

The cash paradox of regulated digital currency and private digital currency

المفارقات النقدية بين العملة الرقمية المنظمة والعملية الرقمية الخاصة

SIAMER Hadjira *, Mouloud MAMMERI University (Algeria)

BOUBAKEUR Mustapha, Akli MOHAND OULHADJ University (Algeria),

Received: 20/03/2024 ; **Revised:** 21/06/2024 ; **Accepted:** 30/06/2024

Abstract

The traditional schema of money or the interest rate balances the demand for stable money and the supply of money fixe by the central Bank no longer sense in the modern financial and economic system characterized by monetary dematerialization giving birth of a Currency managed electronically using information and communication technology , without a physical support the latter was designed by the monetary authorities both too reduce the costs of use and monetary transactions and to satisfy customers by giving them the possibility of managing their portfolio and carrying out transactions from their home, but with the notion of the market economy based on the words of ADAM SMITH « let him pass let him happen » private initiatives in monetary creation have emerged to escape the legal monetary constraint which weighs heavily on economic agents and this how bitcoin emerged as the first private currency not backed by any financial institution , culling into question the sovereignty of monetary authorities.

Keywords: Banking information; information communication technology; private currency; digital currency; cryptocurrency.

Jel Classification Codes : XNN ; XNN

I. Introduction :

In a financial institutions assure the role of trusted third parties for financial transactions (payment , exchange of financial securities ...) they also accompany economic agent in their financing operations (operation with abroad) therefore a false step of these institutions can generate mistrust and panic and therefore banking information and transferred in a secure , confidential and organized way, and for this purpose that banks have introduced the use of information and communication technologies in their various operations including the creation of electronically managed means of payment . they also have the ability to restrict certain participants 'access to the financial system.

After 2009, payment systems were marked by the juxtaposition of virtual and legal currencies, circulating in two dichotomic networks, one free and the other strictly regulated. This incidental phenomenon raises conceptual questions about the fundamentals of the legitimacy of cryptocurrencies, institutional questions on the place and role of regulators, and, finally, the future of sovereign currencies and the means of payment supported by them. These observations highlight the complexity of this new event as well as the challenges posed to the monetary authorities, which have the role of controlling the money supply and safeguarding the sustainability of conventional currencies.

This phenomenon proved real during the 2008 financial crisis, which has challenged the reliability of the banking system, leaving room. indeed, in this article, we try to answer the

* SIAMER Hadjira

following question: what is the difference between paying transaction with the regulated digital currency and private digital currency?

1- The legal (monetary) electronic currency: concept of bases

1-1- Introductions of information and communication technologies in the banking sector

New information and communication technologies are a set of technical knowledge and processes relating to the processing and communication of information.

Information and communication technologies are at least part of the solution to major societal challenges, such as improving the quality of life through access and exchange of information.

And these technological advances now enable information to be exchanged over long distances, they also enable data to be stored and retrieved, thereby making communication cheaper since digitization was originally driven by the search for reducing transaction costs. In fact, these digital technologies and IP (Internet Protocol) allow to promote new economic models such as electronic payment that has gained social acceptance and partially abandon the currency in traditional forms. Knowing that the creators of these new forms of money relied on advertising as a means of massaging the individual. Since economic or technological conditions impose certain sociological structures, but the individual was in close agreement with them and the form of society correctly expressed the psychology of man considered individually. Now this no longer seems to be true, man becomes a mass man, because he cannot remain long in disagreement with his environment.

1-2- Definition

Monetics is a new and sophisticated form of dematerialized currency that ensures cost reduction by giving priority to IT management and the use of advances in telecommunications, improving the security system and reducing the risk of failure while speeding up the execution times of transactions.

Monetics has experienced unprecedented development from the introduction of sophisticated payment systems to the generalization of micro-computer management and the emergence of home banking. As well as cryptology and the advancement of micro circuit cards offer new perspectives to the monetary industry by ensuring unquestionable security and reducing the risk of fraud.

This coin with symbolic wealth finds its consecration today based on the trust and credibility of the user. Adherence to this system of monetary deprivation is based on strict and rigorous criteria.

1-3-specific factors that determine electronic payment methods

The issue of the adoption by users of new electronic systems based on card technology has generated abundant literature to determine how users of the new form of money are convinced of its value.

The theoretical underpinnings mobilized were to respond to this, based mainly on the theory of innovation or the argument of the double effect of networks.

