Original articles

Economia e Sociedade, Campinas, Unicamp. IE.
http://dx.doi.org/10.1590/1982-3533.2021v30n2art08

Cryptocurrencies: technology, initiatives of banks and central banks, and regulatory challenges *

Carlos Eduardo Carvalho **
Desirée Almeida Pires ***
Marcel Artioli ****
Giuliano Contento de Oliveira *****

Abstract

This paper analyses the impacts of the innovation known as distributed ledger technology (DLT) on the monetary system and on financial activities. Private cryptocurrencies, such as Bitcoin, are permissionless means of payment, based on blockchain, a form of DLT. Evaluations suggested that these private cryptocurrencies could compete with the banks payment systems and even supplant state currency. The development of these technologies has the potential to modify profoundly monetary and financial practices, but there are no indications that they may threaten the centrality of state money and the banking system in the contemporary monetary order. Major international banks have developed cryptocurrencies for settlement systems and for interbank transactions, including the so-called stablecoins, issued by highly technological companies with on par conversion into state money. Some central banks are studying the launch of state cryptocurrencies that could coexist with their fiduciary state currency and even replace their paper currency. The use of this technology results in new challenges for regulation, including the fact that cryptocurrencies can be used for money laundering and by organized crime.

Keywords: Cryptocurrencies, Distributed ledger technology – DLT, Blockchain, Bitcoin, Regulation.

Resumo

Criptomoedas: tecnologia, iniciativas de bancos e de bancos centrais, desafios para a regulação

O artigo analisa os impactos das inovações conhecidas como *distributed ledger technology* (DLT) sobre o sistema monetário e sobre as atividades financeiras. As criptomoedas privadas, como o bitcoin, são meios de pagamento de acesso livre, não permissionados, baseados na tecnologia blockchain, uma forma de DLT. Surgiram avaliações de que as criptomoedas privadas poderiam concorrer com os meios de pagamento bancários e com a moeda estatal, ou mesmo suplantá-la. O desenvolvimento destas tecnologias tem potencial para alterar intensamente as práticas monetárias e financeiras, mas não há indicações de que possam ameaçar a centralidade da moeda estatal e do sistema bancário na ordem monetária contemporânea. Grandes bancos internacionais têm desenvolvido criptomoedas para sistemas de liquidação de pagamentos e de transações interbancárias, inclusive as chamadas *stablecoins*, emitidas também por empresas de alta tecnologia, com paridade fixa com a moeda estatal. Bancos Centrais estudam o lançamento de criptomoedas próprias que possam conviver

* Article received on June 13, 2019 and approved on March 4, 2020.

** Professor at the Economics Department/PUC-SP, and Postgraduate Program in International Relations San Tiago Dantas (Unesp/Unicamp/PUC-SP). São Paulo, SP, Brasil. E-mail: cecarv@pucsp.br. ORCiD: https://orcid.org/0000-0002-2962-9422.

*** Doctor in International Relations at the San Tiago Dantas (Unesp/Unicamp/PUC-SP), São Paulo, SP, Brazil. E-mail: d.almeidapires@gmail.com. ORCiD: https://orcid.org/0000-0002-7338-1698.

**** Researcher at the Center for International Studies and Analyses (NEAI) of the Institute of Public Policies and International Relations (IPPRI), São Paulo State University (Unesp), São Paulo, SP, Brazil. E-mail: marcel.artioli@unesp.br. ORCiD: https://orcid.org/0000-0002-6007-3848.

***** Professor of Economics at University of Campinas (Unicamp), Campinas, SP, Brazil. E-mail: giueco@unicamp.br. ORCiD: https://orcid.org/0000-0001-6791-2643.

com sua moeda fiduciária e até substituir o papel-moeda. A aplicação desta tecnologia traz novos desafios para a regulação, inclusive porque criptomoedas podem ser utilizadas para lavagem de dinheiro e crime organizado.

Palavras-chave: Criptomoedas; Tecnologia de contabilidade distribuída – DLT; *Blockchain*, Bitcoin, Regulação.
JEL: O33, E42, E52, O38, G21.

1 Introduction

The broad debate about the so-called cryptocurrencies, especially bitcoin, involves relevant questions: the characterization of its nature; the transformations that it provokes in the structure and practices of the monetary and financial system; banks, financial institutions and central banks' reactions; the challenges to financial regulation; and the fight against organized crime. "Crypto" emphasizes that they offer a way to protect data by transforming readable information into unintelligible codes. They are called "currencies" since they can be used as a medium of payment.

Cryptocurrencies, including bitcoin, use a technology established from a distributed network database, known as a blockchain, or data block (Hong Kong Monetary Authority, 2017, Brazil, 2017). The blockchain is one of the many possible configurations within the broad universe of distributed ledger technology – DLT. This distributed accounting technology is configured from a synergistic combination of game theory, computational cryptography, and software engineering. It is a technological architecture with three basic components: i) a decentralized and encrypted cryptographic book; ii) a protocol delineating the internal processes of the network; iii) an asset to be transacted and modified (BIS, 2018). It is therefore a technological and financial innovation with the potential to greatly modify payment systems and financial market practices.

Cryptocurrencies are a means of payment that use blockchain to protect data transmitted and stored in a decentralized manner. They cannot, however, be classified as money, due to three reasons: (i) its use as means of payment is limited to peer-to-peer operations outside the banking system; (ii) there are no signs that it can be used as a price reference, due to its very limited use and to its high volatile value in any reference (state currency or commodities); and (iii) and it is not a store of value, not only because of its high price volatility, but also due to its unpredictable liquidity in the conversion to any state currency; both problems are due to the absence of a central bank that operates continuously in a broad market, as with national currencies.

The current understanding tends to characterize bitcoin and other non-state certified cryptocurrencies as speculative financial assets and they have been treated this way in regulatory and taxation frameworks in many countries. Hence, private cryptocurrencies are still far from altering essential aspects of the current monetary order, based on state fiduciary currency and bank currency.

Moreover, central banks and large international banks have developed initiatives to use DLT in several ways, including the issuance of cryptocurrencies by some major monetary authorities. Furthermore, these initiatives restrict the possibilities for a new monetary order based on private cryptocurrencies, "free" from central banks' power to issue state money and the decisive performance of the banking system, especially in payment systems and the generation of credit. Still, the increasing use of DLT and cryptocurrencies in the contemporary financial system cannot be disregarded.

This paper discusses DLT and cryptocurrencies, with emphasis on the main one, Bitcoin, and analyzes central banks and big bank initiatives in the face of these new technologies and financial innovations. It is argued that private cryptocurrencies, although representing major financial innovations, do not tend to change, in a minimally predictable period, the prevalence of current monetary order, based on the fiduciary state currency and the banking currency. This is mainly because the banking system, under the command of the major international banks and central banks, is rapidly incorporating and developing the DLT in their operations. This hypothesis evidently does not mean that such transformations will not give rise to considerable challenges posed to financial stability, the taxation capacity of states and the various forms of use of such a system for illicit activities.

This paper sheds light on such issues and is divided as follows: the second section proposes elements to locate the cryptocurrencies within the currency analysis; the third section analyses the technological architecture that supports these innovative systems and their possible unfolding; the fourth section discusses Bitcoin in more detail, including the evolution of its price and variability; the fifth and the sixth sections address the initiatives of major banks and central banks; the seventh section summarizes regulatory trends. The final section presents closing remarks.

2 State money, bank money, means of payment and parallel currencies

As a social institution that organizes and facilitates transactions in a capitalist economy, besides the public's trust and thus widespread acceptance in a contractually and institutionally legitimized collective system, money must fulfill three functions, namely: as a means of payment, a store of value, and a unit of account. The first function of money allows for the immediate settlement of economic transactions, exercising the function of universal equivalent to the economic system. The second, in turn, stems from the fact that money incarnates the very notion of liquidity. This function turns money into a kind of asset which, although it does not allow the holder to receive interest, has a liquidity premium (Keynes, 1936). Finally, the unit of account function plays a central role in a monetary economy of production, since it conceives money's ability to define nominal quantities in terms of monetary prices, allowing for comparability and proportionality between several goods and services from an objective parameter, as well as to record transactions, indispensable conditions for economic calculation.

The monetary system is based on the state money (Wray, 2002) and includes assets with different degrees of convertibility into state money. However, only the fiduciary currency issued by the state encompasses the three functions. The state money is the only one accepted by their respective national state for tax payments and the only one accepted by their central bank for daily settlement transactions to adjust banks' positions. Besides, only the state money holds the unit of account function.

In contemporary societies, there are two basic and largely used means of payment: central banks bills and transferable demand deposits in commercial banks, that can be used by their owners in different ways. Demand deposits in commercial banks are means of payment since they are widely accepted by the public but mainly because they are accepted by banks to settle payments among their depositors. These kinds of payments are effectively settled only when recognized by the receiving bank in a transaction performed in the money market organized around a central bank. These demand deposits are known as commercial bank currency, or private currency, but are not strictly money, since they are not a unit of account.

There are also a great number of financial assets that are stores of value, with different degrees of liquidity. Even though demand deposits are means of payment and can function as a store of value with full liquidity, such attributes depend on public confidence in terms of the possibility of being converted freely and immediately into state money. Likewise, many financial assets may be considered stores of value whether there is a general belief that they will be converted into state money according to the agreed conditions or that they might be sold in exchange for state money with negligible loss of value.

Throughout history, there have been several types of parallel currencies and means of payment, with varying degrees of convertibility into state money. Blanc (1998) identifies four such instruments, according to their origin in specific social groups or contingent constraints: a) foreign or municipal and regional currencies circulating within a state; b) commercial or administrative organization initiatives on an emergency or *ad hoc* basis, limited in time and space; c) instruments created by non-commercial groups of persons which follow a community logic and are organized and maintained from a social base; and d) instruments of non-specifically monetary origin, associated with a limited monetary function in certain circumstances, but whose monetary function is not its main feature, such as the so-called local currencies.

From this perspective, it can be said that cryptocurrencies represent “parallel currencies”, or financial assets without guaranteed convertibility into state money, which seek to compete with the state currency as a means of payment, albeit still restricted.

For the supporters and enthusiasts of private cryptocurrencies, they are *de facto* currencies, or even money, but of a private and decentralized nature, incorruptible and free from government manipulation. It is also alleged that cryptocurrencies are more practical and have lower costs than other forms of already existing means of payment and transfers of values. Behind the so-called cryptocurrencies, as Lakomski-Laguerre; Desmedt (2015) point out, there is an anti-statist and neo-metalist ideology of money, seeking to enable the creation of a monetary order free from banks and monetary authorities, and with its supply fixed by a rigid rule, such as Bitcoin.

