CRYPTOCURRENCIES. TECHNICAL AND FUNCTIONAL ASPECTS

Professor Ph.D. Marius GUST
"Constantin Brâncoveanu" University of Pitești, Romania
E-mail: mariusgust@yahoo.com

Abstract: *Nearly a decade after the appearance of cryptocurrencies, they have grown, both in number and in market, being a reality of our day, and in the last year the media has constantly written about them. Yet they continue to be a mystery. Normal, on the one hand, because not all of us are computer scientists, many are just computer users, but few are the ones who are good at cryptography. Unfortunately, so too few of the founders and users of cryptocurrencies are good at the economy. Maybe that's why they exaggerate when they call their crypto "coins" creations. These creations are not and probably will not be coin for a long time. Cryptocurrency there is something that few are good at, but many want it, because it brings them some wealth. Cryptocurrency and their evolution in the past year have enriched their founders and, being unregulated, we should count the days until we are impoverished. Cryptocurrencies have emerged and developed as a result of a sense of frustration among many who believe that people in the leadership of states and authorities live on their backs, banks steal them, states discriminate against them, judges and lawyers are not right. It is the world of the Internet, the world where people are free and have no bosses and no laws. Cryptocurrencies also mean many personal pride, but also the right to opinion and a social democracy. Or maybe anarchy. How could we justify more than 1500 such assets in less than 10 years.*

Keywords: *bitcoin, litecoin, riiple, ethereum.*
JEL Classification: *G12.*

1. Introduction

Bitcoin was launched in early 2009, the first cryptocurrency, which, for some, meant a real revolution in the system of payments, but also of speculative investments, and for others, another incomprehensible thing that added more and more technology to everyday life. At the same time, the authorities' responses to the new "currency" have gone from indifference, caution to investors and the unseen public, and recently to some bans, sporadic in relation to the dynamics of the phenomenon. I believe that bitcoin, and all that followed, can be seen from two different points of view: on the one hand, the bitcoin and the other so-called cryptocurrencies, another variety of assets offered to the market, and on the other hand the technology itself, the blockchain, which stands behind them.

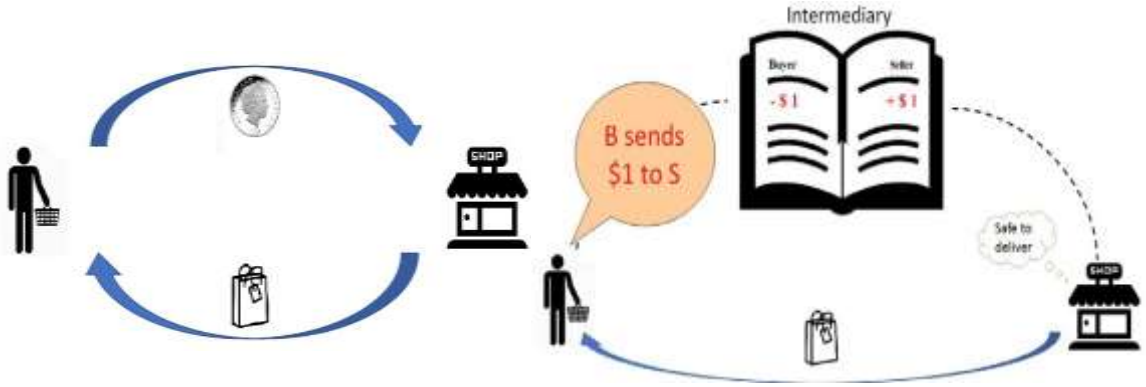
2. Blockchain technology

To understand blockchain technology, we compare the traditional payment system, and payments that involve the use of blockchain technology (Chiu and Koeppl, 2017).

For more than a few thousand years, physical assets (e.g. shells, gold, coins, banknotes) have been used as a means of payment. In this context, a direct exchange of goods between the seller and the buyer is settled by counterparty's delivery of the money-giving asset (e.g. shells, gold, coins, banknotes) (Figure no. 1.a). This option is unavailable when the two parties are not present in the same location (for example, in the case of e-commerce), requiring the use of other assets (such as digital ones) to conclude the transaction. In a digital monetary system, the means of payment is simply a string of bits. The issue is preventing the buyer from reusing the same bit string again for a new transaction. This is called "the problem of double-spending". This problem can easily be solved when there is a trusted third party (for example, a traditional bank, or PayPal for electronic payments) that manages a centralized account and transfers balances by crediting the seller's account and debiting the buyer's account (Figure no. 1.b). For the system to work, it is necessary that the public trust banks or Paypal, and that these do not

cheat.

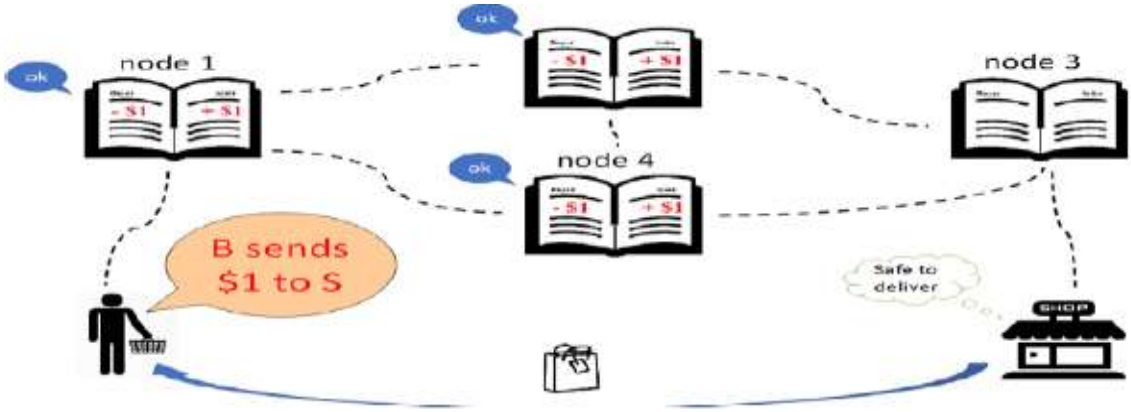
Figure no. 1. Direct payment (a) and payment intermediated by a third party (b)



Source: Chiu, J. and Koeppl, T., 2017. *The Economics of Cryptocurrencies. Bitcoin and Beyond.* Bank of Canada, Victoria University of Wellington, Queen's University.

