TREBALL DE FINAL DE GRAU

UNIVERSITAT DE BARCELONA

Facultat d'Economia i Empresa

University of Barcelona

Faculty of Business and Economics

Case Study

BITCOIN

Two sides of the same coin

Clàudia Abella Serra

Tutor: Emili Batlle Molina
International Business Degree

Barcelona, June 2018

ABSTRACT

Bitcoin arises due to the instability of the financial market, the great economic crisis of 2008, the control and manipulation of financial institutions and governments on the monetary system, and the continuous technological advance. It is a virtual, global, decentralized currency, based on cryptography, the peer to peer network and the blockchain. Created under the pseudonym of Satoshi Nakamoto with the main objective of carrying out economic transactions anywhere in the world, without the need of any intermediary and in a totally anonymous way. That is why it is intended to perform a deep study of this cryptocurrency, current in our society since 2009, trying to explain in a simple and understandable way its nature, implications, and the social and economic context in which it is.

✓ Key words: Bitcoin, blockchain, peer to peer network, cryptocurrencies, Satoshi Nakamoto, miners, virtual wallet, volatility.

RESUM

El Bitcoin sorgeix a causa de la inestabilitat del mercat financer, la gran crisi econòmica del 2008, el control i manipulació de les entitats financeres i dels governs sobre el sistema monetari, i del continu avanç tecnològic. És una moneda virtual, global, descentralitzada, basada en la criptografia, la xarxa "peer to peer" i la cadena de blocs. Creada sota el pseudònim de Satoshi Nakamoto amb l'objectiu principal d'efectuar transaccions econòmiques a qualsevol part del món, sense la necessitat de cap intermediari i de forma totalment anònima. És per això que es pretén realitzar un profund estudi d'aquesta criptomoneda, vigent en la nostra societat des del 2009, intentant explicar d'una forma senzilla i entenedora la seva naturalesa, implicacions, i el context social i econòmic en el qual es troba.

✓ Paraules clau: Bitcoin, cadena de blocs, xarxa peer to peer, criptomonedes, Satoshi Nakamoto, miners, moneder virtual, volatilitat.

TABLE OF CONTENTS

I. INTRODUCTION

When choosing a topic for the Final Work Degree, I decided to do a study on Bitcoin, the most popular cryptocurrency of the moment. Where did the idea come from? During the last two months of 2017, every day there were more and more the news that I read or that I saw on television about that currency. This fact really caught my attention. Bitcoin seemed to me a topic of great interest, on the one hand, due to my lack of knowledge about it. Since I only knew that it was a virtual currency, but I didn't know absolutely anything of its structure or its functioning, however, I was aware of its global growth. On the other hand, because it is a very prevailing and a concept greatly used in the world of economy in the past few months.

The objective of this work is, in particular, to deepen into the topic of Bitcoin from an objective point of view and accessible to all, and in this way to make it known. It is mainly focused on people who have heard about cryptocurrencies at some point in their life, but do not know it in detail, as was my case before doing this work. I was also curious to know when and where this virtual currency came from, how and what was needed to acquire it and what it was that gave it value, as some people had become millionaires for the simple fact of buying Bitcoins years ago.

As it is a general study on Bitcoin, the project has as main part knowing what exactly cryptocurrencies are and more deeply Bitcoin. In order to correctly perform this analysis, I have asked myself some hypotheses, which are the following: if Bitcoin can be definitely considered a currency, verify the risk of its high volatility and determine if it is necessary to regulate it. The last hypothesis I am considering is to analyze whether the large growth of the Bitcoin price that occurred during December 2017 corresponds or not to a new possible financial bubble.

Regarding the methodology of the composition, I have tried to group and summarize the extensive information developed especially in recent years in a simple and understandable way. It is an issue that is evolving every day, so when doing the work, I have focused on the most recent information and more truthful references. I have been documented through different sources of information, mostly Internet, although I have also used books, news articles, reports and videos. I have tried to select the essential information in order to do this project an agile reading that can arouse interest in anyone who reads it, with the aim of understanding and knowing with some depth what Bitcoin is, as it is a difficult concept to interpret. On the other hand, to develop the most analytical part of this work, I have consulted the charts published in the most used Bitcoin Wallet website around the world.

We can divide this project into three parts, the last being the most extensive one. First of all, I have found it opportune to talk about the origin of the currency and the changes that have arisen since its existence. This has allowed me to contextualize and introduce the second part of this work, the cryptocurrencies one. Once this concept is explained, we find the area with the greatest weight, the Bitcoin. As you will see later, I first made a study of its history, then I explained its operation and its structure, which allowed me to visualize the potentials but also the weaknesses of the currency. In addition, an indispensable part is the analysis of the Bitcoin value's evolution over the years, its legal aspect and last but not least, the current situation it is facing in comparison to other virtual currencies. Finally, Chapter VIII contains the general conclusions about the study of Bitcoin.

At the time of doing the project I thought that I would have some inconveniences, since as I mentioned earlier, Bitcoin is a very current topic and the information can vary drastically from one day to the other. However, this has not been the case, so I have not had many problems. I would also like to add that the fact that there is such a broad breadth of information sources, it has generally been a positive aspect. The reason is that in this way I have verified the certainty of each part of the work since this often can lack accuracy because of a lack of scientific and economic approval. However, I have to admit that at the same time the selection of information has been the most difficult task.

Finally, I would like to thank the effort, advice and dedication of Emili Batlle, who from the very beginning accepted to be my tutor and sound him well the idea of doing the work on Bitcoin. That motivated me and pushed me forward, as you always have the question of whether it will be an interesting topic or not to present.

II. MONEY'S ORIGIN AND ITS EVOLUTION

Before talking and getting deep into the cryptocurrencies' world, I would like to explain briefly how currencies emerged, the change that has undergone throughout history and the reason of cryptocurrencies. In that way, it will be easier for all of us to understand what kind of impact these currencies are having and why are creating such a huge revolution nowadays.

Even though it seems hard to believe, money has been part of human history for at least the last 3000 years. Before that time, there was a direct system of trade, known as **bartering** that allowed people to exchange goods and services without the use of cash. This practice is also called "early commodity money". People would barter goods they had in excess for the ones they had in shortage. In order to clarify this concept, here you have an example:

> *Serena loves romantic books, and she only has this type of novels at home. However, now she wants to read police novels. So, she must find a person who not only has police stories but also wants to read romantic books.*

Why bartering was stopped using? Communities grew, which implied a higher number of exchanges among people and a numerous increase of disadvantages.

• Lack of double coincidence: people have to find someone who has a good or service they want and who also wants the good or service they have to offer.

• Lack of common measure of value: As there is no unit of value, the problem arises in what proportion the two good are to be exchanged.

• Difficulty in storing purchasing power: Goods need to be stored, and they deteriorate over time. As a consequence, people found arduous to store wealth for future use in the form of goods like food and cattle.

• Indivisibility of goods: There are some goods that cannot be divided. *Imagine that Serena, instead of police novels, wants to prepare a meal for his son, and for that needs half chicken.* The owner of the chicken cannot give Serena what she wants without killing his chicken.

With the intention to overcome the above drawbacks of bartering, money was created by the society.

We normally think of currency when we talk about money. However, more generally speaking, money is any commodity which satisfies the following:

1. Medium of exchange → it is used to pay for goods and services. It promotes economic efficiency by eliminating two of the four bartering obstacles.

2. Unit of account → have all prices quoted in terms of Euros, Pounds, Dollars… Using money as a unit of account diminishes transaction costs in an economy by reducing the number of prices that need to be considered.

3. Store of value → money is a repository of purchasing power over time.

Now that we have explained which the main characteristics of money are, I will continue with the creation of the first class of money.

2.1 Commodity money:

From ancient times until several hundred years ago, money that consisted on precious metals and other commodities was called commodity money. In 1100 B.C, the Chinese were the first ones who replace the tools and weapons used as a medium of exchange, for miniature circle replicas of the same instruments in bronze. However, the first minted coins were invented in Lydia, the actual Turkey, in 600 B.C. They were made from a mixture of silver and gold that comes from nature, called electrum.

1. Chinese miniature replicas

2. Lydia's first coins

Lydia's currency gives to the country the opportunity to spread both its internal and external trade, making it one of the most powerful and the richest empires in Asia Minor. Nevertheless, as coins are made of precious metals, money is very heavy and is hard to carry from one place to another. Think, how many coins would you have to wear in your pockets if you want to buy a house? It was really necessary to design a new payment system. Thus, metal was substituted for paper.

2.2 Paper money:

The first paper money appeared in China during the Tang Dynasty (618-907). This practice came from the credit notes used by merchants for their long-distance trade. But it was not until 11th century that banks officially accept paper money as a legal payment.

Regarding Europe, paper money was imported through the great explorer Marco Polo near the 14th century. However, its first use took place in Stockholm (Sweden) in 1661. Paper notes soon became common in the market and were allowed as a means of payment. This shift increased international trade transactions, banks began to buy currencies from other states and this is how the first currency market was build up.

3. Frist paper money in China

Nevertheless, as most countries wanted to standardize transactions in the booming world trade market, a new monetary system was established in 1819 by the British. This one was the famous **Gold Standard.**

2.3 Gold Standard:

It was a reality that Gold had the role of payment method from the earliest times, but the first formal measure that authorize gold as a legal institution was taken in 1819 by the British.

Investopedia defines gold standard as: "*A monetary system where a country's currency or paper money has a value directly linked to gold. With the gold standard, countries agreed to convert paper money into a fixed amount of gold. A country that uses the gold standard sets a fixed price for gold and buys and sells gold at that price*."

Its main goal was to establish a fix exchange rate between countries. In this way, international prices could be stabilized, and nations' growth could be easier to control. By 1900, the majority of the developed states were linked to the gold standard. However, after the First

World War (1918) and the Great Depression (1929), all countries, with the exception of US decided to abandon this monetary system. The war nearly bankrupted the Bank of England and devastated Europe's economy, making governments to lose credibility and cooperation.

2.4 The Bretton Woods system:

After World War 2, it was clear the world needed a new financial system, for this reason delegates from 44 countries met in 1944 in New Hampshire to do so. From now on, the U.S dollar would be the only currency linked to the price of gold, 1 ounces of gold per 35$. The other countries had to fix the price of their currencies in relation to the dollar, the unique coin convertible to gold. In this way, the exchange rates remained almost fixed, with a 1% (positive or negative) of variation. This agreement gave to America an enormous power as it was the only country with the ability to print dollars.

Moreover, the agreement results in the creation of two important institutions present in our world today:

International Monetary Fund	- Monitor exchange rates - Lend reserve currencies to nations
World Bank Group	- Give financial assistance to the countries that participate in WWI, for its reconstruction

In 1971, the Bretton Woods system collapsed. United States underwent a large stagflation, and the dollar's value in gold started to deflate. Finally, the President Nixon determined that the dollar was no longer convertible into gold.

2.5 Fiduciary money:

Little by little, the world's economy abandoned the gold standard giving way to the fiduciary money. This new form of money, was based on trust, since a number printed on a piece of paper marked its value. *For instance, no paper money 50 or 100 euros is really worth that, nor is any currency worth the amount that composes it, but the whole community takes these values for granted and valid to be able to market. They trust in the value they represent.*

Fiduciary money is controlled and issued for the Central Banks of each country and supra-

national institutions like the IMF[11], ECB[22] or EIB[33].

