Department of Management

Subject: *International Economics and Industrial Dynamics*

"HISTORY AND EVOLUTION OF THE MAIN CRYPTOCURRENCIES"

Relator:

Prof. Luigi Marengo

Correlator:

Prof. Gianfranco Di Vaio

Candidate:

Vincenzo D'Andrea

ID number:

680091

ACCADEMIC YEAR _2017/2018_

Index

a. Introduction..4

1. Bitcoin 6

1.1 What is a Bitcoin (BTC)..6

1.2 Main characteristics and differences with legal currencies...................................8

1.3 Where to store Bitcoin, how to get and where to use it.......................................10

1.3.1 Bitcoin Wallets 10

1.3.2 How to get BTC...14

1.3.3 Where to use BTC 19

1.4 History and Altcoins...20

1.4.1 History 21

1.4.2 Altcoins...23

2. How does Bitcoin and main cryptocurrencies work...27

2.1 Bitcoin Technology 28

2.1.1 Cryptography 28

2.1.2 Peer-to-peer network and distributable calculation 31

2.2 Private and public keys and addresses 32

2.3 Blockchain 33

2.3.1 Structure of transactions...34

2.3.2 Block structure 37

2.4 Mining 40

2.4.1 What is Mining and how it works 41

2.4.2 Mining rules 42

2.4.3 Solo-mining, pool-mining and cloud-mining 44

2.4.4 Transaction commissions 46

2.4.5 Honesty and Dishonesty of the nodes 48

3. Cryptocurrencies economy 54

3.1 Evolution over time: the ICOs.. 55

3.1.1 ICO regulation 57

3.2 Cryptocurrencies regulation problem all over the world 61

3.2.1 Regulation in USA 62

3.2.2 Regulation in EU 63

3.2.3 Regulation in Italy 67

3.2.4 Countries “against” cryptocurrencies 69

3.3 Future of cryptocurrencies: will they ever replace legal currencies? 73

b. Conclusions 77

c. Bibliography and Sitography 78

d. Summary 82

a. Introduction

What is **Bitcoin[1]?** The first decentralized digital currency. The novelty, even if this currency has been in circulation since 2009, is not so much in the digitization of payments, to which everyone is now accustomed, in the Internet age, to the fact that it is the first attempt at decentralization. Unlike all traditional coins, bitcoins escape from any authority: the mint of the State does not think about them and there is no Central Bank that controls their value or a financial intermediary that validates their transactions. Born with the intent to make transactions on the internet safer and faster, Bitcoin is a new system for electronic transactions that is no longer based on trust in a third-party authority, but on mathematics and cryptography. The central bank is replaced by the Bitcoin platform, a *peer-to-peer (p2p)*[2] network to which everyone can participate, as long that you install the homonymous software in your computer, which is free and open-source[3], even if a high computing power is required. The nodes of the network, using the software within their own devices, contribute in a widespread way to validate and record the transactions between two users who want to exchange units of this new type of currency, ensuring also anonymity thanks to the cryptography inherent in the system. The activity of validation and registration of transactions is called *"mining"*, a term that metaphorically traces the activity of gold mining from a mine, and the nodes that perform it are called *"miners"*. This activity exploits the computational power of the miners' devices, and is remunerated through newly issued bitcoins, according to a precise rewards system.

There are over **17 million bitcoins** in circulation at the moment, while the value of 1 BTC *today*[4] is $ 7,078. The price is determined by the market, by the mechanism of supply and demand, even if it is characterized by a strong volatility. The purpose of this work is to provide a technical, economic and legal analysis of this innovative payment system.

The first chapter is dedicated to a presentation of the phenomenon of cryptocurrencies and more specifically Bitcoin, describing the characteristics and methods of use.

[1] ***Bitcoin*** commonly indicates the payment system, while ***bitcoin*** indicates the currency exchanged through this system.
[2] ***Peer-to-peer (p2p) or peer-to-peer network:*** computer network architecture in which nodes are mutually equal, being able to behave as both a client and a server.
[3] ***Open source:*** software for which the authors publish the source code, allowing its development to anyone.
[4] source: blockchain.info, 29/08/2018

In the second chapter the technical aspects underlying the functioning of the system will be examined in depth.

In the third chapter the economic and legal aspects will be analysed, highlighting the advantages and disadvantages deriving from its use, considering the future prospects.

1. Bitcoin

From the definition given directly by the creator Satoshi Nakatomo, in a discussion on the website bitcointalk.org, that is the most important forum for the Bitcoin community *"There's nothing to relate it (bitcoin) to."*

1.1 What Is a Bitcoin (BTC)

Bitcoin is "*is the first digital decentralized currency*" as it can be read in the bitcoin.org website and is defined as a *"purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution"*. by Satoshi Nakatomo in a paper talking about it.

In these multiples basic definitions is clear that the single word "Bitcoin" has a lot to tell. First of all, the word Bitcoin with "B" capital letter is the whole network of payments, where there is traded a new kind of decentralized value, that means that there is not an entity that controls the emission and regulates it: the bitcoin with lowercase "b".

The creation of this new type of currency arises from the need to disengage from the traditional online payments method, which in addition to the two parties that have to make an exchange includes a trusted third party: financial institutions. In fact, these act as guarantors to avoid the problem of double-spending, that consists to spend the same currency twice as being digital. In this regard, the bitcoin network offers a solution to this double-spending problem by providing an electronic payment system no longer based on trust (and therefore on financial institutions) but on cryptography, *"implementing a mechanism of confirmation and maintaining a universal ledger (called "blockchain") cash monetary system"*.

Therefore, the problem of the necessary control for the normal exchanges in legal value is also solved in this case: in fact the data are diffused and distributed in the network and guaranteed through the adhesion of every single user to a unique protocol, compliant and difficult to force despite the open source nature of the Bitcoin network. Each "node", ie. every hardware device that interfaces with the network that must also be available online at the same time becomes an active and integral part of the currency management process, so that the higher the number of nodes becomes, the more focal becomes the concept of decentralization. This does not imply an obligation for users to be a node and therefore always be connected to the network in order to access the services to buy or exchange money, but users must simply have to create a Bitcoin account. These nodes are only necessary so that are possible and registered the various transactions.

At this point, however, it becomes important to clearly define and clarify some points related to the key concept of decentralization, given that both the software and the protocol of adhesion of individual users have been created by the creator Satoshi Nakamoto and this could generate doubts and perplexities as one might think that he could act as central authority. The problem is dispelled considering that as mentioned previously the nature of the software is open source and free: in fact every single user can bring improvements to the protocol although the latter is difficult to force deep because each node is then free to choose which version of the software to use as long as it complies with the rules and the protocol used by the other nodes. This last point is of fundamental importance because it highlights the aspect of consensus between users and developers for the network to work and this also makes it difficult to centralize this system and to regulate it.

To conclude then it can be said how Bitcoin can be defined as a new innovative payment system whose control is no longer in the hands of a central authority that regulates everything but in which thanks to the diffusion of a specific software and protocol are possible transactions of virtual currency not regulated by a third party that acts as guarantor.

1.2 Main characteristics and differences with legal values

In 2012 the ECB defined virtual currency as *"a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"* and defined as legal currency every legal currency instituted and released by a central authority to which citizens rely to use this currency as a method of payment in exchange for goods and services in the real economy.

Figure 1.1 below illustrates the three virtual currency types classified by the ECB; the bitcoins, being able to be both bought in exchange for legal tender and can be used for the purchase of goods and services are included within the virtual currency systems of third type.

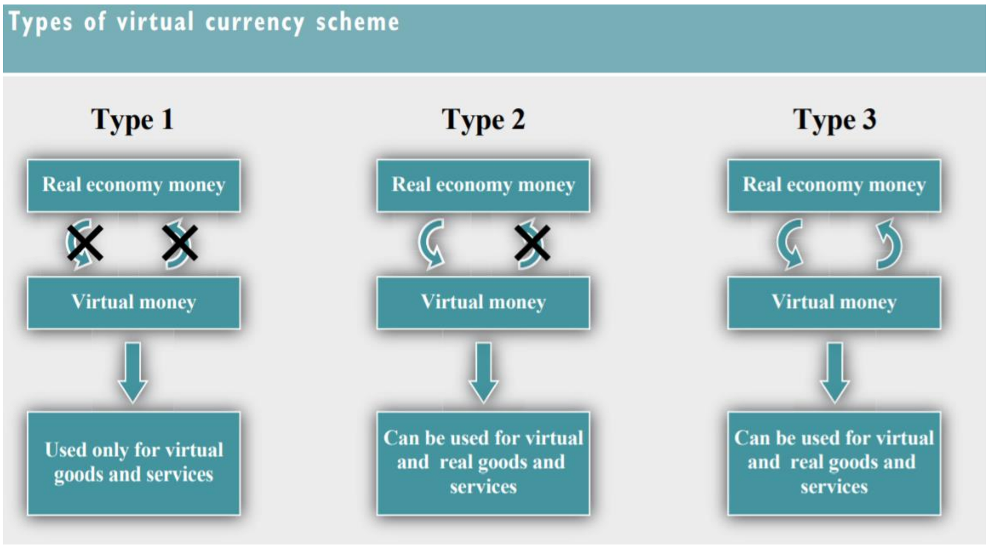

Types of virtual currency scheme
Type 1
Real economy money
Virtual money
Used only for virtual goods and services
Type 2
Real economy money
Virtual money
Can be used for virtual and real goods and services
Type 3
Real economy money
Virtual money
Can be used for virtual and real goods and services

Figure 1.1: cryptocurrency types, (source: ECB)

Cryptocurrencies are digital currencies independent of any central unit, which use cryptography to verify transactions and adjust the issuance of new currency units.

The main characteristics of bitcoins (also common with those of other major cryptocurrencies) are:

- **Decentralization:** It has not been established, it is controlled by any authority central. Transaction checking is performed by many independent entities in decentralized and distributed manner, so the presence of banks and other subjects regulated is no longer necessary.

- **It is not subject to monetary policies:** the absence of a central authority involves also the impossibility that any subject exercises coercive actions on the currency, such as the increase or decrease of currency units in circulation. The money supply is established a priori by the protocol, so that it increases Over time up to the maximum set limit of 21 million units.

- **It has no legal tender:** it is accepted as a means of payment only on a basis voluntary, and therefore cannot be used to pay off obligations pecuniary if the creditor refuses to accept them.

- **Pseudonym:** transactions take place between public addresses from which it is practically impossible to trace the real identity of the natural or legal person that processes the virtual currency exchange. But user identity remains unknown until it is revealed during a transaction or in other cases, so these addresses should be used only once for each transaction.

- **Transparent:** all transactions are recorded in a register open to the public, the blockchain, which anyone can view. Exploring the blockchain is possible to know how many bitcoins every single address at any given time time, being able to go back to the addresses given to them.

- **Low transaction costs:** the absence of subjects that interfere in transactions has the consequence of reducing the costs. On average, the transactions include a debit to the sender of 0.0001 BTC (about 0.02 €) as a commission, but the amount it may be greater or void depending on certain conditions (it will be discussed later).

- **Fast and irreversible transactions:** every bitcoin transaction takes on average 10 minutes to be confirmed. These transactions are irreversible, that is impossible to cancel.

1.3 Where to store bitcoin, how to get and where to spend it

There are several ways to get bitcoins, some simple and some more complex. On the other hand, there are always growing businesses, both physical and online, where they can be spent. However, before thinking of how to get and spend bitcoins and need to be able to do it to receive, and once received, to be able to keep them safe, without risking losing them or to have them "steal". For this purpose, it is necessary to have a Bitcoin wallet, a wallet electronic which performs the same functions as a portfolio material, that is, the custody of our money, which in this case is digital.

1.3.1 Bitcoin Wallet

Bitcoin wallets are not exactly the equivalent of a current account, though the graphical interface offered by the various wallet services allows you to know at any time the total of the bitcoin possessed and the movements in and out, as a kind of account statement in real time.

These are not actually contained within a portfolio but are stored in a register open to the public, *the blockchain*, below specific addresses belonging to different users.

Addresses are reception points and sending and are presented in the form of alphanumeric codes of 33 or 34 characters, generally starting for 1, so as not to contain any user reference, making Bitcoin a pseudonym payment system. The addresses derive by means of algorithms from other codes, the so-called *public keys*, and these once again derive through other algorithms from the so-called *private keys*, so that starting from the address it is impossible to trace the original public key and from this to the private key.

Through the encryption of digital signatures, only the possession of the private key authorizes the user to spend the associated bitcoins at the address derived from it. For this reason the private key does not have to be rendered public, but must be kept in order not to run the risk of someone else taking possession of it.

These wallets store the user's private keys, which allow him to spend the bitcoins associated with the precise address that derives from the public key that its turn derives from the private key in question; this is what happens behind the scenes. In fact, the wallet offers the user an intuitive interface, similar to that of the online banking app that allows him to view the bitcoin balance at his disposal of all the different addresses he has, giving him the possibility to make outgoing transactions towards certain beneficiaries, or to receive payments at a specific address.

When you create a new wallet, one hundred pairs of them are automatically generated private and public keys (*key-pool mechanism*), for which the user can use multiple addresses different, to enjoy greater levels of privacy. So, every transaction is registered in the blockchain, and anyone can see all the movements of an address; if an individual and able to associate an address with a physical identity, then for example to a bargaining where payment details were exchanged, these can control all the movements, for this reason change often address is guarantee of greater privacy.

There are different types of portfolios (only a few are mentioned) to choose from, depending on the levels of user convenience, security and complexity desired, type of device used, if smartphones, desktops and even there is the ability to choose between operating systems:

- ***Desktop Wallet:*** it is a software to install on your computer that allows you to store and store private keys on the hard disk. The installation of these software generally requires the download of the entire blockchain. They are available for different operating systems (windows, Mac, Linux). The security that guarantees this type of wallet can be high, but only if you take the necessary precautions: in fact if the device is not protected by an antivirus or does not provide to protect it or the wallet has not been encrypted with an appropriate password, the user runs the risk that some hackers steal the private keys from their PC, or anyway if the same was lost or left unattended, anyone would have access to the wallet and could spend the bitcoins. Finally, it is highly recommended to make periodic backups of the wallet in order to recover the private keys if the PC is damaged or lost.

- ***Mobile Wallet:*** wallet applications for smartphones that make it possible to keep, to spend or receive bitcoins from your mobile phone quickly and easily. This type of applications does not require the download of the entire blockchain, but only of a part of it, relying on information from other nodes of the network. As for desktop wallet, it is recommended to make periodic backups.

- ***Online Wallet:*** service offered by different websites, (like Coinspace.org BitGo.org) that store private keys storing them in online servers placed under their protection. In other words, the user entrusts the custody of their bitcoins to third parties, in this case a website. Typically, online wallets are offered on an ancillary basis by exchanges, platforms buying and selling bitcoins in exchange for traditional currencies. Considering the unpleasant inconveniences that happened to some of these exchanges in the past, probably this type of wallet is not the safest type, but it is the easier and faster to use, as it can be accessed from anywhere device connected to the internet. So, keep a lot of bitcoins in these types of wallets it is not particularly suitable, while for small but frequent transactions are undoubtedly the most practical to use.

- ***Paper Wallet:*** private and public keys can be stored directly from the same user in a paper support and kept so protected from hackers and from possible failures of their electronic devices. The most common online wallet allows you to export your codes in paper format or alternatively bitaddress.org randomly generates new private and public key pairs, that can be used to receive bitcoins, and then to spend them. Once you've exported your paper wallet, the public key is not more memorized digitally anywhere, so it is recommended to keep it in appropriate manner and maybe create some copies for security. The address can normally receive payments, but to spend such bitcoins the user must re-import your private key online or on a software wallet to sign the outgoing transactions. From this point of view, the security offered by a paper wallet It is very high and works great as a long-term bitcoin deposit but is more complicated to use.

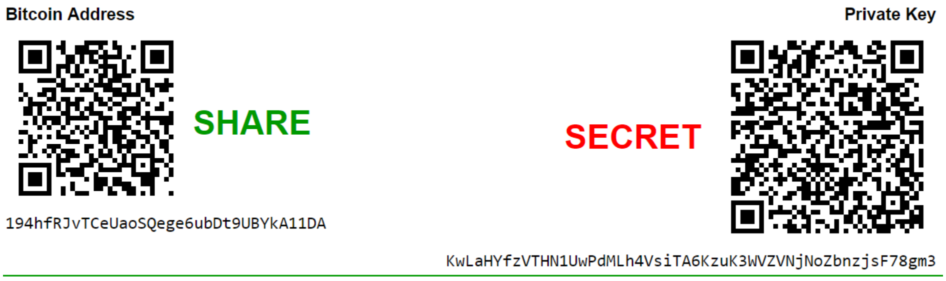

Bitcoin Address
SHARE
194hfRJvTCeUaoSQege6ubDt9UBYkA11DA
Private Key
SECRET
KwLaHYfzVTHN1UwPdMLh4VsiTA6KzuK3WVZVNjNoZbnzjsF78gm3

Figure 1.2: paper wallet example generated on bitaddress.org.

- ***Hardware Wallet:*** these are devices created specifically for storing private keys bitcoin addresses and other cryptocurrencies. It is not done with respect to the other types of wallets entrusting to third parties for the conservation of the codes, there is no risk that they are stolen by a hacker, and they do not have to be re-imported online or in one software to make outgoing transactions. The hardware wallets are goods mini computers with a single function, that of digitally signing transactions with the user's private keys. These usually connect to the computer via USB and interact with the software wallet safely even if the computer would be compromised. The user checks the correctness of the address a from the computer to send bitcoins and authorize the transaction by entering a PIN on your own hardware wallet, which hackers cannot intercept

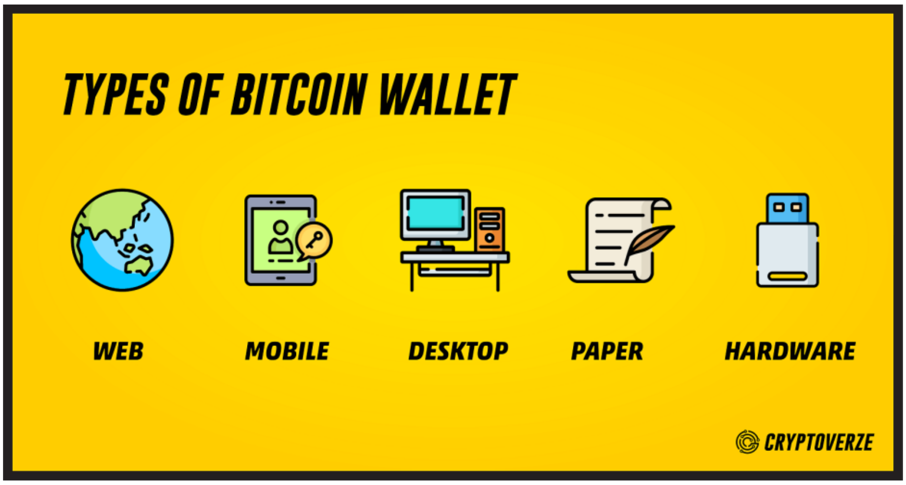


Figure 1.3: types of bitcoin wallet, (source: Cryptoverze)

1.3.2 How to get BTC

Once illustrated how to store BTC, it is good to show how they can be obtained. Obviously, the ways to buy them are many, shown below:

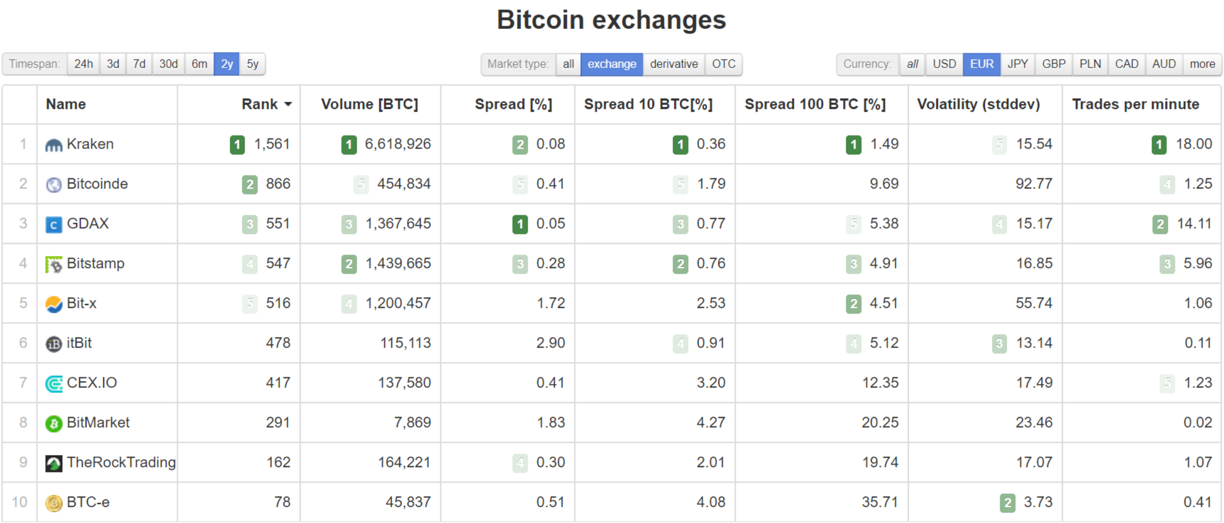
- ***Buy them from people willing to sell them***: localbitcoins.com is the leading face-to-face exchange website platform and is present in 16263 cities and 248 countries including Italy. Who wants to buy bitcoins can decide whether to exchange online, choosing one of the various payment methods (bank transfer, PayPal, Postepay, Skrill, Moneybooker) or arrange a physical meeting with the seller and exchange bitcoins in exchange for cash, in how much you can find offers also relatively close in geographical terms. Face-to-face meetings must take place in places where internet access is available, necessary for processing transactions, while for online exchanges it is always recommended to check seller feedback.

  Another similar platform is bitcoin.meetup.com, a social network that brings together groups of people by areas of interest, including bitcoins. Some of these groups organize periodic meetings, to which it is possible to participate and have a direct contact with the topic and with the people of the "community".

