from the beginning till the finish. In other words, conventionally, two parties who agreed upon a transaction relied on a third-party institution to carry out and record the exchange. For instance, when we pay someone via check, the bank acts as the intermediary to control the transaction. The bank validates the check, verifies that the payer has sufficient funds in her account, deducts the amount, transfers the amount to the payee account, and records the exchange in a ledger. The historical set of records, popularly known as ledger, is a centralized documentation of all the transactions – present and past – and the resulting changes in asset under the control of the bank; the bank has sole authority over and ownership of this central ledger. In today's digital world, the ledger is technologically implemented as a central database by the bank. Each record in the database represents a transaction. What payee and payer get is a printed bank statement which is the relevant portion of the central ledger/database; they can check their respective statements to find that the asset

transfer has really happened. Both payee and payer have a great deal of trust on the bank acting as the unbiased intermediary and hope that the bank would faithfully maintain the ledger/database; otherwise, the whole system will fall apart. Imagine, for instance, that one of your close friends owns the ledger instead of the bank. Your friend could collude with you, falsely claim that you indeed paid, and manipulate the records in the ledger to back up the lie. However, today central ledgers are no longer the only viable option for exchanging our assets. Now, there is distributed ledger technology (DLT).

Technologically speaking, a distributed ledger is simply a distributed database that exists across locations or among multiple participants. Earlier most companies used database that exists in a fixed central location. This can lead to problems of accessibility and security. A distributed database gets rid of these problems, due to which they are becoming increasingly popular in the modern world. Rather than requiring a central authority to update and communicate records to all participants, DLTs can allow their members to securely verify, execute, and record their own transactions without relying on a central middleman. Instead, what they do is that they allow transactions to have public witnesses, thereby solving many trust-related issues. Also, resiliency is one of the strengths of DLT, as the system deploys multiple validating participants (or, nodes in terms of technology). The key features of the Centralised versus decentralised ledgers can perhaps be thought in terms of the agents' role and trust (Table 1).

Table 1: Centralised versus Distributed Ledgers: Key Features

Key aspect	Centralized ledgers (CLs)	Distributed ledgers (DLs)
Middleman or central agent	Relying on intermediaries, CLs are burdened by the fees and inefficiencies of the middleman.	No middlemen and intermediaries. No need to pay a central agent.
Bottleneck in the middle	Speed of transaction is limited by the efficiency of intermediary.	Assets are directly and immediately exchanged from peer to peer (P2P).
Point(s) of failure	Single point of failure – if the central ledger becomes unavailable due to some reason, the complete system fails.	No such threat exists because the ledger is distributed across the system.
Trust	All agents need to trust bankers, lawyers, or politicians holding the ledger and assets.	DLTs are trustless systems, meaning that no participant needs to trust any other participant to guarantee a valid ledger.

Source: Authors

2.2 Blockchain and bitcoin (BTC)

The most popular DLT is based on the concept of *blockchain*. Simply speaking, blockchain is a chain of blocks chronologically arranged in temporal sequence of their creation and addition to the chain. Blockchain keeps on growing over time – initially the chain begins with one block, then it consists of two blocks, next three blocks, and so on. The last block in the chain is always the most recent (or, current) block because blocks can only be appended at the end. No block can be inserted in the middle of the chain. Neither can any block be destroyed or deleted at any later point of time. In fact, once created and made part of the chain, no block can be touched in future for any purpose whatsoever – be it modification of the content of the block, or deletion of some part or whole of the block, or inserting new content inside the block, or any other operation one can think about. The first block in the chain is known as genesis block. Excluding the genesis block, every other block is coupled cryptographically to its immediate previous block, making the complete structure an interlinked chain. These backward couplings across blocks constitute the individual chains in blockchain. Thus, blockchain derives its name from the two words "block" and "chain". Due to the backward nature of the link, starting from any random block it is pretty easy to trace back all the previous blocks up till the genesis block. This sounds quite similar to audit trail, and there comes the application of blockchain in tracking source of assets, or tracing transfer of asset ownership over time, or provenance of supply of some asset. That is why it is drawing so much attention worldwide and gathering traction in governance domain. Coming back to blockchain structure, inside each block transaction(s) are stored. There can be one or more transactions, depending upon the nature of application blockchain is being used for. These transactions need not be only financial transactions. In blockchain parlance, a transaction generically represents change of ownership of any kind of asset. The asset can be physical (e.g., house, land, car, cell phone, cash notes, or coins) or digital (e.g., e-book, computer file, or digital currency), movable (e.g., car or book) or immovable (e.g., house or land), tangible (e.g., camera), or intangible (e.g., apps, mobile wallets). If the asset is tokenized, then transaction reflects how a token moves from past owner to present owner.

In 2008, a group of hackers, using the pseudo name Satoshi Nakamoto, released publicly the Bitcoin whitepaper, wherein they first unveiled the concept of blockchain to the world.[3] They conceptualized the idea of blockchain to showcase the production (aka mining)

[3] Its genesis can be tracked in 2008 when a paper, titled *Bitcoin: A Peer-to-Peer Electronic Cash System* was posted to a cryptography mailing list. Though one Satoshi Nakamoto was mentioned as its author in the post,

and exchange of a cryptographically-verified, decentralised digital currency – now known as bitcoin or BTC. BTC is a kind of tokenized monetary asset that can be used for all sorts of financial transaction. Though it is still hotly debatable whether BTC can play the role as an alternative to government-backed fiat money, blockchain as a techno-economic concept has become immensely popular across the globe and shook the traditional BFSI sector by adding a new feather to the already booming fintech revolution. Blockchain as a technology allows for secure low-cost payment and remittance systems outside conventional banking rails, thereby ushering in the era of digital (crypto) tokens. However, the biggest economic criticism against a cryptocurrency like BTC is its inherent volatility arising out of sheer speculation and not being backed by any fiat, rendering it unsuitable as a traditional medium of exchange in a regulated environment. One important point to mention here is that blockchain as a concept is not necessarily associated with any currency whatsoever i.e., there can be blockchains which do not involve any internal currency like BTC. In short, blockchains can exist even without any inherent currency.