However, due to the huge development of Internet and the global financial crisis in 2008, an alternative to fiduciary money was needed. This is how digital and virtual currencies, like cryptocurrencies emerged.

2.6 Digital vs virtual money

A lot of confusion exists around the terms digital money and virtual money. Let's first define what is understood by digital money. It is any monetary exchange that is made by an electronic medium. When a payment or a shipment of money is done without exchanging physically coins or paper bills, digital money is being used. For instance:

> *People is using digital money when they transfer money from one bank account to another one. Also, when somebody pay with a credit or debit card any good or service.*

Nowadays, practically, all money is digital, as cash only represents approximately the 8% of all the money in circulation.

On the other hand, virtual money, it is defined by the European Central Bank as: "*digital representation of value that is issued and controlled by its developers and used and accepted among the members of a specific (virtual) community*". It only exists in its digital format. In other words: It is some currency created by companies or supporters with the intention of replacing actual cash for a new currency well away from central bank's control.

In conclusion, all virtual currencies are digital. As they do not exist physically, they must be 100% digital. Thus, we can affirm that all virtual money is digital, but not that all digital currencies are virtual. For example, a bank account in euros, is digital but not virtual.

A clear example of virtual money are cryptocurrencies, like Bitcoin, Ripple, Ethereum, Litecoin or Dogecoin. Today cryptocurrencies turned out to be a worldwide phenomenon known by most of the people, companies, banks and governments. Nevertheless, it is an arduous concept to comprehend. Hence, from now on I'm going to center this project on cryptocurrencies and most notably on Bitcoins.

[1] International Monetary Fund
[2] European Central Bank
[3] Euopean Investment Bank

III. CRYPTOCURRENCIES: why did they arise?

When the global financial crisis broke out in 2008, the idea of an effective alternative to fiat money began to be revolved. Internet turned to be a key factor for the development of this thought, as it is available for everyone and we are constantly connected through it. Moreover, computers make our day to day easier, more competent and productive. What used to take us days takes minutes now. Another reality was that after the crisis people lost confidence in Banks. This, led to a new initiative whose main principles were the following: decentralization, transparency and collectivity. That is how cryptocurrencies were introduced little by little in our society during 2009. As we will see later, Bitcoin was the first one.

In general, cryptocurrencies have three main characteristics:

- **They are decentralized:** Meaning that they are not governed or administrated by any financial or governmental entity nor person.

- **They are international**: Allow users to make worldwide transactions through Internet.

- **They use cryptography:** To guarantee transactions' security and to control the creation of additional units of currency.

3.1 Definitions

Once we have explained why they were created, let's illustrate where the word comes from and what it signifies. We have already seen that an important feature of these currencies is that they use cryptography, but maybe you are asking yourself: what is it?

"Cryptography is the use of techniques which make information readable by the sender and receiver, but unintelligible to anyone else. Information is encrypted by the sender before sending and decrypted by the receiver. Thus, cryptography makes privacy possible even on an insecure channel". (Dr. Ronald A Gove "Fundamentals of Cryptography and Encryption", 2007)

"Cryptography is the application of mathematical theory to develop techniques and algorithms that can be applied to data to ensure goals such as confidentiality, data integrity and/or authentication". (Organization for Economic Cooperation and Development, OECD).

"Cryptography is the science of secure communication that, in the presence of adversaries, can listen to and even control the channel of communication. Cryptography is concerned with encryption, the conversion of a message to an encrypted text. An encrypted text that appears

to have no meaning for the adversary who hears on a communication channel, but the recipient knows how to translate it to the original message". (Franco, P. "Understanding Bitcoin: Cryptography, Engineering and Economics", 2014).

4. Cryptography's graphic representation

Now that we know the meaning of cryptography, we are ready to understand the concept of cryptocurrency. As we can deduct, the term "Cryptocurrency" is composed by two different expressions. The prefix "crypto" came from the Greek word "*kruptos*", that means secret, hidden and also the word "currency". Some definitions are shown below:

"A virtual currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank". (Business dictionary)

"*A cryptocurrency is a virtual currency that uses cryptography for security. It is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency, and arguably its most endearing allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation".* (Investopedia)

Following, there is a table that compares traditional money with cryptocurrencies. In this way we will see what we have learned and the differences we are able to identify for the time being.

TRADITIONAL MONEY	CRYPTOCURRENCIES
Physical	Virtual and digital
Linked to a country or group of countries	Global
Issued by governments	Offered through cryptography
Normal security	Optimal security
High monetary policies' influence	Little monetary policies' influence

Henceforth, the focal point of this assignment is going to be the Bitcoin, the first decentralized cryptographic financial network of the world.

IV. BITCOIN

This section is going to be the most extensive of the whole project and it is divided in five different points. I'm going to explain you when and how was created, its functions, its pros and cons and finally its value's development over the years.

4.1 Bitcoin history

As we mentioned before, since 2009 the term of cryptocurrency is heard in our society. Under this denomination, the new concept of money has been given for the exchange of goods and services or the foreign exchange market electronically without the need for intermediaries, which has led to this new scheme being transformed and significantly penetrating the global financial system.

The first cryptocurrency originates under the name of Bitcoin. There are several questions about Bitcoin, but the most typical one is: "Who created it?". The creator of Bitcoin hides under the pseudonym of Satoshi Nakamoto. For many years, find out this mystery became a matter of great interest for many means of communication such as "The New Yorker, Vice or Forbes". Many speculations about the possible founder of this digital active has been made. It has even been thought about the possibility that Satoshi Nakamoto is a group of computer technicians from the European financial sector.

Everything began in 31st October 2008 when someone using the pseudonym Satoshi Nakamoto publishes a message in an Internet forum. The content of the forum was purely scientific, consisting of an academic community mainly mathematical and computer science, "metzdowd.com"[4]; the perfect place to introduce this type of revolutionary currency based on computer science and mathematics. The title of his comment was: "Bitcoin P2P[5] e-cash paper". He announced the following: "*I've been working on a new mean of electronic payment that is completely PEER TO PEER, without the necessity of a third person as intermediary*." It is also available on: "www.bitcoin.org"[6]. This essay described in detail how Bitcoin would work. It was not an easy document to understand, as it included a numerous of technical issues such as: the form of transactions, security, the generation of Bitcoin and the privacy offered by this system; which we will see in detail later on. Two weeks later, the Bitcoin project is registered on "SourceForge.net", a collaborative community for the development

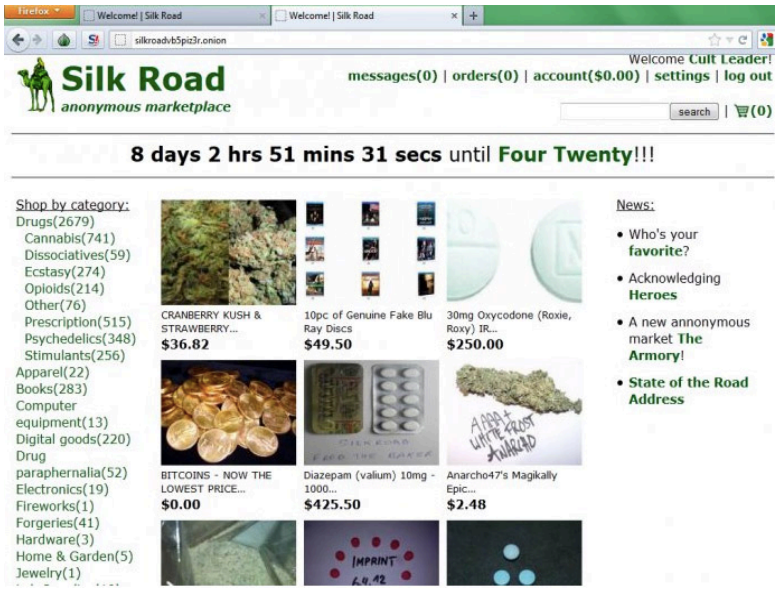
[4] Web where Satoshi Nakamoto published the Cryptography mailing list
[5] Peer to peer: It is a method of file exchange. Establishes a direct connection between computers, without the need for an intermediate service
[6] Bitcoin official website

and distribution of open source software.

On 3th January 2009 at 18:15:05 pm, took place the first Bitcoin transaction between Satoshi Nakamoto and Hal Finney, an American programmer who had a long involvement in the crypto community. This first transaction was called **Genesis Block**, also known as Block 0, is the antecedent that every other block in the chain can trace its lineage back to. The amount transferred were 50 BTC[7] and the text that Satoshi wrote was the following: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.*" This was the Financial Times' headline on 3th January, it warned of the need of millions of dollars for the bank rescue. He did it for two main reasons: The first, to demonstrate that the transaction took place in real time. Secondly, to show that he had created Bitcoin to avoid two major future problems that represented the financial crisis of 2008: bankruptcy and the rescue of financial institutions.

During the rest of 2009, new versions of Bitcoin were released, and people started to be aware of Bitcoin. Nevertheless, it was not until May 22nd 2010, that took place the first real-world transaction. It happened when, Laszlo Hanyecz, a bitcoin miner[8] offer 10.000 BTC for anyone who would order him two pizzas. Someone did, he paid 10.000 BTC for two pizzas valued at 25$. He demonstrated that Bitcoin could be used as a means of exchange. The transaction valued each Bitcoin at around 0,0025$; as we will see later, an exchange rate unthinkable nowadays. During this year, the Japanese website MtGox was launched. It became world's leading Bitcoin exchange site, handling more than the 70% of all BTC transactions in 2014.

5. Silk Road's official website



From now on, Bitcoin value started to rise, achieving on February 2011 parity with the US dollar, which means that 1BTC = 1$. Over time the popularity of this new and novel way of conceiving the currency caught the attention of another type of public that saw great potential in their privacy and began to be used for purposes of concealment of illegal funds and transacttions of dubious legality.

[7] BTC = Bitcoin

[8] Bitcoin miner: people that use special software to solve math problems and get paid for that. They are the ones to approve Bitcoin transactions

Ross Ulbricht, a young man from Texas, with a bachelor's degree in physics, decided to take advantage of Bitcoins creating a new website called Silk Road. His intention was to create a free market place outside the scope of government control. The products sold in this page were mainly drugs, and other illegal goods, which only accepted Bitcoin as a payment method. Because Bitcoin transactions are pseudo anonymous you cannot prosecute who makes or receives the payment. This dark side of Bitcoin attracted the attention of the regulatory entities of the different countries and, as we will see in a later section, favored the regulation of the same in different aspects. In addition, users of this illicit website downloaded a software called "Tor", that encrypts data and enables Internet communication by anonymizing IP addresses. Even thought, the authorities were aware of the existence of Silk Road shortly after its creation, it took them more than two years to disclose Ulbricht's identity. On 1st October 2013, he was arrested and accused by the Federal Bureau of Investigation (FBI) of being the mastermind behind the site. The crimes for which he was accused were the following: conspiracy for drug trafficking, computer hacking and money laundering. Finally, on 29th May 2015, he was sentenced life imprisonment without the possibility of parole.