  Another interesting opportunity is represented by the so-called *"Satoshi Square"*, which are public events that take place mainly in large cities where a public square or park, which is transformed into an open-air bitcoin market. The first was organized by Josh Rossi, as a tribute to "Wall Street", held in New York in May 2013. In addition to facilitating the exchange these events have contributed and are contributing to also give public evidence thus allowing better communication and information in matter.

- ***Buying at online Exchanges:*** there are many sites on the web that allow the purchase of bitcoins in exchange for legal tender or other cryptocurrencies. These platforms play the role of market makers by fixing exchange rates to which the Exchange buys or sells bitcoins in exchange for the main traditional currencies or currencies other virtual currencies. Figure 1.4

classify the main online exchange sites for bitcoin volume (BTC) exchanged in the last two years (2016-2017).



Bitcoin exchanges

Timespan: 24h 3d 7d 30d 6m 2y 5y

Market type: all exchange derivative OTC

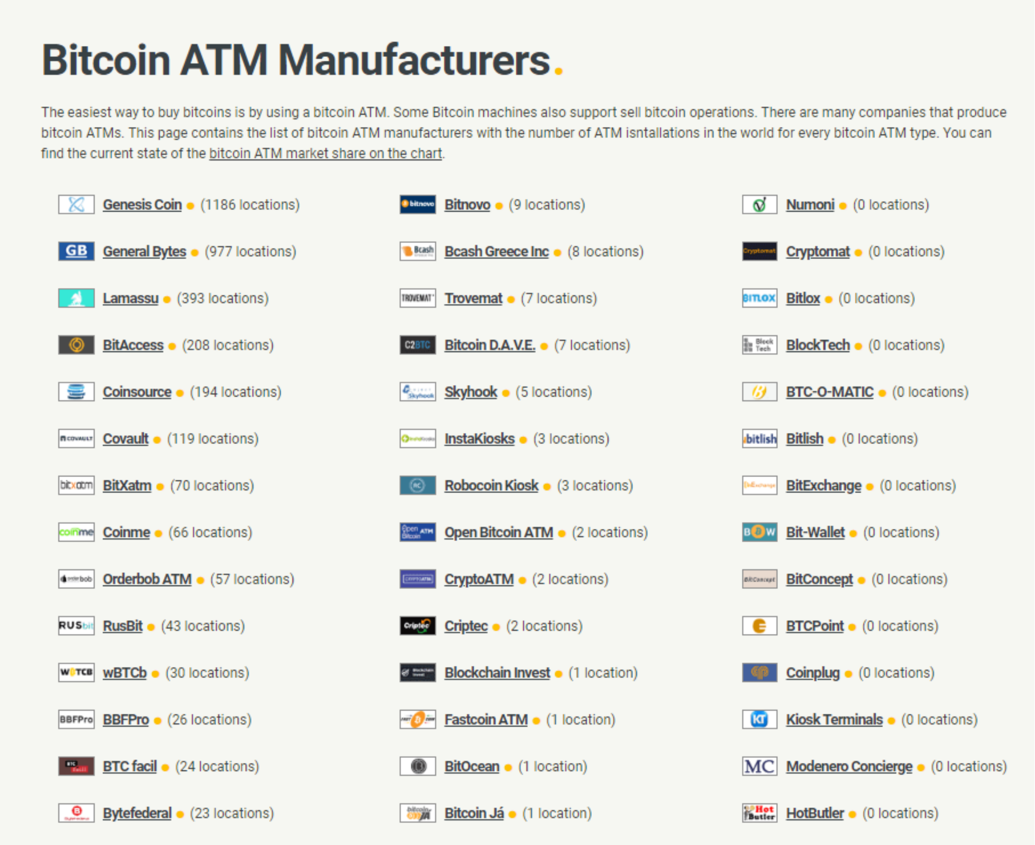
Currency: all USD EUR JPY GBP PLN CAD AUD more

	Name	Rank	Volume [BTC]	Spread [%]	Spread 10 BTC[%]	Spread 100 BTC [%]	Volatility (stddev)	Trades per minute
1	Kraken	1 1,561	1 6,618,926	2 0.08	1 0.36	1 1.49	5 15.54	1 18.00
2	Bitcoinde	2 866	5 454,834	5 0.41	5 1.79	9.69	92.77	4 1.25
3	GDAX	3 551	3 1,367,645	1 0.05	3 0.77	5 5.38	4 15.17	2 14.11
4	Bitstamp	4 547	2 1,439,665	3 0.28	2 0.76	3 4.91	16.85	3 5.96
5	Bit-x	5 516	4 1,200,457	1.72	2.53	2 4.51	55.74	1.06
6	itBit	478	115,113	2.90	4 0.91	4 5.12	3 13.14	0.11
7	CEX.IO	417	137,580	0.41	3.20	12.35	17.49	5 1.23
8	BitMarket	291	7,869	1.83	4.27	20.25	23.46	0.02
9	TheRockTrading	162	164,221	4 0.30	2.01	19.74	17.07	1.07
10	BTC-e	78	45,837	0.51	4.08	35.71	2 3.73	0.41

Figure 1.4: Table with BTC volume traded on main online exchanges

- ***Buying at Bitcoin ATMs:*** it is a much quicker purchase or sale service compared to exchange online and offered by Bitcoin ATMs. The first ATM bitcoin, produced by American company Robocoin, was installed in 2013 at the Waves Coffee House in Vancouver (Canada) and already in its first day of operation recorded as many as 81 transactions totalling over $ 10,000. There are currently 3480 bitcoin ATMs in 72 countries[5], of which 17 in Italy and the number is constantly increasing. In circulation there are different models, among which the most widespread ones.

[5] https://coinatmradar.com/, 17/07/18



Bitcoin ATM Manufacturers.

The easiest way to buy bitcoins is by using a bitcoin ATM. Some Bitcoin machines also support sell bitcoin operations. There are many companies that produce bitcoin ATMs. This page contains the list of bitcoin ATM manufacturers with the number of ATM isntallations in the world for every bitcoin ATM type. You can find the current state of the bitcoin ATM market share on the chart.

Genesis Coin	(1186 locations)
General Bytes	(977 locations)
Lamassu	(393 locations)
BitAccess	(208 locations)
Coinsource	(194 locations)
Covault	(119 locations)
BitXatm	(70 locations)
Coinme	(66 locations)
Orderbob ATM	(57 locations)
RusBit	(43 locations)
wBTCb	(30 locations)
BBFPro	(26 locations)
BTC facil	(24 locations)
Bytefederal	(23 locations)
Bitnovo	(9 locations)
Bcash Greece Inc	(8 locations)
Trovemat	(7 locations)
Bitcoin D.A.V.E.	(7 locations)
Skyhook	(5 locations)
InstaKiosks	(3 locations)
Robocoin Kiosk	(3 locations)
Open Bitcoin ATM	(2 locations)
CryptoATM	(2 locations)
Criptec	(2 locations)
Blockchain Invest	(1 location)
Fastcoin ATM	(1 location)
BitOcean	(1 location)
Bitcoin Já	(1 location)
Numoni	(0 locations)
Cryptomat	(0 locations)
Bitlox	(0 locations)
BlockTech	(0 locations)
BTC-O-MATIC	(0 locations)
Bitlish	(0 locations)
BitExchange	(0 locations)
Bit-Wallet	(0 locations)
BitConcept	(0 locations)
BTCPoint	(0 locations)
Coinplug	(0 locations)
Kiosk Terminals	(0 locations)
Modenero Concierge	(0 locations)
HotButler	(0 locations)

Figure 1.5: Bitcoin ATMs manufacturers for the number of devices in the world (Source: coinatmradar.com, 21/08/18).

These devices are almost always of two types:

1) ***unidirectional,*** that is, they allow to convert only legal currency into bitcoins,

2) ***bidirectional,*** the ones that instead allow both to buy and to sell bitcoins in exchange for legal tender.

Compared to the options listed above, that represented by ATMs bitcoin is more easily and immediately used. If you already own an electronic wallet in fact, buy or sell bitcoins can take anywhere from 15 to 30 seconds, while if you were faced with a *Robocoin Kiosk* or a *BitAccess* can create a new wallet and buy some bitcoins all in less than 5 minutes, thus reducing the time required for authentication normally from an online exchange.

In general, the process of buying (or selling) bitcoins through an ATM takes place in the following phases:

1) *Verification phase:* this phase is possible, given that not all ATM models in circulation they foresee it. The verification can consist of simple insertion of a code that the machine sends to the user by text message after inserting the mobile number, or in the presence of more sophisticated models it consists in the real personal and physical recognition of the user. This is the case of *Robocoin Kiosk,* which can only be accessed creating a personal account. The device at the customer's first access capture scans of the identity document or passport, of the face through the palm of the hand, while from the second access in then the verification will come by simply placing the palm of the hand on the scanner and entering the numeric PIN chosen;

2) *Entering the Bitcoin address:* this step is performed by scanning the QR Code[6] associated with the electronic wallet in which you want to receive bitcoins, or from which you want to withdraw bitcoins in exchange for money. Some of these ATMs also allow the generation of new addresses at the time of use;

3) *Selection of the amount of cash:* that you want to change into bitcoin, and its insertion into the slot. In the case of two-way ATM's, it is possible convert bitcoins into legal currency, while always depending on the model of the device and it is also possible to buy other cryptocurrencies;

4) *Confirmation of the operation.*

- ***<u>Selling goods and services in exchange for bitcoins:</u>*** currently, this option is more easily negotiated by those who conduct a business. I'm always more numerous stores, both physical and online, accepting bitcoin in payments exchange of goods and services.

[6] ***Quick Response Code:*** consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera, and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data is then extracted from patterns that are present in both horizontal and vertical components of the image. (Source: wiki/QR_code)

The easiest way for a merchant to accept payments in bitcoins from their customers and communicate the address and wait for these make payment with your smartphone. However, they are constantly growing services aimed at simplifying and speeding up foreign currency payment procedures digital.

- ***Mining:*** it is the activity of validation and registration of bitcoin transactions that they happen continuously in the system. This activity is carried out by the nodes of the network that or this reason they are called miners, and it consists in doing their own computer of complex cryptographic problems in a repetitive way, expensive in terms of electricity consumption and equipment wear.

  Mining is incentivized by a precise system of rewards, consisting of bitcoins of new issue in quantity and with times established by the protocol, (will be discussed in the next chapter) and represents the only creation and entering new currency units. Each node works autonomously, simultaneously and in competition with everyone the other nodes in order to solve the problem first and win the reward.

  Alternatively, the nodes can work together in groups called mining pools, sharing their computational strength to get more chance to get rewards, in competition with other autonomous nodes or other groups.

  The total computing power of Bitcoin is given by the sum of the powers of all the devices made available by the nodes, and it is important because from this derives the difficulty in cryptographic problems to be solved by miners. In fact, this difficulty yes automatically adjusts so that increasing the total power also increases the difficulty and vice versa, ensuring that transactions are always validated within one a certain amount of time (10 minutes), and the rewards are the same donate in a constant manner.

  For this reason, if at the beginning of Bitcoin the first miners were able to make money also using some more or less recent computers, the progressive increase of the miners and therefore of the power of calculation entered, and the birth of devices always more powerful built specifically for this purpose called ASICs[7], all driven by the progressive spread of Bitcoin as

[7] ***Application Specific Integrated Circuit:*** integrated circuit created specifically to solve a precise calculation application, in this case cryptographic problems of mining (source: wiki/ASIC)

an alternative payment system and consequently from the growth of its price, they have given life to real business related to mining, bringing it to a difficulty too high to support if not through huge investments in specific hardware and energy. The latter option exposed is certainly the most complicated to obtain bitcoins.

1.3.3 Where to use BTC

Bitcoins in particular but also some similar cryptocurrencies can be used for the purchase of goods and services. To find the shops that accept the payment of goods and services with virtual currency, it is useful to consult the coinmap.org website, that includes a map that provides the exact location of the nearby stores.

Moreover, it is possible to consult, especially for the Italian market, the *QuiBitcoin* application, which in addition to indicating the positions of these stores that accept this type of payment also traces the Bitcoin ATMs already mentioned above. These figures are still few in Italy because of the still rather long transaction times. Many of those who instead accept this type of payments use the US *Bitpay* provider and, recently, also the new *Conio* service, which allows the merchant to accept Bitcoin payments, being able to choose whether to receive Bitcoin or Euro in exchange.

As far as e-commerce is concerned, cryptocurrencies are easier to use: in fact, they are widely used and appreciated by sellers because, as already mentioned above, it has the undeniable advantage of the payment irreversibility (after about 10 minutes for validation operation).

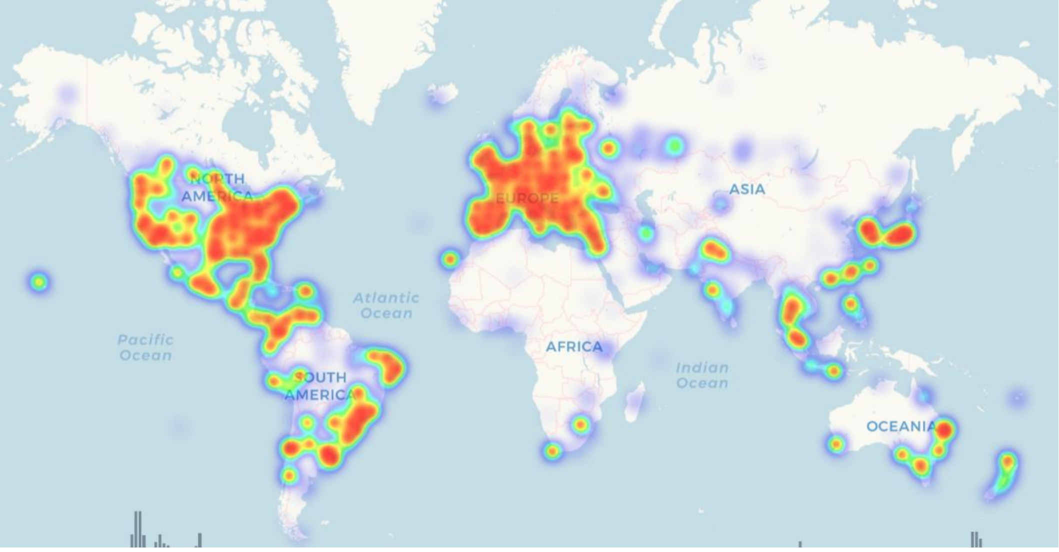


Figure 1.6: ATM world map, (source: www.coinmap.org, 21/08/18)

1.4 History and Altcoins

"I worked on a new electronic money system that is completely peer-to-peer, without any trusted third party" recites the post that Satoshi Nakamoto publishes in November 2008 on the *Cryptography Mailing List* of the metzdowd.com site, a mailing list where to open discussions on the development of technologies regarding cryptography and their impact from the political, economic and social point of view, attaching the .pdf document *"Bitcoin: a peer-to-peer electronic cash system*" in which it explains how it works. *"Bitcoin v0.1"* is the name of the software, released in January 2009 that marked the beginning of the cryptocurrency era. Even if the first few years of Bitcoin's life did not ignite the enthusiasm of the public, 2009 can be considered as a sort of watershed: on the one hand it represents the achievement of an innovative technological milestone due to the many advances in cryptography and computer science and of some failed alternative currency attempts on the other side marks the birth around Bitcoin of a real ecosystem, and the subsequent proliferation of altcoins or alternative digital currencies.

1.4.1 History

Since the '70s research in the cryptographic field leads to important developments, thanks to the Progressive progress towards the digital age that has increased the need for individual security and privacy. The cryptography that until then was only the domain of governments for the security of communications has back to be in the public domain, to ensure high levels of privacy of the new digital systems, including those relating to electronic payments.

In the 1980s, however, the American cryptographer David Chaum perfected the blind signatures system[8] in order to improve the privacy of electronic payment services offered by banks. Chaum extends his research into electronic payment systems, which culminate with the founding of *DigiCash Inc.* in Amsterdam and the launch of the *e-cash* system in the early 1990s.

This electronic payment system was based on the use of virtual money to keep in the computer, controlled cryptographically by the member banks, and allowed to make anonymous and secure purchases on the Internet or in the shops that accepted them, without the need to exchange card credentials of credit. Although this system was sold to several banks, these were still conservative in a market dominated by credit cards, so that it failed a few years after the creation in 1998. Although e-cash was a centralized system being controlled by the issuing bank, it was still founded on solid cryptographic bases.

In 1998, the famous *PayPal* system was born at the hands of Elon Musk who, unlike e-cash, also allows the transfer of money between individuals.

Another development attempt was made in the decade between 1999 and 2009, by *e-gold*, a digital currency exchangeable instantly on the Internet, issued by the private company *Gold & Silver Reserve Inc*. in exchange for gold or silver deposits. This currency was traded between accounts and essentially for the owners was like holding a certain amount of precious metals held by *G&SR* as a reserve. Starting in 1999, the e-gold market quickly took hold,

[8] **Blind signatures:** represent a particular form of digital signature, in which the signer signs the message blindly. The purpose and guarantee the authenticity of the message to the recipient, but in an unidentifiable way (Source: wiki/Blind_signature)

culminating with the creation of the first independent exchange platforms in 2000. E-gold could be used both for transfers of money between individuals, and for online purchases. In 2007, the US government accused e-gold of encouraging money laundering, closing some exchanges and arriving at the final blocking of accounts and transactions in the 2009.

Finally, again in 1998, Wei Dai and Nick Szabo proposed two different decentralized payment systems, which more than anyone approached what Nakamoto will achieve in 2009, even though both projects remained only theoretical. Wei Dai inventor of *b-money* wanted to create an anonymous network in which users identify themselves through pseudonyms, that the transactions were kept on a separate transaction register and that the creation of money should take place through the resolution of problems through the use of a certain computing power, and that finally the transactions took place between addresses digital signature.

If already b-money seemed to approach the future Bitcoin, if only as a basic idea, the research of Nick Szabo, in which he explains the operation of his *bit-gold*, is completer and more exhaustive from the technical point of view. Its creation consists in fact finding a string of bits, called *"challenge string"* through the *proof-of-work*[9] mechanism.

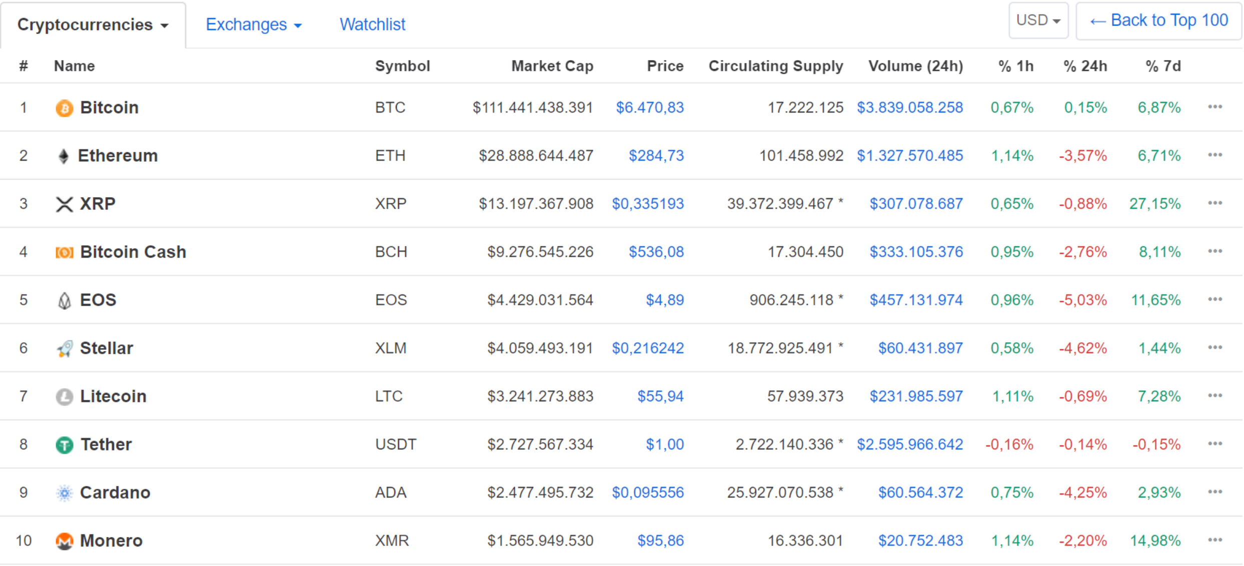
Each of these challenge strings found provides an input to find the next, so a particular challenge string can only be found once and only by a single user, the first in chronological order that solves the problem and then authorizes it to spend it. Transactions occur by digitally signing these bit strings, and receivers can verify their authenticity by consulting the distributed transaction log. Bitcoin is the realization of the ideas and objectives created by a movement created in the 80s called *chypherpunk* based on defending the right to privacy by creating an anonymous payment system alternative to traditional ones, through mathematics and cryptography.

[9] ***Proof-of-work:*** literally proof of work, and a mechanism that imposes on the service applicant the execution of a job or task, which is carried out by the computer and which requires processing time and electricity; an example of pow and represented by the hashcash system, aimed at making wasteful sending of spam by e-mail expensive (Source: wiki/Proof-of-work).

1.4.2 Altcoins

The fundamental open source feature of the Nakatomo project allowed the participation of many developers who, since the creation of Bitcoin in 2009, have made an essential contribution to software development and to the correction of defects such as the vulnerability of the system and then started the creation of similar projects that allowed the creation of the so-called Altcoins.

To date, according to estimates by coinmarketcap.com there are 1865 cryptocurrencies for a market capitalization equal to 211,732,582,263 USD[10] and the number of cryptocurrencies is constantly growing.