The enthusiasm surrounding the possibility that bitcoin could replace the state currency can be attributed to a mythical and deflationary view of the gold standard. It is worth recalling that proposals for the creation of non-state currencies emerged at various moments in history for socialist, community objectives or anti-deflationary purposes. Examples include the response to severe financial crises, such as occurred in the 1930s, or to achieve developmental goals employed by communities or regions of major poverty and with an absence of credit, as the case of local currencies created in recent years[1]. In all these cases, private currencies were created with limited uses and goals, in terms of time and economic space involved.

3 Distributed ledger technology and blockchain

In the last thirty years, the infrastructure of global information technology has changed significantly. The rapid pace of technological change and the reduction in transportation costs have led to advances in online media and payment facilities, with room for relevant technical changes in national and international financial systems (Stopford et al., 1991, Strange, 1998). The advance in the intermediation of transactions using credit cards, developed by companies such as Visa and MasterCard, was possible due to the trust established from encryption standards, resulting in increased security in the use of the network. Furthermore, the World Wide Web (WWW) consortium launched common protocols for the financial transaction system, such as the extension of http (hypertext transfer protocol), which became the basis of internet data communication (Narayanan et al., 2016).

The convergence between encryption standards and so-called digital currencies was linked to the very rapid progress of internet and information technology. Throughout the 2010s, the main innovations were related to the development of cryptocurrencies, such as Bitcoin and altcoins, which are mainly based on blockchain technologies. Although in a strict sense blockchain refers to the chain of cryptographically linked data blocks, this is one possible instrumental configuration within a larger series of technologies, that recent efforts have defined as distributed ledger technology (DLT) systems (Rauchs et al., 2018).

Essentially, the synergetic combination of game theory, computational cryptography and software engineering allowed for the creation of DLT systems (Lamport; Shostak; Pease, 1982). As a rule, a DLT system is a system of electronic records that allows independent entities to establish a consensus around a main group of accounting records - a shared ledger - and their validity, without relying on a central coordinator:

> A system of electronic records that i. enables a network of independent participants to establish a consensus around ii. of the authorized ordering of cryptographically – validated ('signed') transactions. These records are made iii. persistent by replicating the data across multiple nodes and iv. tamper-evident by linking them by cryptographic hashes. v. The shared result of the reconciliation/consensus process – the 'ledger' – serves as the authoritative version for these records (Rauchs et al., 2018, p. 24).

(1) In the first decades of the XIX Century, in the US and in the UK, bills or letters based on working hours for worker's wages were created by socialists, such as Robert Owen, and anarchist-individualists, like Josiah Warren. During the Great Depression, in 1930-1932, in Austria and Germany, there were some local currencies created in small, impoverished communities, with rules for progressive devaluation to induce consumption. In the 1980s, in developed countries (Canada, Norway, LETS (Local Exchange Trading System) appeared to facilitate local trade and development. In Argentina, at the height of the 2000-2002 great financial crisis, parallel currencies were issued by more than ten provincial governments, and local currencies were issued by small communities (exchange clubs). In Brazil, at the beginning of the 1960s the Rio Grande do Sul state government issued the so-called "brizoletas" to pay state servants; in the 1980s and in the 1990s, there were various types of Municipality bonds (Curitiba, Santana do Livramento, Campina do Monte Alegre); more recently, some communitarian banks have issued local currencies.

This technological innovation fits into a more specific field of the computer software industry, which has been built thanks to published technology standards and interface protocols that enable hardware and software products from many vendors to integrate seamlessly into the network. Standards define how programs and commands will work and how data will move through the system – the protocols and communication formats that hardware components must obey, the rules for exchanging signals between the application software and the operating system, the structure processor command descriptions to a printer and so on. This complex of standards and rules forms what is conventionally called ‘architecture’ (Morris; Ferguson, 1993).

The “architecture” of a DLT system consists of layers, components, and processes. Each layer is composed of one or more components involved in the creation or operation of a DLT system. A component is a logical set of related processes required for the operation of the system. A process is a series of actions performed by the actors to achieve a specific goal or a series of objectives involved in the successful operation of a component. The three essential and interdependent layers of DLT systems are: (i) protocol, (ii) network and (iii) data. The first is the set of rules defined by the software that determine how the system operates based on “constitutional” agreements adjusted between all system participants (Rauchs et al., 2018).

This means that there must be consensus among users and other actors for the system to function. This layer is composed of a protocol governance[2], a set of decision-making processes which defines, manages and updates the global rules of the game. This is a subset embedded in the broader governance project, which encompasses the full set of processes and standards that guide and define the coordination and action of the DLT system. Protocol governance can take many forms (hierarchical, anarchic, plutocratic, among others) and on many occasions it might be implicitly settled, but, as a rule, it is arranged in an orderly and legitimate way. For instance, one can argue that an open-source and permissionless DLT system such as Bitcoin is considered to have an anarchic type of governance. Therefore, rather than being guided by a foundation, corporation or even by an ‘enlightened despot’, the decision-making process is usually constructed among developers, miners and users. In other words, this layer defines how legitimacy is conferred as a proposal to network participants.

The network layer interconnects actors[3] and processes which implement the protocol (or technology standard). The network links the actors who collectively store, share, and process data. This layer is structured by three critical components: communication, transaction processing and

(2) The protocol layer is the technology standard that is characterized by two main components: genesis and alteration. On the one hand, the genesis component is related to the interdependencies of the systems (i.e., self-sufficient, dependent, interface and external systems) and with the creation of code bases (i.e., open source or closed source). On the other hand, the change component concerns the governance of the protocol layer. This is structured from the set of decision processes that allow the protocol to be changed in an orderly and legitimate manner.

(3) Rauchs et al. (2018) list four categories of actors performing various functions in DLT systems: (i) Developers write and review the code that underlies the technology building blocks of a DLT system and its connected systems. Developers can be professionals or participating as voluntary contributors; (ii) Administrators control access to the codebase repository core and may decide to add, remove, and change the code to change the rule system. Administrators are often involved in the governance process and can have absolute control over it; (iii) *Gateways* (bridges or network nodes) provide interfaces for the system acting as a bridge between the system and the external world; (iv) The network consists of interconnected participants that communicate by passing on messages to each other.

validation. The first one specifies which actors can become participants and access the network (open versus closed), how data is shared (public vs. private), and who can initiate (unrestricted versus restricted) transactions. The transaction processing component specifies the mechanism for updating the shared set of official records: (i) which participants have the right to update the shared set of official records (without permission versus permissioned) and (ii) how the participants arrive at an agreement regarding the implementation of these updates. Finally, the validation component defines the actions performed by each auditor to verify that the transactions and records follow the rules of the protocol, that is, whether they are valid and not conflicting. This is a crucial aspect of a DLT system that provides nodes (network participants) together with the ability to independently check what happens in the system (Rauchs et al., 2018).

Finally, the data layer is formed by the information flows which circulate through the system carrying specific meaning in connection with the design and functions the system is intended to perform for users. This layer refers to the information processed and stored by the DLT system in the form of a shared data structure (the *ledger*). This data structure is an authoritative version of records shared between users of the system and updated by them over time, i.e., as users engage with each other through the system. Applied to the virtual world, the ledger is structured in a similar way to a shared worksheet, whose copies are distributed over a network and stored by its users, implying the absence of a single central version of the database (BIS, 2018; Rauchs et al., 2018).

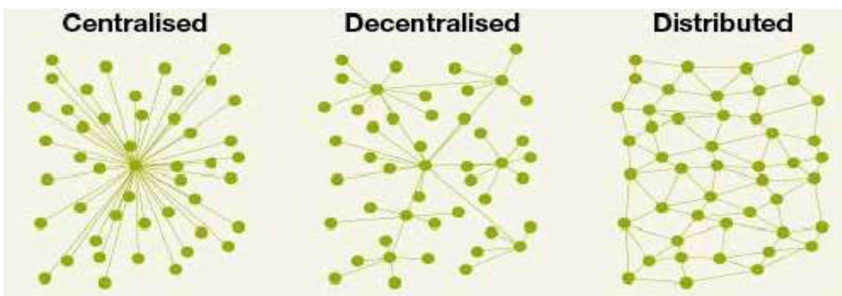
Altogether, the three layers take part in a set of interconnected and hierarchical components and structured interaction processes. The (i) protocol layer defines, manages and updates the global set of rules that make up the system's governance; the (ii) network layer forces the system to follow this set of rules and performs the steps necessary to achieve consensus throughout the system; (iii) the data layer defines the nature and meaning of the data upon which consensus was stipulated (Rauchs et al., 2018).

A DLT system needs to be capable of ensuring five key properties. First, a DLT system encompasses shared maintenance of the data record by allowing multiple parties to create, maintain, and collectively update a shared set of records (the *ledger*). Secondly, a DLT system needs to be capable of ensuring a 'consensus mechanism', in which the member parties must reach a common agreement on the shared data set. This 'multi-party consensus mechanism' results in the DLT system being decentralized, with two contrary features. On the one hand, a DLT system can be permissionless. If there is no need for permission, then there is no dependence on a single party or parallel agreements, and there is no reliable *ex ante* relationship between the parties. On the other hand, a DLT system can be permissioned, that is, if there is a requirement or prerequisites to operate, then the consensus is made through multiple record producers who have been approved and bound by some form of contract or other agreement (Rauchs et al., 2018).

The third property that a DLT system demands is independent validation. Each participant needs to individually verify the state of their transactions and integrity of the system. Also, a DLT system must assure tamper evidence and needs to be tamper resistant. In other words, it requires each participant to be allowed to detect non-consensual changes made to the data in detail so as to reveal even minor changes. Consequently, it becomes difficult for any of the participants to change past data records without leaving a trace (Rauchs et al., 2018). Therefore, a DLT system is a reliable set of records, maintained collaboratively by a significant proportion of network participants at any time, making them unlikely to be erased or manipulated.

According to Rauchs et al. (2018), decentralized and distributed processes can occur in all three layers (i.e., protocol, network, and data). Albeit similar, these processes are different (Figure 1). When storage or computing is distributed, it is divided into parts and occurs on multiple servers or nodes (organized in a "parallel" fashion). In a distributed way, the system offers not only greater efficiency in its operation but also greater resilience in comparison to the operation from only a single node. However, a distributed process may still have a central coordinator to act as an authoritative source of records.