Despite this, the downloads of Bitcoin did not stop growing. Another influential website where you can buy and sell bitcoins was designed, known as "BitInstant". Every time there were more and more Bitcoin miners highly qualified. As a consequence, Nakamoto went from being the leader of the cryptocurrency to take a back seat. That is why on April 2011, he announced in Bitcoin's official site that "he is going to take care of other things". Never again anybody has had news about him after that goodbye message.

6. Bitcoin Foundation logo

During 2012, the acceptance of Bitcoin made a huge boom. The Bitcoin Foundation, a nonprofit corporation with the aim to accelerate the global growth of Bitcoin and standardize it as an exchange method was set up. Moreover, WordPress, the well-known platform to create free websites and blogs started to accept Bitcoins. On December, it was created in France the first Bitcoin exchange to operate as a real bank within the framework of European regulations, named Bitcoin-Central. In this way, clients will be able to deposit their capital into the service in either euros or Bitcoins, and they will be able to convert these funds in both currencies.

Over the next two years, Bitcoin price increased a lot. Even though some days its price dropped, it recovered quickly. At the beginning of 2014, the Bitinstant CEO was arrested over allegations of money laundering related with Silk Road. One month after the fall of Bitinstant, the Japanese MtGox had filed for bankruptcy and reports that 744.000 bitcoins had been

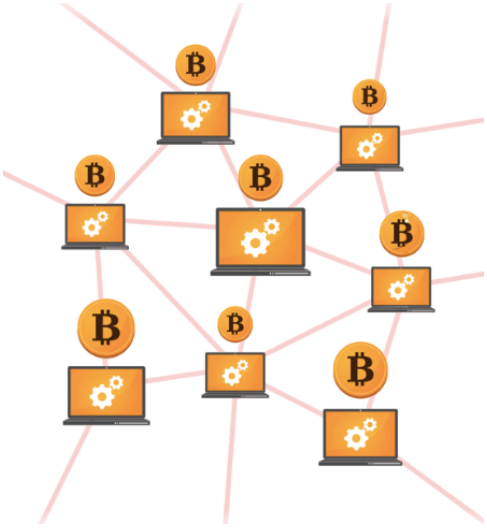
stolen, which represent the 6% of the total in circulation. Nevertheless, downloads and miners keep ahead rising. On December 2014, Microsoft began to accept Bitcoin to buy Windows software and Xbox games.

In 2015, Craig Wright, an Australian computer scientist declared himself publicly as the man hidden behind the pseudonym of Satoshi Nakamoto. But the authorities did not believe him, they claim that the cryptographic keys he presented, with which he developed the Bitcoin platform, were not convincing. So, to this day, Satoshi Nakamoto's identity remains a mystery.

During 2016 and 2017, the big Bitcoin boom comes. In spite of its rise in value, its popularity is demonstrated in other areas. For instance, in September 2016, the number of Bitcoin ATMs around the world reached 775 ATMs, reaching in April 2018 a total of 2662. Another example of its exponential growth is the number of Bitcoins articles published in Google Scholar; 83 in 2009, 427 in 2011, 3790 in 2014 and 5840 in 2017. However, since the end of 2017 this cryptocurrency is losing part of its value as we will see in more detail following. Now that we know the origin of Bitcoin and the most relevant events since its creation, we can take a step to the following point.

4.2 How do they work?

As we have mentioned before, one of the main characteristics of Bitcoin is that its network is based on a "**peer to peer**" or "**P2P**" system. It is a network of computers in which a series of nodes (each of the machines, computer = node) behave as equals to each other. Meaning that they act at the same time as clients and servers with respect to the other nodes of the network. In order to take part of this network, people have to download a program to a computer with which the computer becomes a node of the P2P network. The network allows the direct exchange of information, in any format, between the interconnected computers, as all of them use the same norms for communicating. These norms belong to what is known as Bitcoin Protocol or Blockchain Protocol (in the following point 4.3 I will explain in detail the concept of Blockchain). All movements are registered in this protocol, which is completely public and transparent. Everybody has the permission for checking it. In fact, only in this way Bitcoin has been able to win the trust of so many people worldwide



7. Representation of a P2P network

and grow so much during these years. This has allowed breaking with a problem in all the means of previous payment, the need for a third party. Because it is a decentralized cryptocurrency does not need a central authority consent, as for example that of a bank.

Now that we know that all Bitcoin users are related to each other thanks to P2P system, I am going to explain how transactions are done, what we need for that and where our Bitcoins are saved. At first glance, the functioning of this cryptocurrency is difficult to understand for many people, but you will realize that in fact it is easier than it seems. We will have to have three basic terms in mind, which are: virtual direction, wallet and transaction.

First of all, I would like to explain what a **virtual direction** is. Virtual directions are practically the same as e-mail addresses. Every user of Bitcoin has one, it is essential for receiving and sending money. People get a direction when they register to a Bitcoin app. Thus, depending on how many times do you sing up, you can have as many virtual directions as you want, they completely are free. These addresses are generated by mathematical parameters that allow all addresses to be unique, thus there will never be two identical. With these "credentials" you can access at your Bitcoins from any computer connected to the Internet. Each direction consists of two parts that are mathematically correlated:

PUBLIC DIRECTION	PRIVATE DIRECTION
The one that everybody has information about. Anyone who knows it, is able to send you Bitcoins at any time.	The one that allows you to identify yourself, access the funds you have at that direction or make shipments. It is highly important to keep in secret your private direction. Otherwise, anyone could have access to your Bitcoins.

1Hg7wA7JMuMtpXbPMLi6XXh1XwrKK4fwUC

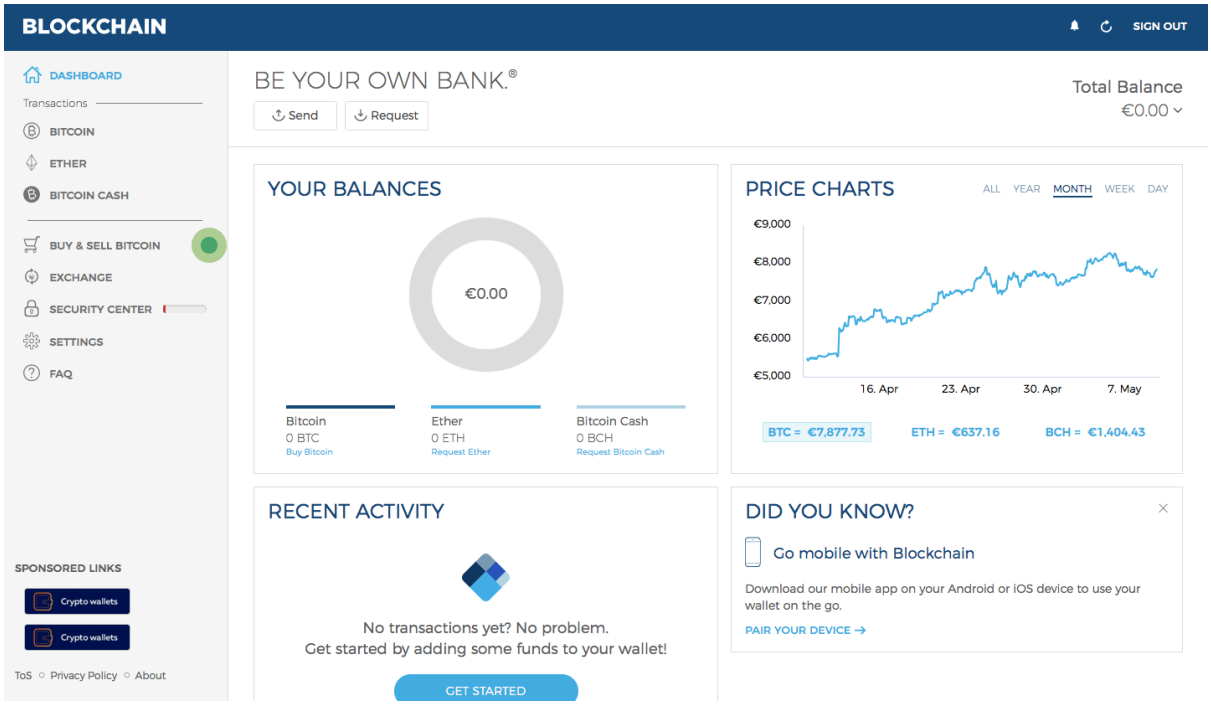
8. Public direction example

The following picture shows an example of a public direction. As we can observe it is composed by a series of numbers and letters, that can be copied like a link. All directions begin with number 1 or 3. In addition, each direction has a QR code that can be easily scanned with a smartphone or tablet. Private directions are even longer than public ones.

Now that we have comprehended what a virtual direction is, let's talk about Bitcoin **Wallets**. It is the place where Bitcoins are kept, equivalent to a bank account. There are hundreds of apps and programs that you can use to check your Bitcoin balance, the only thing that you have to keep in mind is the private virtual direction. Without it, it would be impossible to have access to your wallet. One of the most important aspects when using a Bitcoin application is its security. There are three fundamental characteristics that each Bitcoin application or program should have:

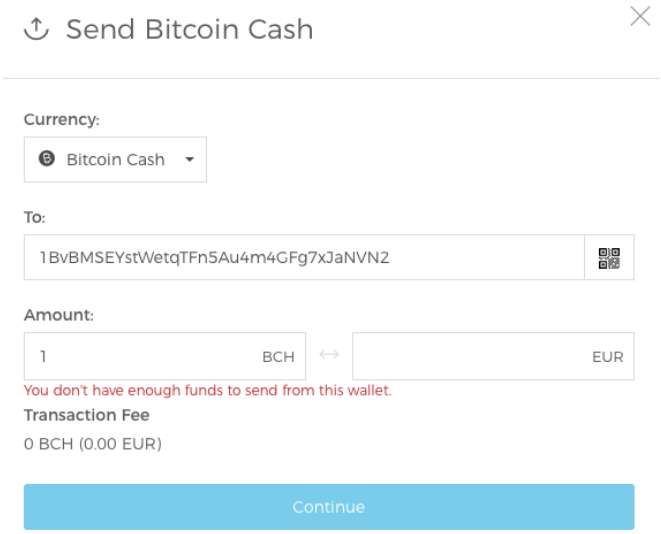
→ To be an open source: Only a program that reveals its internal functioning will be reliable
→ To have many users: It is a good sign of reliability.
→ Incorporate measures to protect the private key: Use of a security word or sentence.

To show you in a better way how it works, I have created an account to one of these Bitcoin Wallets applications, called: "Blockchain".



9. Blockchain wallet application

This first picture shows what you see when you sign in to the app. On the left side, we have the menu and marked in green the option of "buying and selling bitcoins". In the middle of the screen we can observe our total value, in this case 0€ because I do not have any Bitcoin, and additional information. The more Bitcoins the higher the value of our Wallet would be.



10. Blockchain wallet application operation

This second picture represents a Bitcoin transaction, explained in more detail into the next page. As we can see, the currency used is Bitcoin. The following step is writing the public direction of somebody. I used one that I found randomly in Internet. Finally, it shows the BTC amount that I would like to send and the conversion in Euros. However, as my balance is O BTC, the conversion does not appear.