#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d	
1	Bitcoin	BTC	$111.441.438.391	$6.470,83	17.222.125	$3.839.058.258	0,67%	0,15%	6,87%	•••
2	Ethereum	ETH	$28.888.644.487	$284,73	101.458.992	$1.327.570.485	1,14%	-3,57%	6,71%	•••
3	XRP	XRP	$13.197.367.908	$0,335193	39.372.399.467 *	$307.078.687	0,65%	-0,88%	27,15%	•••
4	Bitcoin Cash	BCH	$9.276.545.226	$536,08	17.304.450	$333.105.376	0,95%	-2,76%	8,11%	•••
5	EOS	EOS	$4.429.031.564	$4,89	906.245.118 *	$457.131.974	0,96%	-5,03%	11,65%	•••
6	Stellar	XLM	$4.059.493.191	$0,216242	18.772.925.491 *	$60.431.897	0,58%	-4,62%	1,44%	•••
7	Litecoin	LTC	$3.241.273.883	$55,94	57.939.373	$231.985.597	1,11%	-0,69%	7,28%	•••
8	Tether	USDT	$2.727.567.334	$1,00	2.722.140.336 *	$2.595.966.642	-0,16%	-0,14%	-0,15%	•••
9	Cardano	ADA	$2.477.495.732	$0,095556	25.927.070.538 *	$60.564.372	0,75%	-4,25%	2,93%	•••
10	Monero	XMR	$1.565.949.530	$95,86	16.336.301	$20.752.483	1,14%	-2,20%	14,98%	•••

Figure 1.7: top 10 Cryptocurrencies, https://coinmarketcap.com/all/views/all/, 21/08/18

Many of these cryptocurrencies use the same basic mechanisms as Bitcoin, while others propose different solutions, uses and functionalities compared to Nakatomo's initial project. Among the most important we find **Ethereum,** which has 4 characteristics in common with Bitcoin or has an underlying cryptocurrency, an intrinsic blockchain, a mechanism of decentralization based on proof-of-work and miners who help the network, but, the project Ethereum it moves towards a diametrically opposite direction with respect to the Bitcoin project.

[10] Source: https://coinmarketcap.com/all/views/all/, 21/08/18

The latter was conceived as a network for the transfer of monetary values in a decentralized cryptocurrency, and the main purpose of the blockchain was to represent the guarantee underlying these transactions. It was only recently that Bitcoin's blockchain began to be used in non-financial applications. In contrast, Ethereum was conceived from day one as a software development platform for decentralized applications, and its blockchain was specifically designed to support other applications on it. So, it can be said that Ethereum has taken a cue from the characteristics of Bitcoin to bring however the tricks, remedying its defects, of which the main transaction speed that passes from 10 minutes of Bitcoin at a significantly shorter interval between 5 and 30 seconds.

In addition, Ethereum's cryptocurrency, Ether (ETH), deviates from the Bitcoin currency because its main use is not the payment of goods or services, nor the fact of being *a "digital version"* of gold but rather it is similar to a distribution incentive, a sort of fuel crypto, necessary to pay the transaction costs to run the various smart business logic programs that users send to the blockchain.

Besides to be a network fuel, Ether is also marketable as a cryptocurrency on a variety of open trades, but it is expected that appreciation of its value will be more influenced by the quantity and wealth of transaction demand, rather than by the action of speculators, as happened with Bitcoin. In addition, the Ethereum blockchain was designed to be fully programmable, and is more cost-effective than Bitcoin's, being more scalable, a key requirement for the long-term convenience of a heavily trafficked blockchain. Since it is not focused on carrying out financial transactions, the purpose of the Ethereum blockchain is different from that of the Bitcoin blockchain.

On Ethereum there are no limits to the size of a block, and the system adjusts dynamically as a whole, as part of its basic design.

In addition, Ethereum continues to work to improve the aspects relevant to scalability, and this will have the direct benefit of lowering overall transaction costs. In general, by considering what are the desirable characteristics of a blockchain, they come in mind the following, which are the same characteristics in which Ethereum excels: Programmability, Scalability, Updatability, Management of transactions, Visibility, Convenience, Security, Speed/ Performance, High Availability, Extensibility.

Moreover, while now proof-of-work was chosen as a process that regulates consensus on Ethereum, the plans are that Ethereum will adopt a less expensive method known *as "Proof-of-stake"*[11]. It has been demonstrated that proof-of-stake is an efficient and feasible method of consent, cheaper to operate but at the same time more expensive to attack.

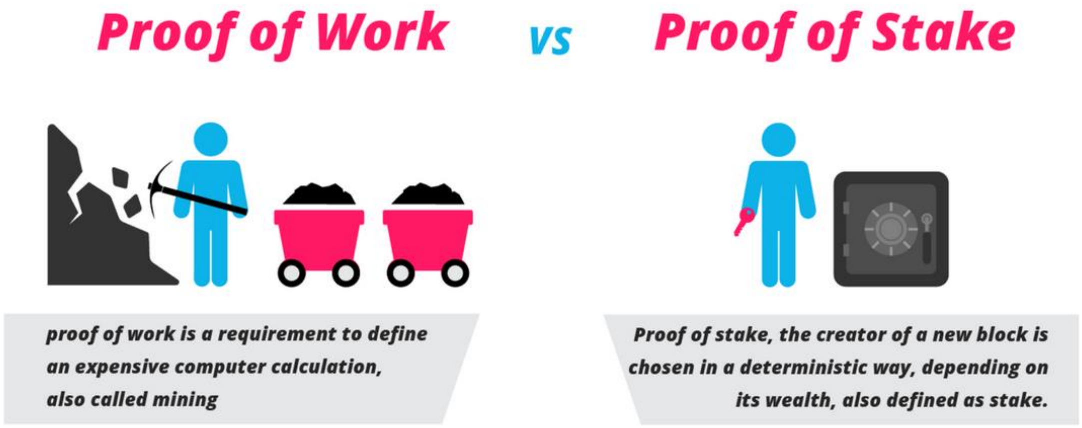

Proof of Work
vs
Proof of Stake
proof of work is a requirement to define an expensive computer calculation, also called mining
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

Figure 1.8: Proof-of-work vs. Proof-of-stake (source: blockgeeks.com)

Finally, mining in the context of Ethereum can be performed by ordinary computers and does not require the specialized computing power that Bitcoin requires, so mining on Ethereum will be cheaper and more accessible to the masses. Anyone who runs Ethereum's client mining software on their computer can become an Ethereum miner.

This is a good strategy, because it makes Ethereum more accessible, and not overly dependent on expensive mining platforms. This also means that, unlike Bitcoin, the functioning of Ethereum does not depend on the accumulation of a phenomenal power of mining. But it is more unbalanced towards self-maintenance through a healthy balance of affordable mining and pay-per-play computational requirements.

[11] ***Proof of stake:*** is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. (source: wiki/Proof_of_stake)

Another important cryptocurrency is **Ripple** (XRP), which is now in third place behind just Bitcoin and Ethereum by capitalization and this presents similarities and differences with Bitcoins.

This has been around since 2013 and its protocol was created by *OpenCoin*, founded in turn by Chris Larsen and Jed McCaleb. On the other hand, Ripple's proposal has a decidedly more innovative content.

Like Bitcoin, Ripple is both a system for electronic payments and a digital currency (XRP), which exploits the peer-to-peer network and encryption to allow decentralization. The big news however lies in the fact that through the Ripple network you can exchange any type of currency, including bitcoins, thanks to much faster transactions (2-5 seconds) that do not require any waiting for their confirmation. Ripple does not therefore arise as a bitcoin competitive system, but rather can be useful to its greater diffusion, thanks to the simplicity of transactions in different currencies and the low transaction costs.

Even though most or perhaps all the remaining altcoins in circulation will never succeed in reaching and overcoming the diffusion that has reached Bitcoin since its birth until today, they contribute, each in an important way, to the innovation and improvement of cryptocurrencies and payment systems in general. The developers and the entire Bitcoin community can take a cue from the attempts made by new projects to make changes and make it better with the passage of time.

2. How does Bitcoin and main cryptocurrencies work

The operation of Bitcoin is in the hands of the network nodes called *"miners".* Through the mining process, they collect transactions that take place continuously, within specific containers called blocks. These blocks are joined together to form the blockchain which is the key organ of the whole system.

The blockchain is a large register open to users, containing every transaction in bitcoin from its birth to today to solve the double-spending[12] problem, and is subjected to continuous updating by the miners. Anyone can view a complete version of the blockchain, installing Bitcoin software or more simply on the web thanks to special sites called block explorer. Bitcoin still manages to ensure high levels of anonymity, as transactions take place between pseudonymous addresses from which it is very difficult to trace the identity of its user.

As stated previously, bitcoin transactions occur between addresses created specifically for this purpose. There are only transactions between addresses, with their budgets increasing or decreasing. Owning bitcoins means possessing the private key associated with at least one of these addresses such that, in any block "solved"[13] by the miners' work, a transaction has been registered in favour of that specific address.

Every bitcoin transaction is perfectly traceable, as at every moment when you consult the blockchain it is possible to know how many bitcoins belong to a given address, and it is also possible to trace to which address he has provided them, and by whom the latter has in turn received.

[12] ***Double-spending:*** the possibility of spending the same unit of digital currency several times; in traditional payment systems this problem is solved by the presence of intermediaries' financial companies that control operations. In Bitcoin, lacking a central authority, this problem is solved by the presence of the blockchain and the work of the miners, who know all the past valid transactions can reject trades that try to spend some bitcoins already spent on past. (source: wiki/double_spending)

[13] As mentioned earlier, miners must solve cryptographic problems; the resolution of these problems head to the creation of a new block, known as "solved".

The blockchain therefore represents the trace and the history of all transactions. It is a reliable tool, which tests because no transaction can conflict with another, since every transaction is Irreversible and is recorded and marked temporally, so no user can send bitcoin that does not own or has already sent to another address, solving the problem of double-spending. In this chapter we propose an analysis of the technical aspects that allow Bitcoin to work.

2.1 Bitcoin Technology

The technology that allows particularly the Bitcoin to work is a combination of more pre-existing technologies. In this section it is proposed a list of the most technologies important at the base of Bitcoin and a brief reference to their operation, preparatory to then be able to go down into the most technical details of the system.

2.1.1 Cryptography

Cryptography is the science that protects information and makes it incomprehensible to those who intercept it, so that it can be read and understood only by the recipient. The message to be protected is called plaintext, while the "hidden" to be incomprehensible is called ciphertext; the transformation from plain text to ciphertext is called encryption, while the inverse transformation is called decryption. The cryptographic transformation is called the encryption algorithm and specifies the procedure that transforms the plaintext into the ciphertext. This transformation is parametric, and there is a "key" parameter: this means that transformation is only a process, but to be implemented it needs further information, on which the result depends. So, to decrypt the message, it is not enough to know the encryption algorithm used, but it is also necessary to know the key.

Generally, in the study of cryptographic algorithms and their security it is assumed that the algorithm is known to all and that what is not known is exclusively the key: this because today it is considered unreliable a cryptographic system whose security is based on the secrecy of the 'algorithm. The traditional cryptography is based on a mechanism for which encryption and decryption are carried out using the same key: this is the reason for symmetric cryptography, or even, given that this key must be known only to the two interlocutors, of secret key cryptography. A well-known algorithm of this type is DES[14] (Data Encryption Standard).

The big problem with this approach, however, is the distribution of keys: if two interlocutors want to use an algorithm of this type to communicate securely, they must first agree in some way on the key. Since the channel used to transmit messages is not secure the key cannot be transferred by this channel. This problem was solved in the 70s with the introduction of public-key cryptography. With algorithms of this type there are two keys: a public one that is to be distributed to all those with whom it wants to communicate and a private one to keep secret.

What is encrypted with the public key can only be decrypted with the corresponding private key, to solve the problem of secretly communicating the key, because this is known to all; to communicate securely with a person, just encrypt the message with his public key. The algorithms of this type are called asymmetric key. One of the major innovations made by asymmetric cryptography is the digital signature: the sender of a message can in fact sign it thanks to its private key that is unique, but all are able to verify the authenticity of the signature thanks to the public key. The signature can then be combined with the normal encryption, obtaining signed and encrypted messages. What the sender encrypts with his private key to guarantee authenticity is not the whole message, but a "footprint" (called digest) obtained through a function (hash function)[15]. The encrypted digest is then attached to the message and constitutes its signature. The recipient calculates the digest of the received message and compares it with the one that is obtained by decrypting the attached signature with the sender's public key: if the signature matches, it is authentic.

[14] ***DES:*** In cryptography the Data Encryption Standard (DES) is an encryption algorithm chosen as standard by the Federal Information Processing Standard (FIPS) for the United States of America in 1976 and later become internationally used. It is based on a symmetric key algorithm with a 64-bit key.
(source https://it.wikipedia.org/wiki/Data_Encryption_Standard)

[15] ***Hash function:*** The hash algorithm processes any number of bits. In computer science it is said that it processes "raw" data. (source: https://it.wikipedia.org/wiki/Hash)

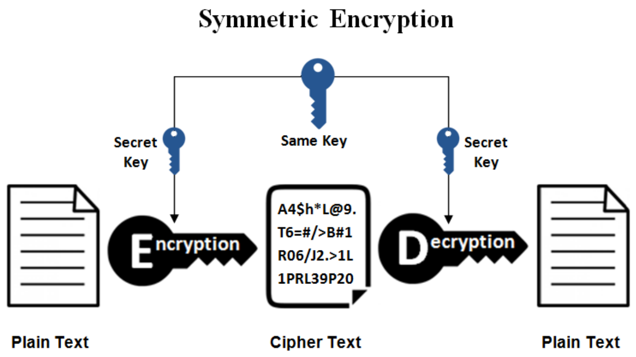


Figure 2.1: explains symmetric encryption (source: SSL2BUY)

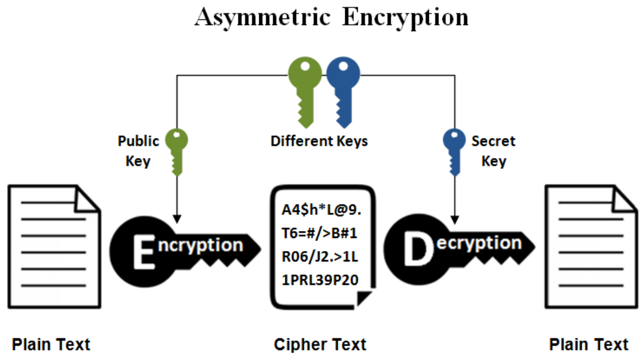


Figure 2.2: Explains Asymmetric Encryption (source: SSL2BUY)

Obviously, the technology used by Satoshi Nakatomo for Bitcoin and that used by other cryptocurrencies is the safest and therefore the asymmetric one.

2.1.2 Peer-to-peer network and distributable calculation

The peer-to-peer network is a computer network architecture in which a single user's computer can communicate directly with other users' computers. In a peer-to-peer network, the nodes are equivalent to each other, thus being able to perform functions both from customers and servants to all other nodes of the network, unlike the more common client-server architecture, in which communication it only takes place between client and server, and not even between client and client.

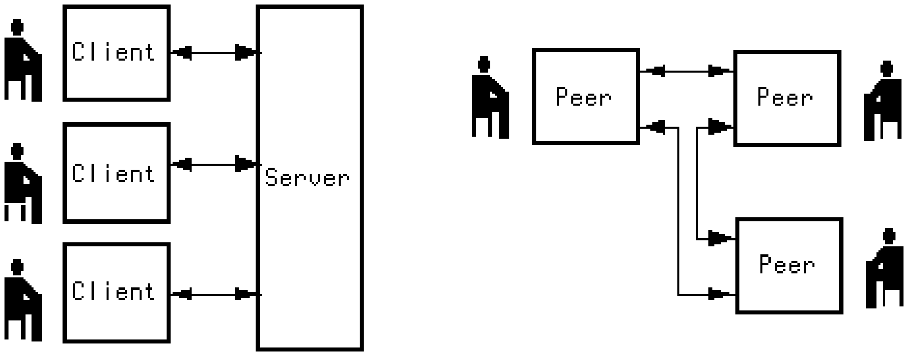


Figure 2.3: comparison between client/server architecture (left) and peer-to-peer architecture (right).

The absence of a central server that plays the role of custody of the managed and exchanged resources makes the p2p network a decentralized system, in which the control is transferred to each single node, and the information is distributed and shared between them through the application of specific algorithms. The p2p model is commonly associated with file sharing programs, but it is not the only application it can be used for. One of these can be distributed computing, which consists in solving computational problems of high complexity by exploiting the computing capacity provided overall by a set of autonomous computers interconnected by a network, just like the p2p network. The term distributed has a broad meaning and wants to indicate both the physical disposition in different geographical areas of the computers, and the autonomy of the processes they perform.

For this reason, the Bitcoin system and other cryptocurrencies can be defined as distributed, a set of autonomous computers connected through the Internet by a peer-to-peer architecture, which allows synchronization and control of the transaction log through the its sharing between the nodes. This control is thus decentralized and distributed, being achieved by solving complex cryptographic calculations by a network of self-contained computers, which provide the computational force necessary for this purpose.

2.2 Private and public keys and addresses

Generally taking advantage of the services offered by the many different Bitcoin wallet suppliers, the user is seen to assign a public address that must disclose whether he wants to receive and own bitcoins, only worrying about remembering the password protection to access his wallet and performing other procedures necessary for securing the same, in order to do not miss the chance to spend your digital money.

To better understand what happens you need to explain the function and the origin of these codes: that is a private key and a random 256-bit code that is used to digitally sign the bitcoin outputs. Only by owning the private key is it possible to spend some bitcoins associated with it. The key or private keys are stored on a computer or smartphone or at servers depending on the type of wallet the user enjoys.

Losing these private keys or not being able to access the file in which they are stored following the destruction of the PC or the loss, involves the loss of bitcoins associated with those keys and the inability to recover them. Similarly, theft of private keys can expose you to the risk of someone else spending those bitcoins.

The public key comes from the private key and comes in the form of a 512-bit code generated by the ECDSA[16] cryptographic algorithm (Elliptic Curve Digital Signature Algorithm). This technology is used to verify digital signatures on transactions, without having to disclose the private key, and is not disclosed until the transaction is digitally signed.

[16] ***ECDSA:*** In cryptography, the Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant to the Digital Signature Algorithm (DSA) using elliptical cryptography.
(source: https://it.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm)

Finally, the public key in turn generates the Bitcoin address at 160 bits through special hashing algorithms always aimed at ensuring security.

2.3 Blockchain

The blockchain is literally a set of blocks, in which a set of subjects makes available to other computer resources such as memory, CPU, band, to make available to a community of users a mainly public database. It exploits peer-to-peer technology and allows anyone to download, thus becoming a "node" of the network. It is essentially the accounting book in which all transactions made in Bitcoin since 2009 are made, made possible by the approval of 50% + 1 of the nodes. These single-block transactions occur continuously in the system, and on average every 10 minutes a new block is produced and attached to the chain, so that the blocks are arranged in chronological order starting from the block of origin, the so-called *genesis block.*

The same mechanism of the chain is also replicated for the transactions contained in the blocks, even if with some difference: in fact every transaction is not connected to its previous one in chronological order, but to its transaction-input, or to the previous exchange, or to the previous exchanges, which provided bitcoins to the receiver, so that they could subsequently become the sender in the transaction in question. The blockchain can be considered a system whose smaller and central particle is represented by the single transaction and proceeding to the outside it is found the block, which contains many of these transactions, and finally the multiple blocks that contain the history of Bitcoin from his birth. The structure and functioning of the blockchain represent the main and fundamental technological innovation in the field of distributed systems. It is therefore defined as an open system of verification that does not need the approval of the banks to carry out a transaction.

Extrapolated from its original context, the blockchain has been used in all areas in which a relationship is needed between several people or groups, with considerable success over the years.

2.3.1 Structure of transactions

Satoshi Nakamoto describes in a post the *"Electronic Token"* as *"a chain of digital signatures"* and adds that *"Each owner transfers the token digitally signing the hash of the previous transaction and the public key of the future owner and adding this information to the token term"*. So let's explain how does transactions work.

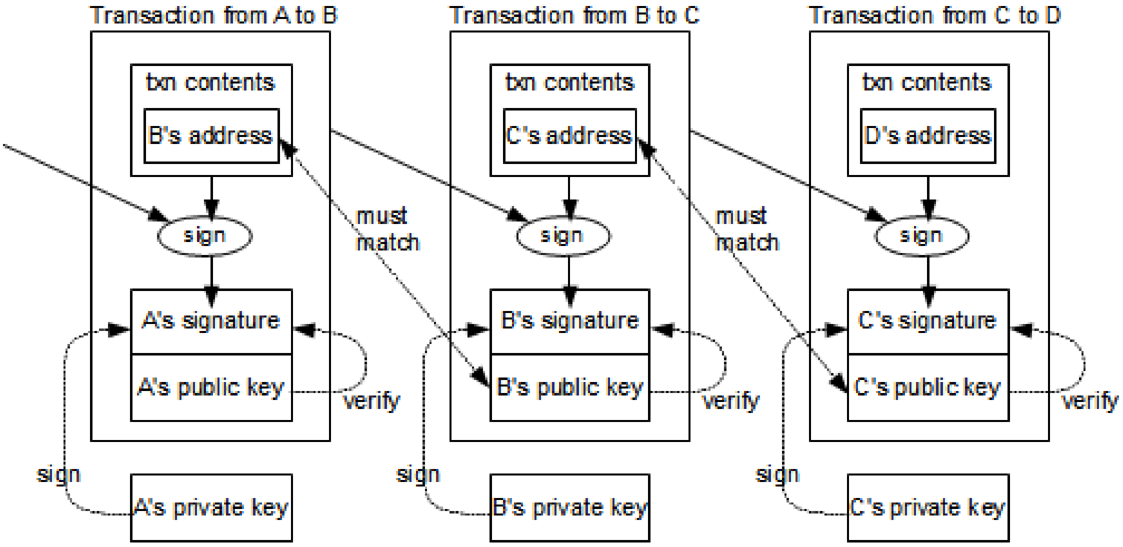


Figure 2.4: structure of Bitcoin transactions (source: bitcoin/wiki)

Considering for example 3 transactions **A**, **B**, **C** and considering the transaction from **B** to Central C, it is possible to reach the following conclusions:

- The transaction "from **A** to **B**" constitutes the input, which then allows **B** to implement the transaction from "**B** to **C**"; the **B** address stored in the first transaction must match the public key of **B** included in the transaction in object from which it derives.

- **B** authorizes the transaction by signing it with its own private key, thus verifying that the public key is the same. The public key of **B** comes into play only when **B** decides on the inputs that already belong to him.

- In this case **B** uses only one input, deriving from the previous exchange with **A**, but the transactions occur by redeeming several inputs and towards more than outputs, creating links chains between transactions that are much more complex. For example, **B** could have sent a larger number of **C** bitcoins; in this case it would have had to completely redeem the input received from A, as well as other inputs received from other individuals previously, until the bitcoin number to be sent to **C** is reached.