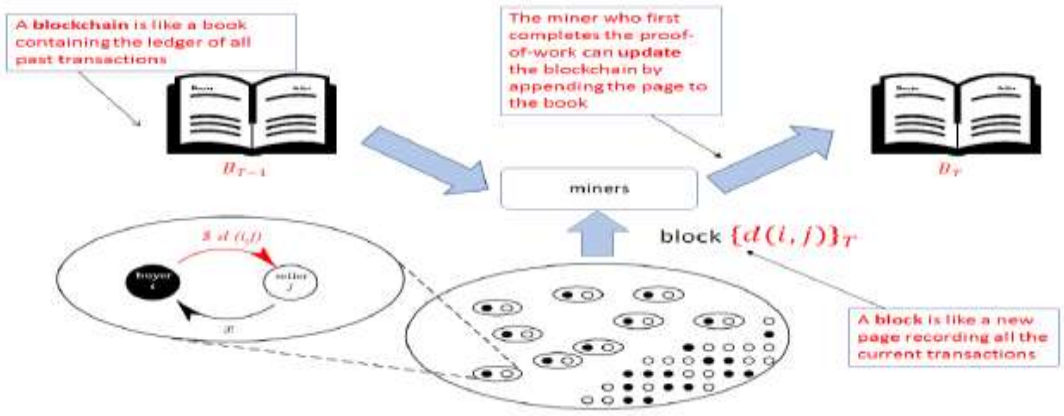
But if users do not trust the intermediary, the third party, because of its behavior, because of the fact that it favors some to the detriment of others, an abusive behavior due to the imposition of high costs etc.? A perfectly feasible solution is that the log, in which all transactions are recorded, of all participants, regardless of whether they are part of the transaction or not, is decentralized, held by all/to appear on the computers of all members of the network (Figure no. 2, where nodes are network participants/network computers).

Figure no. 2. Payment in which the log is kept by all members of the network



Source: Chiu, J. and Koeppl, T., 2017. *The Economics of Cryptocurrencies. Bitcoin and Beyond.* Bank of Canada, Victoria University of Wellington, Queen's University.

Figure no. 3. Validation of Transactions/Mining Process

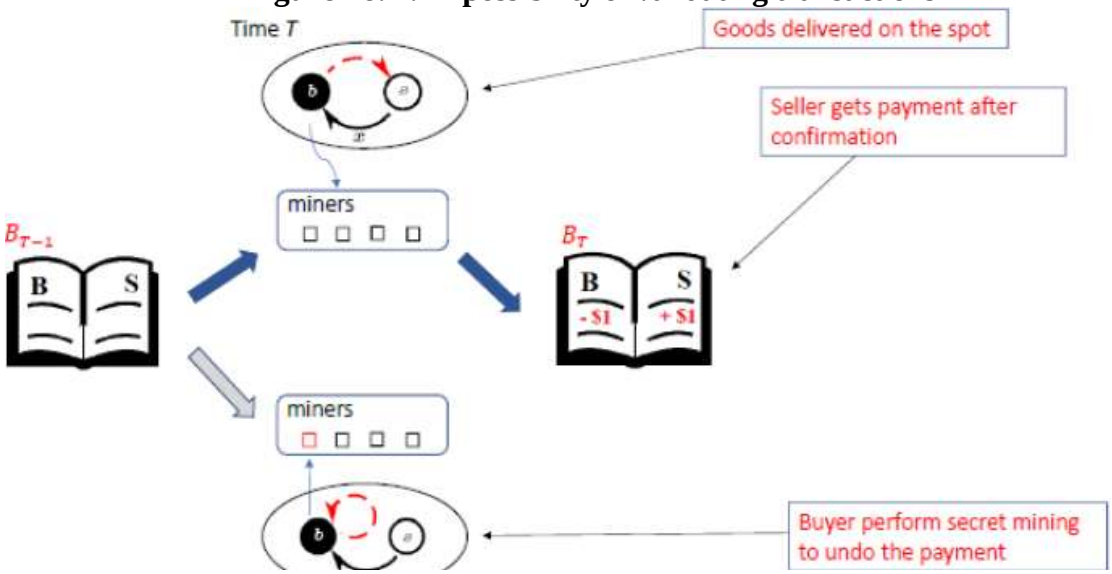


Source: Chiu, J. and Koeppl, T., 2017. *The Economics of Cryptocurrencies. Bitcoin and Beyond.* Bank of Canada, Victoria University of Wellington, Queen's University.

So blockchain technology is a distributed network in which the third party, the trusted person, is absent. Validation of transactions, a process called mining, is performed by network members, miners (who are transaction validators) who compete to solve a costly computational problem (the term used is proof-of-work) and enter this transaction into a new block presenting the current account balances of participants in that network. The winning miner - the one who validates the transaction as soon as possible - receives a reward for their work, consisting of, on the one hand, the creation of new cryptocurrency issued by the network mined, and on the other hand, a transaction fee (Figure no. 3).

Blockchain is therefore a chain formed from all blocks that contain the history of previous transactions, and allow the formation of a public log whose records contain the user's balance.

Figure no. 4. Impossibility of validating transactions



Source: Chiu, J. and Koeppl, T., 2017. *The Economics of Cryptocurrencies. Bitcoin and Beyond.* Bank of Canada, Victoria University of Wellington, Queen's University.

If a user wishes to cancel a past transaction (in fact, to use the same asset previously used for a new payment), this is impossible because: (a) the validation of transactions will not be done by him, but by the other miners , (b) would require rewriting a previous block,

over which other blocks have been placed (it is virtually impossible to enter the block archive, and even if it were, all subsequent blocks would also have to be rewritten, resulting in costly transaction fees that would make the process undesirable) (c) all rewards granted to miners for the validation of past transactions, and cryptocurrencies already produced, would have to be cancelled (Figure no. 4).

Blockchain, also called the "new internet", operates on a peer-to-peer basis. In IT terms, peer-to-peer means a direct connection between computers in the same network, transmitting information to each other without the need for a server computer to manage the exchange of information between them. Also, often the software behind the blockchain is open source, it can be downloaded and used for free, and can be further improved by users.

This makes blockchain technology suitable for recording events, medical records, managing people's identities, processing transactions, documenting the provenance of goods and services, tracking the food trade route, or even polling systems.