As you can observe the steps needed to send Bitcoins are very easy to follow. Anyone could do it. Once virtual directions and wallets have been explained, we move on to the **transactions** mentioned above. The process of sending money, receiving it or making payments with Bitcoin, it works exactly as a money transfer to your bank account. This is one of the reasons of its great success. Each direction has a value, determined by the number of BTC that everyone has. That value can increase or decrease depending on how many transactions we do. This is when the "peer to peer" network that we mentioned in the previous point comes into operation. The interconnected nodes are the ones in charge of registering the new direction's value and spread that information to the entire network. It is important to remind that the transaction is totally unalterable thanks to a complex cryptographic security system. To clarify this process, let's see an example:

> *Serena has 10 Bitcoins, and she wants to send Patrick 4 of them. Serena uses its private direction to identify herself in the network and announces the new transaction. Serena uses Patrick's public direction to send him the Bitcoins. Then, the Bitcoin network registers the corresponding information (both directions and the amount), the one that is stored in the blockchain.*

As all transactions are stored, they are absolutely public and transparent, something that does not happen in the traditional system. Nobody knows the real identity that is hidden behind the direction used. In this way you get a system that is not only secure at the computer level but also gives you confidence by means of its inherent transparency thanks to the mentioned Bitcoin Protocol or Blockchain Protocol.

4.2.1 The miners and their implications

Now that we have understood how Bitcoin transactions are made and what we need for doing them, I am going to explain one of the most frequent questions that arise when people think about Bitcoins: who or how are they created? For answering this question, it is crucial to talk about **miners**.

I am sure that at one time or another if we have heard about Bitcoins in the news or newspapers, we have seen that some kind of reference has been made to the miners. First of all, we should have in mind that Bitcoins are generated when the miners discover a new block[9]. For that, miners use a special software to solve complex mathematical problems and as a reward they receive a proportional amount of Bitcoins. This provide a smart way to issue the currency and also creates an incentive for more people to mine. Thousands of computers around the world "mine" Bitcoins competing with each other. They work 24 hours per day, seven days per week. This mathematical challenge is always the same in its process, however, the variables are different. It can only be solved by trying random numbers without stopping until finding the result that is sought at that moment. The first one who gets it, gets the reward. At the very beginning, solve these types of problems it was relatively easy. In fact, miners solved them with the processor of their PCs. Nevertheless, the number of miners it was getting bigger and bigger. As a consequence, solve these math problems was harder every time, because the Bitcoin network changes automatically its difficulty depending on the number of miners. Hence, the more they were, the more arduous. To overcome this, miners have decided to join in groups and work together with other miners. These groups, are known as, “pool miners”. They find solutions faster than doing it individually and each miner is rewarded depending on the amount of work he or she provides. Soon, miners realize that the processors of their graphics cards were more efficient, but they consumed lot of electricity. Nowadays, there is a specific hardware called ASIC[10] which consumes much less.

11. Bitcoin miner hardware

12. Bitcoin miner USB hardware

[9] Block: Set of new unique transactions recently made in the Bitcoin network. They are verified every 10 minutes through the mining. The set of blocks compose the Blockchain.

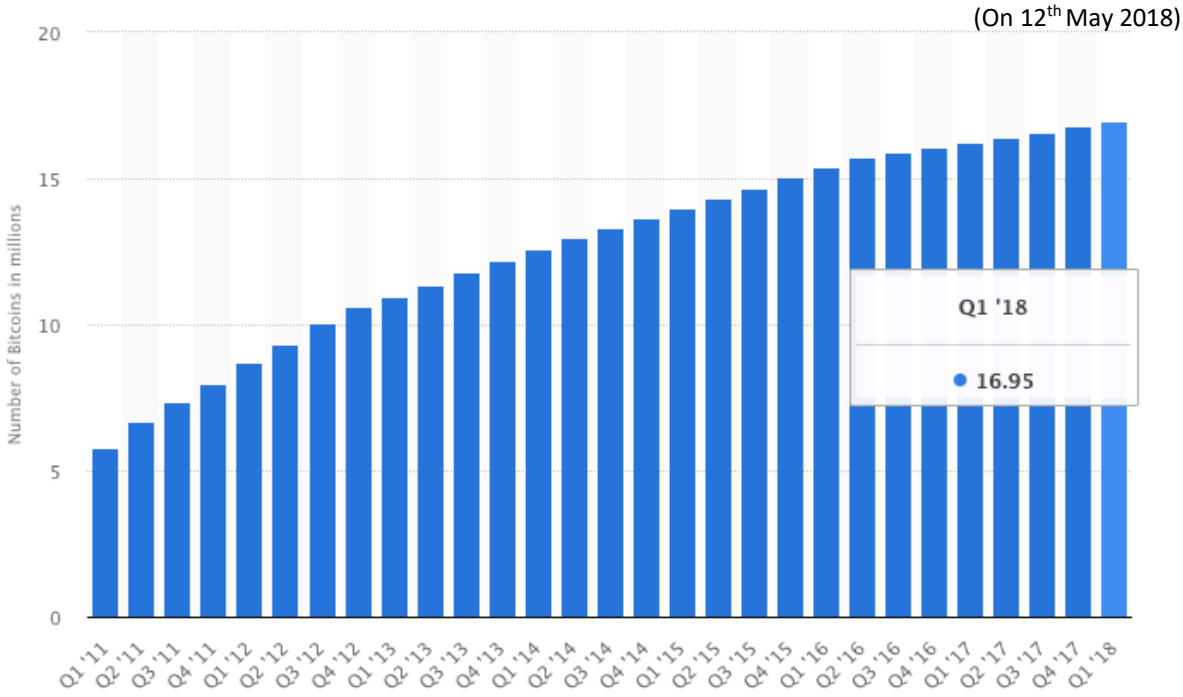
[10] ASIC = Application-Specific Integrated Circuit chip

These two pictures show two types of hardware that miners use to unlock Bitcoins. The unit by which is measured the computing power of the equipment used to obtain cryptocurrencies is called “hash rate”. A higher hash rate implies a higher speed to mine and getting benefits faster. For instance, when the network reaches a hash rate of 10 TH/s, it means that it can do 10 million calculations per second. This hash rate is directly related with miners’ reward as we will see later on. Another important task about miners is that they are the ones who approve transactions. So, we can affirm that miners maintain Bitcoin network stable, safe and secure.

As I have already explained, as new bitcoins are discovered and more miners there are, the complexity of the mathematical problems rise. But, the question is why? The reason is the following: One of the main attractive characteristic of Bitcoins and that I have not discussed yet, is that it is a limited currency. What does it mean? There is a maximum quantity of Bitcoins that can be find out, and this upper limit is **21 million Bitcoins**, which will not be available in full until the year 2140. This is because Satoshi Nakamoto decided to create a deflationary currency, such as gold. It has its logic, if something is scarce naturally, it is more likely to have value. If Bitcoin could be created indefinitely and uncontrollably, it would not have value, or it would be very temporary. If you limit its creation, it increases the probability that this good, have value.

According to the official website of “www.statista.com”, nowadays there are more than 16.950.000 Bitcoins mined. In the following graph, we can see the number of bitcoins in circulation since 2011 until now.

13. Evolution of the number of Bitcoin in circulation (On 12th May 2018)



If in the future the use of Bitcoins continues to increase, we will be able to see transactions by less than 1 BTC. That is possible because Bitcoins are divisible coins. Given its digital nature, it can be divided up to 8 decimal places. This means that the minimum amount of bitcoins that can be owned is 0.00000001 BTC, which as a tribute to the creator is known as a Satoshi. That is, 100.000.000 Satoshis are needed to form a Bitcoin. Next, there is a table with the denomination of each division of Bitcoin.

1 BTC	A Bitcoin
0.01 BTC	A Bitcent
0.001 BTC	A mbit
0.000001 BTC	An Ubit
0.00000001 BTC	A Satoshi

When people began to have knowledge of Bitcoins and their characteristics, two questions related to the limit of them arose.

The first one was: what miners will do when all Bitcoins will be discovered? We should have in mind that without miners, transactions are not approved, and the whole system behind Bitcoin comes down. Today, miners receive a little amount of money for each transaction and proportional reward for block mined. However, when Bitcoin reaches its limit, the unique source of income for the miners will be the commissions for the confirmations of the transactions. So that the miners do not disappear, two things must happen: either that the commissions are higher or that only the most efficient miners survive. Furthermore, there is also the possibility that if the Bitcoin price is low and the cost of electricity is excessively high, maybe miners disappear and with them the virtual currency.

The second one was more related with the rules of Bitcoin. Can someone generate more Bitcoins than the existing ones? Only the limit established in the Bitcoin Protocol could be changed if more than 50% of the miners agreed on changing it. Fact that is practically impossible because it would harm the miners themselves. The more Bitcoins, the lower would be their value. Hence, the answer to this question is clearly no.

On the previous page, we talked about the hash rate, and we have made reference to the relationship between this rate and the miners' reward. So now we will see it.

<u>How is Bitcoin's reward determined?</u>

The founder of Bitcoin, Satoshi Nakamoto, established in the Bitcoin Protocol the reward that the miners will obtain. It is one of the basic rules of the cryptocurrency and it can only be

modified if there is a mutual agreement between the entire Bitcoin network. As we know, the same thing should happen if the bitcoin limit wants to be changed.

The reward per block started at 50 BTC in block number 1 and is divided into halves every 210.000 blocks. This means that each block up to the block 210.000 will be rewarded with 50 BTC, while block 210.001 will be rewarded with 25 BTC. Since the blocks are extracted on average every 10 minutes, 144 blocks are extracted per day on average, the equivalent of 1,8 Bitcoins per day. At 144 blocks per day, 210.000 blocks take an average of four years to mine. We know that nowadays there are more than 16.950.000 BTC mined, thus, 80.71% of the total number of available Bitcoins. So, currently, the reward is 12,5 BTC. The next cut in the reward for mining will occur more or less within two years, at the beginning of June 2020, so it will be reduced to 6,25 BTC. That is why we can say that there is a clear relationship with the hash rate. The higher the speed of the hash, the faster it will unlock the Bitcoins and the faster it will reach the level of Bitcoins needed to reduce the reward of the miners. Hence, another interesting question arises: What happens when blocks reward become smaller? We should take into account two things:

✓ Bitcoin users pay a fee when they send a transaction on the P2P network. Today, these fees are low as the number of users is not very large. Eventually, these transaction rates will increase and will help to compensate for the reduction of the reward by blockade.

✓ Rewards' cuts decrease supply, which may cause the price of Bitcoin to increase. That rise, can help to compensate for the reduction of half of the reward.

Therefore, in some way or another, the miners' compensation will not be greatly affected. Now that we have learned about Bitcoin functioning, the miners and much of its key features, we can move on to the next point. This one is the blockchain, in this way we will hopefully completely understand the use of Bitcoin.

4.3 Blockchain

The Blockchain is a word that we have seen written several times throughout this project. Nevertheless, we have not yet explained what it constitutes nor deepened in why it is so important, since I considered that in order to understand this term I had to explain many other concepts previously. It is the most important innovation and the key element of Bitcoin.

As we already know, one of the most special characteristics of Bitcoins is that they can be transferred to another person without the need of a third party. This is when the blockchain comes into play, which basically eliminates the intermediaries, decentralizing all management. The control of the process is of the users, not of the banks, which are continuously interconnected through the well-known P2P network. So, what exactly is the blockchain?