2.3 Relevant Properties of Blockchain

Arguably, the most important characteristic of blockchain is its transparency. The complete blockchain is not secretly stored in any central database. Rather every entity participating in creating and/or reading the blockchain (or, having some interest in the blockchain) holds a copy of the complete blockchain at its disposal. This is why blockchain is a special type of distributed ledger, where the set of blocks serves the purpose of ledger (log of asset ownership changes over time), and multiplicity of the copies of the same ledger distributed among the entities captures the distributed nature of the ledger. Blockchain is thus resistant to single point of failure, unlike a centralized ledger in our traditional systems (vide Table 1). Moreover, distribution of replicas of ledger among the participants adds mutual trust (via transparency) to the whole system. Whenever a new block is to be appended, it is first broadcast to all entities in the system so that everyone can be on the same page at about the same time. If and only if the majority of the entities agrees to add the block, the block is deemed to be verified to be correct and trustworthy to be appended to the existing blockchain whose length then increases by unity. In this way, through mutual agreement, blockchain grows. Thus, after a reasonable delay spent in arriving at a consensus, again everyone in the system will have

tracking the author in brick-and-mortar form turned out to be elusive. In fact, when on May 2, 2016 Craig Wright, an Australian entrepreneur, claimed that he is he real Satoshi Nakamoto, within 90 minutes his claim has been debunked on an online forum.

an identical and unanimous copy of the updated blockchain. The whole process happens via a pre-determined consensus protocol decided and mutually agreed upon by the entities only. Hence, no central authority is needed. If a participant makes any changes to the ledger, it will reflect the same to every other participant within a few seconds or sometimes, minutes. The fundamental concept behind blockchain and hence DLT is to remove the need for a central authority to verify and check every transaction even in a completely public system with thousands of strangers interacting with each other (vide Table 1). Some distributed ledgers like blockchain use cryptography to store information accurately and safely. In that case, to access this information, entities need to have their keys and cryptographic signatures. However, in a highly secure, private and trusted system, we may forego the stringent requirement of cryptography to keep the process simpler and faster.

The coupling between two blocks is so designed that any forceful tampering with an older block renders all the subsequent blocks in the chain up to the most recent block invalid. That part of the blockchain then needs to be reconstructed afresh from the changed block. This, in turn, calls for nod from majority of the entities holding copies of the blockchain. Plus, convincing remaining entities in the system to believe in the reconstructed blockchain so that they too replace their copies with the new one. This is not an easy task to accomplish in a distributed system whether public or private. The older the block tampered with, the longer the sub-chain (after the block) to be reconstructed, the tougher the task to replace the blockchain. The penalty is huge if caught red-handed – will be thrown out of the system and banned. Hence, if the return is not commensurate with the effort needed to work around the blockchain, no individual entity or a group of entities will be interested to do so. In fact, this massive work factor acts as a big disincentive to any perpetrator (or, a group of wrongdoers) to change any older block maliciously. Thus, blockchain by design is almost tamper-proof or immutable practically. Hence, once a distributed ledger like blockchain stores any information, it becomes an immutable database (or, data warehouse) whose operating rules depend on the participants only – not on any central authority like database administrator.

2.4 Types of Distributed Ledger

A distributed ledger system can be classified as *public* or *private*, depending upon the nature of the participating entities and the rule for their participation in the system. In a public distributed ledger, any entity can openly join or leave the system anytime at will. On the contrary, only member entities can be part of a private distributed ledger, subject to privileges. For example, if all central banks of the world tomorrow form a consortium, similar to BIS, to

run a distributed ledger for their private usage, the consortium will be a private system and the corresponding distributed ledger will be private. On the other hand, bitcoin's blockchain is a public distributed ledger open to each and everyone. In either case, however, the distributed ledger inside the system can be *permissioned* or *permissionless*. The permission in this case is all about who all among the participating entities have the right to append new entries to the ledger (i.e., blocks to the chain in blockchain). If every entity is equally allowed to do so, the ledger is permissionless; else it is permissioned. Thus, in a permissioned one, only some entities, based on the rules and regulations of the system, have the right to append. Obviously, "private & permissioned" is the most restricted case of distributed ledger implementation, whereas "public & permissionless" is the most open case. Bitcoin uses a public & permissionless distributed ledger that is blockchain. Obviously, the complexity of the consensus mechanism is the highest in the public & permissionless case, and it decreases gradually as we move toward private & permissioned end of the distributed ledger spectrum.

3. Definition of Money: A Digression

Before we move to the concept of CBDC, a digression of money and its evolution is in order. Discussion of money is perhaps all pervasive in Economics and we agree with Davidson (1972) when he commented, "While economists have probably spilled more printers' ink over the topic of money than any other, and while monetary theory impinges on almost every other conceivable branch of economic analysis, confusion over the meaning and nature of money continues to plague the economics profession". In fact, following three definitions capture at the plurality of notion of money:

- "Money is defined by its functions …'money is what money does.' " (Hicks, 1967; p. 1).
- "Money is a social phenomenon, and many of its current features depend on what people think it is or ought to be" (Harrod, 1969; p. x).
- "Money is a difficult concept to define, partly because it fulfils not one but three functions, each of them providing a criterion of moneyness . . . those of a unit of account, a medium of exchange, and a store of value " (Scitovsky, 1969, p. 1).

But fundamentally, the notion of money in economics is perhaps best summarised as "Money is a convention, whereby one party accepts it as payment in the expectation that others

will also do so" (Carstens, 2018). Historically, various things have serviced as money – such as, Yap stones, gold coins, cigarettes in war times, or high value paper bills (Figure 1).

Figure 1: Some forms of Money

(1) Stone Money: Yap stone, used as money in the island of Yap in the Pacific Ocean country, Micronesia.