Figure 1
Network differentiation: centralized, decentralized and distributed databases

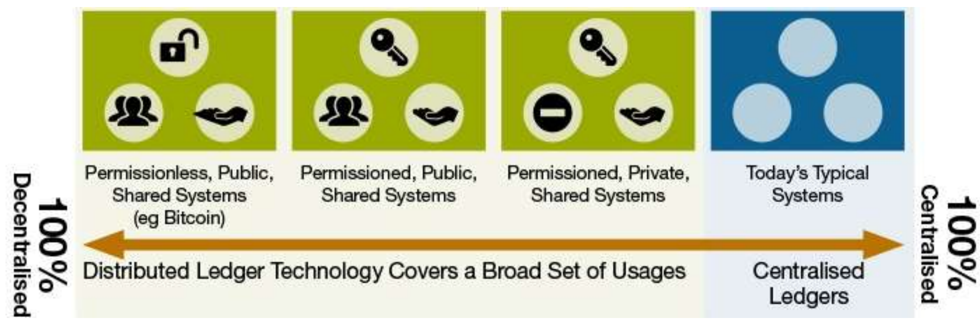


Source: Walport (2016, p. 36).

When a process is decentralized, several nodes are again in use - but in this case, the process is typically replicated across multiple nodes, usually controlled by different entities. This means that each node is managing the same store or running the same program as all others, redundantly. This replication requirement is at the heart of the scalability of some DLT systems to accommodate new users and growth in transaction volume because network resources are limited to that of their weakest node. If a network attempts to exceed this limit, weak nodes cannot remain synchronized and leave the network, which will lead to increased centralization.

Given the characteristics of DLT systems, these innovations hold great potential for transforming current payment systems. The most well-known application are the cryptocurrencies. As mentioned, DLT systems operate as "multiparty consensus machines" and present substantial differences. More precisely, DLT systems can vary depending on the degree of decentralization, to a large extent, but not exhaustively: public permissionless shared systems, public permissioned shared systems, and private permissioned shared systems (Figure 2).

Figure 2
Different DLTs according to their "degrees of centralization"



Source: Walport (2016, p. 35).

A public permissionless shared system aims to build trust in a fully decentralized environment. Public systems of this type allow unrestricted access to the network by any individual with computational resources and adequate internet connection (Mills et al., 2016). A network without typical permission is the peer-to-peer (P2P) framework, like those in which transactions are settled with paper money, where purchases and sales are made without the need for third-party authentication and verification (Bech; Garratt, 2017): no central authority is responsible for the settlement, clearing and recording of transactions. Even though any user can participate, the pre-transactions[4] can only be changed by consensus of the network given that no one has a special key to change the computational file (ledger) that stores the transactions[5] (BIS, 2018).

In contrast, some shared systems may have additional membership criteria, allowing only a limited group of individuals with pre-established requirements to access the network. Regardless of the degree of access, DLT systems can discriminate participants in terms of functions to be performed: in certain shared public systems, a group of participants may be responsible for validating transactions, another one for updating the database, while others are only allowed to read the data (Mills et al., 2016, Walport, 2016).

Permissioned shared systems are like banking payment systems: accounting can only be updated and certified by authorized participants, so-called "trusted nodes," which is a function that may belong to the company that developed the cryptocurrency, for example. As in the traditional payment system, there is an agent that validates and compensates transactions.

The best-known cryptocurrency, Bitcoin, is an open, public and unauthorized shared system that uses encrypted computational puzzles to regulate and limit the creation of cryptocurrencies,

(4) Transaction logs or the set of uncommitted transactions maintained by each individual node: transactions are still not incorporated into a formal record subject to network consensus rules (Rauchs et al., 2018).

(5) Although it is very difficult to alter a DLT system, it can be tampered with by what is conventionally named a 51% attack. This is an attack in which an entity or cartel with the most "votes" (for example, computing power) in a DLT system produces records faster than the rest of the network. Eventually, these records are revealed to the network, causing the "honest" node records to be replaced because of the conflict resolution rule. The 51% attack is the classic attack against DLT systems. PoW-based systems are especially vulnerable to such attacks; a similar attack on PoS-based systems is called a "long-range" attack. It should be noted that in some cases DLT systems are vulnerable to attacks by less than 51% of the voting power (e.g., selfish mining, which is theoretically feasible with only a third of the voting power) (Rauchs et al., 2018).

ensuring participants anonymity and transaction logs in the ledger as a way to avoid double or even unlimited currency spending, that is, the use of the same cryptocurrency more than once (Narayanan et al., 2016). Therefore, it is a very innovative public permissionless shared system, with a high degree of security, but without state safeguards or guarantees.

According to Lakomski-Laguerre and Desmedt (2015), the modern currency is also digital, electronic and virtual, in a more general sense, since it is mediated by data transfers settled by increasingly sophisticated computer systems. From this perspective, according to the authors the digital nature of the cryptocurrencies is their distinguishing factor in relation to the current monetary system: the great innovation regarding the current monetary order is the absence of central authority and the process of self-regulation.

Every cryptocurrency claimed by a user is tied to its identity, which is encrypted by a random alphanumeric sequence, so that only the user can decode it. Thus, every time the user wishes to make a transaction, the database keeping record of the transactions will require a private key to validate such a transaction (Lee, 2015; Narayanan et al., 2016). In the 1990s, this concept started to be marketed and implemented by some banks in the United States in the form of *ecash*, a financial innovation designed by an enterprise named *Digicash*, but its use by the American banking system was short-lived. In general, the encryption protocol dynamics[6] were tied to the connection between the user and the third party responsible for clearing the transaction, which guaranteed anonymity to the user but not to the third parties, the guarantors of the transaction. This cryptographic protocol spread by *Digicash* influenced subsequent technological developments (Clark, 2016).

Additionally, the support for P2P transactions is undoubtedly a central element in understanding the emergence of Bitcoin. But how to assign value to a shortage of digital documents on a network of decentralized transactions, such as a P2P network? In the virtual world, it was necessary to develop a system in which money issuance demanded a time-consuming solution of a computational puzzle. The aim was to create a coin with free circulation attributes and with its real value based on scarcity, as in the case of gold. This idea of assigning some value to digital objects by solving computational algorithms was elaborated in Adam Back's hashcash proposal, whose initial goal involved blocking spam in e-mails (Clark, 2016).

The specific qualities of hashcash ideas encompass four relevant aspects to understanding cryptocurrencies: 1) each transaction must have its own computational puzzle to be solved; 2) the receiving user in a transaction must be able to easily solve the puzzle without having to repeat the solution process; 3) each puzzle must be totally independent from the others, in the sense that the resolution of one does not reduce the time needed to solve another; 4) the more the parts (computers)

(6) Throughout the late 20th century, David Chaum, an American computer scientist and cryptographer, developed encrypted protocols applied to cash, and commercialized his ideas forming a company called *DigiCash*, where actual cash was named 'ecash'. Chaum discovered "how to both keep the system anonymous and avoid double spending by inventing the digital equivalent" (Clark, 2016, p. xvi) of a "blind signature", which consists of a long random serial number or an alphanumeric sequence. Moreover, Chaum and others later set up complex ciphered mechanisms that made users anonymous, so that banks could not track how the former were spending their money. However, *ecash* merchants were not anonymous. They had to return coins as soon as they received them, so the bank knew how much they were making, and so on. There were two major obstacles to *ecash*. First, it was hard to persuade banks and merchants to adopt it, since very few merchants accepted *ecash* and users also did not want *ecash*. Second, *ecash* did not support user-to-user transactions, or at least not very well. It was deeply concentrated on the user-to-merchant transaction. Therefore, merchants were crucial to the system functioning. After some time, credit card companies prevailed to the detriment of *Digicash* (cf. Clark, 2016).

solve the puzzles, achieving better solutions in terms of cost (energy) and speed (time), the more complex the puzzles in new transactions must be (Clark, 2016).

As a result, encrypted transactions can be exemplified as follows: user X wants to send user Y a message anonymously. To do so, user X uses encryption that transforms information to be sent in an alphanumeric sequence, or *hash* value, whose function is to hide its identity, as illustrated in Figure 3. In order to receive the message, user Y needs to decode this encrypted sequence, transforming it into the original information (Lee, 2015).

Figure 3
Encryption and *hash* value

- ✓ **User X information:** transfer of 100 Bitcoins to user Y
- ✓ **Hash value:** *46550fef 26f87ddd 5e15407f 45a0b8d2 9513291c 4e0f0acc*

Source: Own elaboration based on Lee (2015).

As previously stated, one of the relevant properties of this system is that, once the transaction is recorded, no subsequent change is possible. In the case of Bitcoin, the network is publicly held and embedded in computational files that increase the extent to which transactions are incorporated into the ledger over time. The concept that underlies this technology corresponds to the *linked timestamping* system, in which the documents are linked and related, since the subsequent document holds information and the digital signature of the previous document, forming a series that certifies its validity (Narayanan et al., 2016).

Although similar to this dynamic framework, Bitcoin was innovative in relation to the *linked timestamping* system, the so-called *efficient linked timestamping* system. Rather than linking individual digital documents, the enhancement consisted of gathering the records in a list that forms one block, linking it to others, which subsequently gives rise to a blockchain[7]. This structure reduces the number of times needed to verify a document at a random point in the system's history (Narayanan et al., 2016). Therefore, this mode of timestamping ensures that the transaction data is recorded in a "timeline", with dates and times of the previous transaction in the currency code, in order to form a chain (Nakamoto, 2008). In other words, all transactions in Bitcoins are recorded and their validity is conditioned on the approval of the records by the system, in a sequence of actions, as described by Nakamoto, the nickname used by the Bitcoin[8] creator(s):

> 1) New transactions are transmitted to all nodes. 2) Each new member makes a new collection in a block. 3) Each one works to find proof of work for your block. 4) When a node is a working test, it transmits the block to all nodes. 5) Nodes accept the block only if all your transactions are valid and have not yet been spent. 6) The files express their block level in the production of the next block at a time, using a hash of the block accepted as previous hash (Nakamoto, 2008, p. 3)[9].