We can define it as a public general ledger, a huge database, in which all types of transactions are being targeted. This means that it contains a verifiable register of all the transactions that have been made since its creation, in the case of Bitcoin, from the Genesis' Block until today. It is composed of a sequence of blocks that are linked and encrypted to protect the security and privacy of transactions. When a block reaches its total capacity, a new one is created, which is directly related with the preceding one, as each new block includes a specific code from the prior block. Based on the transactions processed in the network, the system will determine how many Bitcoins "each user account" has. Moreover, it can only be updated based on the consensus of most system participants and, once introduced, the information can never be deleted nor modified.

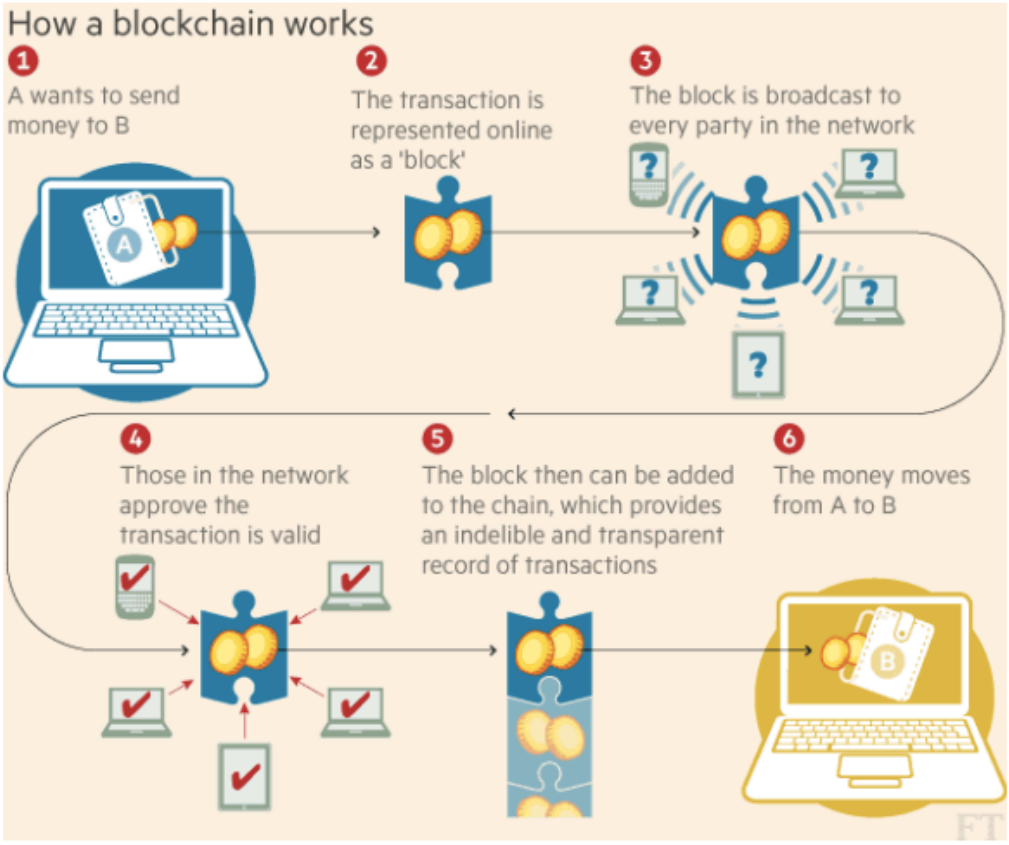
To understand its function in a better way, I am going to put an example similar to the one that I used in point 4.2:

> *Serena (A) wants to send Patrick (B) 1 Bitcoin, but first announces it to everybody with a peculiarity: "nobody knows that Serena is Serena and that Patrick is Patrick". They only know that from digital wallet to another one, that quantity wants to be send. When Serena transmits her message, all users in that network first verify that the home portfolio has enough money to be sent to the destination portfolio.* If that is the case, all write down that transaction, which goes on to complete and become part of one block. It is in this moment when Bitcoins ship from A to B.

As time passes, more and more transactions are completed and moving to that block, which has a limited capacity that depends on the structure of the blockchain and the size of each

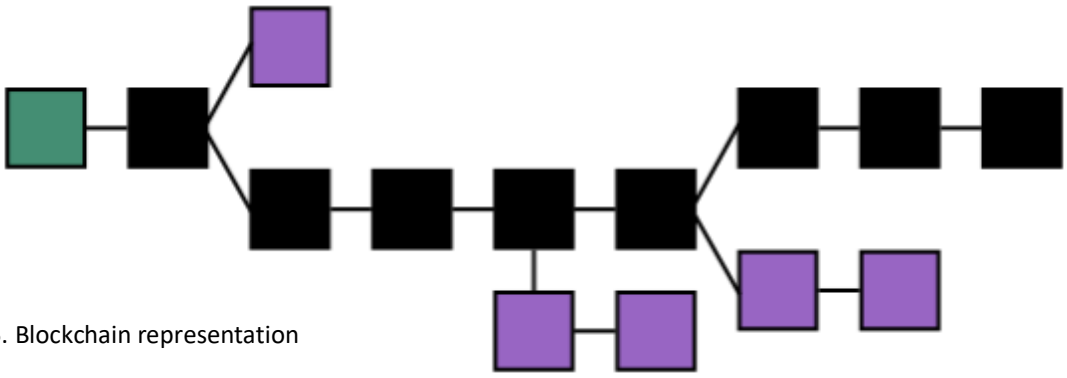
transaction. When a block no longer supports transactions, there comes an important moment: the time to validate it, which is what miners do. The block will be added to the blockchain and the miner who has made the process receives the corresponding reward, new Bitcoins.

Following, you have a graphic representation of the process explained above:



14. Blockchain's process representation

The term of "Blockchain" is created as a combination of two different words. The first one "block" and the second one "chain". It is named like this because when blogs are grouped, they form a kind of chain, as we can see in the picture below. The first of them, the green one, is the so-called "Genesis block" created by Nakamoto, inventor of Bitcoin. As we can



15. Blockchain representation

observe, the blockchain is not lineal, in certain cases the block processing fails generating two paths from the "leader block". This situation arises when two miners arrive at the same time at same block. Both of them solved the mathematic problems, but only one of the generated blocks will be able to be part of the chain. These blocks are the ones in purple, they are called “Orphan blocks”. However, this does not mean that orphan blocks fall into oblivion, but the system adds them back to the pool of transactions pending resolution. The blocks pained in black construct the main chain.

Another advantage that provides the blockchain is that it lets its users know all the route that bitcoin has followed from someone’s wallet before getting to someone else’s wallet, without disclosing any identity. In addition, it confirms that each valuable unit (Bitcoin) it has only been transferred once, which avoids the traditional problem with double spending. Now, I’m going to explain briefly what does in mean.

Basically, in other words, the blockchain prevents the same transaction from occurring twice. With traditional money, physical one, this problem cannot take place. Why?

> *Imagine that Serena goes to Zara and buy a pair of jeans for 20€. She pays in cash. Now that 20€ in cash is in the cash vault of Zara. By all means, she simply cannot spend the same 20€ somewhere else to make another purchase. The service provider at Zara instantly validate that Serena have paid, and she received her pair of jeans in exchange for the money.*

However, with digital money this verification system is missing. This is why Satoshi Nakamoto solved this problem by including a distributed time-server, that is in charge of identifying and ordering the transactions carried out in order and prevents its modification to make another expense. The bitcoin system will confirm the first transaction included in the blockchain. Bitcoin does not establish any special intermediary like banks and it is the network nodes that maintain a copy of this accounting book called Blockchain.

> *Now, suppose that Serena wants to buy a handbag to a merchant. This one costs 1 BTC. She decides to make the transaction. One minute later, she again sign and send the same 1 BTC on another Bitcoin address to try and trick the merchant. What would happen? In this case, just the first transaction will be verified by miners in the next block. Miners will judge the second one as invalid because it would not get enough confirmations, thus it will be pulled from the network.*

Now that we know well how Bitcoin works, we can move on to analyze what its advantages and disadvantages are.

4.4 Benefits and drawbacks

Throughout the present work it has been shown that Bitcoin has many advantages for people that use and has a commercial relationship with them. They are use it for acquiring goods and services or because they think that is a good source of investment. However, it is not beneficial for everybody. As we will see in point 4.5, governments and central banks have imposed some Bitcoin restrictions or even prohibitions. Following up, the pros and cons of this cryptocurrency are presented.

BITCOIN PROS

✓ ***Global currency:*** Money can be sent or received instantly from and to anywhere in the world, at any time. People have not to worry about crossing borders, rescheduling for bank holidays, or any other limitations one might think will occur when transferring money. Since Bitcoin is decentralized, you are the one who have a complete control over your money, no authority has the right to take away your Bitcoin.

✓ ***Fast payments:*** International transactions are received within a maximum of 10 minutes, even on weekends. This is because miners approve transactions every 10 minutes. Moreover, the one who receives the transaction can choose any platform or application to receive it, provide that you know what your passwords are. With banks this process can take several days.

✓ ***Neutral and transparent***: all the information is available in the blockchain, it is public, so that anyone can verify this information whenever they want. Falsification is impossible, as we have seen, if somebody tries to pay twice with the same Bitcoin, the system detects and rejects the transaction. For this reason, merchants' risks are reduced, protecting them from losses caused by fraud.

✓ ***High security:*** Thanks to the blockchain transactions are secured by cryptography. Users have complete control over their transactions. In addition, as we have seen each user has a public and private direction, which allows doing transactions without the need of reveling your identity. Moreover, due to the high complexity of the system it is very difficult to hack.

✓ ***No need of intermediaries***: As we mentioned several times, it is one of the main characteristics of Bitcoin. Any user or buyer may pay directly without the need of a confirmation from a third party (bank).

✓ ***Very low or null commissions:*** Nowadays, there are either no fees, or very low fees within Bitcoin payments, as miners are compensated by the network with newly issued Bitcoins. Another reason is because as there is no bank involved, any commission has to be paid to them. However, you can choose to pay a small voluntary fee to increase the priority of the transaction and remunerate the people who operate the network. It's rare for a Bitcoin transaction to cost more than 1% of its value. Compare that to 2% to 3% for most other digital payments, such as credit cards and PayPal.

✓ ***Protection against Inflation:*** With fiat currency, governments can print as much money as they want, which will make prices rise. Nevertheless, as Bitcoins are limited (21 million), no more Bitcoins will be created. Scarcity is an important aspect of currency which protects it from inflation.

BITCOIN CONS

× ***High energy consumption:*** A lot of energy is needed for mining, it is the greatest enemy for miners. Having mining as the only source of income can be profitable or not, all depends on where you live, the cost of electricity, the total of miners there are in pools and luck. In Spain electricity is very expensive and it is not recommended to mine, but there are other solutions. You can rent miners from other countries and mine without buying the equipment, driving them at a distance. Many of these devices are found in countries with lower electric cost because they are cold and air conditioning is not needed, so they do not overheat. We speak of countries such as Norway, Finland or Iceland.