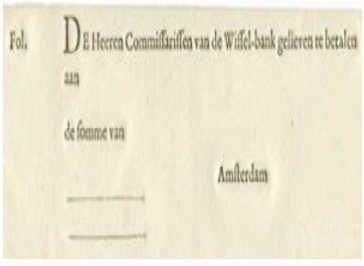
(2) Gold Coins

(3) This **copper** tajadero (chopping knife in Spanish) was a form of money used in central Mexico and parts of Central America.

(4) Cigerattes used as money in the prisoners of war camps during World War II

(5) With a portrait of Woodrow Wilson, the $100,000 note was actually a gold certificate that was created during the Great Depression in 1934, for conducting official transactions between Federal Reserve banks.

(6) Wissel (Wechsel) is bill of exchange or bearer notes, such as those issued by the Bank of Amsterdam in the first half of the 17th century.



Source: Carstens (2018), p. 3.

Thus, a key distinct feature of money is the notion of trust. Typically, this trust comes from the backing of central banks (and government) in case of paper currency and from the backing of the commercial banks (and consequently clearing house) in case of cheques. In case of paper currency, thus, the backing of the state is a key ingredient. It has been rightly noted, "*One of the hallmarks of national sovereignty through the ages has been the right to create money. ..... The ability to create its own domestic money is the key financial distinction of a sovereign state*" (Hirsch, 1969).

Operationally, thus, broad money stock is typically defined as the sum of currency plus all deposits of commercial banks. However, country experiences about the components of monetary aggregates vary and may vary substantially across countries.[4] Various criteria are

[4] See O'Brien (2007) for a discussion on components of different monetary aggregates across the world.

used to include a component under a monetary aggregate, viz., (a) degree of liquidity; (b) size of the denomination or minimum deposits; (c) the original maturity of the deposits; (d) characteristics of the asset holders; (e) foreign currency denominated deposits; (f) the types of money issuers; and (g) the types of financial institutions (O'Brien, 2007).

Of these, the types of money issuers and the types of financial institutions deserve special mention. Typically, central banks and commercial banks are included in all ambit of monetary issuers. Some special types of banks / deposit – accepting institutions are also included in some countries. Illustratively, in India deposits of co-operative banks are included under the definition of broad money; also deposits with the post-offices are included in liquidity aggregates in India. Many countries include Certificates of Deposits (CD) and / or repurchase agreements under some broad liquidity agreements.

But irrespective of the definitions, an important feature of all the components of monetary aggregates is that these reflect an accounting entity in a centralised registry. Illustratively, the role of the centralised registry is taken care of by the central banks in case of currency or clearing house in case of deposits. This particular feature of money gets violated in case of cryptocurrency.

But, how far a central bank digital currency (CBDC) fulfils the properties of money? Being under a centralised registry, it is expected to have huge acceptability as well as liquidity. It is also expected to have less volatility. But, before we move to CBDCs, a discussion on how DLT and Digital Currency are related is in order.

4. Digital Currency vis-à-vis Distributed Ledger Technology (DLT)

From technology perspective, digital currencies are nothing but digital goods. Looking back in history, ICT has given rise to a new kind of goods – called digital goods (Quah, 2003) – which are basically intangible goods that exist in digital form. For example, mobile apps, e-tickets, e-mail, cloud storage, etc. Digital goods may or may not have a physical counterpart. If it has a physical version too, then it is the digital representation of its physical counterpart which is traditionally produced and transferred as tangible goods, but are now produced and transferred electronically as digital goods. Digital currency is one such digital goods. Digital wallet is another.

4.1 Digital Currency as Digital Goods

In general, currency, expressed in common units, represents a financial instrument that holds value and can be used as a medium of exchange of goods and services. Technically

speaking, digital currency is a balance or a record stored in a centralized/distributed database, within digital files or within a stored-value instrument (Chuen, 2015). Examples of digital currencies are money used in internet banking, cryptocurrencies such as bitcoin (BTC), virtual currencies for online communities (e.g., Libra of Facebook), e-Cash in digital wallets, etc. Currency can also be a legal tender as defined by a regulating authority or a common tender by means of acceptance. Therefore, digital currency should ideally qualify as a common tender too. Although digital deposits are there in digital economy for quite some time now, digital currencies are new avatars to facilitate peer-to-peer transfer of value in an instantaneous way that was missing earlier

Apart from seeing it inside our bank accounts, ideally, we should also be able to keep digital currency within our digital wallets just as we keep physical currency inside our physical wallets in real world. There is a plethora of mobile wallets worldwide to store digital money. In India, Paytm leads the pack that also comprises PhonePe, Amazon Pay, Mobiqwik, Jio money wallet, Airtel money wallet, etc. In China, WeChat pay and Alipay wallets are two dominant players. Just as we transfer money from one person to another in the physical world, movement of digital currency from one digital wallet to another should happen over digital channels created with the help of Communications Technology (CT). Examples of digital channels include the Internet, mobile cellular network, intranet, extranet, etc. The beauty of digital channel is that any transport through it happens almost instantaneously anytime anywhere 24x7. By not having a physical form, digital goods are ideal candidates for nearly instantaneous exchanges over digital channels. Virtual currencies and cryptocurrencies already showed the way in the unregulated domain. Regulated digital currency should also follow the footsteps, subject to regulation, for facilitating universally commercial transactions exchanging goods and services (Department of Treasury, Government of the US, 2013).