The issue of the adoption by users of new electronic systems based on card technology has generated abundant literature to determine how users of the new form of money are convinced of its value.

The theoretical underpinnings mobilized were to respond to this, based mainly on the theory of innovation or the argument of the double effect of networks.

1-3-1- the theory of innovation:

The most prominent stylized fact relating to the use of new products or new technologies indicates that the spread of innovation is typically a S curve. The literature has often studied the conditions that give rise to this curve, looking at the processes of ICT dissemination in

companies on the one hand; and on the other hand, the process of disseminating information or innovation among individuals.

In the end, employee satisfaction can significantly influence acceptance and use of new means of payment. In other words, the higher the satisfaction, the easier it will be to adopt it in the future.

1-3-2- the theory of double effect:

The introduction of each new payment instrument is subject to the effects of network externalities. Small and medium-sized enterprises (e-wallet) are characterized by a double networking effect as they depend on their use by others (users and traders).

2- The monetary mass and the monetary system

As a result of what has been said, the developed systems and electronic money are therefore only means of exchange whose media are completely dematerialized, and therefore a third mutation of the fiduciary currency.

The kinematics of payment flows via electronic payment systems does not differ from traditional banking script systems, because in the first instance the user orders the manager of his account (by means of paper or plastic media), to proceed with the payment of his debt. And in a second time, the manager releases his client from the debt by a play of writing in the account.

Thus, the electronic currency is primarily designed as a substitute for the scriptural currency. (for small transaction values). And if we refer to the exchange equation of the quantitative theory of money, these technological innovations will obviously not be without consequences on the amount of currency in circulation, inasmuch as an authorization of payment procedures will allow for better management of monetary units (increasing the transaction capacity of the currency) if the money is destined to finance more than to consume.

3- Emergence of decentralized private currency

3-1- 2008 financial crisis: first step towards the emergence of blockchain

The 2008 financial crisis triggered in the United States has been brutal, its main cause is the securitization of toxic goods, this technique consists of converting low-liquid assets into tradable assets at the financial market level, it is a technique that is very useful economically because it allows to restructure the company's balance sheet while generating funds by reselling its assets, but in the U.S. banks have been strongly encouraged to issue more possible credit including real estate loans that are granted to non-solvent individuals, then they have been securitized(special purpose) enjoying a very good rating from the rating agencies both by lack of transparency and by the complexity of the underlying products.

After first affecting financial assets and producing a fall in stock prices across developed economies, it then spread to the real economy, having a negative impact on all economic variables and then quickly on the entire world's economies. Apart from its economic and social repercussions of large payment systems. This is the emergence of monetary forms of a peculiarity, called cryptocurrencies or virtual currencies. These currencies have the peculiarity of being detached from the institutional and regulatory framework decreed by public authorities. They exchange directly from pair to pair via the Internet, without which they are by nature contrary to the foundations of the legal currency. Cryptocurrencies are not issued by a central bank or private financial institutions. The exchange system is based on a protocol of cryptographic processes, defining the terms of transactions of participants. The principle is based on a double-key cryptography, one that resembles a mail account allowing access to an exchange platform, and the other private equivalent to a bank account number, promoting end-to-end authentication and security of transaction data.