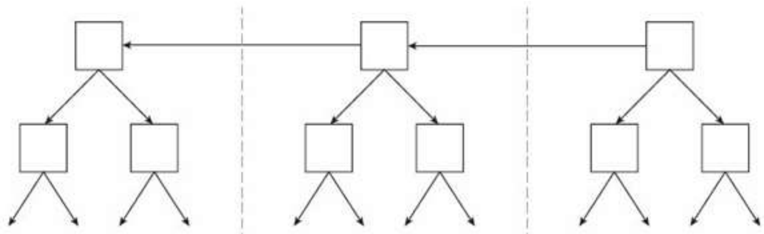
(7) Haber and Stornetta (1991) proposed the term 'registration structure' in the creation of intellectual property as a digital document in order to correct property rights with the creator before it can be copied by others (Cf. Yermack, 2017).

(8) The creation of bitcoin will be detailed in section 4.

(9) Proof-of-work (PoW) is a system that scans the values of currencies, giving authenticity to transactions (Nakamoto, 2008). In other words, it is an algorithm that requires a quantity of work to be calculated, such as hashcash, whose resolution assigns validity to information embedded in the data network.

The arrangement of the registrations forms a block chain (Figure 4).

Figure 4
Efficient linked timestamping system



Source: Narayanan et al. (2016, p. 49).

One can argue that Nakamoto (2008) combined the idea of hashcash computational puzzles protocol with improving timestamping as a way of promoting system security. Each transaction in the public ledger does not need to be guaranteed by a third party, as in DigiCash. Thus, Bitcoin's blockchain is a "public database (giant ledger book), openly maintained by computers all over the world – it is a sequential record of all transactions and current ownership (Blundell-Wignall, 2014, p. 8). The double-spending problem is solved by using timestamping in each transaction, making the system secure to the extent that honest nodes have greater CPU power control than any other attacking nodes (Nakamoto, 2008).

Online payment transactions are basically made possible through financial institutions, trading platforms and payment systems that work as intermediary parts of the process. Mainly based on blockchain technologies, the application of DLT systems has grown significantly in recent years, which shows that large international banks and central banks have sought to lead initiatives for the development of financial and technological innovations.

4 Private cryptocurrencies: the Bitcoin case

The popularity of Bitcoin - the first cryptocurrency launched in the world - rose in the context of the international financial turmoil, which began in 2008 when much of the trust in existing institutions was lost (Blundell-Wignall, 2014). One can argue that public distrust in the traditional banking system may largely account for the success of financial innovations in cryptocurrencies. For this reason, in Bitcoin's founding document, Nakamoto (2008) pointed out that the payment system introduced by the new currency is based above all on a model of trust.

Although the founding document was launched in 2008, the development of the set of ideas that shaped the technological structure behind Bitcoin originated in the cypherpunks movement, combining cypher (referring to cryptography) and rebellious (referring to punk) ideas (Assange et al., 2012). Throughout the 1990s, interactions between the economy and the internet stimulated the emergence of concepts related to freedom of speech, as well as the execution of private transactions. Its enthusiasts argued that, from the notion of using cryptography as a non-violent tool and countering the coercive forces of the state, it would be necessary to establish a systemic architecture in which transactions were distributed in a decentralized way among users, which would eliminate the power of a central decision-making unit to withhold and interfere with payment records and offset transactions (Assange et al., 2012).

Based on these considerations, Nakamoto (2008) emphasized the need for an electronic language that would allow negotiators to perform their transmissions without third party intermediaries, preventing the irreversibility of the payment process and allowing it to be protected by users. Hence, cryptocurrencies claim not only to be a general means of payment with innovative technology, but also a new model of trust, which promises to coordinate productive economic activities. However, there are also weaknesses (risks of fraud and technology failure) and limitations (price instability and low “scalability” - the ability of a technique, a process or a system to expand uniformly) (BIS, 2018).

Recently, Bitcoin has primarily attracted technology enthusiasts who use it for online commerce and groups with libertarian political convictions that approve of the currency for not having government connections[10] and speculators. In terms of stability, an estimation from March 2014 pointed out that the daily volume of 70,000 transactions in Bitcoins involved mostly transfers between speculative investors and not purchases of goods and services, indicating minimal use as a means of payment (Yermack, 2014). It is also extremely difficult to use Bitcoin as a unit of account, since the high daily price volatility requires constant repricing if goods are ‘measured’ in Bitcoins.

Bitcoin is certainly the main cryptocurrency among the almost two thousand cataloged today. It can be created by a *mining process*, that is, from the contribution of those who cooperate for the operation of the Bitcoin’s network by the use of technology (computational processing), in order to provide a solution to the cryptographic problem involved in a block of transactions with the use of this cryptocurrency. However, the supply of Bitcoin is limited to 21 million, and currently about 80% of that total has already been extracted (CNBC Markets, 2018).

As a rule, the Bitcoin *mining process* works as follows: transaction data involving Bitcoin are transmitted to all P2P nodes participating in the network, and the transaction is made via resolution of the computational enigma. Initially, the miner receives 25 Bitcoins for each block of transactions discovered, a payment for having granted his computing power to enable transactions in bitcoin. It is worth mentioning that this occurs while other network participants accept the (data) block in order to make it part of the consensus chain. In addition to this allowance, miners can also be rewarded for transaction fees optionally offered by network users and included in candidate blocks (the ledger) by miners. Rates are offered by users so that their transactions are prioritized by the miners in forming their candidate blocks, thus increasing the chance of a transaction being completed faster.

The rigidity of Bitcoin’s ‘creation’ rule refers to the fact that *mining* new Bitcoins depends exclusively on the following system: 50 Bitcoins are required for the insertion of a new block of transactions in the blockchain every ten minutes[11], in the first four years of its existence; 25 Bitcoins from the fifth year, every ten minutes (insertion of a new block in the chain of blocks), until reaching

(10) These first two are mentioned in Yermack (2014).

(11) In fact, this restrictive aspect of the money supply is necessarily due to the rate of data transfer from one place to another (transfer rate).

210 thousand blocks; and the subsidy[12] will be reduced by half to 210 thousand blocks. Considering this reduction to half the reward (i.e., subsidy and transaction fees) of *mining* activity every four years, on average, the estimated limit of 21 million Bitcoins is reached at 2140 unities. In January 2018, Bitcoin supply reached 16.8 million (i.e., about 80%, which covers 21 million Bitcoins) remaining just 20% of the total to be mined (CNBC Markets, 2018). This leads to increased dispute in the *mining process*, requiring greater and increasing processing capacity of the machines used and with a yield per *mined* block (i.e., fees for processing transactions)[13], since miners must prove that they have strived to process transactions in order to be rewarded. This venture involves the time and energy it takes to run the computer hardware and solve complex equations.

The difficulty in supplying Bitcoins introduces a deflationary bias in an economic system based on private cryptocurrencies. This occurs because Bitcoin's reward halving results in a dwindling finite supply. Effectively, if halving does not increase demand and price, then miners have no stimuli for completing and validating transactions as rewards would be smaller and the value of Bitcoin would not be high enough. This feature, of course, affects speculating with such currency due to its increasing use, albeit globally restricted. The Bitcoin enthusiasts argued that this new currency would avoid inflationary processes. They did not consider, however, that this rigid form of Bitcoin 'creation' introduces a high price variability and deflationary tendencies in an economic system based on this cryptocurrency. After all, there are no banks capable of 'creating' Bitcoins in this system, and a capitalist economy is fundamentally a system of indebtedness, i.e., credit.

The exceptional upward trend in the price of Bitcoin in 2017 can also be explained by the nature of the Bitcoin 'creation' rule, coupled with the significant increase in its usage, albeit largely restricted around the world, particularly for speculative operations. The value of Bitcoin is centered on its implementation in 2009. After an increase of 1,400% during 2017, Bitcoin's value has fallen since mid-December of the same year. In early 2017, the quote was between $ 800 and $ 1,000, on May 16 it reached $ 19,200 and a day later at nearly $ 20,000, followed by a downward trajectory. On June 10, 2018, Bitcoin continued to fall and closed its price at US $ 6,800, just 35% of the previous value of December 16. One year later, on June 25, 2019, its price reached US$ 12,686. In November 2019, the average price was around US$ 7,000 (Valor Econômico, 2018a; Blockchain, 2019).

This movement did not only coincide with but was largely the result of the beginning of negotiations on the futures market on the Chicago Board of Trade. This is because, besides being recognized as a financial asset, there was a significant increase in the supply of Bitcoin as a result of trading futures contracts, which directly impacted its quotation on the spot market. The common

(12) DLT systems present explicit and implicit stimuli to foster record producers to take part in transaction processing by creating and proposing records. According to Rauchs et al. (2018, p. 63) "These incentives can be of a different nature (e.g., monetary, legal, social) and can be expressed directly by protocol rules (e.g., block rewards in a native asset) or by external factors (e.g., contractual agreements established between participants). Open systems such as Bitcoin tend to be secured via economic incentive designs that make use of an endogenous network resource (native asset) as an economic coordination mechanism to align incentives".

(13) Currently, for each mine block, the miner receives 12.5 bitcoin. It is estimated that in a maximum of two years this remuneration will halve to 6.25 bitcoin, and that in 2032, when 99% of the bitcoin has been extracted, the remuneration will be 1 bitcoin per block. (Cf, CNBC Markets, 2018)

strategy of fundraising in the world of cryptocurrencies, consists of Initial Coin Offering (ICO)[14], that is when someone offers investors some units of a new cryptocurrency or a token (digital object) in exchange mostly for Bitcoin or *Ethereum*. Recently, the launch of variations of this modality has grown, as in the case of the Security Token Offering (STO) that operates as a token sale whose features compare to classic titles that are fully regulated and accepted in at least one jurisdiction. Prospectively, ICOs and STOs have increasingly become alternatives to the classic ratio between debt and capital funding as held today by joint ventures, private equity and banks (Strategy & Pwc, 2019). However, even with these practices having become popular in the cryptocurrency market, the sharp decline in the value of these digital currencies, especially in 2018, has led investors to seek funding through traditional financial tools to guarantee some gains on their depreciated assets (Bloomberg, 2019).

Other factors contributed to this recent strong downward movement, with emphasis on the following: i) the emergence and proliferation of fraud, robberies and cyberattacks in the cryptocurrency negotiations and in launching some of them; ii) increasing initiatives for the regulation of cryptocurrencies by governments, including taxation; iii) the emergence of many other cryptocurrencies besides Bitcoin (currently, there are 1897 cryptocurrencies cataloged and marketed daily[15]); and iv) a high concentration of Bitcoin in just a few negotiators, which makes its price very sensitive to their strategies[16]; v) significant reduction of the Bitcoin mining company's remuneration, with a downward trend in the short term, which could make the relation between return and cost of this negative activity[17]; and vi) cooling of the speculative euphoria based on the so-called *greater-fool* theory[18] (Blundell-Wignall, 2014).