Currently, the term "blockchain 2.0" is used, which refers to the new applications of distributed (block) databases. "Blockchain 2.0" technologies outperform transactions, and allow value exchanges, without powerful intermediaries acting as "money and information referees". “Blockchain 2.0” technologies are expected to allow "excluded people to enter the global economy, to protect the privacy of participants," allow people to "generate money from their own information," and provide "the ability to ensure creators are rewarded for their intellectual property". It is also said that "blockchain 2.0" technologies make it possible to preserve a digital identity and provide a way to help solve the problem of social inequality through "the potential change in the way wealth is distributed" (Follow My Vote, 2017).

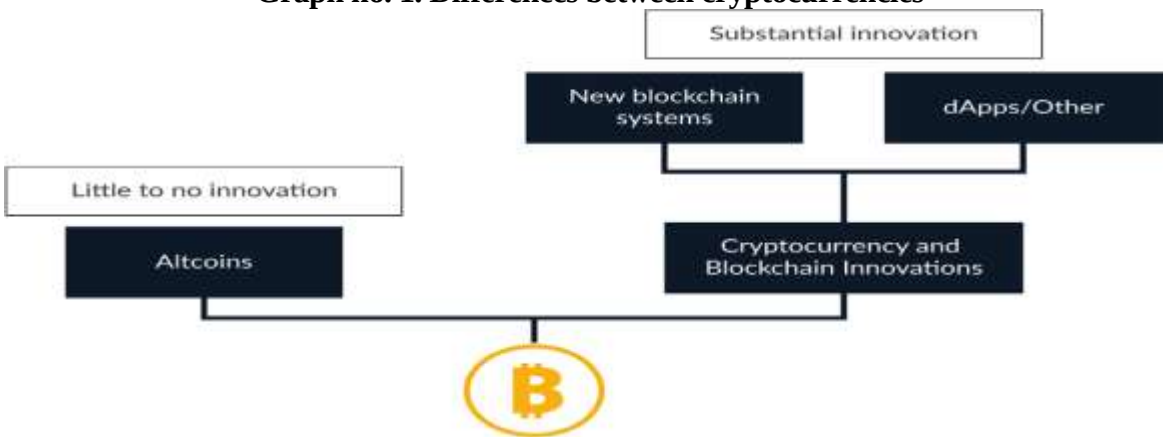
3. Cryptocurrencies

Cryptocurrencies are the result of a combination of achievements in various sciences, such as networking, peer-to-peer, cryptography (hash functions, digital signatures) and economics (game theory).

Cryptocurrency is a digital asset/token that exists in a specific cryptographic system and which generally consists of a P2P network, a consensus/trust mechanism, and a public and private key infrastructure. There is no central authority to govern the system. Instead, all network participants (also known as "nodes") apply the rules governing the system (for example, defining what constitutes a valid transaction, providing the asset/token and its issuance scheme, etc.).

The entire history of all transactions can be verified independently from each node, because everyone has a copy of the log, which is shared. This common log, which is generally based on a chain of transaction blocks ("blockchain"), is constantly updated through a process called "mining", which creates new blocks for new transactions, but new units of the native digital asset/token (i.e. cryptocurrencies) as well, which rewards the participants who validate the transactions. Everyone is free to join and leave the system at any time, and there are no nominal identities attached to the users, but cryptographic identities.

Graph no. 1. Differences between cryptocurrencies



Source: Hileman, G. and Rauchs, M., 2017. *Global Cryptocurrency Benchmarking Study*. Cambridge: University of Cambridge, Judge Business School, The Cambridge Centre for Alternative Finance.

Bitcoin (BTC) began operating in January 2009, and was the first cryptocurrency. The second cryptocurrency was namecoin, appearing two years later, in April 2011. Today there are about a thousand cryptocurrencies, which are traded and grow their market value daily. Common to most cryptocurrencies is the public log ("blockchain"), which is shared between the network participants, and the digital native asset/token (i.e. cryptocurrency) as a way to stimulate participants to run the network without a central authority. However, there are significant differences between cryptocurrencies in the displayed innovation level (Graph no. 1).

Most cryptocurrencies are bitcoin clones or, in the case of others, the difference refers to parameter values (e.g., different block time, currency offer, and issuance scheme). All these cryptocurrencies, because they do not show too much innovation, are called "altcoins" (Hileman and Rauchs, 2017).

From a theoretical point of view, ground zero of the birth of Bitcoin was the publishing, at the end of 2008, of the work of Satoshi Nakamoto "Bitcoin: an electronic cashless peer-to-peer", but Bitcoin was born in January 2009.

The paper suggested creating a "peer-to-peer" or "P2P" network ("system") using a form of online cash ("electronic") that does not require a financial intermediary. The proposal envisaged a form of private currency, which would have been different from national currencies, but which would have similar characteristics and, moreover, would have brought with it the benefits of anonymity for payer and beneficiary and their private lives. Satoshi Nakamoto proposed that the new currency be based on cryptographic evidence instead of a trusted third party, such as a central bank or other institution, to verify transactions. Confidence and transaction validation would be achieved through a public report (blocks) that would track and record all transactions that all members of the system could read and confirm.

Economists and other specialists studying this new category of coins have proposed different denominations for them (Schuhy and Shyz, 2016):

- The European Central Bank, in 2012, proposed the term "**virtual currency**";
- The Bank for International Settlements, in a 2015 report, used the term "**digital money**", having found **similarities** with **"electronic" currency**;
- A more accurate term appears to be the **cryptographic coin** for this type of currency, based on the reality of the cryptographic security underlying it, but

not all new virtual or digital coins are based on cryptography;

- The ECB's classification in 2012 was interesting, highlighting the unregulated nature of the new currencies, in relation to national currencies that are regulated, although many of the new currencies have internal rules regulating their creation;
- Additionally, it should be kept in mind that **national currencies are public**, whereas **these new currencies are private**, being used only in their own networks;
- Finally, consider the **sovereignty of national currencies**, and the **consensual, social, private, decentralized, democratic character of the new currencies**.

Since every coin should have at least three utilities: a means of exchange, a standard value, and a treasury function, my opinion is that the "currency" should not be used to refer to these new creations. Their exchange is rare, too few people and too few transactions are being made with these new currencies for them to be considered a means of exchange (even those who declare that they accept them in payment, use them sporadically, and those who own them use them for speculation rather than exchange). Nor can it be said say that the new currencies are of standard value, given that prices are expressed in national currencies, and then converted into the new currencies (nor would it be a reliable solution to the volatility observed by "pseudo-currencies" lately). Perhaps the treasury function is better represented, but let us not forget that we are talking about minorities. Based on this last point, I believe that the term virtual or cryptoactive asset would better describe them, especially given that in many countries the supervisors focused on them have been the ones regulating the securities markets.