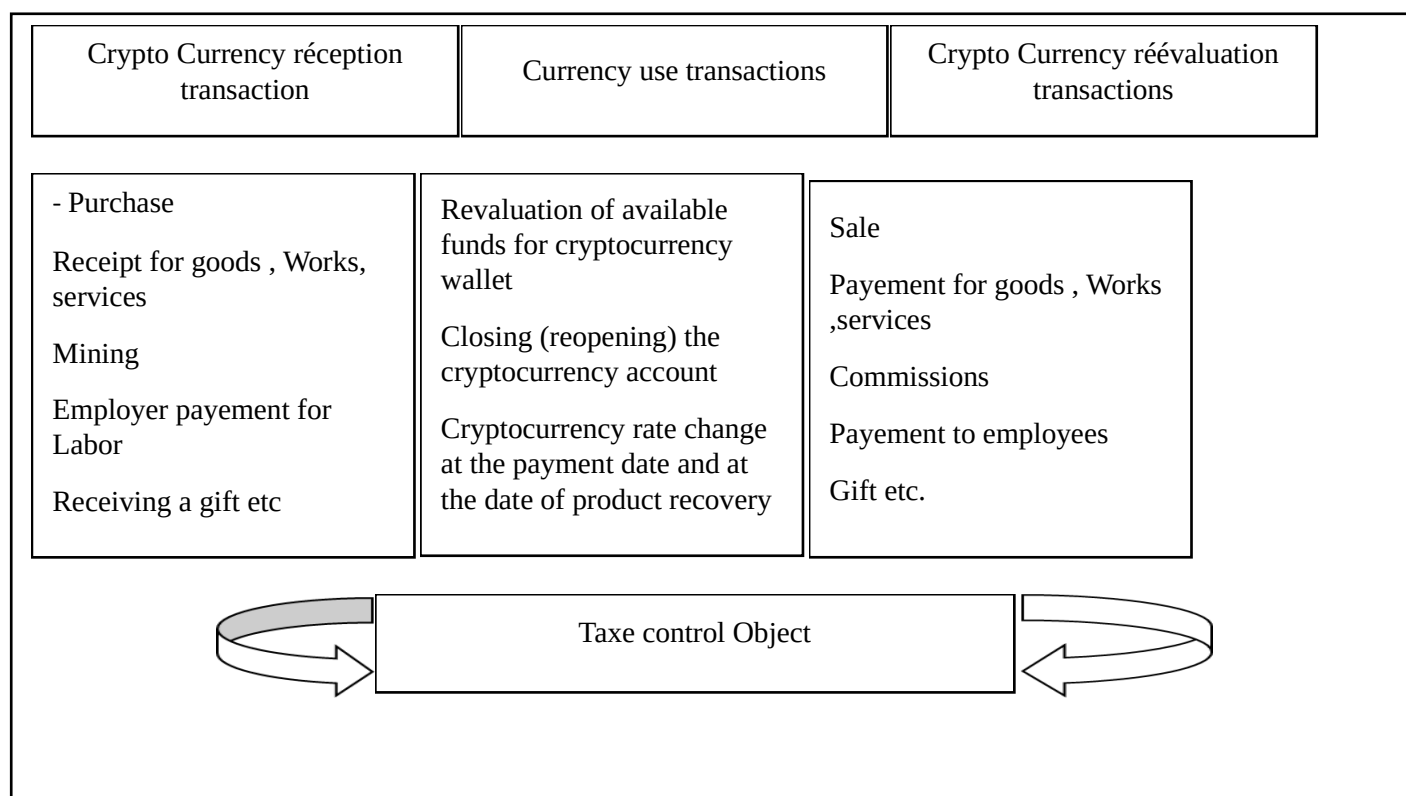
This technology therefore appears in the context of the financial crisis and more of the cry of confidence in the states, the bank, also put in the currency. Initially, the money in all its forms, be it scriptural or fiduciary, has the first quality of trust. This trust, coming from the Latin fiducia is meaning "fiduciary", therefore has the role of making the currency accepted between the economic agents. It is at this moment of loss of confidence of economic agents in the currency that the idea of a virtual currency is formalized, the bitcoin that has the ambition to become a currency equivalent to the euro using blockchain technology, which would represent a new paradigm of trust.

3-2- Definition of Blockchain

The blockchain is a set of blocks protected from any modification, each block contains the identification of its predecessor, it can take the shape of a tree with several branches, the longest of these branches called the main branch is identified by the identity of its terminal block. from this identification it is possible to go back to this main branch to the original block "genesis" and thus to find all the transactions re-registered since.

The blockchain allows to create inviolable digital assets and complete the dematerialization and disintermediation of evidence of traceability transactions or even account units.

Fig number 1: groups of cryptocurrency transactions



4-1- Appearance of bitcoin

The first use of blockchain appeared in 2009 with the introduction of a cryptocurrency called bitcoin. For the first time, an article signed under the pseudonym STOSHI Nakamoto offers a protocol to record electronic transactions in a decentralized, secure and transparent way, making it impossible to double spend bitcoins.

Bitcoin and other active crypto rely on blockchain technology, concretely blockchain users issue encrypted messages that are gathered in blocks of data linked together, each block has its unique cryptographic signature which depends on the information it contains and the signature of the block that precedes it which allows to locate it in the blockchain. the entire chain thus constitutes a secure database containing the history of all exchanges for a given crypto asset since the creation of the chain. The blockchain operates according to a validation

protocol, since the computing power required to record transactions increases as the network grows.