Also, it is worth mentioning that the primary means of accessing Bitcoins is within the scope of the dedicated exchange platforms. According to Lakomski-Laguerre and Desmedt (2015):

> How do you get bitcoins? If we hypothesize a closed and turning system, it would be logical to assume that access to bitcoins comes from a sale (of goods, services, workforce) meaning a contribution to production (from the corresponding commercial space). Although it is possible to obtain bitcoins in exchange for the sale of goods or services within a network of merchants who accept them, this consideration is, on the other hand, still extremely limited. In fact, access to bitcoins is mainly through the sale of official currencies on trading platforms dedicated to a market price that fluctuates according to supply and demand. Therefore, bitcoin becomes a currency among others in a globalized and competitive monetary space and therefore it can be used as a specific asset by any investor motivated by a financial logic of portfolio optimization. With the phenomenal appreciation it has been subject to since its inception and the volatility of

(14) In a narrow definition, ICO (also token or token generation) is a term that describes a limited period in which a company sells a predefined number of digital objects (tokens to the public in exchange for cryptographic currencies or fiduciary currencies (Strategy & Pwc, 2019).

(15) Credit Suisse (2018) points out that in 2017 the Initial Coin Offerings (ICO) raised $ 3 billion, well above the $ 295 million raised between 2014 and 2016. The bank calls the phenomenon of cryptocurrencies prices behavior and ICO 'cryptocurrency mania'.

(16) 97% of bitcoins belong to only 4% of the negotiators (IP addresses) (Credit Suisse, 2018).

(17) With this new reality of *mining* activity, the investment made so far to allow bitcoin transactions can be used to destabilize the bitcoin network or other networks, as well as to steal bitcoin and other cryptocurrencies (Credit Suisse, 2018).

(18) A high speculative demand in which agents believe it is worth buying the currency for a higher value, since there will be another agent willing to buy that same currency for an even greater value than the first.

> its price relative to official currencies, it is clear that today, bitcoin is much more like a speculative asset than a means of payment (free translation).

As previously mentioned, the Bitcoin protocol stipulates that each new block can only be added to the current block at pre-set intervals (of ten minutes). Furthermore, each block can only contain a maximum volume of data (one megabyte), which makes the system capable of processing a maximum of seven transactions per second, falling far short of what is needed to become a potentially 'generalizable' means of payment. Although the system is effective in maintaining the security of the network, it is inefficient as a means of payment worldwide, since the limits seem to extend to the processing capacity of the network as a whole (BIS, 2018).

Recent developments have proposed solutions to the lack of 'scalability' of cryptocurrencies, such as the Lightning Network. This works as a second layer above the Bitcoin DLT system, using the smart contracts[19] functionality to create a secure environment for off-network transactions, that is, an interface system[20]. The microtransactions are therefore processed in an external environment to the network and later have the balances synchronized in the DLT system (i.e., the off-chain registered transactions are only updated on the main blockchain when two parties open and close a channel). Such a configuration claims to be able to make payments instantly, execute millions of transactions per second, and improve the "functionality of the base layer, without compromising network decentralization or security" (Rauchs et al., 2018, p. 48). The Lightning Network is therefore a possible way out of the 'scalability' of payment devices based on public DLT systems (i.e., Bitcoin), but this solution is still under development and will need to be tested before delivering on its promises (BIS, 2018).

The limitations of cryptocurrencies are clear-cut. In Bitcoin's case, there are general implications for material and economic life. The security of the system, based on the proof of work (PoW), is directly linked to the consumption of electricity, since its dynamics requires the resolution of probabilistic algorithms, namely, computational enigmas. According to the BIS (2018), so far, throughout the mining process chain, the total use of electricity for the discovery of new Bitcoins has matched that of medium-sized economies, such as Switzerland. Also, other cryptocurrencies use large amounts of electricity since they are based on DLT systems analogous to Bitcoin. Hence, it is believed that the 'productive' process of digital currencies (e.g., mining process) can have serious consequences for the environment (electric power is a different thing).

Struggling to overcome limiting aspects of blockchain technologies and DLT systems, coordinated actions between financial institutions and government agencies have sought to

(19) A smart contract is a computerized transaction protocol that executes the terms of a contract. The overall objectives of intelligent contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even compliance), minimize malicious and accidental exceptions, and minimize the need for reliable intermediaries. Related economic objectives include reducing losses caused by fraud, arbitrage and enforcement costs, and other transaction costs (Szabo, 1994).

(20) An interface system is a system that, in a timely manner, employs the main functionality provided by another DLT system, but which could be easily reconfigured to use another base layer DLT system, if necessary or desired. This means that if a base system no longer exists, the interface system would be able to survive for at least some time on its own and can continue operating by exploiting the functions of an alternative DLT base layer. The long-term survival of an interface system depends on the continued existence of at least a "base layer" DLT system. Examples include "layer 2" solutions such as the Lightning Network based on Bitcoin and the Raiden Network based on Ethereum. These systems are commonly designed to improve the 'scalability' and functionality of the base layer without compromising network decentralization or security (Rauchs et al., 2018).

incorporate new ways of ensuring transaction security in the decentralized data network (Brazil, 2017). One of the alternatives developed was in the orbit of permissioned DLT systems. Proof-of-stake (PoS) constituted as a 'consensus mechanism' that, instead of requiring the resolution of energy-intensive computational enigmas, requires issuers to constitute capital as collateral, that is, access to a certain amount of currency before being accepted by the network (Rauchs et al., 2018). In 2017, the blockchain consortium Ethereum announced plans to make this logical method the foundation of the mining process of this cryptocurrency. Thus, such efforts seek to develop a technological architecture that is simultaneously less energy-intensive, safe and fast (MIT Technology Review, 2018).

5 Reactions and initiatives from major banks

Major banks have actively reacted to the relevant impacts caused by the use, development and employment of DLT. This innovative technological architecture presents a rather functional character for the modern, non-decentralized financial system due to its potential to facilitate transference of data and to enable greater efficiency and security in financial transactions, in terms of time and transaction costs, with "shared data with common standards; reduced need for reconciliation; and seamless transfer of digital assets." (JP Morgan, 2017, p. 3). Besides allowing a simplified, agile and efficient infrastructure – from more immediate positive effects on the back-office and the internal processes of these institutions, DLT has the potential to allow high-speed transference of data, enabling flexibility in contract settlement capable of providing pricing models and innovative service offerings (JP Morgan, 2017). In this sense, the implications of the DLT for the financial system can be extensive and disruptive, especially for payments, clearing and settlement systems (PCS).

> The concept of distributed ledger technology – or blockchain as it is commonly called – has taken the financial services sector by storm, with venture capital and investment pouring into technology startups. Debate over blockchain's promise, as well as its limitations, is ongoing. For every believer who says blockchain is the most revolutionary technology platform to emerge since the internet, there are skeptics who claim it is merely the latest tulip mania. Nonetheless, a broad consensus is emerging that it represents a real innovation over many of the systems and processes used in financial services and banking today (JP Morgan, 2017, p. 3).

Investments in startups that use DLT, including blockchain, have grown significantly worldwide, notably in the so-called fintech segment, especially in the US. Major international banks are very attentive to this combination of P2P Networking, asymmetric cryptography and cryptographic hashing[21], which underlies Bitcoin and other private cryptocurrencies. In the case of these institutions, this technology has been adapted and employed within a regulatory and institutional framework authorized by the State. This is because it allows the decentralization of agent trust (by requiring the consent of other network participants) and a data processing system potentially capable of making thousands of transactions per second, much more than the databases used by banks today (JP Morgan, 2017). In this sense, this capability would include the so-called smart contracts, which are computerized instructions for financial operations (such as buying a share from a certain quote). Even though banks already hold such pre-programmed instructions, the blockchain's infrastructure

(21) Whilst asymmetric cryptography refers to the possibility of transference of information with verifiability of the authenticity of the sender, but with permission of only the recipients to be able to access the contents of that information, the cryptographic hashing corresponds to the ability to compare and certify a large set of data (information) (JP Morgan, 2017).

would be more efficient when monitoring the list of transactions in a decentralized way, inducing banking and financial automation to another level (Casey; Vigna, 2018).

The motivation of the major banks certainly includes competition from the so-called stablecoins, or e-Money. Stablecoins are financial assets that can be used as means of payment and are issued by private non-financial highly technological companies, backed by state money and with the guarantee of conversion into state money immediately and on par (BIS, 2019).

> Think of WeChat Pay and AliPay in China, M-Pesa in Kenya, Bitt.com in the Caribbean, and USD-coin by Coinbase and Circle. Other major tech companies are also rumored to introduce their own form of eMoney very soon. eMoney, in its various forms, covers more than 25 currencies to date, and that number is growing rapidly. Adoption rates are impressive. In Kenya, for instance, 90 percent of the population over 14 years of age uses M-Pesa. In China, transactions in eMoney reached $18.7 trillion – more than all transactions handled worldwide by Visa and MasterCard combined. Furthermore, many operators now offer debit cards that can be used with stablecoins, turning them into an efficient means of payments for most merchants (Adrian; Tobias, 2019).

According to data from the World Economic Forum 2016, within the world of international finance, more than US$ 1.4 billion had been invested and more than 2500 patents had been recognized between 2013 and 2016, 24 governments and more than 90 central banks had developed studies on DLT applications, more than 90 institutions had participated in DLT consortia and 80% of the analyzed banks had created their own initiatives, among them the largest ones, including JPMorgan, ING, Standard Chartered, Morgan Stanley, Santander.

According to the same study, regarding the major DLT implementation initiatives, the main advantages and potential disruptions of this technology implied: i) operational simplification (DLT can reduce or eliminate manual efforts involved in reconciliation and dispute resolution); ii) improvement in regulatory efficiency (DLT allows monitoring financial activities by regulators and is regulated in real time); iii) diminishing counterpart risk (DLT does not require the reliance on counterparties to fulfill their agreed obligations, since the contracts are coded and executed by a shared and unchanging mechanism); iv) reduction of settlement and clearing time (the DLT disintermediate agents responsible for verifications and validation of transactions, speeding up the process as a whole); v) greater liquidity of capital (DLT reduces volume of uninvested capital and increases transparency in the distribution of liquidity for assets); and vi) fraud mitigation (DLT stores information such as provenance and transaction history in a single database) (World Economic Forum, 2016).