This transaction structure implies that bitcoins do not exist as a separate entity: a user can certainly say that he has 1 bitcoin, for example, but what it is noticed is that the specific user has bitcoin inputs that add up 1 bitcoin. By breaking down a single transaction stored in a block you can see how it appears to be a set of three main information:

1) **Header,** that is the identity card of the transaction, in turn containing the following details:

a) *Hash of the transaction:* hash identifying a specific transaction, that includes and summarizes all the information concerning the specific transaction. This code summarizes the following information as a whole: version number, list of inputs and outputs and the closing time of the block in which it is inserted *(lock time);*

b) *Number of the solved block* in which this transaction has been stored;

c) *Number of inputs:* number of the various previous transactions that supply the total amount of bitcoins used in the transaction in question;

d) *Sum of the bitcoins* resulting from the transactions described in point c);

e) *Number of outputs:* number of different Bitcoin addresses to which outgoing BTCs are sent;

f) *Total outgoing BTC:* sum of the outgoing bitcoins in the transaction in question;

g) *The measure of memory* of the transaction data in terms of physical space occupied on the disk. The Bitcoin system uses this measure to evaluate the measurement limit of the entire block and transaction costs;

h) *the amount of BTC* attributed to the block mining as a transaction fee, if any, represented by the difference between the total of the redeemed BTCs and the total of the outgoing BTCs.

2) **Detail of the inputs:** table listing the details of the transactions that provide the amount of bitcoin used in the transaction in question. In each line there are hash[17] of each transaction-input, amount transferred and Bitcoin address of the receiver. For each input is also the information *ScriptSig*[18].

3) **Detail of the outputs:** table listing the recipient Bitcoin addresses overall of the outgoing amount. In each row are indicated address of recipient, respective amount to these sent and hashes of the eventual transaction in which this is the input. For each output it is found also the *Script Public Key* information, which is a condition to spend the bitcoins referred to that output and is created by the sender.

There are some further considerations to do:

- *The "change" or rest of a transaction:* a user can have different outputs arising from different and previous transactions. The user will be intuitive know the bitcoin budget in his possession, so you can spend it on his own even if bitcoins are stored in the blockchain in the form of output of different transactions, so the various outputs are not joined to form the budget that instead appears within a single wallet. The purpose of this transaction structure is that each output contains the references of the public key of its owner, so that when the owner will want to spend, signing with his private key, the validity will be confirmed by the correct combination between public and private key. In general, the Bitcoin wallets, in the presence of remains, send these quantities to new addresses associated to the same user, which are *"drawn"* from the key-pool available to each wallet, also for the needs of anonymity of transactions. The question of the rest of the transactions becomes relevant when analysing the volume of bitcoin exchanges within the network. Since the "total bitcoin output" item also takes into account the bitcoins returning to the sender as a remainder, and therefore not actually spent, here is

[17] ***Hash:*** the hash is a non-invertible function that maps an arbitrary length string to a string of shorter length. There are numerous algorithms that perform hash functions with properties that depend on the application. (source: wiki/Hash)

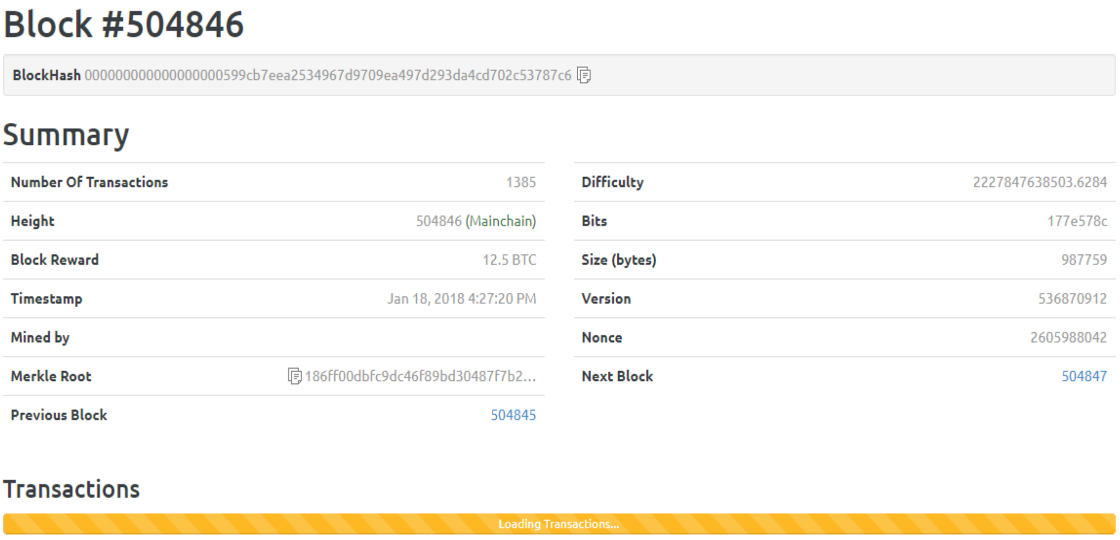
[18] ***ScriptSig:*** is the the first half of a script (source: wiki/transaction)

an analysis based on this data could be quite distorted by the real volume spent in the system, because in fact all the outputs of all the transactions would be computed, without considering that often the second output represents the change that returns in the availability of the sender.

- *Bitcoin transactions are divisible***:** fractions of bitcoin, and this also makes transactions of very low amounts possible depending on the exchange rate with other traditional currencies. The smallest unit is called *"Satoshi"* in honour of its creator, corresponding to 10-8 BTC (0,00000001 BTC).

2.3.2 Block structure

Each block consists of two main parts: the block header, and the list of transactions included in the block as shown in the figure below:



Block #504846

BlockHash 000000000000000000599cb7eea2534967d9709ea497d293da4cd702c53787c6

Summary

Number Of Transactions	1385
Height	504846 (Mainchain)
Block Reward	12.5 BTC
Timestamp	Jan 18, 2018 4:27:20 PM
Mined by	
Merkle Root	186ff00dbfc9dc46f89bd30487f7b2...
Previous Block	504845

Difficulty	2227847638503.6284
Bits	177e578c
Size (bytes)	987759
Version	536870912
Nonce	2605988042
Next Block	504847

Transactions

Loading Transactions...

Figure 2.5: example of a block structure (source: https://www.blockchain.com/it/explorer)

There are some points where to focus:

1) **Block Header:** represents the identity document of the block and contains the following information:

a) ***Number or height of the block:*** progressive number of the block added to chain. The blockchain starts with the genesis block, having number 0;

b) ***Hash:*** hash identifying a specific block;

c) ***Previous block hash:*** summarizes all the information of the previous block;

d) ***Next block hash:*** reference to the next block;

e) ***Time:*** date and time when the block was resolved;

f) ***Difficulty:*** parameter that measures the difficulty of solving the block, understood as the processing time necessary to solve the cryptographic problem in the mining operation;

g) ***Transactions:*** number of transactions included in the block;

h) ***Total BTCs:*** total number of bitcoins sent in block transactions, including transaction fees;

i) ***Size:*** memory occupied overall by the data of all the transactions included in the block;

j) ***Merkle Root:*** hash that summarizes all the transactions included in the block. The different transactions represent the *"leaves"* of the *merkle tree*[19];
k) ***Nonce:*** field used in the mining process, which will be discussed later.

[19] ***Merkle Tree:*** a hash tree or Merkle tree is a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic has of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash list and hash chain. (source: https://en.wikipedia.org/wiki/Merkle_tree)

The first transaction that appears in every list of any block is generally a transaction, different from all others, called a *coinbase*. This transaction represents the reward due to the miner that has solved the block, it has validated and included the last transactions occurred within a block, carrying out the so-called *mining* activity, which will be analysed in more detail during this chapter.

All the commissions of the packaged transactions in the block plus a fixed sum are due to the miner. The latter amount represents newly issued bitcoins, which therefore increases the total number of bitcoins present in the system. The coinbase is a different transaction as it has no input, while the reward plus commissions can be sent to either a single address or multiple addresses making it a standard transaction. For each block there is then a single coinbase that however cannot be spent until it has obtained at least 100 confirmations[20], then the production of at least another hundred blocks.

The reason for this waiting is precautionary, due to the possibility of the phenomenon occurring of the bifurcation of the blockchain *(fork).* Since mining is in fact a challenge in time about who among the nodes could to solve the current block first to win the coinbase, it can therefore happen that different nodes can find a different and valid closing solution of the current block in a very short period. Of consequently, two or more blocks are latched to the previously produced block different and valid, creating a bifurcation in the blockchain.

At this point the miners communicate the solution for closing the block to all the other nodes of the networks, which proceed to verify that there are no inconsistent transactions between those included in the last block and the previous ones recorded in the blockchain. If one of the two blocks include transactions that conflict with the previous ones, then that block does not receive confirmations, otherwise if both valid nodes choose one of the two, usually the first one that appears them in the respective devices.

The confirmation of a block is expressed by the miners simply by choosing which one to start from to lock the next block. It may happen that for short periods of time two parallel bifurcations develop, but between the two will prevail that where most of the total computational force will be used, and the miners who inadvertently were working on that

[20] ***Confirmation:*** a transaction receives a confirmation when it is stored in a block; to new product block and linked to the latter, this transaction receives an additional confirmation

other, will return to the main development. Blocks that are not part of the main chain are called *orphan blocks*, and the miners who created them are not entitled to receive rewards. For the possibility that you generate bifurcations from its acceptance as payment, even the coinbase attributed to the miner of the genesis block is not immediately expendable.

2.4 Mining

The answer to questions on how to make decentralized payment possible, how to make up for the absence of a central authority as a guarantor of currency and transactions and how to guarantee and nurture trust in a system so inherently different from traditional payment systems for the sensitivity to the security of money is mining.

Often, mistakenly reconnects mining activities to the production and emission of new bitcoins even if this is not the main purpose of this activity. In fact, the crucial objective of this process is to maintain the integrity and authenticity of the blockchain, which for users of the Bitcoin platform represents a real bank account. Only if this register can maintain the characteristics mentioned above, users can rest assured that that money belongs to them; if instead it proves to be fragile to counterfeiting attempts, for example aimed at the validation of several inconsistent transactions (*doublespending*), trust in the system would vanish and Bitcoin would be doomed to fail.

The mining activity can theoretically be done by anyone if a user installs the Bitcoin client on your computer. Mining literally exploits the computing power of hardware devices made available by network nodes. It is a difficult and time-consuming operation in terms of computer processing times, so that new blocks are produced within a fixed time frame, regardless of the number of transactions taking place in the network. In fact, if few transactions take place in the network, these cannot be put on hold until a certain threshold is reached, otherwise practicality as a payment system would vanish; moreover, the first mined blocks did not contain any transactions, except the Coinbase, to create and put in circulation the first units of currency.

For each production of a new block an established quantity of new bitcoins is issued, which belongs to the miner who first produced it. This total quantity also includes the total commissions of the transactions recorded in the block.

In short, mining was conceived by Nakatomo to secure the blockchain, and this security is made possible by how many "honest" nodes are present in the network, in order to make the work of "dishonest" nodes difficult if not impossible. instead they want to modify the register to their advantage to spend more times than the currency already spent.

The honesty of the nodes is "bought" by the same protocol through a specific system of attribution of rewards, which encourage such honesty.

Mining is a specific feature of the Bitcoin platform: in fact, other cryptocurrencies, such as for example Ripple, are issued on the market by the company that invented it.

2.4.1 What is Mining and how it works

The production of the new blocks to be attached to the blockchain and the issue of the emission of new coins are closely linked: in fact, the production of each new block corresponds to the new issue of a pre-set quantity of bitcoins.

In fact, all this process on the Bitcoin platform is clear and established. Regardless of how many transactions take place in the system, every two weeks an average of 2,016 new blocks must be produced, about 1 every 10 minutes, even in the absence of transactions. Moreover, every two weeks, if the new blocks produced deviate too much from the target number of 2016, the difficulty of producing a new block is revised downwards or upwards, depending on whether the output of new blocks has been lower or above 2,016. Also, the maximum ceiling of bitcoins in circulation is pre-established, and is about 21 million units, not yet all in circulation (there are in fact 17,232,875 bitcoins in circulation[21]). Finally, the quantity of new bitcoins emitted at each production of a new one is also fixed block. This reward originally stood at 50 BTC per block, but progressively halved every 210,000 new blocks that equate to

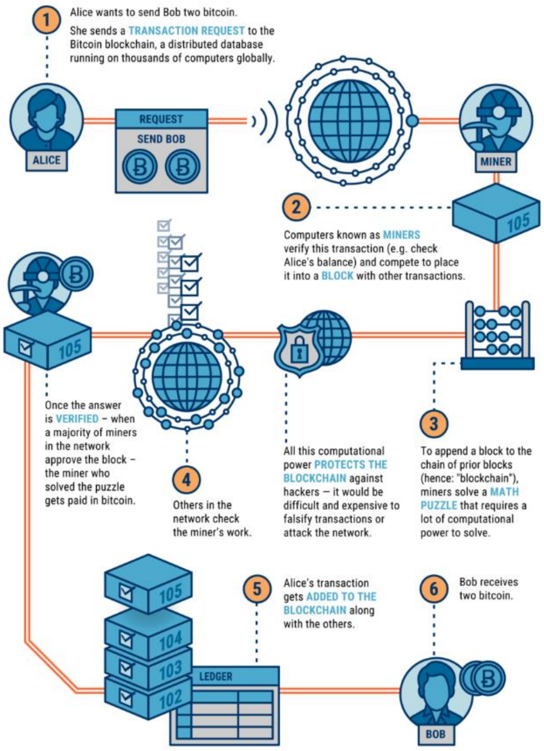
[21] Source: https://www.blockchain.com/it/charts/total-bitcoins, 27/08/2018

approximately a 4-year period. When the reward is close to zero in the future, the only remuneration for miners will be transaction fees.

It is estimated that in 2040 the reward for each block will be less than 0.5 BTC, so the future of Bitcoin will depend on the diffusion that it will obtain as a payment system, as only if many transactions will take place will the miners be encouraged to continue their activity.

2.4.2 Mining Rules

Mining consists of a set of activities aimed at the correct and constant registration of the transactions that take place in the system. These activities are based on the resolution of a proof-of-work, i.e. the task to be performed on your computer that requires processing time. In particular Bitcoin imposes the resolution of a cryptographic algorithm very similar to the *hashcash function*[22].



1 Alice wants to send Bob two bitcoin.

She sends a TRANSACTION REQUEST to the Bitcoin blockchain, a distributed database running on thousands of computers globally.

2 Computers known as MINERS verify this transaction (e.g. check Alice's balance) and compete to place it into a BLOCK with other transactions.

3 To append a block to the chain of prior blocks (hence: "blockchain"), miners solve a MATH PUZZLE that requires a lot of computational power to solve.

All this computational power PROTECTS THE BLOCKCHAIN against hackers – it would be difficult and expensive to falsify transactions or attack the network.

4 Others in the network check the miner's work.

Once the answer is VERIFIED – when a majority of miners in the network approve the block – the miner who solved the puzzle gets paid in bitcoin.

5 Alice's transaction gets ADDED TO THE BLOCKCHAIN along with the others.

6 Bob receives two bitcoin.

Figure 2.6: How does proof-of-work works (source: cbinsights.com)

[22] ***Hashcash function:*** work test system proposed by A. Back in 1997, used to make it expensive in terms of processing time, and therefore of energy consumed, sending spam by email.

The problem has the characteristic of being difficult and expensive to solve, but once the solution has been found, check its validity and it is very easy. This task consists in having hashed a series of specific data of the block header; the resulting hash to be valid must meet the criteria. First The information fields to be hashing are the following:

- Version Number (4 bytes)
- Previous Hash Block (32 bytes)
- Merkle Root (32 bytes)
- Time (4 bytes)
- Bits (4 bytes)
- Nonce (4 bytes)

For a total of 80 bytes that gives life to the next block hash.

The *merkle root*, as seen above, is the hash that summarizes the list of transactions included in the block, including the Coinbase. To do Mining on a block containing only one transaction does not make mining activity faster, so miners will be incentivized to include many transactions, to make their own commissions.

So, when a hash is found that respects the target is equivalent to winning a lottery, because each new attempt that mean an increment of the nonce that doesn't change the probability of solving the block that remains the same. Mining is a problem that must be solved for brute-force, that is, for continuous attempts until an acceptable solution is found.

This system of rules that miners must respect to produce a new block. However, it is necessary for the pre-established times (10 minutes) to be respected.

Recapping the mining process can be broken down into the following steps:

- transmission of transactions to the nodes thanks to the p2p technology;

- Collection from each node of the transactions and production of a new block, processing the merkle root of that specific list to be added next coinbase, and building the input table (block header) that will be submitted to hashing;

- Proof-of-work that can be considered resolved when the hash is lower than the target. The solution is then communicated to the other nodes that were simultaneously working on the solution of the same block;

- The nodes check that the new block does not include inconsistent transactions, and validate the block using the hash to proceed with the production of the block following, continuing in this way the further development of the blockchain, starting over with the resolution of another block.

2.4.3 Solo-mining, pool-mining and cloud-mining

There are three main macro-refinements of mining activity:

1. ***Solo-Mining:*** mining in this case is carried out "solo", individually, in order to win both the reward that sum of the transaction fees included in the new block. The high competitiveness and complexity of mining requires for this specific alternative important investment in computational power (hardware). The greater the power available, the greater the probability of solving blocks and obtaining profits. However, mining-only is a high-risk activity that does not guarantee continuous cash flows since there is a lot of competition as previously mentioned and the problem to be solved is very complex.

2. ***Pool-Mining:*** instead of individually undermining it is possible to do it collectively, joining a *mining pool*, in which several subjects make their own available calculation

power and the profits are divided proportionally to the contribution provided. Pool-mining allows you to participate in mining even if you do not have it a high calculation capacity, which is necessary for mining only. Generally, this second alternative guarantees smaller but continuous bitcoin revenue streams.

3. ***Cloud-Mining:*** it is also possible to participate in the mining activity without possessing materially necessary hardware devices, eliminating problems related to maintenance and physical placement of such equipment. Through cloud mining it is possible to hire a certain amount of computational power and make profits of it in exchange for a fixed rent.

But how much does it cost to produce a Bitcoin today? In addition to the bitcoin prices, mining costs also rose dramatically, both in terms of energy and hardware.

If until a few years ago a good computer was enough to produce Bitcoin, today it requires thousands of powerful processors and graphics cards. Nowadays the specific extraction of bitcoins has been developed computers with specific processors already mentioned above, called ASIC (application-specific integrated circuits); these processors, in addition to having a high cost, also entail a high consumption of electricity.

According to some studies, the energy required by the Personal Computers to validate a single transaction can reach up to 215 kWh. Considering that around 350.000 Bitcoin transactions a day are completed around the world, energy consumption is comparable to that of some entire countries. Mining bitcoins therefore means using considerable amounts in electricity as well as the wear and tear of hardware components.

Bitcoin miners will therefore still have an advantage in continuing mining operations until the cost of producing a single bitcoin will equal its current exchange price.

It should be emphasized that the energy and hardware costs are constantly increasing each year, while the bitcoin reward for this activity is constantly decreasing, as mentioned previously, in fact the reward is decreasing over time: in fact, the initial reward for mining activity was set at 50 bitcoins per block, then passed to 25 bitcoins in 2012 and finally to 12.5 in 2016.

If the price of bitcoin does not continue to rise over time, producing bitcoins would become less and less convenient.

2.4.4 Transaction commissions

One of the main features of Bitcoin, which differentiates it from all the other existing electronic payment systems are the low transaction fees. The sum of the commissions of the transactions verified and recorded in a block reimburse, together with the fixed share of new bitcoins, the work done by the miners.

Given that in the future this fixed portion is destined, as already mentioned, to gradually decline until it is close to zero, as a threshold of around 21 million bitcoins in circulation is foreseen, the miners' remuneration is destined to consist only of commissions of transaction. At that point Bitcoin will continue its proper functioning only if its dissemination and use as a tool for payments will be such as to guarantee the miners an adequate remuneration, so that they will be encouraged to continue their fundamental activity in the future. These fees are the responsibility of the sender, but many transactions may also not provide for no commission, if they meet certain conditions.

The size of the commission depends on the priority given to the transaction, and this priority is established through the weighting of the following factors:

- *"Age" of inputs:* one input is considered older than another if it has not been spent for a long time;

- *Size:* depends on the number of inputs that will be spent in the transaction and the number of recipient outputs, including the output of the change. Transactions that spend older inputs and have higher outputs will have higher priority than transactions that spend more recent inputs and have small amounts.

A transaction can also be processed without including a commission if it complies with the following conditions:

- It has a size of less than 1000 bytes;
- The outputs are at least 0.01 BTC;
- Priority reaches a certain level.

Technically, even all other transactions, while not respecting the parameters mentioned above, they can be prosecuted without including a commission, but the positive or negative outcome will depend only on the miners, as they may never be accepted and therefore never be included in a block. The recent versions of the Bitcoin client, regarding the wallet, are programmed to automatically include a commission depending on the transaction that is about to be processed, while as far as mining is concerned, they can recognize if this transaction has an adequate commission or not.

A *"standard"* transaction generally involves a tax of 0.0001 BTC. By *"standard"* it is intended within the threshold of 1,000 bytes, since each input weights 148 bytes, each output 34 bytes, and to the total must be added 10bytes by default. It must also be borne in mind that on average, transactions weigh approximately 500 bytes. For transactions that they include more inputs or send money to more recipients, exceeding the threshold of 1,000 bytes, it is recommended to include a higher commission.

The existence of a tax, as well to encourage miners considering the transaction in question and include it as soon as possible in one block, also serves to deny the so-called *dust spam*. This type of spam is an attack of type *denial of service*[23], which can be made by anyone who has an interest in the malfunctioning of the system and wants to undermine its stability, and consists in processing very many transactions that go to the same number of addresses but to

[23] ***Denial of service:*** malfunction due to a cyber-attack in which the resources of a computer system that provides a service to clients, such as a web site on a web server, are deliberately depleted until it is no longer able to provide the service to the requesting clients. (source:wiki/denial_of_service)

volumes of bitcoin irrelevant lower than the one-hundredth of fiat currency, increasing the size of the blockchain and making mining more wasteful without an actual purpose of money transfer.