4. Creation of cryptocurrencies

A person can become the owner of cryptocurrency either by participating in their creation, a process that is called mining, or following a transaction/investment process.

Mining is the process through which new cryptocurrency is created, though it should be noted that not all cryptocurrencies are minable. In fact, mining is the process of validating new transactions, i.e. transferring encrypted data from one person to another by creating new blocks containing new transactions, and finally adding that new block to the blockchain (the public log where all transactions with that cryptocurrency are saved). When the miner's computer validates a new block, that computer and therefore its owner will receive a quantity of encryption. For example, in the case of bitcoin, the validation of a new block will provide the miner with 12.5 BTC, after it was halved in 2016 (until then the operation yielded 25 BTC; this remuneration, in the case of bitcoin, but not only, was reduced over time, with a decrease of 0.5 approximately every four years).

The issue of mining (Bitcoin, 2017) is a computer and cryptographic issue. During mining, the computer performs a cryptographic function called hash (for example, for bitcoin, two rounds of an encryption algorithm called SHA256 are executed), on what is called a block header. For each new hash, the mining software will use a different number as the block header's random number, and this number is called nonce. Depending on nonce and what information remains in the block, the cryptographic function will produce a hash (a code, a cipher), which is a string of digits and letters that look like this:

821de96a53a9a93ef6f358fbb998c60802496863052290d4c63735b7fe5bdaac

It is a hexadecimal number, i.e. letters A-F are numbers 10-15. To make mining difficult, there is something called the difficulty target. To create a valid block, the miner must find a code that is below the difficulty target. So if, for example, the target of difficulty is:

10000000000000000000000000000000000000000000000000000000000000000
then any number starting with zero, would be below target, for example:
0787a6fd6e0782f7f8058fbef45f5c17fe89086ad4e78a1520d06505acb4522f
If the difficulty target is reduced to:
01000000000000000000000000000000000000000000000000000000000000000
Then two zeroes are required to begin with in order to be below target:
00db27957bd0ba06a5af9e6c81226d74312a7028cf9a08fa125e49f15cae4979

Because the target is difficult, involving a lot of numbers, a simpler number is used to express the goal, a number called mining difficulty. Mining difficulty expresses how difficult the current block is to be generated, in comparison to the first block created. So a 50000 difficulty means that the current block that needs to be validated requires 50000 times more work than the creator of the cryptocurrency when creating the first block. For example, in the case of bitcoin, the difficulty changes once to 2016 blocks (2016 blocks, in the case of bitcoin, at the current processing power of the network, take about 14 days). From that moment on, the difficulty of mining increases. That's why mining cryptocurrency is getting harder and, as we have seen earlier, paying less.

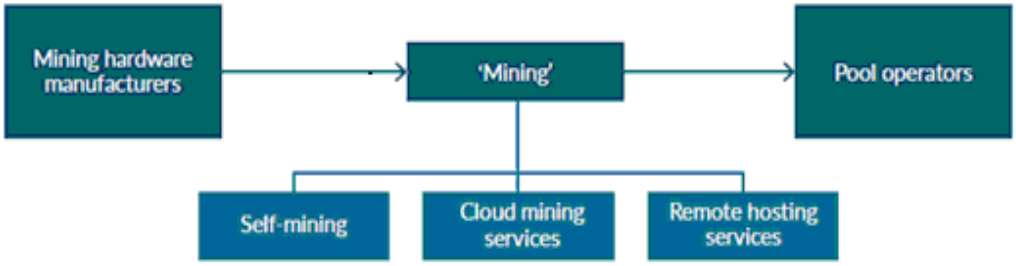
In regards to mining hardware, chronologically, the following have been used:

- central processing units (CPU). These, used at the dawn of cryptocurrencies, are no longer considered up to date; very slow in relation to the current mining difficulty, they would require years to yield a single cryptocurrency unit;
- graphics processing units (GPU). These could be connected in parallel, thus increasing the mining power several times over, at reduced energy consumption;
- field-programmable gate arrays (FPGAs). Although these machines did not boost the mining speed, as was the case with GPUs, they came with the advantage of energy efficiency and ease of use;
- application specific integrated circuits (ASICs) that are built to perform a single task. That is, an ASIC designed to only mine bitcoins will do just that and nothing else. Although ASICs seem particularly rigid in use, they compensate by increasing the hash power (encryption) a hundredfold, while also reducing power consumption.

Additionally, software is required for mining. It can either be installed on the computer, or a browser-based mining software can be used (without being installed on the mining computer). As far as mining technique is concerned, Graph no. 2, gives a complete picture of the different methods.

There are many mining opportunities, such as: mining factories, mining pools, cloud mining, mining through a remote hosting service, mining on one's own. Currently, the most efficient mining methods are mining factories and mining pools (in a common pool, a kind of cooperative where the earnings are divided among members according to certain criteria) because of the high power necessary for encryption, and high costs in terms of both technical equipment and power consumption. In addition, the size of the blockchain is growing steadily. For example, in the case of bitcoin, in August 2014, the blockchain file size, which contains records of all transactions that occurred on the network, reached 20 GB (gigabytes), in January 2015 the size increased to nearly 30 GB, and, between January 2016 and January 2017, the bit block has grown from 50 GB to 100 GB in size. Personal computers would have no place to store so much information.

Graph no. 2. Types of mining



Source: Garrick Hileman, Michel Rauchs, Global Cryptocurrency Benchmarking Study, University of Cambridge, Judge Business School, The Cambridge Centre for Alternative Finance, 2017.

In the second case, of a transaction, a person may come to possess cryptocurrency either by accepting it as a means of payment in selling a good or service, or by investing/speculating the price variations of cryptocurrency (in fact, by buying it), though the various websites that promote cryptocurrencies also indicate other ways (performing various tasks for sites that accept or promote, lend, receive salary in cryptocurrencies etc.).

Regardless of its source – be it mining or transactions/investments - it is necessary for the owner to have a wallet in which to store them. So, acquiring a wallet precedes cryptocurrency ownership.