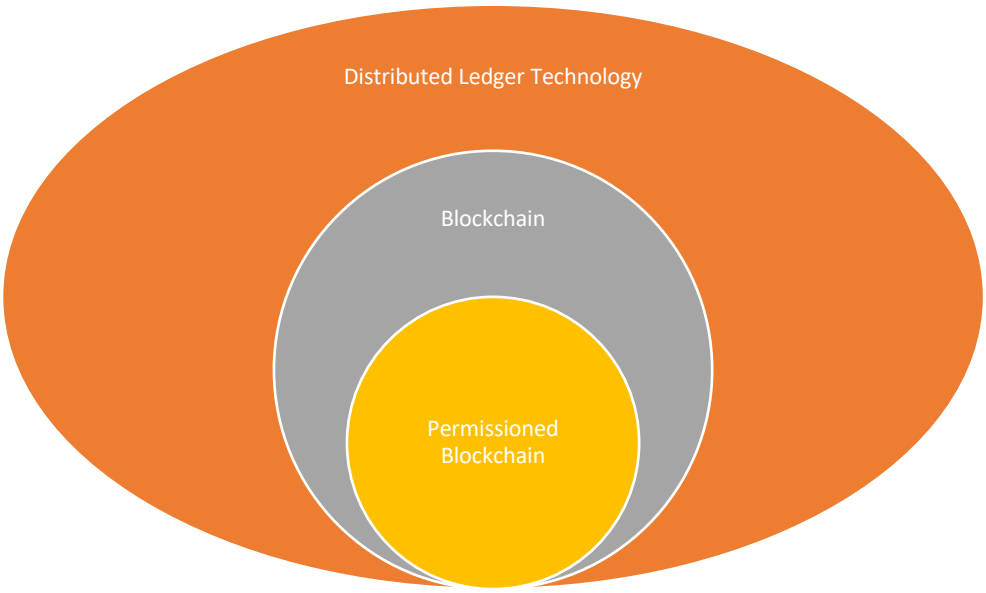
As of Information and Communications Technology (ICT) has fostered an environment where many financial transactions can occur in digital format, innovations should promote new types of applications of digital currencies. When central banks are concerned, CBDC must be subject to regulation if it is to be used legally for a substitutive purpose in facilitating exchange of goods and services. That is possible only if few currencies can operate at the same time. For instance, in India, we do not use USD or EURO in addition to INR because when either party does not recognize USD or EURO it does not ensure value for money. This inhibits economies of scale, rendering the economy far less efficient. Nonetheless, we are passing through a situation when multiple cryptocurrencies are operating alongside one another in most of the

countries even though cryptocurrencies have no intrinsic value, unlike fiat currencies. This clearly contradicts the very concept of money. However, with the advent of ICT traditional banking is poised to undergo a digital metamorphosis, which is very much evident in countries like China and India. Such a digital transformation is very much needed to pave the way for innovations in the BFSI sector. CBDC can be the solution.

4.2 Digital Currency and DLT

Drawing from our discussion in Section 2 on DLT and blockchain, let us understand how DLT can be harnessed to roll out a digital currency like CBDC. Conceptually, DLT and money go hand in hand. Their confluence gives birth to *digital currency* – a financial instrument – in fintech parlance. Blockchain (a special kind of DLT) has already showcased the success one form of digital currency known as cryptocurrency as a medium of trust. However, unlike these cryptos, if the digital currency is backed by a central bank, it is called central bank digital currency (CBDC) which is even more trustworthy. Broadly speaking, CBDC may be placed within the broad genre of permissioned blockchain (Figure 2).

Figure 2: Hierarchy of Blockchain



Source: Cambridge Centre for Alternative Finance (2017), "Global Blockchain Benchmarking Study."

An inherent but not necessarily invoked feature of any DLT implementation is that it also allows tokenization i.e., converting any assets into digital tokens that electronically represents a real tradable asset, whether physical or digital. Tokenization is somewhat similar

to the traditional process of securitization, with a digital twist. Tokenization is not new in digital payment because it is the technology behind popular payment services such as mobile wallets. Tokenization reduces risk, fosters trust, and enables e-payment so much so that the tokens can be traded even on a secondary market. Now, if central banks issue securities in tokenized form within their own DLT environment, including turning fiat money into cash tokens, then those will be nothing but CBDC. With this feature, the CBDC token will have a cash like property in a digital form. CBDC will be protected from value debasement because central bank will commit to its price stability. If a CBDC loses credibility, as is the case with fiat currency in some weak monetary systems with high inflation, it will be swapped out for more stable CBDC. The supply of CBDC will track potential nominal GDP, so that prices will not undergo speculative inflation or deflation.

4.3 Characteristics of CBDC as Digital Currency

Digital currency may be regulated or unregulated (Table 2). Regulated digital money is already in vogue at the back end for central bank reserves for quite some time now ever since banking systems adopted computerization. It has gained momentum with the introduction of core banking system and internet/mobile banking. However, till date it is primarily considered – as a digital representation of physical money – within a closed national system. Neither its convertibility with unregulated digital currencies is ever seriously thought about, even after increasing popularity of cryptocurrencies worldwide. Nor it has been opened out for innovations in the financial domain. Only recently, open banking (or, neo banking) is gathering traction in Europe.

Table 2: Forms of Currency

Format ***Legal status***	***Physical***	***Digital***
Regulated	Banknotes and coins	E-money, Commercial bank money (deposits), CBDC
Unregulated	Certain types of local currencies, coupons	Virtual currency, cryptocurrency, e-coupons

Source: European Central Bank (2012)

BIS argues that CBDC should "do no harm" to monetary and financial stability. It should coexist with cash and other types of money in a flexible and innovative payment ecosystem. As expected, CBDC should be indeed reasonably similar to the banknotes and coins

in your wallet. CBDC should differ from the digital deposit you have in your bank account in the same way a banknote differs from your money in account. The money you have with the bank is typically not legal tender. But CBDC would have legal tender status and would not be your bank's liability. CBDC is a digital form of currency that is backed by a Central Bank and through that has legal tender status. This definition means it is recognized by law as a means to settle debts or meet financial obligations such as tax payments. Additionally, it should promote broader innovation and efficiency in the payment ecosystem. In fact, contrasting US dollar (fiat money) vis-à-vis bitcoin (perhaps the most well-known cryptocurrency) may drive home the essential properties one can look for from a CBDC (Table 3).