× ***High volatility and uncertainty****:* The Bitcoin market is similar to that of the stock market, prices increase and decrease constantly. Bitcoin has volatility mainly due to three facts. The first one is that it is so new. Secondly that there is a limited amount of coins and the demand for them increases by each passing day. Third, there is no authority regulating its use. Most speculators wish to take advantage of it, but some investors think of it as too risky and therefore all the investors do not invest in Bitcoins. As we will examine in point 4.5, during lasts years, Bitcoin price has grown exponentially. Nevertheless, its price has also dropped in some cases, for instance, when Mt. Gox collapsed the value fell by more than 50%. Due to this volatility, uncertainty also increases, and with it the risk.

× ***Black market:*** A clear example that we have seen previously was the Silk Road website. Criminals could take advantage of the private identity that this system offers, by buying or selling illegal goods in exchange of Bitcoins. This would harm Bitcoin reputation.

× ***Low regulation:*** Some users have been affected for transactions' fraud. For instance, they purchase goods that the seller never delivers, and they can't request a refund through Bitcoin. Not having a centralized currency by a State or a Central Bank has its consequences. On the other hand, other newer cryptocurrencies, such as Ripple, have rudimentary chargeback and refund functions, but this feature has yet to be built into Bitcoin. Although as we will see later, some regulations have been implemented for Bitcoin.

× ***Still developing:*** It is true that during the last three years, Bitcoin has grown so much. However, lot of people are not aware of cryptocurrencies and therefore of the Bitcoin. A fact that demonstrates this disadvantage is the number of transactions done per second. While only 240 transactions per minute with Bitcoin are made, VISA registers 100.020 transactions per minute. Although many businesses have implemented this currency as a means of payment, there are still very few if we compare them with the total. Another factor that aggravates this disadvantage is that Internet is not available in all countries. According to data recorded by the World Bank, there are still more than 3.000 million people who do not have Internet access, which represents the 40% of world population.

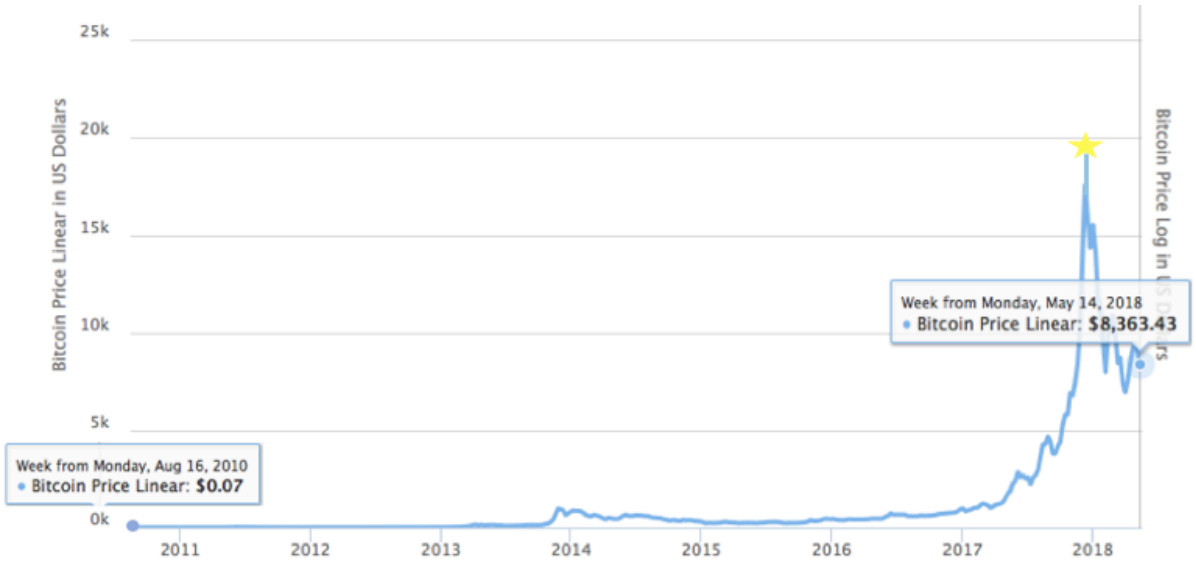
× ***Can be replaced by other Cryptocurrencies:*** The creation of Bitcoin has given way to other cryptocurrencies that could shade Bitcoin in the future. Many of them are structurally similar to Bitcoin, but others introduce new improvements. In point 7, we will see some of them.

Here we have both sides of the coin. There are always pros and cons to any situation in life. Bitcoin, as you can prove, it is not perfect. It is obviously that has many benefits that physical currencies do not provide to its users; nevertheless, it also has its drawbacks. This is because Bitcoin is still a very new currency. If Bitcoin wants to succeed, more people would need to understand what it is and how it works. However, we should have in mind that regardless of the temptation Bitcoin offers as a means of exchange, there is no proof that it will be a viable substitute for traditional currencies.

4.5 Bitcoin's value and transactions evolution

Bitcoin, as we already introduced, it is characterized by its high volatility. Throughout its short, but intense existence, a single Bitcoin has gone from literally worth nothing to almost 19800$. From here, two questions arouse the curiosity of many people: "how much a Bitcoin cost?" and "how and who determines its price?".

The Bitcoin market exchange works exactly like the market for any other product, taking into account the supply and demand; with the handicap that Bitcoin is based on the trust of its users. This means that its price its determined by its buyers and sellers, it will be worth what people are willing to pay for it. Hence, the more people buy Bitcoins on the platform the more their price will rise and the same will happen the other way around, the more people sell their Bitcoins the more their price will go down. Logically, another key factor related to the demand that determines the value of Bitcoin is its popularity: the more known the currency is and the more people want to use it, the more its demand in the exchange markets will increase and it will increase in value. It is important to highlight that the Bitcoin market regulates itself, there is no financial entity or authority that control its price. Bitcoins purchase and sale offers are reflected in the "Order book". A digital place where the offers of purchase and sale of Bitcoin are in standby until another user accepts the offer (purchase or sale) and the transaction is made. Following, I will show the value's evolution that this cryptocurrency has experienced since its beginnings until today.

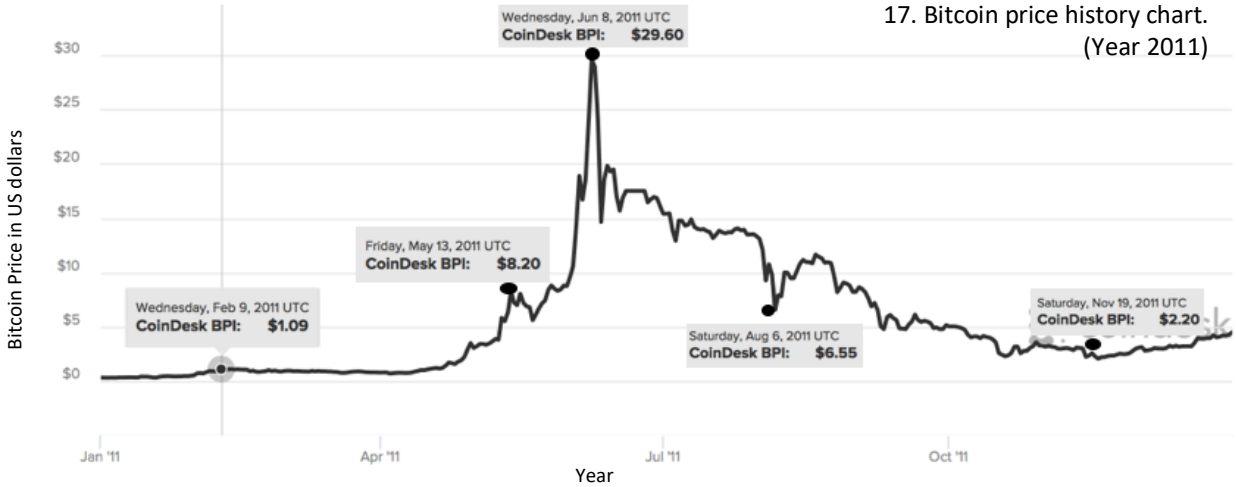


16. Bitcoin price history chart.
(On 14th May 2018)

Despite Bitcoin was created on 2009, any exchange took place, technically, it was worth 0$ during that year. As we have seen in point 4.1, it was not until May 22nd 2010, that took place the first real-world transaction, when Hanyecz paid 10.000 BTC for to pizzas, valued each BTC at around 0,0025$. The initial date of this chart is on 16th August 2010, when Bitcoin price was 0,07$. The last date shown is May 14th, when I checked the website. That day the average Bitcoin value was 8363,43$. It cannot be denied that there is big difference in comparison with the first value, fact that has made Bitcoin so popular during the last two years. The blue line that forms the graph, despite being very general, has allowed us to have an overview of the path that Bitcoin has followed since its beginning, as the data of 9 years is shown. Nevertheless, I am going to add more graphs where we can see more in detail the changes that this cryptocurrency has experienced during shorter periods of time. In this way, it will be easier to verify one of the main hypothesis of this project, analyze Bitcoin's volatility.

Many economists from around the world, such as J. Stiglitz, P. Krugman and R. Shiller, all three winners of the Nobel Prize in Economics, assure that Bitcoin is another "financial bubble". Other well-known economists like X. Sala Martín, professor at the University of Columbia and P. Donovan, chief economist at Swiss Bank UBS, also point to the Bitcoin bubble. Since the existence of Bitcoin, it is possible to distinguish three large "bubbles" that have experienced this currency, which we will see below. All three "bubbles" coincide with one incident: the price of the currency shoots up and then fall dramatically in a matter of days, not to say hours.

■ The following Chart, which goes from the 1st January 2011 until 30th December 2011, shows the first big fall of Bitcoin in its history, called "Silk Road's Bubble". In order to be able to evaluate it, we have to move to 2011. As we have seen before, on February 9th 2011 the Bitcoin surpassed, for the first time, the dollar. Four months later, on 1st June of the same year, a report about "The Silk Road", the famous black market, was published. From then on, the press began publishing articles about it and Bitcoin price stared to rise. As I mentioned



17. Bitcoin price history chart. (Year 2011)

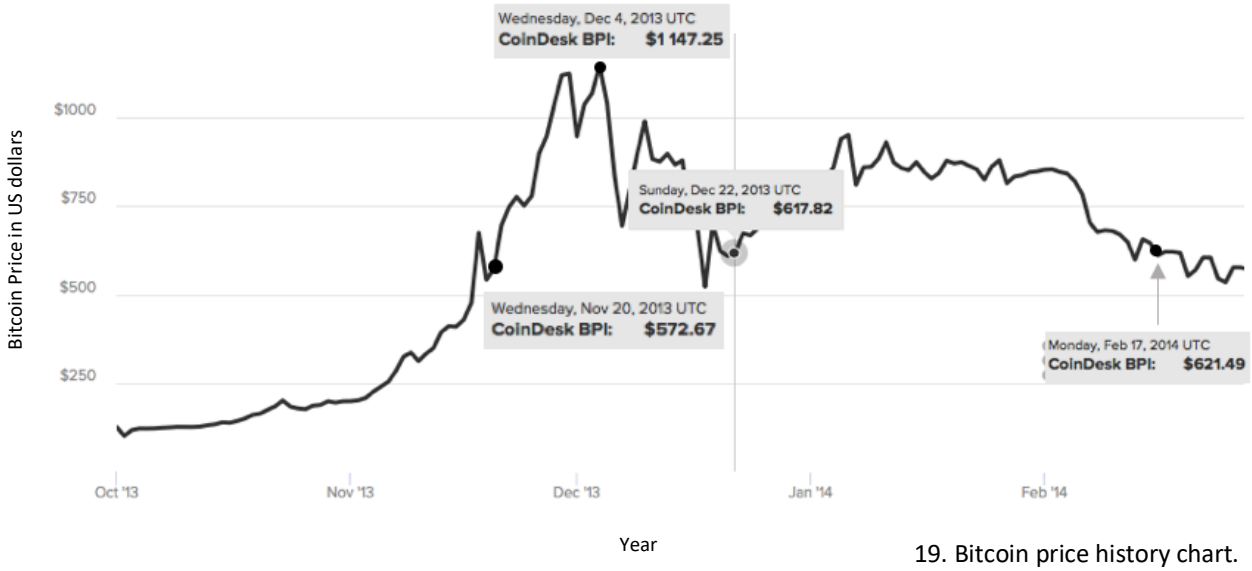
earlier, the popularity of Bitcoin increases the demand and consequently its price. This is exactly what the graph represents. On 8th June of that year, the currency peaked at 29,6$, a real large increase compared to the value it had at the beginning of 2011. However, the euphoria did not last long. When the Silk Road's publications were no longer the first news, the price began to drop, on 6th August, it was 6,55$ and as we can see in the graph, it would continue to do so. In 2012, the price of Bitcoin remained more or less stable it rose from being valued at 6,33$ at the beginning of the year to ending it above 17$.