Cryptocurrency wallets contain not the coin units, but private keys required to access the address where these are found, and to sign transactions when cryptocurrency is spent. Cryptocurrency wallets are available in the following forms:

- Desktop wallets (in fact, software installed on the computer; some secured, some even anonymous);
- Mobile wallets (a smartphone app). A difference between desktop and mobile wallets is that, while the former can contain the entire blockchain, the latter contain only a small part of the blockchain, relying instead on other nodes in the cryptocurrency's network;
- Web wallets store online private keys on a server connected to the internet and controlled by someone else, the advantage being that they can be accessed anywhere, but are also at risk;
- Hardware wallets are specially designed to keep electronic keys and facilitate payments;
- Off-line wallets (software not connected to the Internet);
- Paper wallets (enable the transformation of private keys into QR codes, that can be printed and stored outside of a computer).

5. Public and private keys

Cryptocurrency transactions and ownership rely on two elements: the public key/address and the private key/address, sometimes called the key pair. These two keys are actually two strings of characters, the public key being generated by the private key. When someone makes a cryptocurrency transaction, they will generate the key pair; the public key is the one that will appear in the blockchain (Figure no. 5), viewable by any member of the network, and the private key, generated at the same time as the public one, intended for the recipient of the cryptocurrency to be able to access/use cryptocurrency. Anyone can send cryptocurrency to the public key/address, but that amount can only be accessed by the owner of the private key, generated at the time of the cryptocurrency's handover. Disclosure of the private key is synonymous with the loss of one's cryptocurrency.

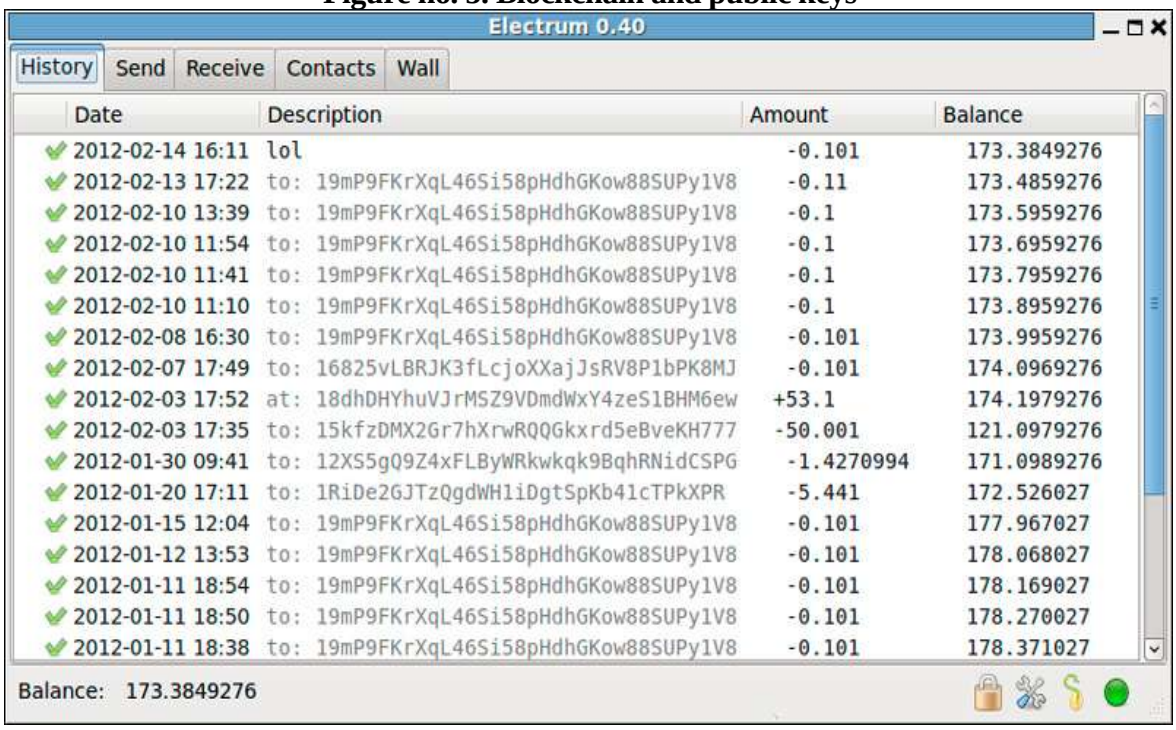
Cryptographers propose that private key generation be made using either a random character set that cannot be guessed, or an easy to memorize authentication phrase.

In fact, when someone, a payer, sends cryptocurrency to its beneficiary, the payer will use the private key to sign a payment message, which contains the payer information, the payment amount (in bitcoin, the source of transactions whose value is used for payment) , and the address of the beneficiary. The payment message will leave the payee's cryptocurrency wallet to the network that manages the cryptocurrency. From there, network miners check the transaction by placing it in a transaction block and, eventually, validating/decrypting it to place it in the blockchain. The recipient will have to wait until the miners decrypt (validate) the transaction. For example, in case of bitcoin, each block takes 10 minutes to mine. So if the payment is the extinction of a purchase of goods or services, the payee seller lets you wait until the block in which the transaction was placed is validated by the miners.

But it's possible that some vendors - cryptocurrency recipients do not wait for the transaction's validation, trusting that you will not attempt to spend the same cryptocurrency elsewhere before the transaction is confirmed (in the case of low-value payments).

It is noteworthy that the difference between some cryptocurrencies lies in their bookkeeping. In bitcoins, everyone's balance is unknown. Owned bitcoins are transaction parts, not balances, as in other cryptocurrencies. So, when making a bitcoin payment, the transactions from which the payment amount is due must be chosen, and the value of these transactions cannot be shared. This means that enough transactions will be made to cover the amount of the payment. If the previous transaction, from which the payment amount is due, is higher than the latter, the payer will make two payments, the normal one to the beneficiary, and the remainder to himself.

Figure no. 5. Blockchain and public keys



Source: Bitcoin, 2017. *Home*. [online] Available at: < https://bitcoinx.ro/> [Accessed 18 December 2017].

Any part of a transaction that is not taken over by the recipient or returned as change is considered a commission. It goes to the miner who was able to validate/decrypt the

transaction block as an extra reward, in addition to the cryptocurrency creation. Miners opt for high-value transactions, because rewards are high.

6. Other cryptocurrencies

So far, the example used has been the bitcoin. However, the cryptocurrency market currently has nearly 1,000 such currencies. Considering the volume of cryptocurrency transactions in 2017, bitcoin, ethereum, ripple and liteco come out on top, treated as different cryptocurrencies and excluding bifurcations.