Different kinds of blockchain have developed it is distinguished by the degree of openness of the network. The size of the added blocks, the nature and transparency of the information disseminated, the methods used to reach consensus and validate transactions, the modes of consultation of the registry, the modes of governance to update the protocol.

Each blockchain works with a virtual currency also called crypto currency , transactions are grouped by block so that each block is validated by the nodes of the blockchain network also called miners . The validation by these nodes results in the resolution of a computer algorithm for the protocol poor of work, once each transaction verified the block is also

4-2- Bitcoin Management

Contrary to the naive idea that one could make of a virtual currency, a bitcoin does not have a wallet in the form of a file or folder, instead it accesses a registry that is a public account ledger. Recording all transactions in bitcoin taking place since the implementation of the protocol it is from this register that he can calculate his personal fortune.

At any time, everyone can know how many bitcoins there are on each existing account, and participate in the verification of new transactions, while respecting the anonymity of minors who are not required to declare themselves, therefore it is only by the coherence and the general and unanimous agreement of those who participate and agree on the content of each account that nothing materializes it, and that no authority guarantees. It is therefore necessary that the cryptographic software construction ensures by itself that no one can increase the total of bitcoins held, nor modify accounts without everyone discovering it in a very short time. It has no police, the very design of the currency must prevent fraud and malfunction, it is managed collectively under the intervention of the cryptographic program which contains two keys:

A public key that can be circulated (this is the account number) And a private key that must absolutely remain secret (this is the password to access the movement of accounts) which constitutes a series of numbers and letters difficult to remember indeed some minors prefer to manage the account using a «wallet» software. and if one of the two keys is accidentally erased; then its contents will be permanently lost, and if another person knows these keys, he can use them because the identity of minors is not useful at any time, it is therefore necessary that the cryptographic software construction ensures by itself that no one can increase or modify the total of bitcoins holding the very design of the currency must prevent only the fraud and malfunctions.

5- the usefulness of blockchain

The novelty brought by the bitcoin system was to be operate a secure blockchain system in a completely decentralized manner, this means that there is not, as in the conventional system , a central entity(such as central bank for example) which plays the role of trusted third party in other words bitcoin is designed to digitized trust by developing in place of the third very strong protection systems to guarantee the authenticity of the originators (that is , the holder of an active crypto is legitimate) and the integrity of the transactions(it is not possible to modify a recorded transaction).

In systems like bitcoin, it is technology associated with the validation of transactions by a majority of users themselves that constitutes the security of the chain, as a reward for their validation work (mining process), so-called miners get bitcoins. The fact that it is decentralized means that it is largely resistant to potential attacks and stop attempts.it is not located in a single server, if part of the system is down after a cyber-attack for example, other transactions can continue their progress.

Transaction fees for buying and transferring cryptocurrency through the blockchain are minimal, as there is no intermediary in the cryptocurrency transaction process between two

individuals, the transaction costs are then reduced housing compared to those found in a conventional transaction in legal tender.

Bitcoin is part of an innovation strategy for products, services and payment systems offered by a company, for example creatines digital entertainment companies use bitcoin as a means of transaction for online shopping.

The value of cryptocurrencies is known to be specifically very volatile, we have seen among other things in the period of April 2019 and June 2019 bitcoin went a value of 4825 dollars to 13054 dollars, so in the space of two months its value has almost tripled, it could be for some industries a big disadvantage, but for some industries especially travel it is a very advantageous marketing tool this allows dynamic prices offered based on the value of bitcoin.

6- Bitcoin versus e-money

Electronic money is generally defined as a value stored in electronic form issued after receipt of funds in the amount must not be less than the value of the issued currency unit accepted as a means of payment by third parties other than the issuer. in the framework of an electronic money program, the link between electronic money and the fiat money on which it is remains intact, and funds are expressed in units of that currency.

In a virtual currency program, however, that unit of account has no counterpart in fiat currency apart from the format, there is little similarity between bitcoin and electronic money. Electronic money like money other digital forms of fiat money like credit and debit cards, in order to mitigate systemic and consumer protection risks, a cash amount corresponding to the value of the e-money issued must be deposited with a financial institution subject to prudential rules. unlike bitcoin, electronic money is not a new currency and it is under the supervision of the same central authority as underlying national currency.

7- Banking intermediation and blockchain

7-1- development of the banking business in the age of digitalization

Banks are generally presented as financial institutions that collect deposits from the public and provide loans to households and businesses.