In summary, the DLT architecture, including blockchain, has the potential to reduce collateral risk, making the real-time calculation of the risk of the underlying asset viable and, therefore, creating more accurate pricing of assets, enabling greater segmentation and positioning of financial products and services, providing scale and scope economies for banking and non-banking financial institutions, allowing a more efficient system of asset management, among others. From the point of view of the major international banks, the use of this technology tends to enable more efficient use of resources, providing faster operations and lower costs of financial products and services offered by the financial system (JP Morgan, 2017). This is the reason JPMorgan (2017, p. 4) states: “Our view is that blockchain's impact may eventually reshape market structure, product capabilities and the client experience, ultimately having a lasting influence on the global economic system".

Therefore, this shows that DLT is far beyond the emergence and viability of so-called cryptocurrencies, since it has been increasingly used by corporations inserted in the current monetary order. Major international banks have joined the Swiss investment bank UBS to create a virtual currency that can clear and settle financial transactions and start operating at the end of 2018. The initiative seeks to overcome the doubts and risks of fraud involving the DLT, with emphasis on blockchain configuration, and, for this reason, central banks and regulatory agencies have also participated in discussions on the subject (Valor Econômico, 2017).

This project aims to increase efficiency of financial markets by creating a currency that allows clearing and settlement. Reducing risk, accelerating back-office settlement systems, releasing capital for international operations are some of UBS' goals in partnership with major international banks:

> The settlement currency, based on a product developed by Clearmatics Technologies, aims to allow financial groups to carry out payments among themselves or to buy financial instruments such as bonds and stocks, without waiting for traditional money transfers to be completed. Instead, they would use digital currencies that are directly convertible into money in central banks, reducing time, cost and capital required for the after-deal clearing and settlement. Digital currencies, each of which are convertible into different currencies, would be stored using the blockchain – a distributed accounting scheme –, allowing quick exchanges by the financial instruments previously negotiated (Valor Econômico, 2017; free translation).

According to UBS (2017), in accordance with JP Morgan (2017) in this regard, blockchain technology, one of the possible DLT configurations, could allow a reformulation of the financial system, making its transactions simpler and less expensive. Besides that, it guarantees, on the one hand, greater control and privacy of financial transactions to individuals and, on the other, better monitoring and protection of regulator mechanisms.

The bank also highlights technical, systemic, legal and regulatory difficulties that may arise from blockchain technology, such as the need to operate transactions with speed, scale and security; how to transfer real money into the chain; issues of privacy and digital identity; how contracts for transactions carried out by the new technology will be made; and how the international jurisdiction that will regulate blockchain will be structured in order to protect both individuals and the financial system as whole (UBS, 2016).

The USC (utility settlement coin) is a digital currency based on blockchain technology whose purpose is to be converted into state currencies, allowing securities transactions to take place between financial institutions, reducing the time and costs of settlement and compensation (UBS, 2016). The USC was launched in 2016 by the initial partnership among UBS, Deutsche Bank, Santander Bank, BNY Mellon and the FinTech Clearmatics, which today includes other international banks such as NEX, Barclays, Credit Suisse, Canadian Imperial Bank of Commerce, HSBC, MUFG and State Street (Valor Econômico, 2017).

For Hyder Jaffrey, head of strategic investment and financial technology innovation at UBS, USC can both help in improving the management of bank risk and in increasing capital efficiency.

The initiative will not produce a new cryptocurrency but a new cryptocash, since it will be a way of representing national currencies in a ledger, that is, a value in USC will correspond to the same value in national currency. Therefore, "the cash is on the ledger and will always be backed by real cash held at the central bank – in much the same way cash is technically a promissory note that used to be backed by physical gold" (Financial Institutions Hub, 2017).

According to Jaffrey, it is possible to delineate a spectrum for cryptocurrencies: at one end, there would be those without regulation and outside governmental control, like Bitcoin; at the other end, the central banks cryptocurrencies which are digital cryptographic currencies of the existing currencies. In the middle of this spectrum would be the USC, which has at the same time Bitcoin characteristics, such as the ability to settle transactions in real time, and central banks' currencies characteristics. In this sense, it will always have the same value because it is backed by these Central Bank currencies, which means it will not suffer price changes like Bitcoin (Financial Institutions Hub, 2017). He also points out that the USC will be a change factor in institutional banking models:

> New and highly efficient models for settlement, collateral management, know your customer (KYC), anti-money laundering (AML), reporting, etc. will all be made possible. A further iteration will start to enable new fully digital securities such as digital bonds, equities and derivatives that all live on a Distributed Ledger marketplace (Financial Institutions Hub, 2017).

JPMorgan Chase, in partnership with the Royal Bank of Canada and the Australia and New Zealand Banking Group, announced the launch of the Interbank Information Network (IIN) in mid-October 2017, a blockchain technology-based interbank transfer system that would enable a significant reduction in the time of resource transfer between banks on a global scale, due to the reduction of the time needed to verify payments. According to the bank, this timespan would be reduced from weeks to just a few hours. It is emblematic that JPMorgan Chase CEO and Chairman Jamie Dimon said just a month before the IIN's launch that Bitcoin is a "fraud that won't end well". However, when IIN was announced, he stated that "the blockchain is a technology which is a good technology. We actually use it. It will be useful in a lot of different things. God bless the blockchain." (Cheng, 2017).

These movements show that major international banks have not only reacted to the emergence of blockchain technology, but, more importantly, acted in a highly active and strategic way in this process, either through partnerships and acquisitions of fintechs, or through relevant advances in the development and application of such technology in their operations. Initiatives such as Project Jasper, Corda, Hyperledger, among others, are examples of innovative blockchain platforms, whose business strategies are varied, but that seek to serve an expanding financial industry, especially in relationships between central banks and the interbank transaction sector. In the case of Project Jasper, their aim is to develop a technological architecture directed at compensating payments and transfer values within the interbank universe, whose primary element would be the protection of privacy within the decentralized dimension of a ledger (Brazil, 2017; Chapman et al., 2017).

The Corda platform was another relevant initiative established by a large global consortium of DLT development, the R3. Formed by financial sector giants such as SBI Group, Bank of America Merrill Lynch, HSBC, Wells Fargo, Bradesco Bank and Itaú Unibanco, this consortium announced investments worth US$ 120 million for development of payment system technology (R3, 2018). The

Corda platform is a blockchain architecture inspired by a publicly owned DLT, in which “trusted nodes” perform Corda network and smart contracts (CorDapps) protocols. Although the information is recorded in a global DLT, the Corda blockchain is not shared globally: instead, each node participating in the network stores a fraction of the distributed ledger. This fraction corresponds to the set of transactions in which the determined “trusted node” has participated. Thereby, both sides of the transaction will see the same version of any transactions shared by those in the DLT, but the pairs will not have access to the transactions of which they are not part. In other words, it constitutes a level of decentralization of transactions that is associated with party privacy (Brazil, 2017).

The Hyperledger Project has been developed collaboratively among members of various industries such as IBM, ConsenSys, Cisco, Intel, Accenture, the R3 consortium itself and several others, aiming to improve various aspects surrounding the performance and robustness of global industries. The Hyperledger Fabric is a platform that has been used to develop applications, by both the industrial and banking sectors, already with some operational and commercialized products. In Brazil, the FEBRABAN Blockchain Working Group, composed of several national and international banks, has been conducting a series of tests for financial services in Corda, Hyperledger Fabric and Ethereum, highlighting the dynamic nature of the Brazilian financial sector (Funke, 2017).

These institutions are aware that in addition to cryptocurrencies, blockchain technology represents an asset that can reshape not only the financial system based on the state currency, but mainly, the banking currency. This is something that, of course, the deregulated and decentralized cryptocurrencies enthusiasts did not expect.

6 Central Bank Digital Currencies

The motivations for the creation of cryptocurrencies by CBs obviously include the concern to keep up with the technological innovations of private cryptocurrencies. CB are also seeking to reduce the costs and risks of the banking system on settling payments and transferring values. Another challenge is the declining demand for paper money, albeit at different rates between countries. Perceived risks include threats to the banking system in times of a crisis of distrust in large institutions, when demand for state-issued cryptocurrencies could aggravate liquidity crises of the major banks. Finally, there is the risk posed by a large use of private cryptocurrencies in criminal activities and money laundering.

The designation adopted by The Bank of International Settlements (BIS, 2018), Central Bank Digital Currencies (CBDC), is one of the most used in debates and projects in progress – Central Bank Digital Money, Central Bank Electronic Money, Central Bank Cryptocurrencies, besides proposals in progress, such as the Swedish e-krona and FedCoin in the United States. One of the reasons for the adoption of the term CBDC from the BIS (2018) in this paper is because it emphasizes the aspect of means of payment held by the public, like traditional currency, paper money or coin, although this is not the only version in studies, as discussed below.

According to Bech and Garratt (2017), a CBDC can be understood as an electronic currency issued by a central bank, which can be transacted in a decentralized way (P2P), without a central payment clearing authority. This innovative initiative could have implications both for the retail sector and the wholesale sector of the international monetary and financial system. Unlike private cryptocurrencies, such as Bitcoin, these digital coins would be under the responsibility of the monetary authority based on state power, which would have implications for the anonymous character of the transactions. In other words, while private cryptocurrencies may favor the practice of illegal activities through the anonymity of the third party, such as tax evasion, terrorist financing and money laundering, the CBDC could allow a digital substitute for the state currency, with properties like those already in force and tied to the central bank's money. Therefore, as a cryptocurrency issuer, the central bank could discretionarily decide on prerequisites and the necessary information for customers to transact the digital currency.

According to BIS (2018, p. 8)), "In wholesale markets settlement systems could be more efficient – in terms of costs and use of collateral and liquidity – by using wholesale CBDC. (…) If complemented by direct participation of non-banks in the settlement process, gins could further increase, including through facilitating the use of new technologies for asset transfers, authentication, record keeping, data management and risk management" (BIS, 2018, p. 8).

In general, payment clearances in wholesale systems are transactions of high value and high priority, as in the case of interbank transfers. In this sense, the technical advances would be directly related to the operational costs of transactions and efficiency. Although studies have focused on the efficiency attributed to alternative authentication systems such as the PoS (Hong Kong Monetary Authority, 2017) and on the use of blockchain within regional arrangements (Bank of France apud Bech; Garratt, 2016), there is a great deal of doubt surrounding the adoption of decentralized data logging technology.