2.4.5 Honesty and Dishonesty of the nodes

The functioning of Bitcoin as a decentralized system depends, however, primarily on the honesty of the nodes that verify and validate the transactions, excluding any possibility of *doublespending.* A node is *honest* if it uses its own computational force to produce blocks that do not contain inconsistent transactions with each other or with those previously recorded in the blockchain, and if they contribute to the mining of the blocks to be hooked to the progressively longer chain. The longest chain of blocks, from the genesis block to the current block, manifests the majority, understood as that sequence of blocks that required the greatest computational effort to be produced as well as the adhesion and acceptance of that track block after block, and the will to continue to lengthen it.

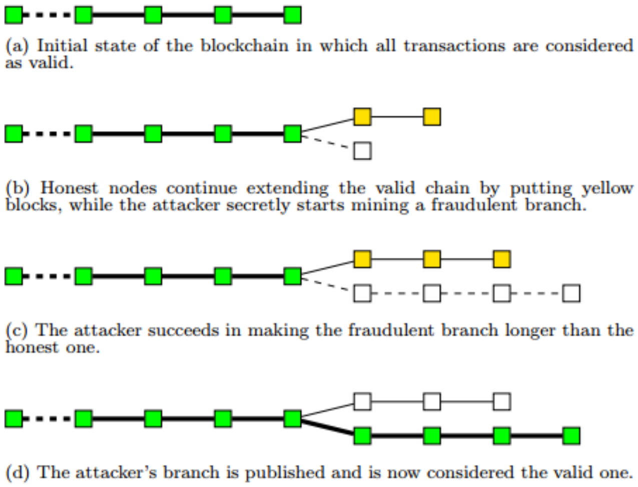
However, if a node wants to behave in a dishonest way, not having the private keys related to the addresses of high users of Bitcoin, cannot simply subtract funds from others and credit them in their address. His job is to collect the transactions and register them, but for example it would be impossible to tamper with a single transaction and credit the amount to his address, because the encryption to protect the system is practically unavoidable, considering that it is impossible to obtain the private key from the public one or from the address. The only way to steal a user's funds by clearing the address is to launch an attack on Bitcoin-related services such as wallets or exchange trying to steal private keys as already happened in the past. In these attacks is not in fact the blockchain to be targeted, but computers, or servers any "place" in which a private key can be stored. There are two types of attacks that a dishonest node could try to commit:

1) ***Double spending attack:*** With this type of attack, the dishonest miner has the objective of defrauding a specific user who believes he has received the payment, only to find out in a subsequent moment that the transaction was unsuccessful; the miner in question and the trader's customer target of the attack, so it will be called a node / customer.

The double-spending as already mentioned several times is the possibility of spending the same unit of digital currency more than once, problem that is resolved in a decentralized way by Bitcoin through the holding of the blockchain, which however is vulnerable to this type of attack. When a block is resolved, the transactions contained therein are said to be confirmed once, and each block that is added to the latter receive confirmation more. The confirmation is basically the proof that the miners have accepted that version of the blockchain and are working to continue its *"history"*.

Since there is the possibility that bifurcations can be created in the chain and a version of the blockchain will prevail rather than the other one, a transaction cannot be considered safe from the double-spending until he has received a certain number of confirmations.

Taking advantage of this aspect the dishonest node, it could score a double-spending attack in the following way:



(a) Initial state of the blockchain in which all transactions are considered as valid.

(b) Honest nodes continue extending the valid chain by putting yellow blocks, while the attacker secretly starts mining a fraudulent branch.

(c) The attacker succeeds in making the fraudulent branch longer than the honest one.

(d) The attacker's branch is published and is now considered the valid one.

Figure 2.7: double spending attack steps

- The node / customer processes a transaction in favour of the trader

- The dealer sees the transaction in his favour appear in the blockchain about ten minutes, and then received confirmation;

- The trader who ignores the client's bad intentions may already proceed to the sale of the property, regardless of whether one or two confirmations do not guarantee at 100% the payment;
- Even before the first transaction is included in a block, the node / customer works secretly (strategy called selfish mining[24] or stealth mining) the production of another block containing a second transaction that sends the same bitcoins to a different account that belongs to them, excluding the first transaction that will be inconsistent;

- The node / customer only reports to the network the first transaction since it already exists working secretly to the block that will include the second transaction, otherwise the nodes would see that the former is inconsistent with the second and the trader would not see any confirmation;

- It will then produce a bifurcation formed by a block containing the first transaction called A, and another containing the second transaction called B;

- For this attack to succeed it is necessary that the bifurcation originated from the block containing B is longer than the other, due to the fact the longest chain represents the greater effort spent from the genesis block to the current one and therefore the majority and for this to happen, it may require the node / client to undermine further blocks successive ones in order to beat the parallel chain;

- At that point the other honest nodes will go to work on the chain in which it is present B, while the blocks of the other bifurcation will become orphans, and since A is inconsistent with B, and B has already received confirmation, it will be rejected by the network, with negative consequences for the trader who will see the product unpaid.

[24] ***Selfish-mining:*** strategy through which a miner intentionally creates a bifurcation in the blockchain, solving a block but not communicating the solution to the other miners. The selfish-miner will produce new ones blocks to hook to its private chain, to release it in the network when it is longer than the public one. If he succeeded, he would make all the work done by the honest miners vain from the beginning of the bifurcation up to that point, making own all the rewards for the resolution of the new blocks. Selfish-mining is a mining strategy, difficult to implement but anyway possible, thus representing a system vulnerability.

On the other hand, regarding the probability of this attack being successful, they have been described in the bitcoin paper by Satoshi Nakamoto who describes this problem from a statistical point of view, reaching the following conclusions:

- If the power of the node / customer power of the honest nodes, that is, if h is greater than 50%, the attack will be successful in 100% of cases regardless of n confirmations.

- Given a number n of confirmations, the greater the computational capacity h possessed by node / customer, the greater the probability that the attack will succeed; date h (lower at 50%), with the increase of n the probability of success of the attack decreases;

- Given the different levels of computing power of the node / customer, a trader should wait to wait for the following n confirmations because the risk of being defrauded falls below 0.1%.

Regarding the possibility of a double-spending attack, the *"Bitcoin developer guide"* available at bitcoin.org believes that at least six confirmations should be expected to consider a secure payment from this type of attack, considering the enormous computing power that the node / customer should possess in order to replace six blocks, but it is up to each dealer to decide how many confirmations to wait, especially in relation to the amount of the transaction.

2) ***51% attack:*** It is the situation in which a single node (or an organized whole) comes to dispose of more of the goal of the total computational power of the network. Consider that it is not necessary to hold precisely 51% of the *hash rate*[25] but just to overcome the majority to be able to launch this type of attack. This eventuality represents a threat to the stability of Bitcoin, as such a node, for as long as he possessed more than half the power, he would have the power to:

[25] ***Hash rate:*** By hash rate we mean the unit of measurement of the processing power of the Bitcoin network. For security purposes the Bitcoin network must perform intensive mathematical operations. When the network reaches a hash rate of 10 Th / s, it means that it can perform one trillion calculations per second. (source: https://bitcoin.org/it/glossario#hash-rate)

- Always succeed in a double-spend attack, regardless of the number of confirmations expected by the trader, as he will always be able to secretly build an alternative chain longer than the honest one;

- To exercise the monopoly of the mining activity, never considering the blocks eventually produced by the other miners, sure that in the distance its chain would always be longer than that of the others, making own all the rewards;

- Deciding not to include any transaction, or even any, within its blocks, strong that "his" chain will always win. In fact, it could only produce empty blocks, relegating all the transactions processed by users to zero confirmations. Certainly, a miner holding such a computing power could also decide to remain honest, having in any case a chance to resolve each new block exceeding 50% and therefore a very high expected profit. Moreover, all the other miners would have no reason to continue their business and waste time and electricity without getting remuneration, while the trust in Bitcoin as a payment system would vanish very quickly.

The following figures[26] explain the five steps of these attacks:

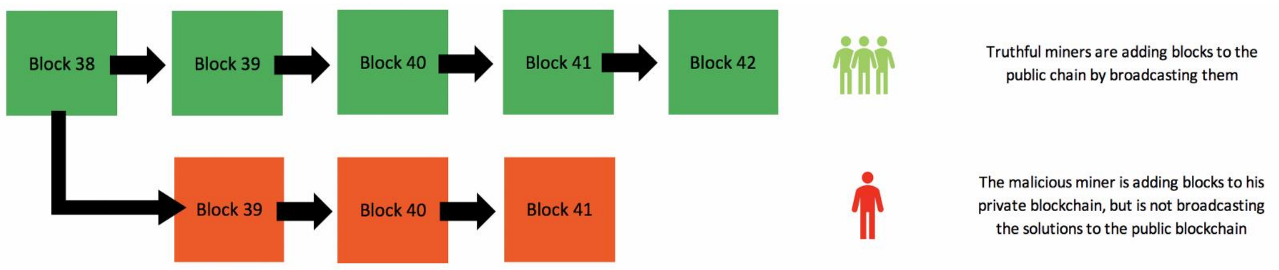
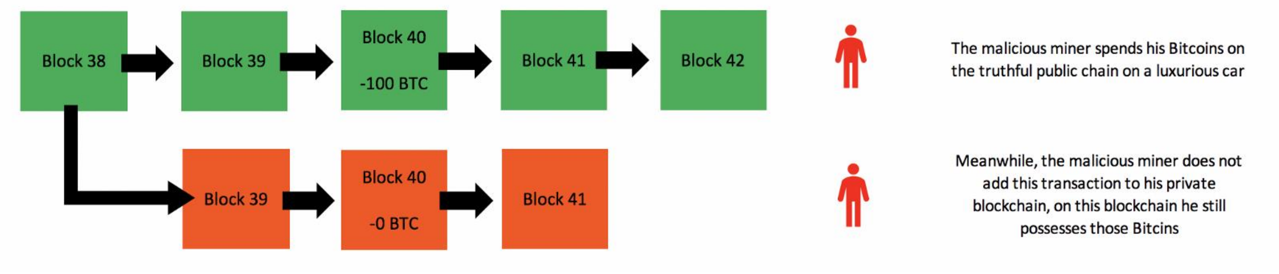
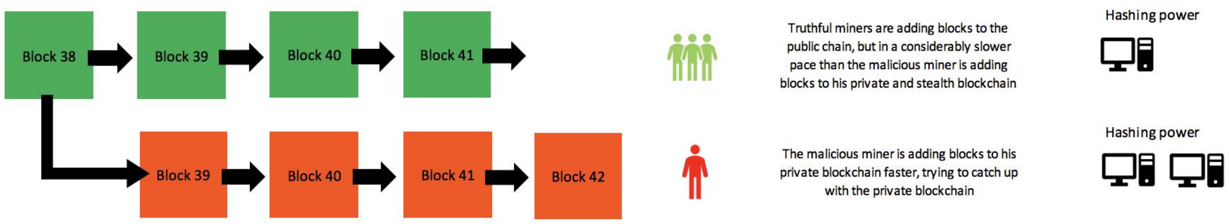

Block 38
Block 39
Block 40
Block 41
Block 42
Truthful miners are adding blocks to the public chain by broadcasting them
Block 39
Block 40
Block 41
The malicious miner is adding blocks to his private blockchain, but is not broadcasting the solutions to the public blockchain

Figure 2.7: Explains that there are two versions of the blockchain and the red one must be considered the *"hidden"* one.


Block 38
Block 39
Block 40
-100 BTC
Block 41
Block 42
The malicious miner spends his Bitcoins on the truthful public chain on a luxurious car
Block 39
Block 40
-0 BTC
Block 41
Meanwhile, the malicious miner does not add this transaction to his private blockchain, on this blockchain he still possesses those Bitcins

[26] Source of the figures 2.7, 2.8, 2.9, 2.10, 2.11: medium.com

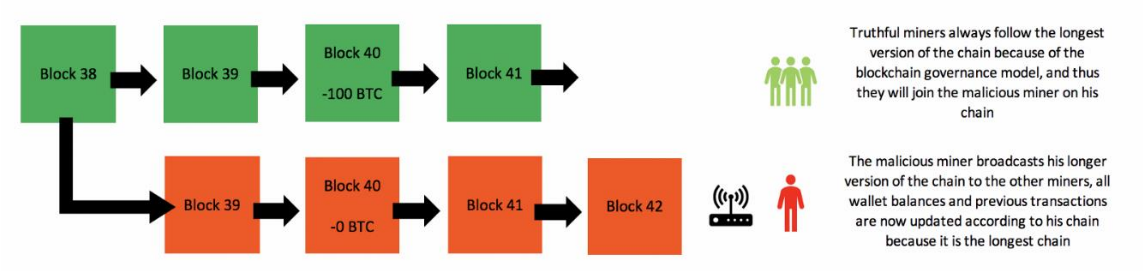
Figure 2.8: the malicious miner doesn't add the transaction to his private blockchain.



Truthful miners are adding blocks to the public chain, but in a considerably slower pace than the malicious miner is adding blocks to his private and stealth blockchain

The malicious miner is adding blocks to his private blockchain faster, trying to catch up with the private blockchain

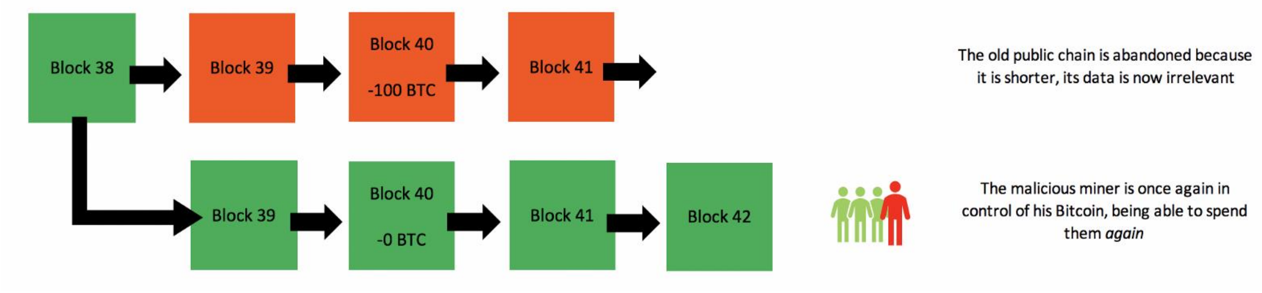
Figure 2.9: explanation when there is more hashing power



Truthful miners always follow the longest version of the chain because of the blockchain governance model, and thus they will join the malicious miner on his chain

The malicious miner broadcasts his longer version of the chain to the other miners, all wallet balances and previous transactions are now updated according to his chain because it is the longest chain

Figure 2.10: broadcasting the hidden chain



The old public chain is abandoned because it is shorter, its data is now irrelevant

The malicious miner is once again in control of his Bitcoin, being able to spend them *again*

Figure 2.11: changing the chain *(doublespending).*

But these kinds of attacks are extremely difficult to perform. As described above, a miner will need more hashing power than the rest of the network to achieve this goal. Considering that there are millions of miners on the Bitcoin blockchain, a dishonest miner would have to spend a very huge amount of money on mining hardware to be competitive with the rest of the network. Today the most powerful computers in the world are not directly competitive with the total computational power of the network.

There are countless other arguments yet against the execution of a 51% attack. For example, the costs of electricity, the rent of space and the storage of all mining hardware, to cover traces and money laundering. An operation like this is simply too demanding for what the attacker will give in return, at least in the case of Bitcoin's blockchain.

3. Cryptocurrencies economy

The technological innovation introduced by Nakatomo, with Bitcoin, has led to the creation of a real ecosystem around this new payment system. An ecosystem in continuous evolution, formed by different actors with respect to the world of traditional payments and new business models generally focused on obtaining and on services concerning the use, exchange and investment of bitcoins or other alternative cryptocurrencies. The economy of these cryptocurrencies is young but in constant turmoil and there are several actors that gravitate around this world:

- ***Developers:*** contribute to the development and improvement of systems from technical point of view and the resolution of the vulnerabilities that are discovered.

- ***Miners:*** allow the operation of some systems by validating and registering transactions in the blockchain, creating and obtaining new units as a reward evaluates according to the methods already described. The profit opportunity offered by mining has attracted many subjects and many resources, especially since the second half of 2013, which has become a real entrepreneurial activity, thanks also to the introduction in the market of equipment designed specifically for this purpose.

- ***Users:*** all the subjects that for different purposes and needs use the various systems, from the merchants who accept them in exchange for goods and services, to the people that conserve them for speculative purposes

- ***Wallet services providers:*** provide different types of portfolios electronic, designed for different needs, so that the user can receive, send or keep bitcoins.

- ***Exchange platforms:*** purchase and sale service in exchange for various legal currencies, other cryptocurrencies or precious metals. These are generally non-financial corporations.

- ***Financial services providers:*** online platforms that offer investment opportunities on cryptocurrency. These subjects facilitate access to the crypto world, facilitating investment in start-ups or in specific financial products, from ETFs to derivative products that bet on the price trend of bitcoins.

- ***Payment processors:*** services that facilitate the acceptance of cryptocurrencies like means of payment for both physical and online stores, also offering services such as the immediate change in legal currency, to avoid burdening the risk arising from the volatility of the cryptocurrency price in the merchant's financial statements.

- ***Other subjects:*** category of subjects indirectly involved in the environment, but important to identify the overall turnover. Among these can be found companies that manufacture specific hardware for mining, wallet and ATMs, those that develop software with different applications in the use of currency, and finally all the start-ups that take advantage of the various technologies, that of the blockchain as a basis for new applications, different from those of payments.

3.1 Evolution over time: the ICOs

With the passing of the years from 2009 to today Bitcoin has literally left its mark, opening up a new world of opportunities. In fact, the cryptocurrencies have taken more and more foot moving from the only Bitcoin to 1856[27] today. All this was made possible by the so-called ***Initial Coin Offering*** (ICO), which is an unregulated crowdfunding medium in the financial sector. The first ICOs were introduced to allow the collection of new funds for the creation of new cryptocurrencies, but the current ones are also used for other purposes. In principle, tokens[28] of the new currency to be issued in exchange for money are sold to enable it to be launched. The ICO differs from the *Tender Offer* (TO) because the first is not regulated by the States and this could lead to the lack of a guarantee on the property or other rights.

[27] Source: https://coinmarketcap.com/all/views/all/, 21/08/18

[28] ***Tokens:*** "coin" that the company sells on the market at a certain chosen price. Those who purchase them become a shareholder of the company.

The first ICO was made in 2013 for the launch of the cryptocurrency *Mastercoin*, followed in 2014 by that of the cryptocurrency Ethereum. This new technique has become increasingly popular, so much so that as of May 2017 there are approximately 20 ICO per month.

In table 3.1 below it can be seen that at the regulatory level on ICO there is still a long way to go, also considering the controversies of some countries that refuse to take hold of this new technique:

Jurisdiction	***Comments***
Australia	ASIC issued a guide in September 2017 establishing that the legality of an ICO depends on detailed circumstances
Canada	It’s working on legislation for ICOs.
Cina	On September 4, 2017 7 Chinese financial regulatory organizations ban any ICOs in China, requesting that the money be returned to investors otherwise they will be "severely punished according to law" This action by Chinese regulators resulted in large sell-offs for most cryptocurrencies. Prior to the Chinese ban, ICOs had raised nearly $ 400 million from about 100,000 Chinese investors. A week later, however, I will be the only one that ICOs is only temporary until ICO regulatory policies are in place.
South Korea	The Financial Services Commission has banned ICOs in September 2017 and promises "severe penalties" for those who violate them.
UAE	The Abu Dhabi Global Market has established an official guide on ICOs in October 2017.
France	Since October 2017, the Autorite des marches financiers (AMF) has been working on government regulations for the use of blockchain technology in capital transactions.
Hong Kong	The Securities and Futures Commission established in September 2017 that "tokens" (coins) may constitute securities for purposes of the Ordinance on "Securities and Futures", in which case, managing token is a regular activity under Hong Kong’s law.
Isle of Man	He is working on legislation for ICOs.
New Zeland	In October 2017, the Financial Markets Authority (FMA) issued guidelines on the current regulatory environment for ICOs.
USA	In July 2017, the U.S. The Securities and Exchange Commission (SEC) indicated that it could have the authority to apply the Federal Security Act on ICOs. The SEC

Jurisdiction	***Comments***
	does not stipulate that all blockchain tokens can be considered "securities", but this should be verified on a case-by-case basis. SEC action could encourage "mainstream" investors to invest in ICOs although iCOs usually discourage US investors from participating
Switzerland	Although Switzerland previously had a friendly jurisdiction over ICO, the Swiss Financial Market Supervisory Authority announced in September 2017 a survey of a series of unspecified ICOs, which will examine whether they are compliant with Swiss regulations.

Table 3.1: ICO regulation in various countries (source: https://it.wikipedia.org/wiki/Initial_coin_offering)

3.1.1ICO regulation

In the light of the measures referred to above by the national supervisory authorities, it appears necessary to understand the expectation that the lenders have in buying the tokens offered for sale. In particular, the examination concerns the rights that the token incorporates, rights that are dependent on the project and the business model that the company proposes. Juridically, a token is a digital information that typically confers a property right to a subject about the information itself, which is registered on a Blockchain (or other distributed register) that can be transferred via a protocol and, finally, can incorporate (or not) other additional rights. Thus, three token classes can be identified:

- ***Class 1 token (no counterparty):*** the token (which in this case is a real coin) can be transferred through transactions on Blockchain which guarantees the non-modifiability of the same. This type does not confer rights towards a counterparty but has only the function to register a property right of the token itself or the existence (on Blockchain) of a given subject / object. In particular, the token does not represent any underlying assets nor does its owner have any rights other than that owned by the token. This category includes the native cryptocurrency tokens which constitute exchanges and representations of value that can be exchanged between different subjects. Examples are *Bitcoin, Bitcoin Cash, Litecoin.*

- ***Class 2 tokens (rights to counterparties):*** tokens in this category give owners the rights to exercise against or the person who generated the tokens or to third parties. Some examples can be:

    1. ***Tokens for payments of a specific amount:*** in these cases the holder has the right to receive a payment for a specific amount (like the exchange certificates known in our legal system);

    2. ***Tokens for future payments:*** gives the right to receive future payments, based on certain conditions;

    3. ***Tokens for the provision of services or receipt of goods (including intangible assets):*** the holder has the right to receive a certain service or good from the issuer or a third party who has entered into commercial agreements with them. This area also includes tokens for access to IT infrastructures, which may also have the characteristics of native cryptocurrency, and give the possibility to use a specific Blockchain infrastructure;

    4. ***Representative asset tokens:*** represents the right of ownership of a particular asset (tangible or intangible) and may also represent shares of the legal entity issuing or of third parties.