Table 3: Characteristics of Currencies: Bitcoin vis-a-vis USD

		Bitcoin	**USD**
Economic Demand Factors	Intrinsic value	None	None
	Claim to issuers?	No	Yes
	Legal tender	No	Yes
	Used as a medium of exchange	Small, but rising especially in online retail	Yes
	Used as unit of account	No	Yes
	Used as store of value	Yes, subject to very high exchange rate risk and sudden confidence shock	Yes, subject to inflation risk
Supply structures	Monopoly/decentralized	Decentralized	Monopoly
	Supply source	Private	Public
	Supply quantity	Inflexible	Flexible
	Supply rule	Computer program	Rule-based (e.g., Inflation target)
	Supply rule change (by issuers) possible?	Yes with agreement of majority miners	Yes
	Cost of production	High (electricity consumption for computation)	Low
Macro-financial stability risks	Risk of hyperinflation due to over-supply?	No for individual virtual currencies	Possible (with policy mismanagement)
	Risk of long-term hyper-deflation	High	Low
	Base money quantity changes to temporary shocks?	No (limited even with rule changes)	Yes
	Can the issuer be lender of last resort with outside money?	No	Yes

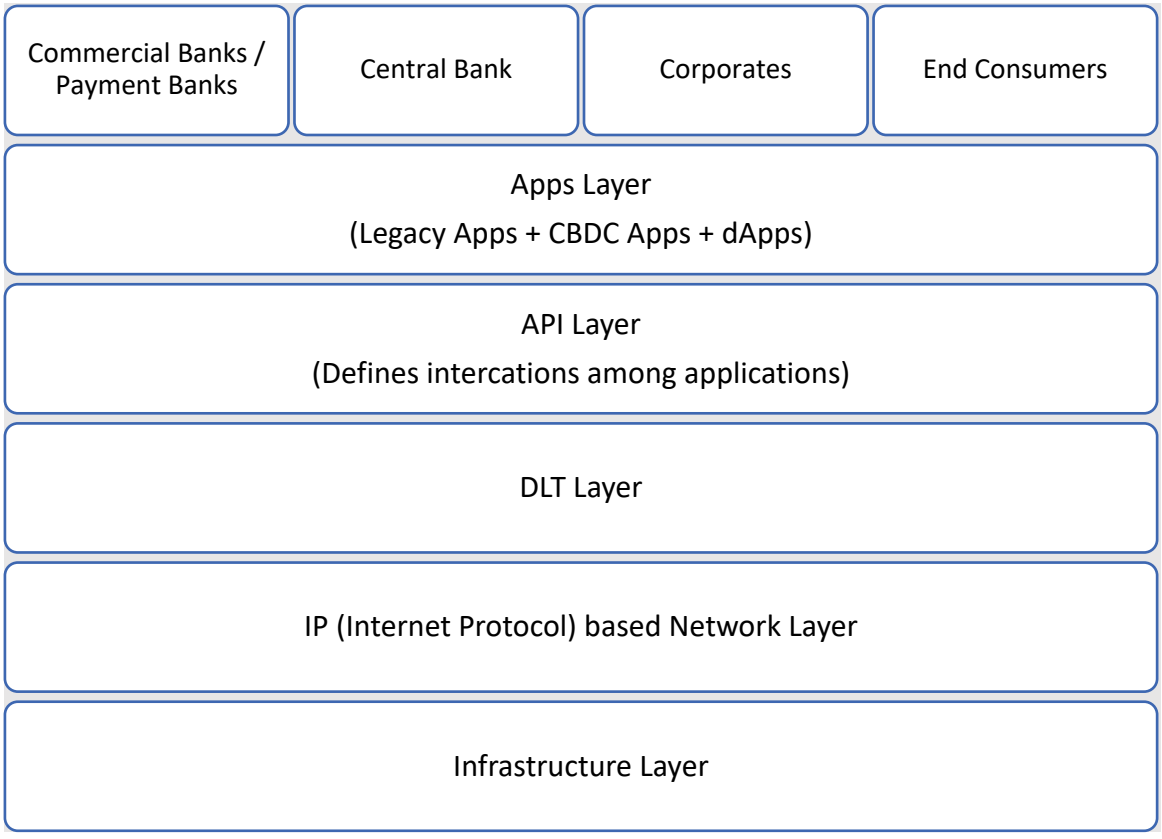
Source: IMF (2016): "Virtual Currencies and Beyond: Initial Considerations*", IMF Staff Discussion Note,* No. SDN / 16/ 03.

4.4 CBDC Implementation Outlook

Obviously, DLT will facilitate transparency in CBDC lifecycle management: issuance, destruction, distribution, and transfer. The central bank, as the sole CBDC issuer, will be responsible for issuing, destroying and controlling CBDC in circulation. While central bank

alone will be responsible for issuing and destroying CBDC, other banks and business houses will be involved in distribution and transfer of CBDC. Commercial banks (and Payment Banks like Paytm) will be responsible for handling user/wallet related operations (such as KYC processes), distribution of CBDC, exchange of CBDC, and handling CBDC deposits. Hence, commercial banks are indispensable in this ecosystem, even though they may not be responsible for the settlement and provision of transaction finality in the DLT. Seamless interoperability of the DLT with commercial/payment banks' platforms is crucial for handling these operations. Corporates and end consumers must first obtain a CBDC wallet post KYC verification of their identities. Once they receive CBDC into their wallet from commercial/payment banks, they can make peer-to-peer (P2P) transfers on a real time basis, similar to UPI transfers. Admittedly, CBDC will naturally inherit many of the advantages of cryptocurrencies, most of which do not necessarily depend on trust and the accounting is done though a distributed ledger facility, without a central authority. Architecturally, the complete system can be designed as a multi-layer structure (Figure 3).