The current discussion points out some basic structures of CBDC. Specifically with regard to the format, these elementary frameworks would include: i) open-access public accounts cleared by central banks; or open-access tokens traded in a decentralized way with degrees of anonymity (i.e. guarantee of complete or partial anonymity); ii) degrees of paper money substitution (i.e. total or partial substitution of paper money; iii) some types of indexation (i.e. fixed nominal value, with or without interest; constant real value, with nominal value indexed to a price index or determined by the Central Bank, with a specific interest rate for the CBDC); iv) banks competencies (i.e. admission of public accounts in central banks or public accounts maintained only at banks, as it is at present).

Considering these alternatives, the CBDC could be: (i) something like currency itself, a monetary asset for the public, credit-risk free, with a defined nominal value; or (ii) a credit-risk free, principal-remunerated asset, but with the risk of price fluctuation, including discounts, if the CB wishes. The implications for the monetary system have sparked great interest, with many interpretations and questions.

One of the problems is the lack of emphasis on how the CBDC could impact the supply of credit in the economy, including: (i) if the accounts in the CBDC are individual, it can be assumed that the function of creating currency and credit by banks may disappear, particularly in the case of the banking system as a short-term creditor along with the clearing of payments; (ii) if the supply of demand deposit accounts continues to be exclusively of the banks, the scenario would be similar to the current one; (iii) if parity is fixed relative to paper money, there would be little change; but (iv), if the CBDC sets interest rates or sets exchange rates in paper currency, there is much to consider about the implications for the banks activity.

7 Challenges for regulation

The use of blockchain technology as an unregulated financial innovation and the increasing use of digital currencies, however, can result in, for example: i) the possibility of market volatility and fraud, ii) the emergence of new currencies, that the public favors, eliminating others, and iii) the need for regulation. The anonymity guaranteed by the cryptocurrencies prevents financial regulation, advantageous for illegal activities, such as financing of terrorism, money laundering and tax evasion, constituting new forms of international crimes.

The first problem related to virtual currency regulation is the difficulty in defining what these currencies really are, since they combine characteristics of currencies, payment systems and commodities. In this sense, it would be necessary to standardize the classification so that regulatory authorities could apply the same policies. Since they are decentralized and transnational, transactions in virtual currencies become not only difficult to track, but also carry the need for jurisdiction, with regulations across national boundaries that differ from traditional regulatory models. Furthermore, countries have dealt differently with these currencies, with some banning their use, such as Bolivia and Russia, and others warning against the risks involved (International Monetary Fund, 2016). A survey of national regulation in 2014 presented by Blundell-Wignall (2014) indicated that some countries such as China had banned the use of Bitcoin, and others, including Germany, France, Thailand and South Korea, had repudiated its use as currency.

In one paper on the ways to prevent and respond to new forms of transnational crimes, published around the time of the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice in 2015, increasing payments through anonymous virtual coins is considered a mechanism for financing terrorist groups, as well as a way to incite online violence. The report also points out that new anonymity technologies on the internet may encourage more individuals to engage in criminal activity, given the difficulties in identifying and enforcing laws on those committing such crimes. Virtual currencies may also act as a new *modus operandi* for transnational crime (United Nations, 2015a).

In the same way, the IMF (2016) points out that risks such as money laundering, terrorist financing and tax evasion may be associated with the technological anonymity, which may even pose risks concerning consumer protection and financial stability if the volume of transactions increases considerably, besides issues related to capital movement regulation. In addition, for the IMF, blockchain technology would be less worrying than virtual currencies because it can be used in closed systems managed and regulated by financial institutions.

At the UN Congress, emphasis was placed on the need to strengthen partnerships between law enforcement authorities and researchers to develop techniques that could allow for investigating and characterizing transactions in virtual currencies. The member countries of the UN were advised that research techniques on the use of virtual money laundering currencies, among other internet crimes such as financial fraud and online drug trafficking, should be shared in order to develop the necessary skills for authorities in combating such crimes (United Nations, 2015b).

According to the United Nations Office on Drugs and Crime (2016), there are some investigative challenges involving virtual currencies. For instance, the difficulty in enforcing laws on users due to their anonymity, not only because it is difficult to identify and to detect potential criminals, but also because there are only a few tools and techniques currently available to investigate the actions involving such currencies; not to mention that any evidence of crimes executed using these currencies will be electronic, which still has weak forms of investigation and rule enforcement. For the UN agency, public and institutional awareness, harmonization of legal issues, and cooperation between agencies are measures that should be taken.

Some options adopted involve applying regulations to participants in this market or to institutions, such as banks, in order to restrict their interaction with the participants. At the international level, multiple agencies have promoted discussions on international cryptocurrencies, pointing out the risks and benefits associated with their use. They sought to identify areas of cooperation between states and institutions for regulation and supervision, as well as to develop technologies to deal with innovation and the sharing of successful experiences that may result in setting standards of investigation and legal processing (International Monetary Fund, 2016).

In 2013, the Financial Crimes Enforcement Network (FinCEN), linked to the US Treasury Department, issued a statement on the enforcement of regulations on users (those who have virtual currencies to buy goods and services), administrators (those who can put coins into and take coins out of circulation) and individuals who exchange virtual coins (those who aim to exchange virtual coins for real currencies), that is, people who create, obtain, distribute, exchange, accept or transmit this type of coins. For FinCEN, the virtual currency has no legal status in any jurisdiction (Financial Crimes Enforcement Network, 2013).

A report from the Economic Commission for Latin America and the Caribbean (ECLAC) in 2015 highlighted the risks and opportunities involving virtual currencies. The negative connotation that some associate with the criminal purposes of using such coins would make it less likely that governments and the public take advantage of the potential benefits of this technology. The report emphasizes the need for dialogue between technology creators and members of the state in order to develop laws and regulatory mechanisms, aiming to use systems based on virtual currencies to benefit society. If, on the one hand, virtual currencies facilitate illicit activities and cybercrimes, on the other hand, they solve the problem of double spending associated with the first forms of electronic currencies (e. g. *Digicash* and *Hashcash*). In order to avoid their use in criminal activities, transactions must be thoroughly investigated and systems for customer recognition must be developed so that anonymous transactions can be traced.

8 Concluding remarks

Private cryptocurrencies in general, and Bitcoin in particular, despite representing a major financial innovation, are unlikely to change the current monetary order based on state money and the banking system in the foreseeable future. Moreover, Bitcoin and other private cryptocurrencies price instability raises doubts about their future. Failures in the regulation of the infrastructure of transactions, as well as possible breaches of rules established by the Securities Commission Exchange of the United States, leads to less disclosure of cryptocurrencies, thus curbing widespread acceptance.

Furthermore, private cryptocurrencies tend to be managed by developer communities, which are not accountable to users. It is difficult to imagine a deregulated monetary order because control over money by states constitutes one of the fundamental pillars of state sovereignty and the hegemony of central countries in the contemporary international monetary and financial system.

In addition to the high volatility, the digital portfolios in which the bitcoins are kept can be the target of cyber-attacks, reducing the security of their possession and, consequently, undermining their potential to be used as a store of value as well as their attractiveness as means of payment. Indeed, these barriers tend to limit the capacity to expand the use of private cryptocurrencies – the degree of scalability already mentioned.

For enthusiasts of private cryptocurrencies, they have potential widespread use, especially as a means of payment, since they have no storage costs and have the advantage of being able to be digitally divided, as well as not requiring intermediaries for their exchanges (Blundell-Wignall, 2014). Nevertheless, in practice the use of these currencies as a means of payment is largely geared towards transactions in online markets, and their commercial use is of little relevance worldwide.

As discussed, even the IMF (2016) highlights the fact that these currencies do not fulfill the three functions of money. In addition to the high price volatility limiting their use as a store of value, the Fund highlights the restricted use as a means of payment, due to their limited acceptance, and the little evidence that they are used as a unit of account. They also cannot be deposited in banks, as is the case with national currencies, and their possession takes place through virtual portfolios, which do not present any guarantee of security to the deposits. These facts indicate that, despite the nomenclature, private cryptocurrencies cannot be considered money in the sense of fulfilling their three fundamental functions.

This paper shows that distributed ledger technologies, that made cryptocurrencies feasible and have led some to foresee a possible new deregulated and decentralized monetary order, have been incorporated and developed by large banks and central banks. In other words, major international banks and central banks have been actively positioned in this process and, thus, they strongly restrict the spaces for a new monetary order based on private cryptocurrencies without banks and central banks. These initiatives are being conducted to largely incorporate DLT in the present monetary order. This process can induce the banking system to carry out even more efficient operations, including financing in the interbank system.

A cryptographic-based monetary order suggests profound changes not only in the operations and behavior of banking systems, but also, and not least, in the management of money, credit, and interest rates. There is therefore a broad research agenda on the impacts of DLT technology on the functioning and regulation of modern financial systems, as well as on monetary policy.

References

ADRIAN, T. *Stablecoins, Central Bank digital currencies, and cross-border payments*: a new look at the International Monetary System. Remarks at the IMF-Swiss National Bank Conference, Zurich, May 2019.

ASSANGE, J.; APPELBAUM, J.; MULLER-MAGUHN, A.; ZIMMERMANN, J. *Cypherpunks*: freedom and the future of the internet. OR Books, 2012.

BECH, M.; GARRATT, R., Central bank cryptocurrencies. *BIS Quarterly Review*, p. 55-70, Sept. 2017.

BIS. *Central bank digital currencies*. Basel: BIS, 2018. Available at: www.bis.org. Accessed on: May 5, 2018.

BIS – Bank for International Settlements. G7 Working Group on Stablecoins. *Investigating the impact of global stablecoins*. Oct., 2019.

BLANC, J. Las monedas paralelas: evaluación y teorías del fenómeno. 1998. Available at: https://halshs.archives-ouvertes.fr/halshs-00111649. Accessed: Aug. 26, 2017.

BLOOMBERG. *Crypto survivors find a rare lifeline*. 2019. Available at: https://www.bloomberg.com/crypto. Accessed on: Mar. 31, 2019.

BLUNDELL-WIGNALL, A. *The Bitcoin question*: currency versus trust-less transfer technology. OECD Publishing, 2014. (OECD Working Papers on Finance, Insurance and Private Pensions, n. 37). Available at: http://dx.doi.org/10.1787/5jz2pwjd9t20-en. Accessed: May 22, 2017.

BRAZIL. Central Brank of. *Distributed ledger technical research*. Brasilia, DF, Aug. 2017.

CAMBRIDGE Centre for Alternative Finance. *Judge business school*. University of Cambridge. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013. Accessed: Jan. 23, 2019.