- ***Class 3 tokens (co-ownership rights):*** the last category concerns tokens that have a mixed function, as they represent a property but also confer different rights, such as voting rights, economic rights, etc. In this type the holder does not have a right that can be exercised to the issuer of the security or to a third party.

In Italy, on the other hand, it can be seen differences in treatment in the following terms:

- ***Class 1 tokens:*** as specified above, this type does not confer rights towards anyone and has the characteristics typical of virtual currency. In such hypotheses, for the purpose of a first definition and regulation, it is possible to refer to the recent modification of the so-called discipline anti-money laundering, descripted in the ***Legislative Decree 25/5/2017, n. 90*** which amended the ***Legislative Decree n. 231/2007***, inserting the definition of *"virtual currency"*, as *"the digital representation of value, not issued by a central bank or by a public authority, not necessarily connected to a currency having legal tender, used as a medium of exchange for the purchase of goods and services and transferred, stored and negotiated electronically"*. The definition is used in the legislative decree in question to declare applicable the rules set forth in it to *"service providers related to the use of virtual currency, limited to the performance of the conversion of virtual currencies from or into currencies with a forced price"*. When a person operates in Italy, he must register in the currency exchange list and must apply the provisions of the so-called discipline. anti-money laundering both regarding customer due diligence and to reporting suspicious transactions. Therefore, the realization of an ICO on token of class 1 requires that the sale of the token takes place in Italy through subjects authorized to the currency exchange activities which provide for the fulfilment of the obligations under the anti-money laundering regulations.

- ***Class 2 tokens:*** within this class there are different types, all of which have in common the fact that the token owner is entitled to either the issuer or third parties. In reality these rights can be configured in the most varied way and it would be simplistic and certainly incomplete to attempt to carry out a comprehensive analysis of their composition. It is possible, however, to try to identify "subclasses" in which to outline, in broad terms, the applicable discipline:

    - ***Class 2.a tokens:*** tokens that confer the right to a specific payment or to future payments, token representing assets. Depending on how the token is configured, it may be included in the category of transferable securities, financial instruments or similar or as a participatory tool for risk capital. This would make applicable the various provisions of company law, of the TUF - ***Legislative Decree No. 58/1998*** and the rules regarding the appeal to the savings public, with particular reference to the obligation to draft and communicate an information prospectus, to the application of the MIFID directive and to the regulation of the issuers contained both in the same TUF both in the ***Consob regulation no. 11971/1999.*** In the case of the offer of equity risk capital instruments, in addition, an ICO placed through an exchange could be in conflict with the Italian law on equity crowdfunding dictated by the ***law December 17, 2012, n. 221*** and by ***Consob regulation no. 19520/2013*** which establishes the possibility of resorting to this form of collection only in favour of particular types of companies such as start-ups or innovative companies and through online portals managed by persons registered in a special register held by Consob. On the other hand, if the token cannot be assimilated to a financial instrument, it is always necessary to verify that it does not fall within the rules relating to the collection of public savings, this activity reserved for banks.

- ***Class 2.b tokens):*** token for the provision of services or the receipt of assets and tokens representing assets that are not financial or participative instruments. In this case the ICO regulations do not assume the connotations of the offer of a financial instrument, but confers the right, towards the issuer of the token or third parties, to receive a certain service or to use an asset. Basically, in the Initial Coin Offering phase, various formulas are proposed with which they assure advantages to buyers who acquire the tokens compared to the subsequent users. These are cases that by analogy could be reported to crowdfunding, in the form of the reward crowdfunding that is traced back either to the discipline of modal donation or to the sale of future things. In these hypotheses the Initial Coin Offering is a real offer to the public. and the services can take the most varied content, making it difficult to frame the contract that is concluded with the purchase of the token within a typical case assuming instead the character of mixed store, however regulated by the contractual autonomy of the parties.

The content of the service, therefore, will be that established by the party that promotes the offer by binding to the public to lend, even in the future, the obligations deducted in the contract itself.

- ***Tokens Class 3:*** tokens that confer co-ownership rights. The owner in this case has a property right on a smart contracts platform over a series of *"ancillary"* rights. These rights are not directed towards the issuer but are handled automatically by the platform itself. Moreover, the holder can be granted an economic compensation deriving from the use by third parties of the platform. It is, in all evidence, a situation attributable to the communion, being able to be seen the smart contracts platform as the undivided asset on which the individual holder exercises his rights in conjunction with the other owners.

The Initial Coin Offering, which quickly spread during the second half of 2017, certainly represents a new opportunity for companies to raise capital in order to carry out industrial projects. The "market" that has recently developed in the context of altcoin that is token alternative to the more known Bitcoin and the success and diffusion of such instruments, have meant that the majority of the supervisory authorities suspiciously look at the new phenomenon, on the other hand aware that this is a new opportunity to raise capital on the part of companies that should not be completely prohibited.

3.2 Cryptocurrencies regulation problem all over the world

Cryptocurrencies have long been at the centre of the international debate to find a legal framework, given that many states consider them widely different. Several States regard them with scepticism and believe that their use can have a negative impact on the economy, others either do not speak or allow free movement. Some Western powers like the United States and Great Britain have shown a generally positive attitude towards new technologies that enable virtual coins, others like Canada and Australia are still deciding what to do, but there are also countries like Russia, China and South Korea that have substantially prohibited them, only to change their mind, at least partially (only Russia) in recent times and the rest of this chapter will be examined how the issue of regulation in the different states is evolving.

3.2.1 Regulation in USA

The US federal government has not exercised its constitutional prerogative to regulate the Blockchain, just as it does with financial rules, so each state is free to introduce its own regulations. in June 2015, the State of New York became the first to regulate companies engaged in the virtual currency sector through a state agency. In 2017, at least 8 states have worked on bills that accept or promote the use of Bitcoin and Blockchain, and at least two of them have already approved laws in this regard. ***Smart contracts***[29] were legally recognized in Arizona, in Vermont the blockchain and in Delaware it is aimed at authorizing the registration of the shares held in the form of blockchain by the companies that are in that State.

There is a huge amount of people who wants for Bitcoins and some other cryptocurrencies to be guaranteed the same financial safeguards as traditional assets. Last July, the *U.S. Commodity Futures Trading Commission* has granted the permission to *LedgerX* to exercise, a cryptocurrency trading platform, which debuted in October, making it the first place to exchange digital money regulated at federal level.

In November 2017, the inspector general of the *United States Department of the Treasury* said he wanted to review the cryptocurrency practices because there are real risks of money laundering and terrorist financing. The same Department, in the 2013 guidelines, had argued that *"virtual currencies have no legal status in any jurisdiction"*. In the same November the Secretary of the Treasury, Steven Mnuchin, announced that he had created working groups on Bitcoins, an argument which, he said, would be analysed *"with extreme care"*.

Currently, there is no clarity in the political direction regarding cryptocurrency regulation in the United States. As required by US law, regulatory signals on the encrypted currency of the SEC

[29] ***Smart contracts:*** IT protocols that facilitate, verify, or enforce, negotiate or execute a contract, sometimes allowing partial or total exclusion of a SOURCE contract clause: https://it.wikipedia.org/wiki / Smart_contract)

and the *Commodities and Futures Trading Commission* (CFTC) appear to be in conflict with each other. The declaration of the *Internal Revenue Service* (IRS), which considers crypto-currencies as taxable properties and not as currencies, has added a new dimension to the situation. The *Securities and Exchange Commission* (SEC) stated that it has not to be approved the negotiation of assets based on cryptographic currency. This means that, from the point of view of the SEC, the ICOs, the ***Exchange-traded funds*[30] *(ETFs)*** and other cryptographic activities are not approved by the SEC for trading in the United States. On the other hand, the CFTC considers Bitcoin as a commodity and has not only licensed Bitcoin futures but has also licensed grants to offer assets in encrypted currency for trading.

United States law enforcement authorities have expressed concern that crypto-currencies can be used for money laundering. Arrests and seizures of Bitcoin have been carried out. Even the big investment banks (Goldman Sachs and JPMorgan Chase) have banned the use of their credit and debit cards to fund cryptographic currency trading accounts. The United States is still trying to define some sort of political direction for crypto-currencies, given that many Americans are trading them in offshore scholarships or local stock exchanges.

3.2.2 Regulation in EU

Also Europe is looking for rules for cryptocurrencies and the European Union has repeatedly raised the alarm. At the end of 2017, the vice-president of the *EU Commission* responsible for EU, Valdis Dombrovskis, warned investors against the risks associated with cryptocurrency. *"Investors - he said - must know that the price of Bitcoin can fall at any time"*. He then asked supervisory authorities such as the *European Banking Authority* (EBA) and the *European Securities and Markets Authority* (ESMA) to clarify why *"there are obvious risks to investors and consumers associated with price volatility"*.

In turn, the president of ESMA, Steven Maijoor, wanted to warn more recently about ICO, a system of fund-raising based on cryptocurrencies that allows companies to obtain liquidity by

[30] ***ETF:*** a type of investment fund and belong in particular to the ETPs (Exchange Traded Products), that is, to the macro family of products with a listed index Source: https://it.wikipedia.org/wiki/Exchange-traded_fund)

issuing their own cryptocurrency which is almost always based on the Ethereum technology. With the ICO, according to Maijoor, there would be no protection guaranteed by regulated investments and all the capital invested can be lost. As a principle the ICO can guarantee services in exchange for the currency that is purchased, or a share in revenues, but this takes place in an unregulated space.

On 7 September 2017 the President of the European Central Bank (ECB) Mario Draghi rejected the Estonian proposal to launch a state digital currency, the "*estcoin"*, stating that the ECB would not allow either that country or others to European Union to introduce its own virtual currency.

Always the Governor of the ECB, in an open session with the students, said that he looked at the blockchain technology with interest, as it could introduce important innovations in other sectors as well. The *European Commission* set up the ***Blockchain Observatory and Forum,*** with the aim of monitoring the most interesting blockchain developments and projects on the European territory, making funding available to encourage governments, industries and European citizens to take advantage of the opportunities provided by this new technology.

As for the individual States of the Union, ***France*** recently raised barriers against Bitcoin and all cryptocurrencies in an attempt to block their use in illicit activities, from tax avoidance to money laundering to terrorist financing. French Finance Minister Bruno Le Marie has instructed the former Lieutenant Governor of the *French Central Bank* Jean-Pierre Landau to draw up rules to monitor the development of virtual currencies, indicating that Bitcoin and cryptocurrencies pose *"high risks of speculation and possible manipulation financial"*. The French body for the regulation of the stock market has issued an official statement stating the need for a prior authorization to offer derivatives on cryptocurrencies, also clarifying that it is forbidden to promote such offers through electronic tools (in relation to the MIFID II).

An assist comes from ***Germany***: Joachim Wuermeling, a member of the *Bundesbank* board, said cryptocurrencies should be regulated by global rules. In fact, according to his thinking, national rules are not sufficient to manage a global phenomenon; effective regulation of digital currencies requires international cooperation. However, under German law, digital currencies are financial instruments, more precisely a form of "private money" that can be taxed as capital. But certain uses require licenses or permits. More recently, the *German Federal Financial Supervision*

Authority (BaFin) has issued a statement to clarify the obligations to which ICO promoters must comply. The German approach versus ICO seeks not to provide general classifications, but to clarify the applicable law in the event that the token can be assimilated to the share of an investment fund, a share capital stock or generally as a financial instrument, also recalling that, depending on the configuration, the token negotiation could be included in a banking activity, in an issue activity or as a financial service, thus requiring prior authorization for the exercise and subjecting it to the related discipline.

Spain looks closely at the *"tax" issue*: cryptocurrencies are taxable as electronic payment systems according to a law that regulates betting, but as for other areas it is not yet clear how they should be managed and regulated.

In ***Sweden***, informal statements by a tax authority suggest that digital currencies are not currencies but must be treated as assets.

Austria regulates financial services involving virtual currencies.

The *National Bank of* ***Belgium*** has warned investors and savers of the risks related to cryptocurrencies and has declared them illegal properties, while the Ministry of Justice has announced its intention to impose a strict regulation on the activities related to them.

Gibraltar, after the adoption of the regulatory framework that came into force on 1 January 2018, which essentially applies the rules for financial intermediaries to the crypto providers, has announced that a law on ICO will soon be enacted with a specific figure, that of the sponsor, which would act as guarantor of the operations.

The European *"kingdom"* of Bitcoins and cryptocurrencies is instead ***Switzerland***, which has become one of the main European hubs for the development of blockchain and cryptocurrencies. It is no coincidence that he established the Crypto Valley Association, a non-profit ecosystem on cryptography and blockchain technology, which began to develop a code of conduct on ICOs. Swiss financial regulators have defined the requirements for Bitcoin operators and established that digital currency platforms are subject to anti-money laundering laws. In Saint Moritz, for example, they even began to accept Bitcoins as payment for sky-lifts. In September 2017, the Swiss authority responsible for monitoring financial markets issued guidelines on increasing

ICOs in the country. In addition, rumours hover over the creation of a possible hybrid bank, with a mix of legal and virtual currency.

On 16 February 2018 FINMA, the *Swiss Financial Market Supervisory Authority*, published guidelines for updating the previous supervisory report of September 2017, with which it sought to clarify the hypotheses in which the promoters of an ICO are subject to the rules valid for banks and intermediaries, with prior authorization to the activity and subject to prudential supervision, and when the discipline aimed at countering money laundering should be considered applicable.

It is interesting to note that in this document the Swiss Authority seeks to provide useful tools to operators in order to identify the rules to which they must submit based on the different economic function of the issued tokens, according to a classification in *a) payment token; b) Utility token and c) investment token*.

Beginning the analysis from the Europe area, some positions were recorded by the Central Bank, which recently published a clarification regarding Bitcoin, explaining the dangers for investors, while excluding that it is his job to regulate this matter.

3.2.3 Regulation in Italy

In October 2016, the deputy Stefano Quintarelli, together with other 13 colleagues, presented a draft law on cryptocurrencies. It was the first attempt in Italy to regulate a very complex sector based on some declared principles: to raise public awareness and institutions, to give positive value to the use of digital currencies and to work instead on abuse.

In May 2017, the *Legislative Decree 25 May 2017, n. 90* which contains the IV Anti-Money Laundering Directive. As of July 4, 2017, the only anti-money laundering document to which system operators will have to comply to define their obligations is *Legislative Decree 90/2017* which, in implementation of the *Fourth Anti-Money Laundering Directive (EU Directive 2015 / 849),* called suitable measures to protect the integrity of the economic and financial system and the correctness of the conduct of the operators required to comply with them. The aim of the new legislation is to make the internal system increasingly effective in counteracting the growing diversification of the criminal market, dictating more stringent anti-money laundering and counter-terrorism financing provisions.

Firstly, the decree confirmed the proper verification, registration and reporting of suspicious transactions, with the updates required by the fourth directive. To this end, the provision emphasized the issue of promptness of the proper verification of customers: those who take a new mandate, in fact, must be able to immediately guarantee the identification of the client and the actual owner.

The control, which consists of the acquisition and evaluation of information on the client and the purpose and nature of the professional service, must be carried out before the continuation of the continuative relationship or the assignment of the assignment.

Therefore, the person in charge must first:

- proceed with the identification of the customer through the verification of an identity document

- acquire and evaluate information on the purpose and nature of the continuing relationship or professional service;

- constantly monitor the relationship with the customer throughout its duration, through the examination of the overall operation of the same, the verification and updating of data and information acquired in the performance of activities.

To comply with the logic of the system, therefore, the legislation provides for an increasingly massive involvement of the "obliged parties" of a banking and financial nature in support of those institutionally assigned to combat the phenomenon. The former, distinctly identified by *art. 3 of the 90/2017 decree* are required to adequately verify the clientele and the actual owner through their identification.

To decode and dismantle those structures of financial engineering that often allow to shield capital of illicit origin, the Government has not only provided "facilitated access" to some sensitive data such as, for example, establishing *the "Register of effective owners of legal entities and trust expressed ".*

In fact, it is envisaged to centralize in a specific section of the business register, information on the actual ownership of productive trust of tax effects, companies, corporate groups and entities and in order to allow obliged parties to fulfil the obligation of adequate verification by doing so. play on information that makes *"public faith"*.

The idea of concentrating information on the actual beneficiaries of companies and bodies in one place, in fact, can not only help industry operators not only significantly reduce the volumes of paper that each person should ask and keep, but also to acquire information faster, easier and safer.

3.2.4 Countries “against” cryptocurrencies

China

It is usually thought that Bitcoins and digital currencies are totally prohibited and illegal in China, but this is not the case. On the contrary, the Asian country has become the biggest Bitcoin exchange market in the world. The ban is only on banks, since the central banking authority, the *People's Bank of China*, is 70% owned by the government. Banking institutions and their employees cannot sell or buy Bitcoin through banking services, nor offer services or do business with the Bitcoin industry. Recently, the Deputy Governor of the *Chinese Central Bank*, Pan Gongsheng, has asked to block all websites and apps that allow centralized exchanges of virtual currencies. Instead it is not illegal for ordinary citizens to trade in Bitcoin. In August 2017, however, China declared ICOs illegal.

Between closing exchange platforms and banning new offers of digital currencies, for Chinese and Koreans it is becoming almost impossible to operate on Bitcoins. With repercussions on the market, thus causing the price of bitcoin and other cryptocurrencies to fall in general.

In particular, China has implemented an escalation of measures to prevent the Chinese from buying and selling cryptocurrencies. Local authorities should also ban all platforms that offer centralized cryptocurrency trading services, according to what was said by the deputy governor of the *People's Bank of China*, Pan Gongsheng, who added that all national and foreign sites, mobile apps will be banned. providing centralized services for Chinese, cryptocurrency payment services platforms and services that more generally assist users in moving funds abroad. These measures to block all remaining chances that Chinese citizens had to operate on cryptocurrencies in a regime of inconvertibility of the local currency. China has essentially declared war on a market that in 2017 was worth more than three quarters of the global one on Bitcoin. The local authorities have thus closed the major platforms to exchange cryptocurrencies, effectively blocking the operations of the Chinese, held back by the impossibility of converting the yuan.

Indeed, the Chinese move is attributable in the first instance to the need to put a brake on trading that had become a way for everyone to export currency. With the result of accentuating the pressure also on the controlled exchange and to put in difficulty the Chinese authorities. It is no coincidence that the squeeze was implemented on the eve of a delicate Congress of the *Communist Party* that registered the regime's equilibrium. The ban on exchange was anticipated by the ban on ICOs. In recent weeks, the squeeze has expanded to miners, who take advantage of the cheap energy of some areas of the country to do business in the certification activity of Bitcoin transactions, the true focus of the whole system.

South Korea

The progressive success of Bitcoin in South Korea, which at the end of 2017 was worth around a fifth of global trade on the best-known cryptocurrency, also led Seoul to put a brake on activity. Last week local authorities have effectively blocked the operation by asking the exchanges to no longer allow the transfer of assets in cryptocurrencies outside centralized services: who bought Bitcoin was forced to keep them at the exchange and then, in fact, was unable to sell them.

The measure had caused a progressive surge in prices on Korean platforms, until *Coinmarketcap*, the reference site for quotes based on average values at the time, had to exclude the prices of the Korean exchanges, with the result of provoking a fall of almost 15% only as a result of the provision. That was followed by a tax evasion investigation that actually blocked the platforms. But Korea does not seem intent on stopping here: the government has fancied being ready to take measures to ban cryptocurrencies trading. And to prevent the anonymity of cryptocurrency owners.

To scare even in this case is the effect that the wave of purchases is likely to have on the exchange. Suffice it to say that in December 2017, Bitcoin rose from $ 10,000 up to a peak close to 20,000, with daily trading of around $ 30 billion in turnover. It is therefore clear that purchases have also influenced the exchange rate of the Korean won.

This phenomenon is mainly explained by the need to keep the exchange under control. But, unlike China, citizens in Korea have free access to foreign platforms and, therefore, the ban on exchange makes life more difficult, but does not prevent the online use of foreign exchange.

Russia

Currently, Bitcoins are practically banned in Russia, although not yet officially. In December 2017, a legislative proposal was prepared by the Central Bank and the Ministry of Finance to settle cryptocurrencies and ICOs. The regulators have released some details of the provision, for example on the possibility of taxing Bitcoin mining. After an initial ***"hostile"*** attitude of the Russian government towards the Bitcoin, the *Kremlin's economic advisor*, Sergei Glazev, said that the new cryptocurrencies could be used to *"carry out sensitive activities on behalf of the State"*. Or to avoid international sanctions in economic exchanges between countries

In Russia, both miners and cryptocurrency holders will be governed by the already in force Internal Income Code.

Anatoly Aksakov, president of the *Committee on Financial Markets* in the *Duma*, explained that the legislators intend to approve legislation on digital coins during the autumn session of the parliament. The document will not however contain different tax regimes for cryptocurrency holders: this means the distribution of digital coins will be taxed according to the existing provisions.

In particular, individuals involved in the distribution of virtual currencies will have to pay a normal income tax, while fees for legal entities will be different depending on the type of activity. However, if the government deems it necessary, in the future two different tax schemes could be implemented for the mining and provision of cryptocurrencies.

In May, the *Duma Committee for State Deeds* officially supported the first reading of an initiative aimed at establishing standards for the digital economy within the Civil Code of the Russian Federation. The purpose of the law is to *"minimize the risks related to the use of digital objects for the transfer of funds in an unregulated environment"*.

Recently, Herman Gref, CEO of the main bank in Russia, said that in his opinion governments *"will not give up their centralized role"* in the issue of money.

Rest of the world

In ***Bangladesh***, the Central Bank has ruled that the exchange of Bitcoins or other digital currencies could cost up to 12 years in prison.

Even in ***Bolivia,*** the currencies "not issued and controlled by the government" are declared illegal.
Also in ***Ecuador*** there is a ban, but basically because this nation is developing its own system of national electronic money.