Litcoin (LTC) is a bitcoin fork, created in 2011 (three years after bitcoin), that has double the value of bitcoin (25LTC / block), but which, like bitcoin, is halved every four years, the time per block is 2.5 minutes (one quarter of bitcoin's), a maximum of litcoins four times the number of bitcoins (84 million units), and a different encryption system.

Ripple (XRP). The Ripple company, which founded this cryptocurrency, originally a real-time remittances and exchange system, decided in 2012 to also issue an account unit like cryptocurrencies which, besides financial transactions, also sought to introduce tokens. It should be noted that the system is decentralized and can operate without the parent company, and among its validators is the Massachusetts Institute of Technology. The Ripple network allows transactions in both conventional currencies (which is why it is accepted by a number of financial institutions, which have themselves integrated the network into their own internal systems) and in its unit of account, ripple. The system is slightly different from networks that emit bitcoin or other cryptocurrencies, because the two-party transactions are based on trust. Users must specify which other users they trust and with what quantity. Thus, when a non-XRP payment is made between two users who have mutual trust, the credit line balance is adjusted within the limits set by each user. To send money between users who have not established a trust relationship directly, the system tries to find a path between the two users through others in the system so that each link is between two users who have a trust relationship. The resulting balances along the path between the two users without a relationship are then simultaneously adjusted to "atomic". This payment mechanism through a trustworthy network of participants is called "rippling". The network accepts currency deposits from users, records the balances from the transfers in the Ripple distributed registry, and redeems account balances when withdrawing deposits. Users need to place trust in the Ripple network. This creation of trust-based lines indicates to the Ripple that the user is "trustworthy". In addition, the user must also set a quantitative limit on this confidence level and create a similar limit for each coin they put on the network.

Ripple is based on a shared registry, which is a distributed database that stores information on all Ripple accounts. It is managed by a network of independent validation servers that regularly compare transaction logs. Servers can belong to anyone, including banks. A new registry is created every few seconds, and the last closed registry is a perfect record of all Ripple accounts as determined by the server network. A transaction can be any modification proposed in the registry, and can be entered by any server in the network. The servers are trying to reach a consensus on the transactions to be included in the registry, creating a new "last closed registry". The consensus process that validates the new registry is distributed; the goal of the consensus is for each server to include the same set of transactions in the current registry. Servers are constantly receiving transactions on the network, and their validation is agreed upon by a "super-majority" of network participants. If "super-majority" is not in consensus, "this means that the volume of transactions was too high or the latency of the network too high for the consensus process to produce consistent proposals,"and the nodes retry the consensus process. Each round of consensus reduces disagreement until "super-majority" is achieved. The intentional result of this process is

that the disputed transactions are removed from the proposals, while widely accepted transactions are included in the registries/blocks.

The Ripple cryptocurrency cannot be mined, and at its genesis, 100 billion XRPs were created. Of these, 20 billion were retained by the creators (the founders of Ripple Labs), about 80% of the total were intended to stimulate market creation activity, to increase Ripple liquidity and to strengthen the overall health of Ripple markets, while a sum of 0.2% of the total Ripple was awarded to charitable organizations. The system introduces up to 1 billion Ripple to the market on a monthly basis for various projects. Another feature is that, in order to engage in transactions, each Ripple account must have a small margin of 20 XRP, and pays a trading fee, which increases if the user performs numerous transactions.

Table no. 1. Comparison between major cryptocurrencies

Cryptocurrency	Bitcoins	Litecoin	Ripples	Ether/ Ethereum
Type	Blockchain, Cryptocurrency	Blockchain, Cryptocurrency	Real-time gross settlement, currency exchange, remittance	Decentralized computing, Blockchain, Cryptocurrency
Symbol	BTC, XBT	LTC	XRP	ETH
Subunits				
$1/_{1000}$	millibitcoin	lites		
$1/_{1000000}$	bit	photons		Gwei (10^-9)
$1/_{100000000}$	satoshi	litoshis		Wei (10^-18)
Original creator	Satoshi Nakamoto	Charlie Lee	Arthur Britto, David Schwartz, Ryan Fugger	Vitalik Buterin, Mihai Alisie, Anthony Di Iorio, and Charles Hoskinson
Launch date	9 January 2009	7 October 2011	2012	30 July 2015
Remuneration graph	Proof-of-work	Proof-of-work		Proof-of-work
Encryption function	SHA-256	scrypt		Keccak
Programming language		C++	C++	Go, C++, Rust
Operating system		Windows, OS X, Linux, Android	GNU/Linux (RHEL, CentOS, Ubuntu), Windows, OS X	Linux, Windows, macOS, POSIX, Raspbian
Remuneration per block	12,5 BTC	25 LTC		3 ETH
Creation time per block	10 minut	2,5 minut		14-15 seconde
Units in circulation	16.858.762	55.558.418	39.009.215.838	97.762.514
Unit creation limit	21.000.000	84.000.000	100.000.000.000	

Ethereum is a distributed open-source, public, block-based platform that also emits an Ethereum/Ether cryptocurrency. Ether, like bitcoin, is mined and can be transferred between accounts and used to reward the participating mining nodes to validate transactions. Ethereum was proposed at the end of 2013 and was launched on July 30, 2015, with 11.9 million pre-emptive currencies. In 2016, due to the collapse of the DAO project (the disappearance of $50 million, contributions to a smart contract), Ethereum was divided into two separate blocks - the new separate version became Ethereum (ETH), and the original continued as Ethereum Classic.

Ethereum/Ether is different from Bitcoin in several aspects:

- it operates using accounts and balances in a way called "state" transactions. The State is the current balance of all accounts and is not stored on the block, but on a separate tree called "Merkle Patricia Tree". Ether accounts are pseudonyms because they are not linked to individuals but rather to one or more specific addresses;
- block time is 14-15 seconds, compared to bitcoins' 10 minutes;
- mining Ether generates new cryptocurrency at a usually consistent rate (3 ETH/block), whereas bitcoin production rate is halved every 4 years;
- transaction fees vary according to complexity, which is calculated according to used bandwidth and storage needs (in a system known as GAS), while for

bitcoin transactions, tax is competitive and determined by transaction size measured in bytes;

- Ethereum GAS units each have a price that can be specified in a transaction, and are usually measured in Gwei (an Ethereum subdivision equal to 10^9), while Bitcoin's operations are taxed in Satoshis per byte;
- transaction fees are generally considerably lower for ether than bitcoin. For example, in December 2017, the transaction fee for ether was $0.33, while bitcoin ranged from $1 to $55;
- Ethereum uses an account system where transactions in Wei (another Ethereum subdivision equal to 10^18) are debited in some accounts and credited to others, unlike the BitTorrent UTXO system, which records the transactions, the amounts spent and the amounts received, respectively (money transfer and reception of a benefit or good in exchange).