Figure 3: Possible Architecture for CBDC Implementation



Source: Authors

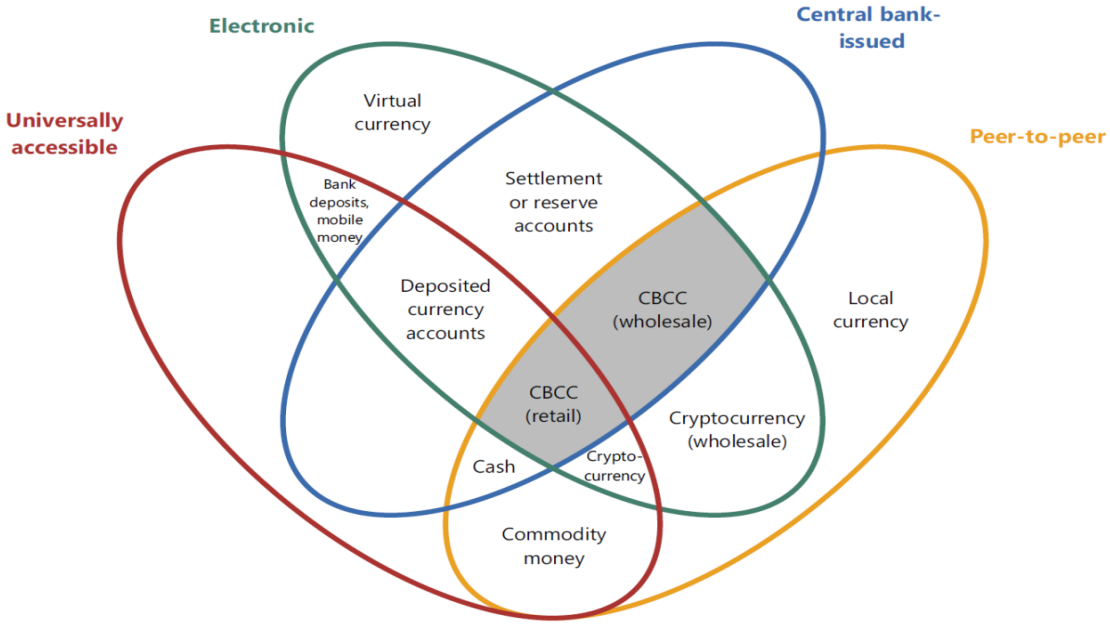
5. Central Bank Digital Currency (CBDC) – Conceptual Hardles

5.1 Locating the CBDC

Where does one locate Central Bank Digital Currency (CBDC) in the technological scheme of digital currencies? Admittedly, its utility lies in providing a frictionless way for people to transfer and use funds. Governments need to offer CBDC in order to retain monetary independence. In digital economy, as cash disappears and payments revolve around social and economic platforms rather than banks' credit provision, the traditional transmission channels of monetary policy weaken significantly.

Conceptually, the CBDCs can be located in the taxonomy of money flower based on four key properties: issuer (central bank or other); form (digital or physical); accessibility (widely or restricted); and technology (token- or account-based) (Bech and Garratt, 2017). Money is typically based on one of two basic technologies: (a) tokens of stored value or (b) tokens of accounts (Ward and Rochemont, 2019). Cash and many digital currencies are token-based, whereas balances in reserve accounts and most forms of commercial bank money are account-based (Figure 4).

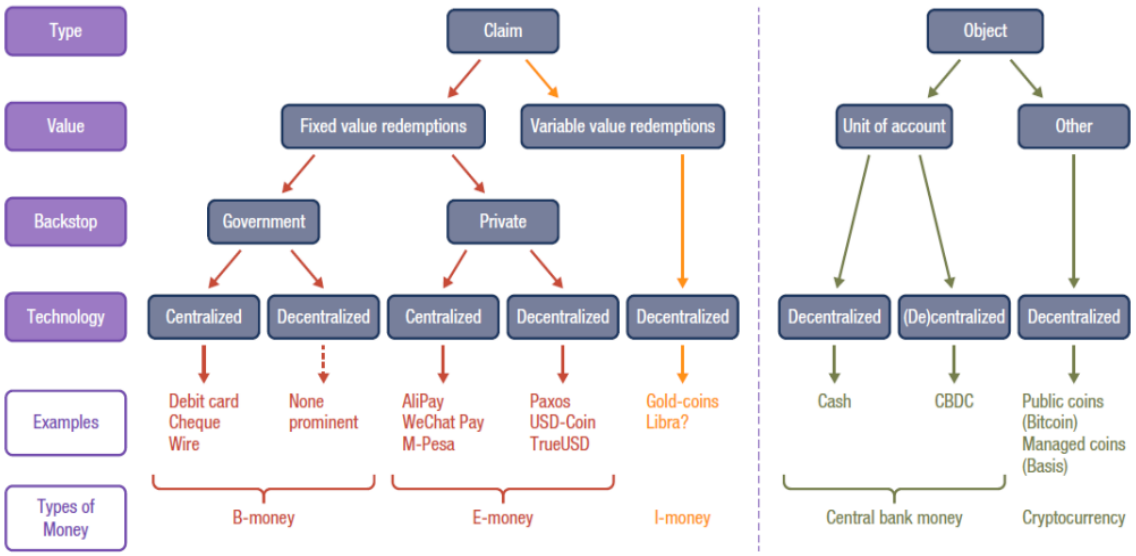
Figure 4: The Money Flower: A Taxonomy of Money



CBCC: Central Bank Cryptocurrencies;
Source: Bech and Garratt (2017), p. 60.

If one accepts the definition of CBDC as "a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank" (BIS, 2020), then in terms of competitor digital currencies, CBDCs can be located more specifically. In fact, in terms of various digital currencies that are currently available, following Adrain and Mancini-Griffoli (2019), one can adopt the following taxonomic classification in terms of type, value, backstop, or technology (Figure 5).

Figure 5: Different kinds of Virtual Money



Source: Adrain and Mancini-Griffoli (2019)

Thus, there are two main forms of money: account-based (claim) and token-based (object). The key difference between the two types of money lies in the verification process for payments. In an account-based system, what must be verified is the payer's identity. In a token system, instead the authenticity of the item (object) to be exchanged needs to be verified. Cash and coins are types of token money that have existed for centuries. In a cash transaction, the payee will accept payment only if she believes the cash is genuine, meaning the payee effectively assumes liability if the cash is counterfeit. Modern e-money and cryptocurrencies are also token-based money (object). For example, to transact currency on Alipay's network, all that is needed is a password linked to a particular digital "wallet." No one is required to verify that the person who presented the password is the wallet's true owner. Similarly, to

transact cryptocurrency, the payer must sign transactions with a "private key" linked to a particular set of coins, but the transaction is valid regardless of who presents that key. Importantly, account-based money tends to be inside money linked to the creation of credit, whereas token-based money is typically unrelated to the provision of credit. Hence, an expansion in the supply of account-based money may have quite different implications from an expansion in the supply of token-based money.