Finally, ***India*** that was the first country to launch a Bitcoin exchange, BTCXIndia, which was then closed for reasons still unclear.

3.3 Future of cryptocurrencies: will they ever replace legal currencies?

According to the economic tradition, a currency to be defined as such, must satisfy three main functions:

1) ***Value reserve:*** the currency must be able to preserve its value over time so that users can decide whether to use it immediately or accumulate it in order to spend it in the future;

2) ***Means of exchange:*** money must act as a payment instrument in exchange for goods and services and must be commonly accepted;

3) ***Unit of account:*** the currency must perform the function of common unit of measure, through which to determine the price of goods and facilitate the measurement of economic transactions.

The behaviour of bitcoins in relation to the 3 characteristics mentioned above and its possible evolution will be described below.

If is taken into consideration the first function, that is the ***value reserve function***, it is not possible at this time to establish whether the bitcoin will retain its value in the future. Although there is a limit on the total number of cryptocurrency units in circulation, and this limit together with all the other rules established by the protocol are difficult to distort through substantial modifications, the future demand for bitcoins cannot be predicted with certainty, a real determinant of the price of cryptocurrency. The future demand for bitcoins will depend on its future use as a payment tool. The value of the bitcoin is currently too volatile to be considered an instrument of value reserve, and it is very difficult to predict whether this volatility will persist in the future or if the bitcoin will reach a stable price level.

The medium of exchange function is that the bitcoin seems to be able to satisfy more than all the others and it is also that for which it has been conceived. With Bitcoin you can make payments easily, quickly, with high levels of privacy and low costs when compared to all other traditional payment systems. However, cryptocurrency is not universally accepted as a means of payment for goods and services, so it is still difficult to spend them, but there are constantly increasing businesses, both physical and online, willing to accept them. As seen above, the money volumes exchanged through Bitcoin are only a very small fraction of the total volumes exchanged through the traditional electronic payment systems, and this fraction is even more infinitesimal if it is considered that many bitcoin transactions do not concern the purchase of goods or services but are processed only for speculative purposes. However, even in the context of this second function it cannot be exempted from considerations regarding the future of Bitcoin.

Considering the mining activity and the ways in which it is remunerated, it is necessary to outline the scenarios that could arise in the future when the rewards foreseen for the resolution of each block will be almost nil, and the only profitable source will be represented by the transaction fees: the *first possible scenario* could be the diffusion of bitcoins as a means of payment could lead to an increase in the number of daily transactions and therefore in the total revenues deriving from commissions, compensating for the cancellation of the rewards for the resolved blocks; *the second possible scenario* could foresee an increase in the cost of commissions, cancelling one of the main advantages deriving from the use of cryptocurrency; *the third possible scenario* would be the abandonment of mining by numerous individuals or companies as it is no longer profitable, with the risk that this activity will be concentrated in the hands of a few subjects or, at worst, degenerate into a monopoly, deleting the most innovative feature of the system, or the decentralization. Therefore, not even the future use of bitcoins as a means of exchange is so certain, and it is difficult to predict currently.

The last function, the of ***units of account*** one, is hardly satisfactory from the bitcoin the current state. The high volatility that characterizes the price of cryptocurrency is not allows an easy use as a unit of measurement to determine the value of the assets. Traders should update goods prices in bitcoins even several times throughout the day, since the exchange rate with the dollar or other legal currencies also changes several times on the same day. For this reason, the prices of the goods remain in any case denominated in legal currency and converted into bitcoins at the time of sale according to the current exchange rate.

From what has emerged so far, can be understood the bitcoins’ difficulty in satisfying in exhaustive way of the three functions that are commonly expected from a legal currency, both currently and in the future. Since there is not a central authority that impose the use or acceptance of bitcoin as a payment instrument, his future can only depend on the will of individuals to use and accept it.

There are doubts that hover around the bitcoin and other cryptocurrencies as regards their diffusion. The first is linked to the high price volatility: in fact, as already mentioned, the maximum pre-set limit of bitcoin units in circulation (21 million-unit cap) makes its offer curve inelastic, i.e.. insensitive to the variations in the cryptocurrency demand of individuals, variations that are reflected in its price. Even in the hypothesis that the market discovered the real value of bitcoin as a medium of exchange, however, changes in the demand for bitcoin would determine more or less consistent price fluctuations, considering that the demand can vary due to many factors, for example to the seasonality of sales or to economic cycles. If the offer will be rendered more elastic, increasing or decreasing the rewards for block resolution in relation to the number of transactions processed in a predetermined period of time or by changing the protocol and introducing new units of money, the effects of changes in demand would reflect the same in price but in a less accentuated manner, ensuring greater stability.

Another doubt is related to the possibility that Bitcoin may one day lose its original characteristics. As mentioned earlier, transaction fees may not be enough to remunerate miners' work and generate negative effects, but bitcoin's competitiveness may well persist with some of the traditional payment systems. Instead the progressive abandonment of mining by miners with lower computational powers, which would no longer be able to meet the costs of electricity and maintenance, would focus this activity in the hands of a few individuals, or a single miner, that would become a kind of central authority or to carry out a *51% attack* as mentioned in the previous chapter; in this situation would appear a real failure of Bitcoin as a decentralized system, the confidence in the correctness of the blockchain could be less seen the enormous powers of fraud in the hands of the monopolist, with serious repercussions in the use of cryptocurrency and finally in its value.

In light of what has been analysed up to now, it can be concluded that bitcoin is very difficult to replace legal currencies in the future, since it does not seem able to satisfy the functions of value reserve and unit of account. The bitcoin as a medium of exchange could instead find even wider consents in the future, considering the amount of innovation brought by the phenomenon of cryptocurrencies and blockchain. Fundamental for this diffusion will be the development of services connected to the world of cryptocurrency, which will have to offer greater guarantees of security and make this world, if possible, even easier and more accessible. The decisions of the Governments regarding the legislative and fiscal qualification within which to include Bitcoin and the other cryptocurrencies will also be fundamental.

b. Conclusions

Within this elaborate it has been analysed the technical characteristics that allow the functioning of cryptocurrencies and in particular of the one that gave rise to this new world, Bitcoin, passing through the blockchain, a register distributed and open to anyone, that keeping track of all the transactions solves the problem of double-spending without the need for a central authority. The blockchain with its impenetrability is certainly the most innovative element of this new system, whose application started from Bitcoin but seems able to revolutionize all the centralized management systems as it is used to. The analysis of the functioning of the system has highlighted some vulnerabilities of the latter, which could raise some concerns about the real future of cryptocurrency, even if for now there are remote eventualities.

Many more worries about the future of cryptocurrency have emerged instead from its analysis from an economic point of view: bitcoin is not currently suitable for use as a currency: the only function that seems able to satisfy and that of medium of exchange, reason for which it was created, but the number of people willing to accept them is still too small to allow the ease of use; the volatility of its price, which is determined by the market, does not allow its use either as a reserve of value, or as a unit of account. The volume traded by bitcoin transactions has grown exponentially in the last 2 years even if it still cannot be considered a threat to traditional payment systems, even if there have been reactions from the regulatory point of view given the ever-increasing use above all of the Bitcoin platform but many of the cryptocurrencies.

The uncertainty about its future, the lack of a clear stance on the part of many of the world's governments from a regulatory and fiscal point of view, the vulnerability of related services and the lack of protection of consumers who use them, as well as the above reasons, have hindered the definitive spread of cryptocurrencies, which currently behave more as a tool on which to speculate than as a tool for payments. Rather than looking at the future of cryptocurrencies, which as of today are said to be used for speculative purposes, by working for the inclusion of blockchain technology and always look for new uses in other sectors.

c. Bibliography and Sitography

- http://www.lastampa.it/2017/12/12/economia/la-febbre-da-bitcoin-arriva-anche-al-bancomat-vAUE2O1FYe3pD6ORpnk9XL/pagina.html

- “Bitcoin Manifesto”, Satoshi Nakatomo, 2015, Antonio Tombolini Editore

- http://www.oxforddictionaries.com/definition/english/cryptocurrency

- DAI Wei, "B-money“URL: http://www.weidai.com/bmoney.txt, 1998.

- http://www.diritto24.ilsole24ore.com/art/dirittoLavoro/2017-07-07/antiriciclaggio-obblighi-adeguata-verifica-clientela-luce-nuova-normativa-antiriciclaggio--111421.php

- Cryptography@metzdowd.com

- https://coinsutra.com/bitcoin-double-spending/European Central Bank (October 2012). "1". Virtual Currency Schemes (PDF). Frankfurt am Main: European Central Bank. p. 5. ISBN 978-92-899-0862-7.

- http://notiziedeattualita.com/blockchain-la-struttura-dei-blocchi

- Bitcoin.org

- https://www.mme.ch/fileadmin/files/documents/Publikationen/170926_BCP_Framework_-_Genesis_Version.pdf

- crypt.la/2014/01/06/satoshi-nakamoto-quotes,+

- http://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg

- ECB, “Virtual currency schemes”, URL:

- https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, ottobre 2012.

- ECB, “Virtual currency schemes – a further analysis”, URL:

- https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

- E-GOLD, Wikipedia, L’enciclopedia libera, URL: https://en.wikipedia.org/wiki/E-gold

- FINCEN, “Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies”, URL: http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

- FUNZIONE CRITTOGRAFICA DI HASH, Wikipedia, L’enciclopedia libera, URL: https://it.wikipedia.org/wiki/Funzione_crittografica_di_hash

- THE NILSON REPORT: GENERAL PURPOSE U.S. CARDS 2014, URL: http://www.nilsonreport.com/

- VOORHEES E., “What is Bitcoin?”, Bitcoin Magazine, URL: https://bitcoinmagazine.com/19020/bitcoin/

- WAGNER A., “Digital currency vs virtual currency”, Bitcoin Magazine, 22/08/’14, URL: https://bitcoinmagazine.com/15862/digital-vs-virtual-currencies/107

- WAGNER A., “The role and future of altcoins”, Bitcoin Magazine, URL: https://bitcoinmagazine.com/13150/role-future-altcoins/

- WAGNER K., “World’s first bitcoin ATM opnes in Vancouver, Canada”, meshable.com, URL: http://mashable.com/2013/10/30/bitcoin-atm-2/

- WILMOTH J, “What is altocoin?”, cryptocoinsnews.com, URL: https://www.cryptocoinsnews.com/altcoin/

- https://www.ethereum.org/

- https://ripple.com/

- https://coinmarketcap.com/all/views/all/

- http://coinmap.org/welcome/

- https://cryptoverze.com/bitcoin-wallet/

- https://www.ilbitcoin.news/la-vera-rivoluzione-non-e-la-blockchain-ma-la-crittografia/

- https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

- M. Bellino, I rischi legati all’ecosistema Bitcoin: i nuovi intermediari, in Riv. dir. banc., dirittobancario.it, 30, 2018.

- Catania, Leopoldo and Grassi, Stefano, Modelling Crypto-Currencies Financial Time-Series (December 7, 2017). CEIS Working Paper No. 417. Available at SSRN: https://ssrn.com/abstract=3084109 or http://dx.doi.org/10.2139/ssrn.3084109

- Ogunbadewa, Ajibola, The Bitcoin Virtual Currency: A Safe Haven for Money Launderers? (September 4, 2013). Available at SSRN: https://ssrn.com/abstract=2402632 or http://dx.doi.org/10.2139/ssrn.2402632

- Hacker, Philipp and Thomale, Chris, Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law (November 22, 2017). Available at SSRN: https://ssrn.com/abstract=3075820 or http://dx.doi.org/10.2139/ssrn.3075820

- Gasparri, TIMIDI TENTATIVI GIURIDICI DI MESSA A FUOCO DEL BITCOIN: MIRAGGIO MONETAIO CRITTOANARCHICO O SOLUZIONE TECNOLOGICA IN CERCA DI UN PROBLEMA? in Diritto dell'Informazione e dell'Informatica (Il), fasc.3, 2015, pag. 415.

- Vardi, “CRIPTOVALUTE” E DINTORNI: ALCUNE CONSIDERAZIONI SULLA NATURA GIURIDICA DEI BITCOIN, in Diritto dell'Informazione e dell'Informatica (Il), fasc.3, 2015, pag. 443.

- Capaccioli, Criptovalute e bitcoin. Un'analisi giuridica, Giuffrè, 2015

- https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf.

- https://www.tokens24.com/it/cryptopedia/basics/lecosistema-crypto

- https://www.bitcoinmining.com/

- risoluzione dell'Agenzia delle Entrate sul trattamento (simile alla valuta estera; ris. 72E/2016).

- a new challenge for the regulator, on OPEN REVIEW OF MANAGEMENT, BANKING AND FINANCE, 2018

- Passaretta, Bitcoin, il primo precedente giudiziario in Italia, Trib di Verona, Sent. 27.1.2017, in n Banca, borsa e tit. cred., 2017, II, p. 471.

- https://www.blockchain.com/it/charts/total-bitcoins

- https://www.ilbitcoin.news/vari-tipi-mining-facciamo-chiarezza/

- https://www.blockchain4innovation.it/esperti/ico-initial-coin-offering-ricostruzione-giuridica-del-fenomeno/

- https://www.tokens24.com/it/cryptopedia/basics/regolamento-sulla-criptovaluta-globale-2018

- Stefano Capaccioli, autore di Criptovalute e bitcoin: un’analisi giuridica

- https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474

- https://www.deepdotweb.com/2016/12/31/two-new-models-double-spending-attacks-bitcoins-blockchain/

- https://www.cbinsights.com/research/what-is-blockchain-technology/

- https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

- Cryptocurrencies, The Economist, 01/09/18

d. Summary

Introduction

What is Bitcoin? The first decentralized digital currency. The novelty, even if this currency has been in circulation since 2009, is not so much in the digitization of payments, to which everyone is now accustomed, in the Internet age, to the fact that it is the first attempt at decentralization. Unlike all traditional coins, bitcoins escape from any authority: the mint of the State does not think about them and there is no Central Bank that controls their value or a financial intermediary that validates their transactions. Born with the intent to make transactions on the internet safer and faster, Bitcoin is a new system for electronic transactions that is no longer based on trust in a third-party authority, but on mathematics and cryptography. The central bank is replaced by the Bitcoin platform, a *peer-to-peer (p2p)* network to which everyone can participate, as long that you install the homonymous software in your computer, which is free and open-source, even if a high computing power is required. The nodes of the network, using the software within their own devices, contribute in a widespread way to validate and record the transactions between two users who want to exchange units of this new type of currency, ensuring also anonymity thanks to the cryptography inherent in the system. The activity of validation and registration of transactions is called *"mining"*, a term that metaphorically traces the activity of gold mining from a mine, and the nodes that perform it are called *"miners"*. This activity exploits the computational power of the miners' devices, and is remunerated through newly issued bitcoins, according to a precise rewards system.

There are over **17 million bitcoins** in circulation at the moment, while the value of 1 BTC *today* is $ 7,078. The price is determined by the market, by the mechanism of supply and demand, even if it is characterized by a strong volatility. The purpose of this work is to provide a technical, economic and legal analysis of this innovative payment system.

The first chapter is dedicated to a presentation of the phenomenon of cryptocurrencies and more specifically Bitcoin, describing the characteristics and methods of use.

In the second chapter the technical aspects underlying the functioning of the system will be examined in depth.

In the third chapter the economic and legal aspects will be analysed, highlighting the advantages and disadvantages deriving from its use, considering the future prospects.

1. Bitcoin

Bitcoin is "*is the first digital decentralized currency*" as it can be read in the bitcoin.org website and is defined as a *"purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution"*. by Satoshi Nakatomo in a paper talking about it.

So, it can be said how Bitcoin can be defined as a new innovative payment system whose control is no longer in the hands of a central authority that regulates everything but in which thanks to the diffusion of a specific software and protocol are possible transactions of virtual currency not regulated by a third party that acts as guarantor.

In 2012 the ECB defined virtual currency as *"a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"* and defined as legal currency every legal currency instituted and released by a central authority to which citizens rely to use this currency as a method of payment in exchange for goods and services in the real economy.

The main characteristics of bitcoins (also common with those of other major cryptocurrencies) are:

- **Decentralization**
- **It is not subject to monetary policies**
- **It has no legal tender**
- **Pseudonym**
- **Transparent**
- **Low transaction costs**
- **Fast and irreversible transactions**

Bitcoin wallets are not exactly the equivalent of a current account, though the graphical interface offered by the various wallet services allows you to know at any time the total of the bitcoin possessed and the movements in and out, as a kind of account statement in real time.

There are different types of portfolios (only a few are mentioned) to choose from, depending on the levels of user convenience, security and complexity desired, type of device used, if smartphones, desktops and even there is the ability to choose between operating systems:

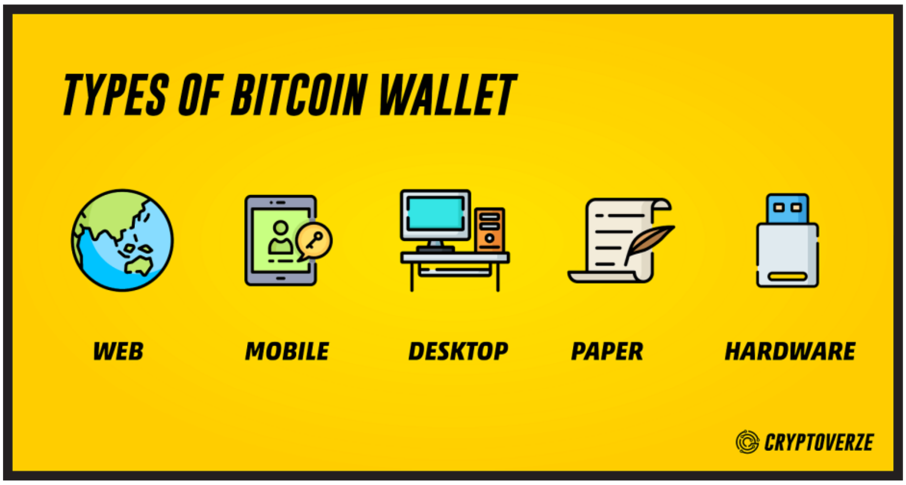
- ***Desktop Wallet:*** it is a software to install on your computer that allows you to store and store private keys on the hard disk.

- ***Mobile Wallet:*** wallet applications for smartphones that make it possible to keep, to spend or receive bitcoins from your mobile phone quickly and easily.

- ***Online Wallet:*** service offered by different websites, (like Coinspace.org BitGo.org) that store private keys storing them in online servers placed under their protection. In other words, the user entrusts the custody of their bitcoins to third parties, in this case a website.

- ***Paper Wallet:*** private and public keys can be stored directly from the same user in a paper support and kept so protected from hackers and from possible failures of their electronic devices.

- ***Hardware Wallet:*** these are devices created specifically for storing private keys bitcoin addresses and other cryptocurrencies.



Once illustrated how to store BTC, it is good to show how they can be obtained. Obviously, the ways to buy them are many, shown below:

- ***<u>Buy them from people willing to sell them</u>***: localbitcoins.com is the leading face-to-face exchange website platform and is present in 16263 cities and 248 countries including Italy. Who wants to buy bitcoins can decide whether to exchange online, choosing one of the various payment methods (bank transfer, paypal, postepay, Skrill, Moneybooker).

- ***<u>Buying at online Exchanges:</u>*** there are many sites on the web that allow the purchase of bitcoins in exchange for legal tender or other cryptocurrencies. These platforms play the role of market makers by fixing exchange rates to which the Exchange buys or sells bitcoins in exchange for the main traditional currencies or currencies other virtual currencies.

- ***<u>Buying at Bitcoin ATMs:</u>*** it is a much quicker purchase or sale service compared to exchange online and offered by Bitcoin ATMs. There are currently 3480 bitcoin ATMs in 72 countries, of which 17 in Italy and the number is constantly increasing. In circulation there are different models, among which the most widespread ones. These devices are almost always of two types:

    1) ***unidirectional,*** that is, they allow to convert only legal currency into bitcoins,

    2) ***bidirectional,*** the ones that instead allow both to buy and to sell bitcoins in exchange for legal tender.

In general, the process of buying (or selling) bitcoins through an ATM takes place in the following phases:

1) *Verification phase*
2) *Entering the Bitcoin address*
3) *Selection of the amount of cash*
4) *Confirmation of the operation.*

- ***Selling goods and services in exchange for bitcoins:*** currently, this option is more easily negotiated by those who conduct a business. I'm always more numerous stores, both physical and online, accepting bitcoin in payments exchange of goods and services.

- ***Mining:*** it is the activity of validation and registration of bitcoin transactions that they happen continuously in the system. Mining is incentivized by a precise system of rewards.

History and altcoins

Since the '70s research in the cryptographic field leads to important developments, thanks to the Progressive progress towards the digital age that has increased the need for individual security and privacy. The cryptography that until then was only the domain of governments for the security of communications has back to be in the public domain, to ensure high levels of privacy of the new digital systems, including those relating to electronic payments. In the 1980s, however, the American cryptographer David Chaum perfected the blind signatures system in order to improve the privacy of electronic payment services offered by banks. Chaum extends his research into electronic payment systems, which culminate with the founding of *DigiCash Inc.* in Amsterdam and the launch of the *e-cash* system in the early 1990s. This electronic payment system was based on the use of virtual money to keep in the computer, controlled cryptographically by the member banks, and allowed to make anonymous and secure purchases on the Internet or in the shops that accepted them, without the need to exchange card credentials of credit. Although this system was sold to several banks, these were still conservative in a market dominated by credit cards, so that it failed a few years after the creation in 1998. Although e-cash was a centralized system being controlled by the issuing bank, it was still founded on solid cryptographic bases.

In 1998, the famous *PayPal* system was born at the hands of Elon Musk who, unlike e-cash, also allows the transfer of money between individuals.

Another development attempt was made in the decade between 1999 and 2009, by *e-gold*, a digital currency exchangeable instantly on the Internet, issued by the private company *Gold & Silver Reserve Inc*. in exchange for gold or silver deposits. This currency was traded between accounts and essentially for the owners was like holding a certain amount of precious metals held by *G&SR* as a reserve. Finally, again in 1998, Wei Dai and Nick Szabo proposed two different decentralized payment systems, which more than anyone approached what Nakamoto will achieve in 2009, even though both projects remained only theoretical.