CASEY, M. J.; VIGNA, P. In blockchain we trust. *MIT Technology Review*, Apr. 9, 2018. Available at: https://www.technologyreview.com/s/610781/in-blockchain-we-trust/. Accessed: Jun. 10, 2018.

CEPAL – Comissão Econômica para a América Latina e o Caribe. *Report of the second expert group meeting on opportunities and risks associated with the advent of digital currency in the Caribbean*. 2015. Available at: http://repositorio.cepal.org/bitstream/handle/11362/38260/LCCARL461_en.pdf?sequence=1. Accessed: Aug. 26, 2017.

CHAPMAN, J.; GA RRATT, R.; HENDRY, S.; MCCORMACK, A.; MCMAHON, W. Project jasper: are distributed wholesale payment systems feasible yet? *Financial System*, 2017. Available at: https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf. Accessed: Oct. 22, 2018.

CHENG, E. *Jamie Dimon is betting big on the technology behind 'fraud' bitcoin*. 2017. Available at: https://www.cnbc.com/2017/10/16/jpmorgans-dimon-betting-on-blockchain-even-as-he-calls-bitcoin-stupid.html. Accessed: Oct. 20, 2017.

CLARK, J. The long road to bitcoin. In: NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. *Bitcoin and cryptocurrency technologies*: a comprehensive introduction. Princeton University Press, 2016. p. ix–xxvii.

CNBC MARKETS. There are now 17 million bitcoins in existence – only 4 million left to 'mine' 2018. Available at: https://www.cnbc.com/2018/04/26/there-are-now-17-million-bitcoins-in-existence--only-4-million-left-to-mine.html. Accessed: Oct. 21, 2018.

CREDIT SUISSE. *Blockchain 2.0.* Credit Suisse: Zurich. 2018. Available at: https://mail.google.com/mail/u/0/#inbox/163f0ef9d3bad6de?compose=163f11d32d413cd5&projector=1&messagePartId=0.1. Accessed: Jun. 11, 2018.

DE CONTI, B. M.; PRATES, D. M.; PLIHON, D. O sistema monetário internacional e seu caráter hierarquizado. In: CINTRA, M. A. M.; MARTINS, A. R. A. (Org.). *As transformações no sistema monetário internacional*. Brasília: IPEA, 2013.

FINANCIAL CRIMES ENFORCEMENT NETWORK. Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies. 2013. Available at: https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering. Accessed on: Sept. 19, 2017.

FINANCIAL INSTITUTIONS HUB. *Interview*: banking on the blockchain. 2017. Available at: http://financialinstitutions.bakermckenzie.com/2017/06/07/banking-on-the-blockchain/. Accessed: Sept. 5, 2017.

FUNKE, M. Ciab FEBRABAN apresenta testes com *blockchain. Revista Ciab FEBRABAN*, São Paulo, v. 69, p. 42-47, May/Jun. 2017.

HABER, Stuart; STORNETTA, W. Scott. How to time-stamp a digital document. In: Conference on the Theory and Application of Cryptography, p. 437-455, Aug. 1990. Springer, Berlin, Heidelberg.

HAYEK, F. [1976]. *Denationalisation of money: the argument refined*. An analysis of the theory and practice of concurrent currencies. 3rd ed. London: The Institute of Economic Affairs, 1990.

HONG KONG MONETARY AUTHORITY. *Whitepaper 2.0 on distributed ledger technology*. Oct. 25, 2017. Available at: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171025e1a1.pdf. Accessed: Jun. 9, 2018.

HORNBORG, A. *Global magic*: technologies of appropriation from Ancient Rome to Wall Street. Palgrave Macmillan US, 2016.

INTERNATIONAL MONETARY FUND. Virtual currencies and beyond: initial considerations. 2016. Available at: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf. Accessed: Aug. 26, 2017.

JPMORGAN. *Unlocking economic advantage with blockchain*: a guide for asset managers. New York: JPMorgan, 2017.

KEYNES, J. M. (1936). *A teoria geral do emprego, do juro e da moeda*. 3. ed. São Paulo: Nova Cultural, 1985. (Os Economistas).

LAKOMSKI-LAGUERRE, O.; DESMEDT, L. L'alternative monétaire Bitcoin: une perspective institutionnaliste. *Revue de la Régulation*, 18, 2 semestre/Autumn 2015: Contestations monétaires. Une économie politique de la monnaie.

LAMPORT, Leslie; SHOSTAK, Robert; PEASE, Marshall. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, v. 4, n. 3, p. 382-401.

LEE, L. New kids on the blockchain: how bitcoin's technology could reinvent the stock market hastings bus. *LJ*, v. 12, p. 81, 2015.

MILLS, D.; WANG, K.; MALONE, B.; RAVI, A.; MARQUARDT, J.; CHEN, C.; ANTON, B.; BREZINSKI, T.; FAHY, L.; LIAO, K.; KARGENIAN, V.; ELLITHORPE, M.; NG, W.; BAIRD, M. *Distributed ledger technology in payments, clearing, and settlement*. Washington: Board of Governors of the Federal Reserve System, 2016. (Finance and Economics Discussion Series, 2016-095). Available at: https://doi.org/10.17016/FEDS.2016.095. Accessed: Oct. 22, 2018.

MIT TECHNOLOGY REVIEW. Bitcoin is eating Quebec. 2018. Available at: https://www.technologyreview.com/s/610786/bitcoin-is-eating-quebec/. Accessed: Jun. 8, 2018.

MORRIS, C. R.; FERGUSON, C. H. How architecture wins technology wars. *Harvard Business Review*, v. 71, n. 2, p. 86-96, 1993.

NAKAMOTO, S. *Bitcoin*: a peer-to-peer electronic cash system. 2008. 9p. Available at: https://bitcoin.org/bitcoin.pdf. Accessed: May 22, 2017.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. *Bitcoin and cryptocurrency technologies*: a comprehensive introduction. Princeton University Press, 2016.

NEW YORK TIMES. As bitcoin bubble loses air, frauds and flaws rise to surface. 2017. Available at: https://www.nytimes.com/2018/02/05/technology/virtual-currency-regulation.html. Accessed: Jun. 8, 2018.

PRATES, D. M. As assimetrias do sistema monetário e financeiro internacional. *Revista de Economia Contemporânea*, Rio de Janeiro, v. 9, n. 2, p. 263-288, May/Aug. 2005.

R3. *Delivering blockchain technology to transform the way the world does business*. 2018. Available at: https://www.r3.com/wp-content/uploads/2018/09/US_18_R3_FS_v7.pdf. Accessed: Oct. 22, 2018.

RAUCHS, M., GLIDDEN, A., GORDON, B., PIETERS, G. C., RECANATINI, M., ROSTAND, F., ZHANG, B. Z. *Distributed ledger technology systems*: a conceptual framework. 2018.

STOPFORD, J. M. et al. *Rival states, rival firms*: competition for world market shares. Cambridge University Press, 1991.

STRATEGY&; PWC. *4th ICO / STO Report*: a strategic perspective. Mar. 2019. Available at: https://cryptovalley.swiss/wp-content/uploads/ch-20190308-strategyand-ico-sto-report-q1-2019.pdf Accessed: Mar. 31, 2019.

SUSAN, S. *Mad money*: when markets outgrow governments. Ann Arbor: The University of Michigan Press, 1998.

SZABO, N. *Smart contracts*. Unpublished manuscript. 1994. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Accessed: Dec. 21, 2018.

THE NEW YORK TIMES. *5 reasons cryptocurrency prices are plunging again*. Available at: https://www.nytimes.com/2018/11/21/technology/cryptocurrency-price-drop.html. Accessed: Dec. 1, 2018.

THE TELEGRAPH. *Bitcoin exchange collapses after second cyber attack in a year*. 2017. Available at: https://www.telegraph.co.uk/technology/2017/12/19/bitcoin-exchange-collapses-second-cyber-attack-year/. Accessed: Jun. 8, 2018.

UBS. *Building the trust engine*. 2016. Available at: https://www.ubs.com/magazines/news-for-banks/en/products-and-services/2016/building-the-trust-engine.html. Accessed: Sept. 5, 2017.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. *Anti-corruption alert*: laundering of crime proceeds using virtual currencies. 2016. Available at: http://www.unodc.org/documents/indonesia//publication/alert/POIDN_Alert_No._1_-_2016.pdf. Accessed: Aug. 26, 2017.

UNITED NATIONS. *Thirteenth United Nations Congress on Crime Prevention and Criminal Justice*: Working Paper – Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime. 2015a. Available at: https://www.unodc.org/documents/congress/Documentation/A-CONF.222-8/ACONF222_8_e_V1500538.pdf. Accessed: Aug. 26, 2017.

UNITED NATIONS. *Thirteenth United Nations Congress on Crime Prevention and Criminal Justice*: Background Paper – Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation. 2015b. Available at: https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_e_V1500663.pdf. Accessed: Aug. 26, 2017.

VALOR ECONÔMICO. *Seis grandes bancos internacionais aderem a projeto de moeda digital*. 2017. Available at: http://www.valor.com.br/financas/5103260/seis-grandes-bancos-internacionais-aderem-projeto-de-moeda-digital. Accessed: Sept. 5, 2017.

VALOR ECONÔMICO. *Bitcoin segue em queda e fica abaixo de US$ 4 mil*. 2018a. Available at: https://www.valor.com.br/financas/6000649/bitcoin-segue-em-queda-e-fica-abaixo-de-us-4-mil. Accessed: Dec. 1, 2018.

VALOR ECONÔMICO. *Criptomoedas sofrem desvalorização em 2018*. 2018b Available at: https://www.valor.com.br/empresas/6006483/criptomoedas-sofrem-desvalorizacao-em-2018. Accessed: Mar. 20, 2019.

WALPORT, M. *Distributed ledger technology*: beyond blockchain. UK Government Office for Science, 2016. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Accessed: Dec. 1, 2018.

WRAY, R. State money. *International Journal of Political Economy*, v. 32, n. 3, Fall 2002.

WORLD ECONOMIC FORUM. *The future of financial infrastructure*. Cologny, Suiça: Future of Financial Services Series, 2016.

YERMACK, D. *Is bitcoin a real currency?* An economic appraisal. Massachusetts: National Bureau of Economic Research, 2014. 24p. Available at: http://www.nber.org/papers/w19747. Accessed: May 22, 2017.

YERMACK, D. Corporate governance and blockchains. *Review of Finance*, v. 21, n. 1, p. 7-31, 2017.