Several ubiquitous forms of digital money are, in fact, independent currencies. For example, the basket underlying Facebook's Libra currency would consist of many official currencies, so Libra would be denominated in its own unit of account and thus be independent. Fiat cryptocurrencies are clearly independent currencies, as they are not convertible into anything and have their own unit of account. This includes all of the most popular cryptocurrencies, such as Bitcoin and Ether. Even some stable coins, which are backed by a bank account owned by the issuing entity, are independent currencies, because they could continue to exist on an exchange even after the issuer unilaterally abandons the currency's backing.

Other types of digital money are not fully independent currencies but nevertheless enable transfers of value that were not previously possible. For instance, many mobile applications now permit peer-to-peer digital transfers, whereas digital transfers under the traditional banking system were typically limited to purchases. These applications, such as Alipay in China or M-Pesa in Kenya, permit existing currencies to circulate in a new way and among new populations, but their issuers are legally bound to maintain convertibility to their countries' currencies (renminbi in the case of Alipay and shilling for M-Pesa).

5.2 Potential Design Issues

Recently, the BIS along with a number of central banks from the developed countries has released a report on some fundamental principles and core features of CBDC (BIS, 2020).[5] Interestingly, none of the central banks contributing to this report have reached a decision regarding issuing a CBDC. Instead, they put forward the following three key principle:

(i) a central bank should not compromise monetary or financial stability by issuing a CBDC;

[5] The report is prepared jointly by Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the US Federal Reserve System and Bank for International Settlements.

(ii) a CBDC would need to coexist with and complement existing forms of money;

(iii) a CBDC should promote innovation and efficiency with an appropriate role for the private sector.

To fulfil the foundational principles, the BIS has identified fourteen core features of a potential CBDC covering the CBDC instrument, the underlying system and the broader institutional framework (Table 4).

Table 4: Core Features of a CBDC

Instrument features	**Convertible**	To maintain singleness of the currency a CBDC should exchange at par with cash and private money.
	Convenient	CBDC payments should be as easy as using cash, tapping with a card or scanning a mobile phone to encourage adoption and accessibility.
	Accepted and available	A CBDC should be usable in many of the same types of transactions as cash, including point of sale and person-to-person. This will include some ability to make offline transactions (possibly for limited periods and up to predetermined thresholds).
	Low cost	CBDC payments should be at very low or no cost to end users, who should also face minimal requirements for technological investment.
System features	**Secure**	Both the infrastructure and participants of a CBDC system should be extremely resistant to cyber-attacks and other threats. This should also include ensuring effective protection from counterfeiting.
	Instant	Instant or near-instant final settlement should be available to end users of the system.
	Resilient	A CBDC system should be extremely resilient to operational failure and disruptions, natural disasters, electrical outages and other issues. There should be some ability for end users to make offline payments if network connections are unavailable.
	Available	End users of the system should be able to make payments 24/7/365.
	Throughput	The system should be able to process a very high number of transactions.
	Scalable	To accommodate the potential for large future volumes, a CBDC system should be able to expand.
	Interoperable	The system needs to offer sufficient interaction mechanisms with private sector digital payment systems and arrangements to allow easy flow of funds between systems.
	Flexible and adaptable	A CBDC system should be flexible and adaptable to changing conditions and policy imperatives.
Institutional features	**Robust legal framework**	A central bank should have clear authority underpinning its issuance of a CBDC.
	Standards	A CBDC system (infrastructure and participating entities) will need to conform to the appropriate regulatory standards (e.g., entities offering transfer, storage or custody of CBDC should be held to equivalent regulatory and prudential standards as firms offering similar services for cash or existing digital money).

Source: BIS (2020).

Taken together, these principles tend to emphasize the safety aspects of a potential CBDC. Needless to say, these principles are the first step towards innovating a CBDC. In context of these principles, a commentator has noted aptly:

> "The possible adverse impact of a CBDC on bank funding and financial intermediation, including the potential for destabilising runs into central bank money, has been a concern of central banks. Any decision to launch a CBDC would depend on an informed judgment that these risks can be managed, likely through some combination of safeguards incorporated in the design of a CBDC and financial system policies more generally. Understanding the potential market structure effects of CBDC, their implications for financial stability, and any potential mitigants is a further area of work for this group. The next stage of CBDC research

and development will emphasise individual and collective practical policy analysis and applied technical experimentation by central banks. The report highlights CBDC design and technology considerations, including initial thoughts on where trade-offs lie. Far more work is required to truly understand the many issues, including where and how a central bank should play a direct role in an ecosystem and what the appropriate role might be for private participation. The speed of innovation in payments and money means that these questions are ever more urgent" (Lovegrove, 2020).

5.3 An Emerging Country Perspective

Understandably, to begin with a number of emerging countries, perhaps with the exception of China, was quite cagey about introduction of CBDC. Apart from the fear unknown, losing the power to issue paper currency and loss of seigniorage revenue on the part of the government, threats to financial stability – all have expressed from time to time.

In fact, in Indian context, an apprehension has been expressed that introduction of CBDC may lead to disintermediation of the banking system. In other words, a CBDC could not only have the potential to replace cash but chequable bank deposits as well. A recent report of the Reserve Bank of India (RBI), has noted, "The public can convert their CASA deposits with banks into CBDC, thereby raising the cost of bank-based financial intermediation with implications for growth and financial stability. In countries with significant credit markets, commercial banks may lose their primacy as the major conduit of monetary policy transmission (RBI, 2021; p. 154).

