Citação: (CARVALHO et al., 2021)

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

Referência bibliográfica: CARVALHO, C. E. et al. Cryptocurrencies: technology, initiatives of banks and central banks, and regulatory challenges. **Economia e Sociedade**, v. 30, n. 2, p. 467–496, jul. 2021.

Fichamento

|  |  |  |
| --- | --- | --- |
| Pagina | Texto | Comentário |
| 2 | “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.  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. |  |
| 4 - 5 | 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 neometalist 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 years1 . In all these cases, private currencies were created with limited uses and goals, in terms of time and economic space involved. |  |
| 5 | 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.  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: |  |
| 6 | 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.  This means that there must be consensus among users and other actors for the system to function. This layer is composed of a protocol governance2 , 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. |  |
| 12 | 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).  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) |  |
| 13 | 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 connections10 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.**  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. |  |
| 14 - 15 | 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.  The common 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 daily15); and iv) a high concentration of Bitcoin in just a few negotiators, which makes its price very sensitive to their strategies16; 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 activity17; and vi) cooling of the speculative euphoria based on the so-called greaterfool theory18 (Blundell-Wignall, 2014). |  |
| 16 - 17 | 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 contracts19 functionality to create a secure environment for off-network transactions, that is, an interface system20. 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).  Struggling to overcome limiting aspects of blockchain technologies and DLT systems, coordinated actions between financial institutions and government agencies have sought to 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-ofstake (PoS) constituted as a ‘consensus mechanism’ that, instead of requiring the resolution of energyintensive 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). |  |
| 17 | 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).  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 hashing21, 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). |  |
| 18 | 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 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). |  |
| 19 | 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) |  |
| 20 | 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).  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 midOctober 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) |  |
| 21 - 22 | 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.  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 |  |
| 22 | 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. |  |
| 23 | 7 Challenges for regulation  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).  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). |  |