The cryptocurrencies market currently has about 1,000 such coins, and the most important one, depending on the US dollar capitalization, is shown in Table no. 2.

Table no. 2. Top 50 cryptocurrencies following March 7, 2018 market cap

	Name	Symbol	Cap (mil. USD)	Price (USD)		Name	Symbol	Cap (mil. USD)	Price (USD)
1	Bitcoin	BTC	166.644	9.857,2	26	BitShares	BTS	458	0,2
2	Ethereum	ETH	72.715	741,7	27	Decred	DCR	429	62,2
3	Ripple	XRP	33.657	0,9	28	Komodo	KMD	353	3,4
4	Bitcoin Cash	BCH	18.384	1.081,1	29	Electroneum	ETN	349	0,1
5	Litecoin	LTC	10.078	181,5	30	Ardor	ARDR	343	0,3
6	Cardano	ADA	6.380	0,2	31	Ark	ARK	335	3,3
7	NEO	NEO	6.269	96,5	32	Syscoin	SYS	304	0,6
8	Stellar	XLM	5.795	0,3	33	Cryptonex	CNX	301	6,7
9	Monero	XMR	5.187	328,3	34	Hshare	HSR	283	6,6
10	Dash	DASH	4.049	510,4	35	PIVX	PIVX	276	5,0
11	IOTA	MIOTA	4.041	1,5	36	DigiByte	DGB	271	0,0
12	NEM	XEM	2.633	0,3	37	MonaCoin	MONA	257	4,4
13	Ethereum Classic	ETC	2.160	21,5	38	Byteball	GBYTE	237	366,6
14	Qtum	QTUM	1.597	21,6	39	Factom	FCT	236	27,0
15	Lisk	LSK	1.552	15,1	40	Particl	PART	228	25,7
16	Bitcoin Gold	BTG	1.533	90,9	41	ReddCoin	RDD	198	0,0
17	Nano	NANO	1.527	11,5	42	GXShares	GXS	195	3,3
18	Zcash	ZEC	1.174	342,3	43	ZCoin	XZC	185	43,3
19	Steem	STEEM	685	2,7	44	Nexus	NXS	183	3,3
20	Bytecoin	BCN	647	0,0	45	Blocknet	BLOCK	176	34,9
21	Stratis	STRAT	617	6,2	46	Nxt	NXT	174	0,2
22	Verge	XVG	610	0,0	47	Neblio	NEBL	163	12,7
23	Waves	WAVES	584	5,8	48	Emercoin	EMC	154	3,7
24	Siacoin	SC	496	0,0	49	SmartCash	SMART	132	0,2
25	Dogecoin	DOGE	470	0,0	50	Vertcoin	VTC	130	3,0

Source: CoinMarketCap, 2017. *Home*. [online] Available at: <https://coinmarketcap.com> [Accessed 18 December 2017].

Table no. 2 shows the market situation on March 7, 2017. Note that although we only list 50 of the approximately 1,000 cryptocurrencies, the fiftieth currency has a capitalization of $130 million. But the market is a diverse one; investors can find almost anything on the market. Any idea can find its equal on the cryptocurrency market. Here's a demonstration in Table no. 3.

An important problem is the bifurcation frequency of the original cryptocurrencies, due not only to attempts to improve technical problems in use or disunity in the distribution mode

(the original creators possessing important encrypted portfolios, while the last entrants need to be content with crumbs, or paying high prices for placements), but also the personal pride of miners or users, who are trying to find new free winning tracks. For example, in the case of bitcoin, there were 17 coins with the name of bitcoin, excluding the 15 listed in 2017, but only three seemed to be more important. For litcoin, we count 8 varieties, none of which are important. In Ethereum, the bifurcations were lower, with only three varieties, and Ripple did not record any bifurcation, probably because of the different system.

Table no. 3. Cryptocurrency – curiosity on March 7, 2017

Position	Name	Symbol	Market Cap (mil. USD)	Price (USD)
173	PinkCoin	PINK	9,66	0,025295
194	EuropeCoin	ERC	6,71	0,66967
215	CannabisCoin	CANN	4,88	0,063164
316	PetroDollar	XPD	1,33	0,020821
333	Deutsche eMark	DEM	1,03	0,029113
352	Happycoin	HPC	0,72	0,052164
356	TrumpCoin	TRUMP	0,70	0,105857
386	MACRON	MCRN	0,45	0,00112
389	Phantomx	PNX	0,42	0,027344
405	Philosopher Stones	PHS	0,32	0,053671
408	Mao Zedong	MAO	0,30	0,047903
431	Honey	HONEY	0,20	0,444662
433	Eurocoin	EUC	0,19	0,015282
435	Theresa May Coin	MAY	0,18	0,005277
478	HarmonyCoin	HMC	0,00	0,006701
636	Marijuanacoin	MAR	0,11	0,065598
710	PizzaCoin	PIZZA	0,00	0,002053
762	LePen	LEPEN	nn	0,000391
834	KlondikeCoin	KDC	nn	0,018575
840	CoffeeCoin	CFC	nn	0,002542
842	Happy Creator Coin	HCC	nn	0,000098
844	Halloween Coin	HALLO	nn	0,000293
866	GAY Money	GAY	nn	0,029035
888	SportsCoin	SPORT	nn	0,001466

Source: CoinMarketCap, 2017. *Home*. [online] Available at: <https://coinmarketcap.com> [Accessed 18 December 2017].