■ The second big crack, named "Cyprus' bubble", takes place at the beginning of 2013. The next graph shows data from January to July 2013. Cyprus had become a kind of tax haven in the middle of the Mediterranean and the crisis threatened to wipe out all the country's savings. The situation was so tense that between March 16th and 28th authorities forbidden to take money. This made many Cypriots see Bitcoin as the only way to survive and began to invest their savings in it. Therefore, its price rises a lot; in less than one month, Bitcoin grew a 375%. As the graph proves, when the bank freeze finishes on the 28th, the value was 86,18$. In a matter of days, on 9th April, the cryptocurrency attained the 230$. In this case, too, exactly how it succeeded with first Bitcoin bubble, in less than a week, when the situation normalized, the price had collapsed to 68$. During the next 6 months, there was no such drastic change.

18. Bitcoin price history chart.
(January – July 2013)

■ The third Bitcoin bubble takes place on 2013 too, known as "China's bubble". Specifically, it began on November 20th when Yi Gang, the director of the State Administration of Foreign Exchange and the deputy governor of the People's Bank of China declare that it would adopt a long-term perspective on Bitcoin. This made once again the price of Bitcoin to shoot up.

That same day, the value was 572,67$, but just 14 days later move up to 1147,25$, it had grown more than 50%. The boom was such that China was forced to legislate against the use of the cryptocurrency. Few days after that regulations, Bitcoin price declined to 600$ more or less. After that bubble, Bitcoin did not suffer anymore sudden ups and downs, although it reduced its value. That is why, at the beginning of 2014, the currency was approximately around 620$. However, one year later, in March 2015, its value did not exceed 250$.

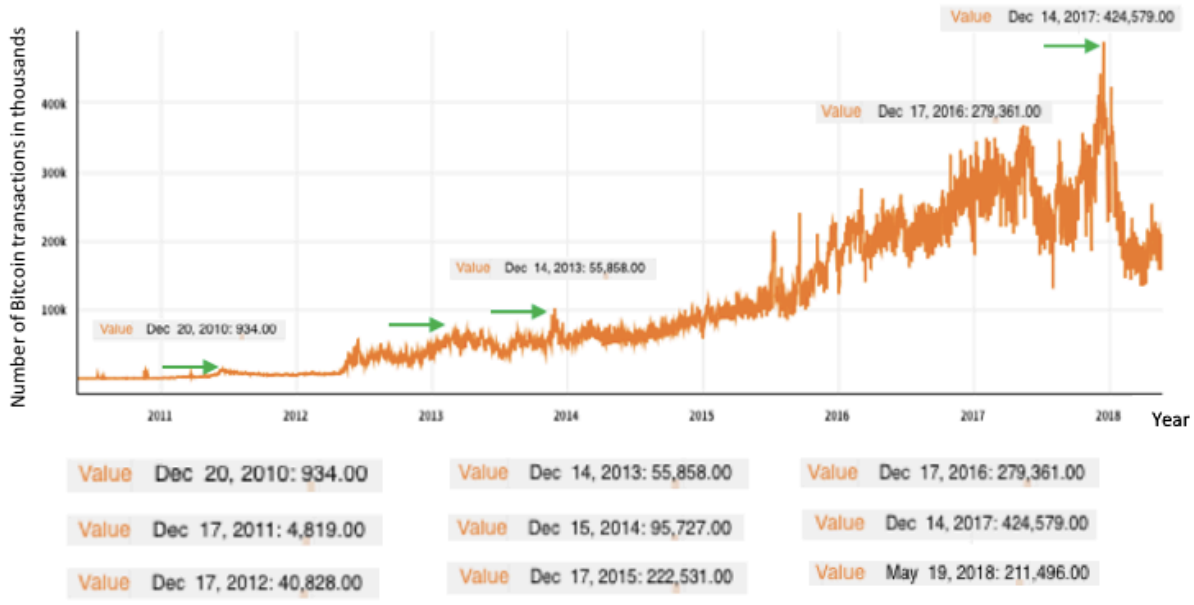


19. Bitcoin price history chart.
(October 2013 – February 2014)

If we look at the picture number 16, during 2016 there was not any rough change in the value of Bitcoin. Nonetheless, in 2017, the map changes completely. Bitcoin price hits its record on December 2017 with an approximate value of 19800$, indicated with a yellow star. It is with no doubt the year of Bitcoin. This great growth is due to the fact that it began to attract the attention of a larger number of investors and each month was going through a new record. Furthermore, it started to be more accepted by society, the amount of transactions expanded tremendously, and more and more stores accepted Bitcoin as a means of payment. However, since the beginning of 2018, the price of Bitcoin has fallen sharply, decreasing until it reached on May 14th the value of 8363,43$, a 57.7% less. This decline occurred when South Korea announced that it could completely ban cryptocurrencies' trade or impose strict regulations.

These graphics, throughout the history of Bitcoin, have allowed us to verify one of its main drawbacks: Bitcoin is a completely volatile currency, and therefore invest in it is too risky. For this reason, the virtual currency does not achieve full market confidence. Furthermore, looking ahead it shows great uncertainty, that's why many economists believe that Bitcoin would not go too far, they consider that it is another financial bubble.

Another fact that is directly related to the increase in the price of Bitcoin, is to analyze the number of transactions made over the years. The following graph shows the evolution of the whole transactions from 2010 to May 19th 2018, day in which I have consulted the graph. At first glance, we can see that the quantity of transactions increases year after year. To perceive this evolution in detail, I have picked up the data for a specific day of December each year.



20. Bitcoin transactions history chart.
(May 2010 – May 2018)

The difference is abysmal, beginning on December 20th 2010 with 934 transactions per day and ending on December 14th 2017 with a total of 424.579. Additionally, if we look closely at and compare the dates when the "four" possible Bitcoin bubbles were produced, we can see peaks higher compared to the rest of the month of the same period of time (indicated with green arrows). This fact confirms that in the four cases, when the price rose exponentially, the number of transactions also did. Yesterday, on 19th May 2018, the total amount of transactions made were 211.496.

Now that we have analyzed deeply the volatility of Bitcoin, we will move towards the legal aspect of the currency. It is true that one of its main benefits is that the government has a very little implication, but at the same time, it is a disadvantage when problems arise, as regulation is scarce. However, as we notice, regulations are increasingly being implemented.

V. LEGAL CONTEXT

Bitcoin's popularity has increased exponentially over the past year and it seems as if 2018 is destined to become the year of regulatory reckoning. Many governments have felt threatened by Bitcoin, as they cannot control them and that is why more and more countries are imposing regulations. However, as we will see, some countries with a lack of understanding of cryptocurrencies, have gone as far as to put out-right bans on Bitcoin trading. I have divided this point into two sections in order to have a clear vision of the regulation in Spain, and then another one regarding the regulation in International Markets.

5.1 Bitcoin regulation in Spain

Cryptocurrencies and especially the Bitcoin have always captured Spain's interest, placing it in one of the countries most implicated to the development and positioning of the cryptocurrency. In 2014, Barcelona was the first city of the state to receive a Bitcoin ATM. The following year, was characterized by the increase in demand for Bitcoin and the incorporation of new ATMs, compared to the rest of the EU countries. By 2016, Spain had become the first European country with the highest investments in the blockchain sector thanks to the support of the industry. This support from the government suggests that Bitcoin is legal in Spain, but is it really like that?

It is true that Bitcoin is not legally recognized as a digital currency or mean of payment by Spanish law. However, this does not mean that the cryptocurrency is illegal, since based on the recommendations of the Court of Justice of the European Union (CJEU)[11], it is accepted as a digital currency. However, there are a series of guidelines that mark the way of Bitcoin in Spain.

According to the General Accounting Plan (9th registration and valuation rule)[12] and the Spanish Civil Code, Bitcoin is not treated as a financial asset, but as an intangible asset. This means that it must be taxed as a service. Even though it is a digital good, in fact is a type of service provided by Nakamoto's network, making use of the work of the miners.

As we already know, Bitcoins can be acquired and sold without the need of signing any document by any of the interested parties.

[11] http://eur-lex.europa.eu/legal-ontent/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2015.414.01.0006.01.ENG

[12] http://www.boe.es/boe/dias/2007/11/20/pdfs/C00001-00152.pdf

• Bitcoins acquisition

In Spain, the acquisition of Bitcoins is regulated in "Real Decreto Legislativo" 1/1993, by the BOE (Agencia Estatal del Boletín Ofical del Estado)[13]. This rule indicates the following: "said acquisition is a transaction subject and not exempt to Impuesto sobre Transmisiones Patrimoniales (ITP)". The tan per cent applied is different in each autonomous community. For instance, in Catalonia and Madrid, a 4% of the total Bitcoin acquisition must be paid.

• Bitcoins payment

Regarding Bitcoin payments, the following must be applied:

- The paying company must issue a sales invoice for those Bitcoins (RD 1619/2012 article 2 from BOE)[14].

- The individual, who must be of legal age or emancipated must be able to perform acts of sale of services. Other minors may also pay with Bitcoins, provided the capacity is maintained and this act of exchange is accepted for them (article 1269 Spanish Civil Code)[15].

On 27th April 2015, the "Dirección General de Tributos" (DGT)[16], declared that Bitcoin exchanges, and also the other virtual currencies, are legal financial transactions, and that is the reason why they must be exempt from VAT. But, although Bitcoin is exempt from VAT, it is not from IRPF (Impuesto sobre la Renta de Personas Físicas).

Last but not least, the "Agencia Estatal de Administración Tributaria Española", expressed that anyone who work as a Bitcoin miner have to be registered with the Spanish authorities and pay taxes to the government. This claim made Bitcoin mining a legal economic activity.

Hence, we can sum up that despite these previous guidelines there is no State regulation of Bitcoin in Spain yet. The government says it will wait for an agreement from all the member countries of the European Union to regulate the use of Bitcoin and recognize its legal nature.