A knotty issue in this context is the presence of negative interest rate that are prevalent in some of the advanced countries currently. Would such negative interest rate be applicable on CBDCs as well? One recently proposed solution to limit disintermediation is the introduction of a 2-tier remuneration system for CBDCs was provided by Bindseil and Pannetta (2020). They proposed a two tier system as follows:

> "….The tier one remuneration rate, r_1, should never fall below zero, while the tier two remuneration rate, r_2, should be set such that tier two deposits are rather unattractive as a store of value (i.e. less attractive than bank deposits or other short-term financial assets, even when taking into account risk premia). The two rates could co-move in parallel with policy interest rates, with an additional special provision when zero lower bound territory is approached. The rates on CBDC would not be regarded as policy rates. Moving the rates would simply serve to keep a similar spread over time to other central bank rates and thus, in principle, to other market rates".

However, a potential benefit of CBDC could come from their potential and usage of sterilization in presence of volatile capital flows. In that sense, CBDC could act as a retail instrument of sterilization.

6. Concluding Observations

Though money is a socio-economic construct, technology has played a key role in its evolution. History of money is full of innovations and various things have acted as money. The advent of digital money is transforming the nature of currency competition, the structure of the international monetary system, and the role of regulated public money. In the long list of digital *avatars* of money, CBDC could be the newest kid in the block. In this paper, we have tried to put forward a synthesis of the technology behind and the economics of CBDCs. At the risk of rash generalizations and missing the nuances, the following broad pointers may be highlighted.

First, we have argued that despite various misgivings, regulators across the world have moved in the right direction. There is now near-consensus that CBDC should be treated as intangible personal digital good like copyrights, patents, and trademarks.

Second, ownership disputes must be resolved using distributed ledger technology, subject to the evolving regulatory practices.

Third, CBDC must have a broad trading base to operate to be an effective medium of exchange.

Finally, CBDC must inherit desirable properties of other similar financial instruments (e.g., plastic cards, digital wallet money, cryptocurrencies, etc.) for the sake of initial interoperability.

Apprehensions about the possible impact of CBDC still exist in regulators' minds – possible financial instability and loss of seigniorage revenue are some of the prime concerns. But there has been hardly any instance in history where a new technology has been rejected just because of certain apprehensions and possible implications for the state power. Given the popularity of various forms of cryptocurrency, we expect that introduction of CBDC is a matter of time. Admittedly, operational details are yet to be firmed up and devil could lie in those details. But moving forward, introduction of CBDCs could well auger well in what is commonly known as Industry 5.0.

References (All the URLS have been accessed in March – April 2021)

Adrian, Tobias., and Mancini-Griffoli, Tommaso (2019): "The rise of digital money", *IMF FinTech notes*, available at https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097

BBC News (2012): "Virtual cash exchange becomes bank", (December 7, 2012), available at http://www.bbc.co.uk/news/technology-20641465?print=true.

Bech, Morten and Rodney Garratt (2017): "Central Bank Crypotocurrencies", *BIS Quarterly Review*, September 2017, pp. 55-70.

Bindseil, U., & F. Panetta (2020), "CBDC Remuneration in a World with Low or Negative Nominal Interest Rates", available at https://voxeu.org/article/cbdc-remuneration-world-low-or-negative-nominal-interest-rates

BIS (2020): "Central bank digital currencies: foundational principles and core features", Report No. 1, available at https://www.bis.org/publ/othp33.pdf

Carstens, Agustín (2018): "Money in the digital age: what role for central banks?" Lecture at the House of Finance, Goethe University Frankfurt, 6 February 2018, available at https://www.bis.org/speeches/sp180206.pdf

Chuen, David LEE Kuo (2015): "Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data", Elsevier Monographs, Elsevier Publishing, ISBN: 978-0-12-802117-0. http://www.sciencedirect.com/science/book/9780128021170

Davidson, Paul (1972): "Money and the Real World ", Economic Journal, 82 (325; March 1972): 101-115

Department of the Treasury, Government of the US (2013): "Application of FinCEN's regulation to persons administering, exchanging, or using virtual currencies", Guidance Note of the Financial Crime Enforcement (Washington DC), No. FIN-2013-G001 available at https://www.govinfo.gov/app/details/CFR-2011-title31-vol3/CFR-2011-title31-vol3-sec1010-100.

Economist (2013): "Digital currencies: A new specie: Regulators should keep their hands off new forms of digital money such as Bitcoin", April 13, available at http://www. economist.com/printed itio n/2013-04-3.

European Central Bank (2012): "Virtual Currency Schemes", p.5. available at http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Harrod, R. F. (1969): *Money*, London: Macmillan.

Hicks, J. R. (1967): *Critical Essays in Monetary Theory*, Oxford: Oxford University Press.

Hirsch, Fred (1969): *Money International*, New York: Penguin Books

IMF (2016): "Virtual Currencies and Beyond: Initial Considerations*", IMF Staff Discussion Note,* No. SDN / 16/ 03.

Lovegrove, Simon (2020): "Central banks and BIS publish first central bank digital currency report laying out key requirements", available at https://www.regulationtomorrow.com/eu/central-banks-and-bis-publish-first-central-bank-digital-currency-report-laying-out-key-requirements/

Nobuhiro Kiyotaki and John Moore (2002): "Evil Is the Root of All Money", *American Economic Review*, 92(2): 62-66.

O'Brien, Yueh-Yun C. (2007): "Measurement of Monetary Aggregates across Countries", Finance and Economics Discussion Series, Divisions of Research & Statistics and Monetary Affairs, U.S Federal Reserve Board, No. 2007.02, available at https://www.federalreserve.gov/pubs/feds/2007/200702/200702pap.pdf

Quah, Danny (2003): "Digital goods and the new economy", CEP discussion paper CEPDP0563. Centre for Economic Performance (CEP), London School of Economics and Political Science, London, UK. available at http://eprints.lse.ac.uk/2236/1/Digital_Goods_and_the_New_Economy.pdf

Scitovsky, T (1969): Money and The Balance of Payments, Chicago: Rand McNally.

Ward, Orla and Sabrina Rochemont (2019): "Understanding Central Bank Digital Currencies (CBDC)", Discussion Paper, The Institute and Faculty of Actuaries, UK, available at https://www.actuaries.org.uk/system/files/field/document/Understanding%20CBDCs%20Final%20-%20disc.pdf

****