Table no. 4. Bitcoin, litcoin and ethereum bifurcations before 2017

Position	Name	Market cap (mil. $)	Price ($)	Position	Name	Market cap (mil. $)	Price ($)
1	Bitcoin	166.643,7	9.857,19	2	Ethereum	72.714,8	741,66
4	Bitcoin Cash	18.384,4	1.081,12	13	Ethereum Classic	2.159,7	21,52
16	Bitcoin Gold	1.533,4	90,91	414	Ethereum Dark	0,3	0,19
53	BitcoinDark	118,1	91,63				
183	BitcoinZ	8,2	0,01				
195	Bitcoin Plus	6,7	63,01				
332	Bitcoin Scrypt	1,0	0,06	5	Litecoin	10.078,5	181,51
412	Bitcoin Fast	0,3	0,03	270	LiteDoge	2,7	0,00
529	BTCtalkcoin	0,6	0,01	370	Litecoin Plus	0,5	0,46
593	Bitcoin 21	0,2	0,24	432	LiteBitcoin	0,2	0,01
600	Bitcoin Planet	0,2	0,03	458	LiteCoin Ultra	0,1	0,07
629	AntiBitcoin	0,1	0,01	645	Litecred	0,1	0,00
716	Bitcoin Diamond	?	4,70	700	Antilitecoin	0,0	0,00
722	BitcoinX	?	0,01	732	Litecoin Cash	?	0,48
729	Super Bitcoin	?	15,13				
777	Bitcoin God	?	30,45				
782	Bitcoin Atom	?	13,89				

Source: CoinMarketCap, 2017. *Home*. [online] Available at: <https://coinmarketcap.com> [Accessed 18 December 2017].

7. Initial coin offerings

Now, in the years of cryptocurrencies, even start-ups are revising their funding techniques. Thus, some start-ups no longer resort to venture capital, crowdfunding, business angels, and instead access blockchain technology and so-called smart contracts.

Initial coin offerings (ICO) and initial token offerings (ITO), named after initial public offering (IPO), are one of the methods through which start-ups found financing using the blockchain and cryptocurrencies.

If, through an IPO, a company issues, in a legal and regulated manner, securities to investors via ICO or ITO, a start-up issues to investors, using blockchain technology, virtual assets (called digital tokens) or the start-up's proprietary cryptocurrency and receives cryptocurrency from investors, especially ether or, more rarely, bitcoin. It should be noted that in an ICO, new virtual assets (digital tokens) are premeditated (their number is known from the beginning) and usually have a pre-launch price, theoretically lower (to attract investors) in relation to how much they are estimated to be worth later. Another difference is that, to ensure a certain level of security for investors, money amounts resulting from ICO do not go directly into start-up accounts, but are kept in some sort of escrow accounts, open to a third party (usually the ICO platform, such as Ethereum), which will give it to the issuer after a predetermined protocol (although there are some loopholes to justify the withdrawal of money, in spite of protocol interdictions).

These protocols (called smart contracts) are computer programs that can automatically execute the terms of a contract. That is, the software executes the elements of the contract if certain conditions are met or they are not executed if the conditions are not present. Intelligent contracts are implemented in the blockchain, and their promoters consider eliminating impartial lawyers and judges from between the contracting parties.

Investors are informed about ICOs through online channels (forums and sites dedicated to cryptocurrencies), which also mention the purpose of collecting funds: developing information technology products or services through use, in many cases, of the blockchain.

Virtual assets (so-called digital tokens) or start-ups' proprietary cryptocurrency issued within an ICO may be used: (a) either as voting rights and/or as rights to a portion of future start-up incomes (b) either accessing or purchasing the product/service that the issuing start-up will develop, (c) either they may be exchanged for national or virtual currencies (Ștețiu, 2017).

The launch of an ICO requires the start-up to publish a brief, unregulated, and unapproved prospectus, called "white paper", which describes the start-up's objective, the purpose for which the assets (digital tokens) are produced, some details about the business and its market, how the ICO funds will be used, etc.

Being uncontrolled, these white papers do not provide too much security to investors. It is mentioned that investors take risks such as: abandoning the project, the platform on which the ICO will be launched refusing to issue the token and, last but not least, the token issuer to lie about the stage at which the project finds itself (Iacob, 2018).

Although not generally regulated, the ICO explosion of 2017 has made regulators pay closer attention to this market. Thus, in the United States, the US Securities and Exchange Commission (SEC) began to regard them as securities and to request their issue through the required prospectus for the other securities, and this approach will likely be reproduced by similar authorities in financially developed countries. It should be noted that in September 2017, China banned ICO.

8. Conclusion

Nearly a decade after the appearance of cryptocurrencies, they have grown in both number and market, becoming a reality of everyday life, and in the last year, the media has constantly written about them. Yet they continue to be a mystery. Understandable, on the one hand, as not all of us are computer scientists, but simply computer users, with only a few who are good at cryptography. Unfortunately, just as few of the founders and users of cryptocurrencies are economists. Perhaps that is why they exaggerate when they call their creations "currency". These creations are not and probably never will be currencies for a long time. Cryptocurrencies are something that few are good at, but many want, because it brings them some wealth. Cryptocurrencies and their evolution over the past year have enriched their founders and, being unregulated, will impoverish the many before long. Cryptocurrencies have emerged and developed as a result of the frustration experienced by many who believe that the heads of states and authorities exploit them: banks rob them, states discriminate against them, judges and lawyers are not fair. It is the world of the Internet, a world where people are free without bosses or laws. Cryptocurrencies also mean many personal egos, but also the right to opinion and a social democracy. Or maybe anarchy. How could we justify over 1500 such assets in less than 10 years.

References:

1. Bitcoin, 2017. *Home*. [online] Available at: <https://bitcoinx.ro/> [Accessed 18 December 2017].
2. Bitcoin.org, 2017. *Introduction*. [online] Available at: <https://bitcoin.org/en/> [Accessed 18 December 2017].
3. Chiu, J. and Koeppl, T., 2017. *The Economics of Cryptocurrencies. Bitcoin and Beyond.* Bank of Canada, Victoria University of Wellington, Queen's University.
4. CoinMarketCap, 2017. *Home*. [online] Available at: <https://coinmarketcap.com> [Accessed 18 December 2017].
5. Hileman, G. and Rauchs, M., 2017. *Global Cryptocurrency Benchmarking Study*. Cambridge: University of Cambridge, Judge Business School, The Cambridge Centre for Alternative Finance.
6. Follow My Vote, 2017. *What is Blockchain Technology?* [online] Available at: <https://bitcoinx.ro/> [Accessed 18 December 2017].
7. Iacob, A., 2018. *Finanțarea startup-urilor prin criptomonede: Accelerator versus ICO*. [online] Available at: <www.startupcafe.ro> [Accessed 18 December 2017].
8. Schuhy, S. and Shyz, O., 2016. *U.S. Consumers' Adoption and Use of Bitcoin and Other Virtual Currencies (Preliminary and incomplete).* Boston: Federal Reserve Bank of Boston, MIT Sloan School of Management.
9. Ștețiu, D., 2017. *Ofertele inițiale de monede (ICO) bazate pe tehnologia blockchain.* [online] Available at: <www.juridice.ro> [Accessed 18 December 2017].