Such a definition, if it is, does not however sufficiently reflect the great diversity and the real complexity of banking operations, particularly in the era blockchain, which are ultimately not well known to the general public even a large public has bank account.

Banks are indeed major plyers in an economy, they play a leading role financing the economy and therefore in growth and job creation: bank loans support household housing and consumption projects and banks support the development of businesses by financing them through credit.

In addition, to enhance the savings of their customer's, banks offer a wide variety of liquid or blocked products with guaranteed or unsecured returns; they also provide that a network of agencies and distributors and a range of means of payment that contribute greatly to facilitating daily exchanges between economic agents.

7-2- impact of blockchain on the banking business

let us think about the influence of blockchain on payment methods and specifically on international financial asset transfers .a transfer of assets or value has always been a long and costly process so two concepts must be taken into account : time and money , when we talk about asset transfer or value we are talking about international transfers , a cross-border money transfer via a bank takes several days while the use of cryptocurrency would make it possible to obtain an almost instantaneous transfer, it is also important to remember that bank commissions now represent the largest share in the distribution of their net banking income (GNP), the intermediation margin losing ground against low rates . these diversified commissions come from international transfer fees.

If we talk about the cost of a money transfer by cryptocurrency or online bank using the blockchain and well this one is weaker and transparent this notable difference is observed in particular in the transfers outside the zone, calls in particular SWIFT (society for worldwide interbank financial telecommunication).

The issue of transfers through a physical bank includes initial fees and exchange fees, a world bank study (2018) shows that cost of an international transfer between individuals would be around 11% of its amount, far from 3% targeted by the UN, while those of an online provider would approach 2,6%

8-limitations of using blockchain

The use of this technology revolutionizing the concept of trust still raises various questions, relating to social and environmental responsibility, the legal scope of the term or the protection of users 'data.

8-1- limit of use : beyond a certain threshold the slow processing of transactions and number of transactions processed make it inefficient , moreover the blockchain is not inviolable , in theory the fact that transactions are controlled by majority of users guarantees its reliability , in practice certain configurations that depend on the technological choices chosen, a mechanism of collusion between users can lead to a takeover : the transactions to be validated can then be chosen or the history modified , moreover , sometimes the creators of the system commit coding errors that make blockchains vulnerable .

8-2- environmental limits: today we live in a world sensitive to the environmental consequences of our activities. So, what about blockchain technology? This technology poses a major energy problem, particularly with regard to public blockchains, including Bitcoin. Its distributed operation via computers capable of performing powerful mathematical calculations consumes a lot of energy, which grows according to the size of the blockchain, and therefore over time. Thus, proof of work mining can find its limits in its environmental impact. However, it is necessary to relativize and not forget that not all public blockchains work on a system identical to that of Bitcoin, and that some are much less energy consuming. Alternative means of mining have developed, such as the Proof of Stake, in other words the "proof of stake", which no longer relies on the amount of work provided, but on the amount of cryptocurrency owned by the minters (equivalent to "miners"), which will then require less energy consumption. In addition, a validation system inspired by the Proof of Stake has developed to perfect the classic proof of stake; it is the Delegated Proof of Stake in other words "the delegated proof of stake". This consensus system consists in fact in setting up a voting system by which users designate representatives to validate their blocks.

8-3- Dependency Limits: The concept of mining by the Proof of Work shows once again a weakness; that related to the dependence of users on miners. It should be noted that China has the main mining centers grouped within miners' cooperatives or "pool" of miners commonly known as Antopol, BTC.com or F2pool. This concentration of mining pools is justified by the low cost of electricity. Today this concentration of Chinese pool is estimated at more than 50% of the mining rate.

8-4- Legal Limitations: Blockchain goes beyond the usual legal categories and escapes all boundaries. The first legal issue arises when we look at user liability. Indeed, the decentralized governance mode of a public blockchain is problematic in the sense that it becomes difficult to identify a single responsible in this technology where transactions are exposed publicly, accessible to all and where no central authority exists. Secondly, when the blockchain processes personal data, the technology seems to ask compatibility questions about the rights imposed by the General Regulation on the Protection of Personal Data (GDPR) whose purpose is to protect the privacy and data of users. Indeed, two types of personal data can be identified within a blockchain:

Identification of participants and minors via their public key to identify the issuer and receiver of a transaction. - Data entered in transactions with public visibility. The immutable feature of the blockchain therefore conflicts with users' rights, including the right to be forgotten. The right to digital oblivion is a concept practiced by the Court of Justice of the European Union (CJEU) since 2014 in the judgment of Google Spain. It consists of a right given to citizens of the European Union to request the erasure of the results of searches on their private data from

a search engine. This right aims to protect the privacy of users. The blockchain does not allow to delete illegal information without the majority of the network is in agreement, raises concerns about this right. One can then wonder how the right to be forgotten online could be extended, in addition to search engines, to the blockchain. Today, the NCITF (National commission for information technology and free domes) has addressed the issue in a 2018 report, and distinguishes between two elements to apply the GDPR: personal data and the controller. We have seen that identifying the responsible person can be a difficult task since the GDPR requires designating a natural or legal person. However, the blockchain operates in a decentralized way without an administrator, where even the identity of the creator under the nickname of Satoshi Nakamoto, is not known. The CNIL therefore notes that any person who has a writing right on the channel and decides to submit the transaction to minors can be considered responsible. (CNIL report, 2018)

8-5- Limits of Anonymity: Widely presented as an advantage, the anonymity of users of public blockchains is debated. Indeed, this feature is problematic when the blockchain is misused, and is not favorable to the fight against money laundering.

8-6- Technical Competency Limitations: Because of its disruptive nature, blockchain moves away from usual practices and requires specific skills. The general public could therefore have difficulty adapting, but also understanding its usefulness due to its complexity. Because of the recency of this technology, we also face a lack of technical skills on the part of companies.

II. Conclusion:

In the economies of developing countries, money is an element of exchange, of accumulation of values, possessing money serves primarily to acquire a certain number of goods, some of which are vital or the external sign of social advancement. The abundance of money directly promotes consumption. So, the change from money to electronic form makes it difficult to control the latter since it is intended for exchange without carrying out a positive action on the gross national product. This will have a negative impact on the circulation tension of the currency. In contrast, in the economies of developed countries, basic needs are met. Money supply appears as much as capital to make profit as as means of exchange, the problems of investment become as important as that posed by consumption which leads to an increase in the gross national product, so the currency's circulation coefficient is high.

Because of this strength of the real economy in developed countries its latest leave more to private initiative to create wealth thus using blockchain technology to make payment and exchanges .indeed after its use of blockchain in early 2009, a large number of sectors and uses may be disrupted by blockchain , but have seen that the latter allows various applications in the banking industry such as asset transfer, the use of this technology as registry can act as threat an opportunity .indeed its application in the payment field to give rise to virtual currency that is not backed by any financial institution, as a result , banks are faced with competition , which forces them to optimize certain processes and create new jobs.

Bitcoin want to be a universal currency , it has this power of conversion to all currencies; like the dollar and the euro without being controlled by the state , which weakens sovereignty and can be weakened or destroyed , the unanimity that bitcoin has engendered can disintegrate and the conflicts it managed to silence can be reborn; is then questioned the claim to money to be radically different from financial assets and secular commodities , a difference that underpins his authority .it must compete with partial currencies that claim to want to replace it like bitcoin.

Hover this technology still shows a low impact due to its nascent stage of development and whose regulation needs to be adjusted, even if some features of the blockchain can be promising, its application to banking activities involving the processing of large financial flows will require significant technical and regulatory challenges to be addressed.

Referrals and references:

Books

- Philippe HERLIN, la révolution du bitcoin et des monnaies complémentaires, édition Eyrolles 2013 ;
- ZOLLINGER Lamarque, e-marketing et stratégie de la banque ; DUNOD, paris 1999.
- Zunayr, MIKDASHI ; les banques à l'ère de la mondialisation, éd Economica, paris 1998.
- JEAN-PAUL Delahaye ; le bitcoin, première crypto-monnaie ; bulletin de la société informatique de France, number4, october2014, pp67-104.

Web sites

- Anna KRAMARARENHO, <http://doi.org/10.1051/Shsconf/20196706031>
- Martin VRGACKA , basic aspects of cryptocurrencies , issn: 1339-3723, volume 2 , issue 2, 2014 ,available on : [http://www.reseaurchgate.net / publication /292586903](http://www.reseaurchgate.net/publication/292586903).
- World Bank ECA Economics UDPATE, cryptocurrencies and Blockchain, office of the chief economist, May 2018, available on: www.worldbank.org.