The fundamental open source feature of the Nakatomo project allowed the participation of many developers who, since the creation of Bitcoin in 2009, have made an essential contribution to software development and to the correction of defects such as the vulnerability of the system and then started the creation of similar projects that allowed the creation of the so-called Altcoins.

To date, according to estimates by coinmarketcap.com there are 1865 cryptocurrencies for a market capitalization equal to 211,732,582,263 USD and the number of cryptocurrencies is constantly growing.

2. How does Bitcoin and main cryptocurrencies work

The operation of Bitcoin is in the hands of the network nodes called *"miners".* Through the mining process, they collect transactions that take place continuously, within specific containers called blocks. These blocks are joined together to form the blockchain which is the key organ of the whole system.

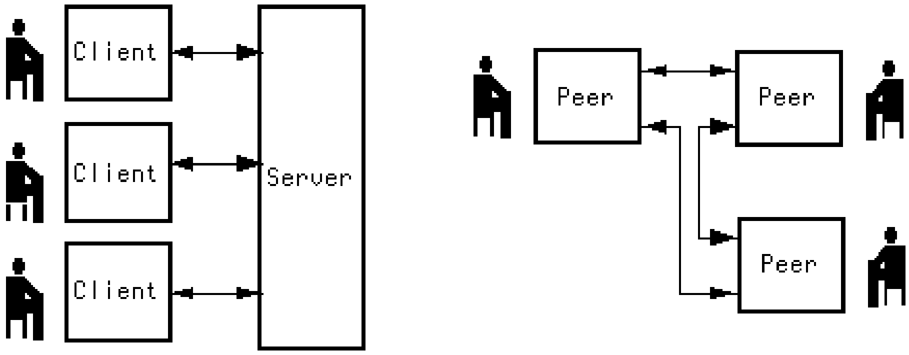
The blockchain is a large register open to users, containing every transaction in bitcoin from its birth to today to solve the double-spending problem, and is subjected to continuous updating by the miners. Anyone can view a complete version of the blockchain, installing Bitcoin software or more simply on the web thanks to special sites called block explorer. Bitcoin still manages to ensure high levels of anonymity, as transactions take place between pseudonymous addresses from which it is very difficult to trace the identity of its user.

The blockchain therefore represents the trace and the history of all transactions. It is a reliable tool, which tests because no transaction can conflict with another, since every transaction is Irreversible and is recorded and marked temporally, so no user can send bitcoin that does not own or has already sent to another address, solving the problem of double-spending. In this chapter we propose an analysis of the technical aspects that allow Bitcoin to work.

Cryptography is the science that protects information and makes it incomprehensible to those who intercept it, so that it can be read and understood only by the recipient. The message to be protected is called plaintext, while the "hidden" to be incomprehensible is called ciphertext; the transformation from plain text to ciphertext is called encryption, while the inverse transformation is called decryption.

Peer to peer network

The peer-to-peer network is a computer network architecture in which a single user's computer can communicate directly with other users' computers. In a peer-to-peer network, the nodes are equivalent to each other, thus being able to perform functions both from customers and servants to all other nodes of the network, unlike the more common client-server architecture, in which communication it only takes place between client and server, and not even between client and client.



The absence of a central server that plays the role of custody of the managed and exchanged resources makes the p2p network a decentralized system, in which the control is transferred to each single node, and the information is distributed and shared between them through the application of specific algorithms. The p2p model is commonly associated with file sharing programs, but it is not the only application it can be used for. One of these can be distributed computing, which consists in solving computational problems of high complexity by exploiting the computing capacity provided overall by a set of autonomous computers interconnected by a network, just like the p2p network. The term distributed has a broad meaning and wants to indicate both the physical disposition in different geographical areas of the computers, and the autonomy of the processes they perform.

Public and private keys and addresses

Generally taking advantage of the services offered by the many different Bitcoin wallet suppliers, the user is seen to assign a public address that must disclose whether he wants to receive and own bitcoins, only worrying about remembering the password protection to access his wallet and performing other procedures necessary for securing the same, in order to do not miss the chance to spend your digital money.

To better understand what happens you need to explain the function and the origin of these codes: that is a private key that is used to digitally sign the bitcoin outputs. Only by owning the private key is it possible to spend some bitcoins associated with it. The key or private keys are stored on a computer or smartphone or at servers depending on the type of wallet the user enjoys.

Losing these private keys or not being able to access the file in which they are stored following the destruction of the PC or the loss, involves the loss of bitcoins associated with those keys and the inability to recover them. Similarly, theft of private keys can expose you to the risk of someone else spending those bitcoins.

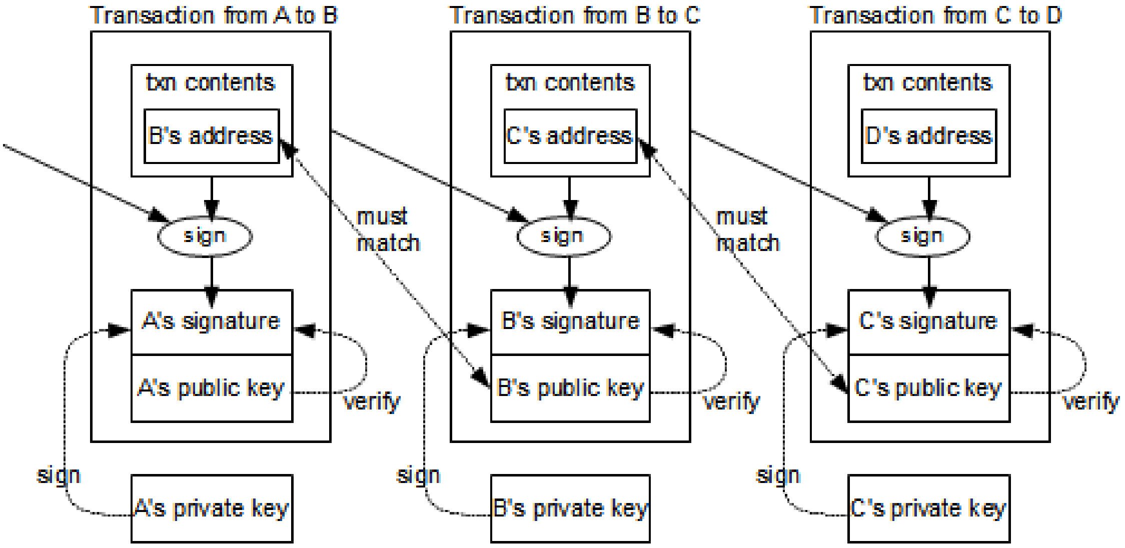
Finally, the public key in turn generates the Bitcoin address at 160 bits through special hashing algorithms always aimed at ensuring security.

Blockchain

The blockchain is literally a set of blocks, in which a set of subjects makes available to other computer resources such as memory, CPU, band, to make available to a community of users a mainly public database. It exploits peer-to-peer technology and allows anyone to download, thus becoming a "node" of the network. It is essentially the accounting book in which all transactions made in Bitcoin since 2009 are made, made possible by the approval of 50% + 1 of the nodes. These single-block transactions occur continuously in the system, and on average every 10 minutes a new block is produced and attached to the chain, so that the blocks are arranged in chronological order starting from the block of origin, the so-called *genesis block.*

The same mechanism of the chain is also replicated for the transactions contained in the blocks, even if with some difference: in fact every transaction is not connected to its previous one in chronological order, but to its transaction-input, or to the previous exchange, or to the previous exchanges, which provided bitcoins to the receiver, so that they could subsequently become the sender in the transaction in question. The blockchain can be considered a system whose smaller and central particle is represented by the single transaction and proceeding to the outside it is found the block, which contains many of these transactions, and finally the multiple blocks that contain the history of Bitcoin from his birth. The structure and functioning of the blockchain represent the main and fundamental technological innovation in the field of distributed systems. It is therefore defined as an open system of verification that does not need the approval of the banks to carry out a transaction. Extrapolated from its original context, the blockchain has been used in all areas in which a relationship is needed between several people or groups, with considerable success over the years.

How transaction works:



By breaking down a single transaction stored in a block you can see how it appears to be a set of three main information:

1) **Header,** that is the identity card of the transaction, in turn containing the following details:

a) *Hash of the transaction:* hash identifying a specific transaction, that includes and summarizes all the information concerning the specific transaction. This code summarizes the following information as a whole: version number, list of inputs and outputs and the closing time of the block in which it is inserted *(lock time);*

b) *Number of the solved block* in which this transaction has been stored

c) *Number of inputs:* number of the various previous transactions that supply the total amount of bitcoins used in the transaction in question;

d) *Sum of the bitcoins* resulting from the transactions described in point c)

e) *Number of outputs:* number of different Bitcoin addresses to which outgoing BTCs are sent

f) *Total outgoing BTC:* sum of the outgoing bitcoins in the transaction in question

g) *The measure of memory* of the transaction data in terms of physical space occupied on the disk.

h) *the amount of BTC* attributed to the block mining as a transaction fee

2) **Detail of the inputs**

3) **Detail of the outputs**

There are some further considerations to do:

- *The "change" or rest of a transaction*
- *Bitcoin transactions are divisible*

Mining

The answer to questions on how to make decentralized payment possible, how to make up for the absence of a central authority as a guarantor of currency and transactions and how to guarantee and nurture trust in a system so inherently different from traditional payment systems for the sensitivity to the security of money is mining.

Often, mistakenly reconnects mining activities to the production and emission of new bitcoins even if this is not the main purpose of this activity. In fact, the crucial objective of this process is to maintain the integrity and authenticity of the blockchain, which for users of the Bitcoin platform represents a real bank account. Only if this register can maintain the characteristics mentioned above, users can rest assured that that money belongs to them; if instead it proves to be fragile to counterfeiting attempts, for example aimed at the validation of several inconsistent transactions (*doublespending*), trust in the system would vanish and Bitcoin would be doomed to fail.

The mining activity can theoretically be done by anyone if a user installs the Bitcoin client on your computer. Mining literally exploits the computing power of hardware devices made available by network nodes. It is a difficult and time-consuming operation in terms of computer processing times, so that new blocks are produced within a fixed time frame, regardless of the number of transactions taking place in the network. In fact, if few transactions take place in the network, these cannot be put on hold until a certain threshold is reached, otherwise practicality as a payment system would vanish; moreover, the first mined blocks did not contain any transactions, except the Coinbase, to create and put in circulation the first units of currency.

For each production of a new block an established quantity of new bitcoins is issued, which belongs to the miner who first produced it. This total quantity also includes the total commissions of the transactions recorded in the block.

In short, mining was conceived by Nakatomo to secure the blockchain, and this security is made possible by how many "honest" nodes are present in the network, in order to make the work of "dishonest" nodes difficult if not impossible. instead they want to modify the register to their advantage to spend more times than the currency already spent.

The honesty of the nodes is "bought" by the same protocol through a specific system of attribution of rewards, which encourage such honesty.

Mining is a specific feature of the Bitcoin platform: in fact, other cryptocurrencies, such as for example Ripple, are issued on the market by the company that invented it.

There are three main macro-refinements of mining activity:

1. ***Solo-Mining:*** mining in this case is carried out “solo”, individually, in order to win both the reward that sum of the transaction fees included in the new block. T
2. ***Pool-Mining:*** instead of individually undermining it is possible to do it collectively, joining a *mining pool*
3. ***Cloud-Mining:*** it is also possible to participate in the mining activity without possessing materially necessary hardware devices

Transaction Commissions

One of the main features of Bitcoin, which differentiates it from all the other existing electronic payment systems are the low transaction fees. The sum of the commissions of the transactions verified and recorded in a block reimburse, together with the fixed share of new bitcoins, the work done by the miners.

Given that in the future this fixed portion is destined, as already mentioned, to gradually decline until it is close to zero, as a threshold of around 21 million bitcoins in circulation is foreseen, the miners' remuneration is destined to consist only of commissions of transaction. At that point Bitcoin will continue its proper functioning only if its dissemination and use as a tool for payments will be such as to guarantee the miners an adequate remuneration, so that they will be encouraged to continue their fundamental activity in the future. These fees are the responsibility of the sender, but many transactions may also not provide for no commission, if they meet certain conditions.

Dishonesty of the nodes

There are two types of attacks that a dishonest node could try to commit:

1) ***Double spending attack:*** With this type of attack, the dishonest miner has the objective of defrauding a specific user who believes he has received the payment, only to find out in a subsequent moment that the transaction was unsuccessful; the miner in question and the trader's customer target of the attack, so it will be called a node / customer.

   The double-spending as already mentioned several times is the possibility of spending the same unit of digital currency more than once. When a block is resolved, the transactions contained therein are said to be confirmed once, and each block that is added to the latter receive confirmation more. The confirmation is basically the proof that the miners have accepted that version of the blockchain and are working to continue its *"history"*.

2) ***51% attack:*** It is the situation in which a single node (or an organized whole) comes to dispose of more of the goal of the total computational power of the network. Consider that it is not necessary to hold precisely 51% of the hash rate but just to overcome the majority to be able to launch this type of attack. This eventuality represents a threat to the stability

of Bitcoin, as such a node, for as long as he possessed more than half the power, he would have the power to:

- Always succeed in a double-spend attack
- To exercise the monopoly of the mining activity
- Deciding not to include any transaction, or even any, within its blocks, strong that "his" chain will always win.

The technological innovation introduced by Nakatomo, with Bitcoin, has led to the creation of a real ecosystem around this new payment system. An ecosystem in continuous evolution, formed by different actors with respect to the world of traditional payments and new business models generally focused on obtaining and on services concerning the use, exchange and investment of bitcoins or other alternative cryptocurrencies. The economy of these cryptocurrencies is young but in constant turmoil and there are several actors that gravitate around this world:

- ***Developers***
- ***Miners***
- ***Users***
- ***Wallet services providers***
- ***Exchange platforms***
- ***Financial services providers***
- ***Payment processors***
- ***Other subjects***

ICO’s

With the passing of the years from 2009 to today Bitcoin has literally left its mark, opening up a new world of opportunities. In fact, the cryptocurrencies have taken more and more foot moving from the only Bitcoin to 1856 today. All this was made possible by the so-called ***Initial Coin Offering*** (ICO), which is an unregulated crowdfounding medium in the financial sector. The first ICOs were introduced to allow the collection of new funds for the creation of new cryptocurrencies, but the current ones are also used for other purposes. In principle, tokens of the new currency to be issued in exchange for money are sold to enable it to be launched. The ICO differs from the *Tender Offer* (TO) because the first is not regulated by the States and this could lead to the lack of a guarantee on the property or other rights.

In the light of the measures referred to above by the national supervisory authorities, it appears necessary to understand the expectation that the lenders have in buying the tokens offered for sale. In particular, the examination concerns the rights that the token incorporates, rights that are dependent on the project and the business model that the company proposes. Juridically, a token is a digital information that typically confers a property right to a subject about the information itself, which is registered on a Blockchain (or other distributed register) that can be transferred via a protocol and, finally, can incorporate (or not) other additional rights.

Regulation

Cryptocurrencies have long been at the centre of the international debate to find a legal framework, given that many states consider them widely different. Several States regard them with scepticism and believe that their use can have a negative impact on the economy, others either do not speak or allow free movement. Some Western powers like the United States and Great Britain have shown a generally positive attitude towards new technologies that enable virtual coins, others like Canada and Australia are still deciding what to do, but there are also countries like Russia, China and South Korea that have substantially prohibited them, only to change their mind, at least partially (only Russia) in recent times n the rest of this chapter will be examined how the issue of regulation in the different states is evolving.

Usa

The US federal government has not exercised its constitutional prerogative to regulate the Blockchain, just as it does with financial rules, so each state is free to introduce its own regulations. in June 2015, the State of New York became the first to regulate companies engaged in the virtual currency sector through a state agency. In 2017, at least 8 states have worked on bills that accept or promote the use of Bitcoin and Blockchain, and at least two of them have already approved laws in this regard. ***Smart contracts*** were legally recognized in Arizona, in Vermont the blockchain and in Delaware it is aimed at authorizing the registration of the shares held in the form of blockchain by the companies that are in that State. Currently, there is no clarity in the political direction regarding cryptocurrency regulation in the United States

EU

Also Europe is looking for rules for cryptocurrencies and the European Union has repeatedly raised the alarm. At the end of 2017, the vice-president of the *EU Commission* responsible for EU, Valdis Dombrovskis, warned investors against the risks associated with cryptocurrency. *"Investors - he said - must know that the price of Bitcoin can fall at any time"*. He then asked supervisory authorities such as the *European Banking Authority* (EBA) and the *European Securities and Markets Authority* (ESMA) to clarify why *"there are obvious risks to investors and consumers associated with price volatility"*.

In turn, the president of ESMA, Steven Maijoor, wanted to warn more recently about ICO, a system of fund-raising based on cryptocurrencies that allows companies to obtain liquidity by issuing their own cryptocurrency which is almost always based on the Ethereum technology. With the ICO, according to Maijoor, there would be no protection guaranteed by regulated investments and all the capital invested can be lost. As a principle the ICO can guarantee services in exchange for the currency that is purchased, or a share in revenues, but this takes place in an unregulated space.

Italy

In May 2017, the *Legislative Decree 25 May 2017, n. 90* which contains the IV Anti-Money Laundering Directive. As of July 4, 2017, the only anti-money laundering document to which system operators will have to comply to define their obligations is *Legislative Decree 90/2017* which, in implementation of the *Fourth Anti-Money Laundering Directive (EU Directive 2015 / 849),* called suitable measures to protect the integrity of the economic and financial system and the correctness of the conduct of the operators required to comply with them. The aim of the new legislation is to make the internal system increasingly effective in counteracting the growing diversification of the criminal market, dictating more stringent anti-money laundering and counter-terrorism financing provisions.

Countries against cryptocurrencies

China

It is usually thought that Bitcoins and digital currencies are totally prohibited and illegal in China, but this is not the case. On the contrary, the Asian country has become the biggest Bitcoin exchange market in the world. The ban is only on banks, since the central banking authority, the *People's Bank of China*, is 70% owned by the government. Banking institutions and their employees cannot sell or buy Bitcoin through banking services, nor offer services or do business with the Bitcoin industry. Recently, the Deputy Governor of the *Chinese Central Bank*, Pan Gongsheng, has asked to block all websites and apps that allow centralized exchanges of virtual currencies. Instead it is not illegal for ordinary citizens to trade in Bitcoin. In August 2017, however, China declared ICOs illegal.

South Korea

Local authorities have effectively blocked the operation by asking the exchanges to no longer allow the transfer of assets in cryptocurrencies outside centralized services: who bought Bitcoin was forced to keep them at the exchange and then, in fact, was unable to sell them. The measure had caused a progressive surge in prices on Korean platforms, until *Coinmarketcap*, the reference site for quotes based on average values at the time, had to exclude the prices of the Korean exchanges, with the result of provoking a fall of almost 15% only as a result of the provision. That was followed by a tax evasion investigation that actually blocked the platforms. But Korea does not seem intent on stopping here: the government has fancied being ready to take measures to ban cryptocurrencies trading. And to prevent the anonymity of cryptocurrency owners.

Russia

Currently, Bitcoins are practically banned in Russia, although not yet officially. In December 2017, a legislative proposal was prepared by the Central Bank and the Ministry of Finance to settle cryptocurrencies and ICOs. The regulators have released some details of the provision, for example on the possibility of taxing Bitcoin mining. In Russia, both miners and cryptocurrency holders will be governed by the already in force Internal Income Code. In particular, individuals involved in the distribution of virtual currencies will have to pay a normal income tax, while fees for legal entities will be different depending on the type of activity. However, if the government deems it necessary, in the future two different tax schemes could be implemented for the mining and provision of cryptocurrencies.

Rest of the world

In ***Bangladesh***, the Central Bank has ruled that the exchange of Bitcoins or other digital currencies could cost up to 12 years in prison.

Even in ***Bolivia,*** the currencies "not issued and controlled by the government" are declared illegal.

Also in ***Ecuador*** there is a ban, but basically because this nation is developing its own system of national electronic money.

Finally, ***India*** that was the first country to launch a Bitcoin exchange, BTCXIndia, which was then closed for reasons still unclear.

Can cryptocurrencies replace legal values?

According to the economic tradition, a currency to be defined as such, must satisfy three main functions that cryptocurrencies does not fit.

1) ***Value reserve:*** the currency must be able to preserve its value over time so that users can decide whether to use it immediately or accumulate it in order to spend it in the future;

2) ***Means of exchange:*** money must act as a payment instrument in exchange for goods and services and must be commonly accepted;

3) ***Unit of account:*** the currency must perform the function of common unit of measure, through which to determine the price of goods and facilitate the measurement of economic transactions.

Conclusions

Within this elaborate it has been analysed the technical characteristics that allow the functioning of cryptocurrencies and in particular of the one that gave rise to this new world, Bitcoin, passing through the blockchain, a register distributed and open to anyone, that keeping track of all the transactions solves the problem of double-spending without the need for a central authority. The blockchain with its impenetrability is certainly the most innovative element of this new system, whose application started from Bitcoin but seems able to revolutionize all the centralized management systems as it are used to. The analysis of the functioning of the system has highlighted some vulnerabilities of the latter, which could raise some concerns about the real future of cryptocurrency, even if for now there are remote eventualities.

Many more worries about the future of cryptocurrency have emerged instead from its analysis from an economic point of view: bitcoin is not currently suitable for use as a currency: the only function that seems able to satisfy and that of medium of exchange, reason for which it was created, but the number of people willing to accept them is still too small to allow the ease of use; the volatility of its price, which is determined by the market, does not allow its use either as a reserve of value, or as a unit of account. The volume traded by bitcoin transactions has grown exponentially in the last 2 years even if it still cannot be considered a threat to traditional payment systems, even if there have been reactions from the regulatory point of view given the ever-increasing use above all of the Bitcoin platform but many of the cryptocurrencies.

The uncertainty about its future, the lack of a clear stance on the part of many of the world's governments from a regulatory and fiscal point of view, the vulnerability of related services and the lack of protection of consumers who use them, as well as the above reasons, have hindered the definitive spread of cryptocurrencies, which currently behave more as a tool on which to speculate than as a tool for payments. Rather than looking at the future of cryptocurrencies, which as of today are said to be used for speculative purposes, by working for the inclusion of blockchain technology and always look for new uses in other sectors.