[13] https://www.boe.es/buscar/act.php?id=BOE-A-1993-25359

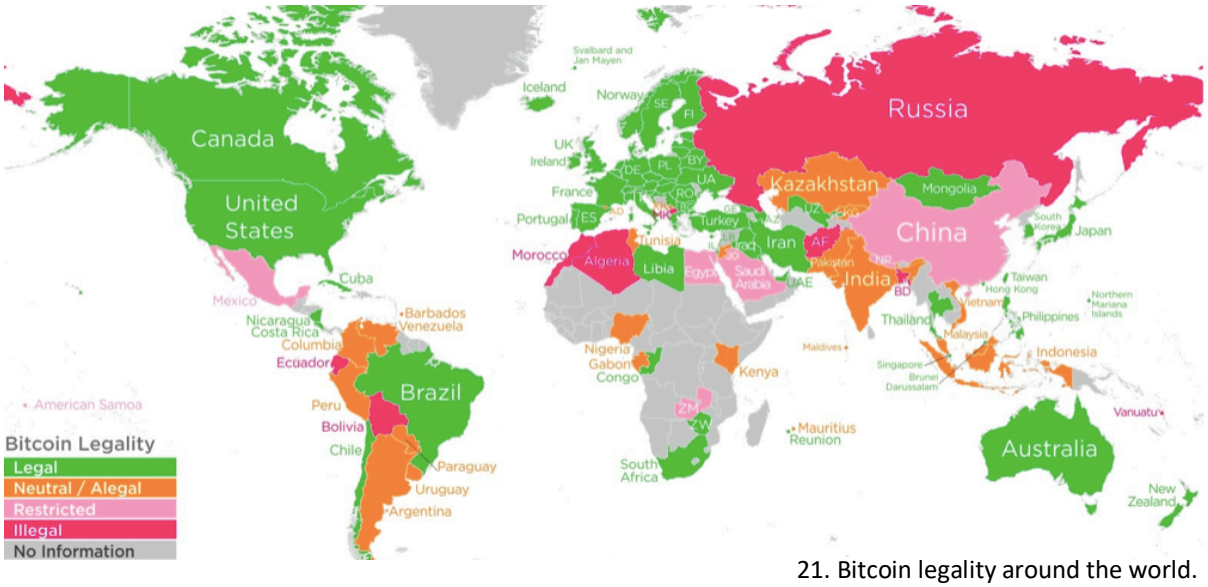
[14] http://www.boe.es/buscar/act.php?id=BOE-A-2012-14696

[15] http://civil.udg.edu/normacivil/estatal/CC/4T2.htm

[16] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2006.347.01.0001.01.SPA

5.2 Bitcoin regulation in International Markets

The following map shows Bitcoin legality around the world. As we can observe, a color legend is used to differentiate the varying degrees of acceptance this cryptocurrency has worldwide. In green, we have the countries that consider Bitcoin legal. Then, in orange, the ones that are not outright legalizing Bitcoin nor having any restriction. Light pink states are restricting them. Dark pink countries symbolize markets where Bitcoin has been declared entirely illegal and criminalized. Finally, in gray, countries that lack of Bitcoin legislation's information.



21. Bitcoin legality around the world.
(Consulted on 26th May, 2018)

Following, I would like to comment in more detail on the current position of some countries regarding Bitcoin and how the views of their governments have evolved over the years.

European Union	Bitcoin is classified as a legal type of financial transactions in EU, thus, as we have seen on point 5.1 is exempt from VAT. However, there is some controversy with the different financial institutions. The European Commission, recognize the need for dialogue and deliberation, while the European Central Bank (ECB) believes that Bitcoin is not yet mature enough for regulation and that traditional financial sector regulation is not applicable to Bitcoin because it does not involve traditional financial actors. Nevertheless, on 20th April 2018, the EU Comission Vice-President Vladis Dombrovskis asserted that the European Parliament's members voted by a large majority, a series of Bitcoin's measures. Rules aimed, in part, to prevent the use of cryptocurrencies in money laundering and terrorism financing by addressing the anonymity for exchanges, platforms and wallet providers.

United Kingdom	On April 29th 2018, the Britain's Financial Conduct Authority (FCA) announced that sees bitcoin as a "commodity," and therefore does plan to regulate it, to protect the consumer.
Macedonia	It is the only country in Europe in which it is totally illegal, goes against the law and therefore implies imprisonment.

United States of America	Even though Bitcoin is seen as a legal tender, USA has no coherent direction on its cryptocurrency regulation. This is mainly because of the fractured regulatory map. However, some states are more advanced than others in cryptocurrency oversight. *For instance, New York and Washington.* In early 2018, the Securities and Exchange Commission (SEC) advised investors of cryptocurrency investing risks and suggested the need for a regulation of cryptocurrency.
Canada	Canada was one of the first countries to draw up what could be considered "Bitcoin legislation," with the passage of Bill C-31 in 2014, compelling users to comply with anti-money laundering and know-your-client requirements. Bitcoin is declared as a good by the Canadian Revenue Agency (CRA). The taxes that are applied will depend on whether the benefit obtained is a business of purchase or sale or if it is an investment.

Venezuela	Venezuela is not characterized for being a major world economy or a large portion of the cryptocurrency investing community, but the government, under the restrictive regime of Nicolás Maduro, announced on 20th February 2018, its own cryptocurrency called "**Petro**". It becomes the first country in the world with its own cryptocurrency. This currency will be guaranteed by the reserves of petroleum, gas, gold and diamonds. "For every Petro, a barrel of oil," said Maduro. The initial value of the oil was valued at 60$, the equivalent of a barrel of oil, and the price will vary according to the Venezuelan crude oil basket. In a country where the fiat currency is worth little, analysts point the currency has been created to avoid the international restrictions that the country is facing and to overcome the difficulties to finance themselves in the markets. To encourage its official use, Maduro ordered to the Oil State Companies to make a percentage of their sales and purchases in Petros.
Argentina	Painted in orange, Argentina has not yet designed any regulation for the crypto-currency, although the Central Bank has pointed official warnings of the risks included.

Russia	Russia has always remained on the fringes of cryptocurrencies, to the point of declaring them illegal. But as Bitcoin increase its popularity worldwide, Russian authorities have changed their mind. On January 2018, Russia's Finance Ministry said that it was working on legislation to regulate Bitcoin transactions without fully banning them as a means of payment. Nonetheless, he highlighted that digital currencies would not be allowed to replace the Russian Ruble.
India	At the end of 2017 the country's finance minister clarified that Bitcoin is not a legal tender. Also, the Reserve Bank of India, has forbidden Indian financial institutions from working with cryptocurrency exchanges.

Japan	It was the first country to expressly declare Bitcoin as a legal tender. However, there are no laws in Japan regulating the use of Bitcoins.
China	Until 2017, China took several actions to clamp down on all things cryptocurrency. Starting by ordering a bank account freeze associated with exchanges, kicked out bitcoin miners, and instituted a nationwide ban on internet and mobile access to all things related to cryptocurrency trading. In 2017, the situation changed completely. Chinese Bitcoin miners made up over 50% of the worldwide mining population and Bitcoin adoption increased at a rate higher than any other country.
South Korea	In early 2018, South Korea banned anonymous virtual currency accounts. Nevertheless, an unexpected shift happened in April. The country's financial authorities are in talks with Japan and China to over joint oversight of Bitcoin investment.

In conclusion, the regulation of Bitcoin has never been a worrying issue for any country, since nobody imagined that the growth of this virtual currency would be so great. Additionally, since it is not issued by any government or central bank, there is no specific regulation that controls it. This is the main reason why many countries have begun to consider the regulation of the cryptocurrency. As the map image shows, Eastern Countries seem more closed off to Bitcoin compared to Western nations. Nowadays, of the total 246 countries, 99 (40% of the World, colors green and orange) have unrestricted Bitcoin laws, 17 (7% of the World, colors light pink and dark) has restricted or illegalized the use of Bitcoin and the remaining 130 (53% of the World, color gray) have not yet express its opinion towards Bitcoin. So, it is obvious that there is still a long way to go, since it is still an emerging industry not fully understood by global regulators, that is why most of the countries authorities are just beginning to talk about it.

VI. CURIOSITIES OF BITCOIN

Along the project, I have found some Bitcoin facts that were interesting and that is why I decided to join them all and add this point.

♦ The famous economist Milton Friedman predicted Bitcoins 10 years before they were invented. You can see it, in the link that I attached at the end of this page[17] .

♦ It is said that, in its beginnings there were those who mined Bitcoins with a Super Nintendo.

♦ A man from London bought in 2009 the amount of 7500 bitcoins and now he does not remember his private direction. In addition, in 2013 he threw away his hard drive where he stored all the information to be able to access the virtual wallet.

♦ In summer 2011, an electrical engineer went on a road trip from the East Coast to Los Angeles, only using Bitcoins thought the whole trip.

♦ In 2013, took place the largest Bitcoin transaction registered until now, which contained 194.993 BTC.

♦ Also, in 2013, the University of Nicosia from Cyprus, announced to accept Bitcoins to pay for academic fees.

♦ When the FBI shut down the operations of the Silk Road, it also confiscated all the owner's assets. That is the reason why the FBI has one of the world's largest Bitcoin wallets.

♦ In 2016 Satoshi Nakamoto was nominated for the Nobel Prize in Economics. However, the same Swedish Academy discarded it because his true identity remained unknown.

♦ From January 2018, a church in Zürich accepts donations in Bitcoin and other cryptocurrencies.

♦ Nowadays, the amount of electricity running the Bitcoin Network could power 1,3 million homes.

♦ Kristoffer Koch, a Norwegian student, forgot that he had bought 27$ in Bitcoins in 2009, at that time they were 5000 bitcoins. Currently, he is a millionaire.

[17] https://www.youtube.com/watch?v=6MnQJFEVY7s

VII. COMPARISON OF BITCOIN WITH OTHER CRYPTOCURRENCIES

After the success of Bitcoin, other cryptocurrencies were launched. These are known as Altcoins. This term is a combination of two words: "alt", which signifies “alternative” and "coin". Altcoins project themselves as better substitutes to Bitcoin and can differ from it in a range of ways. For instance, some have a different coin distribution method, different mining algorithms and others offer even more privacy than Bitcoin. However, there are also many Altcoins that do not have any interesting feature that makes them stand out. There are hundreds of Altcoins, but I am only going to compare Bitcoin with the three most popular ones: Ethereum, Ripple and Litecoin.

7.1 Ethereum

Ethereum was announced at the North American Bitcoin Conference that took place in 2014 by Vitalik Buterin, a young boy from Russia. Since that moment it has received a lot of attention. Ethereum is, for the moment, the second largest cryptographic currency in the world behind Bitcoin. The main cause of its rising popularity has been its constant comparison to Bitcoin. However, as we will see below, they are quite different. Thus, in order to compare them first we will study their similarities and then their differences.

22. Ethereum’s logo

SIMILARITIES

- Both are considerate it decentralized cryptocurrencies. Ethereum acronym is ETH.
- They are based on blockchain technology. Vitalik Buterin, became interested in this new tool when he saw the potential that blockchain technology had. He started writing in an Internet forum about Bitcoin, then became co-founder of Bitcoin Magazine and finally put himself at the helm of his great project: Ethereum.
- Both currencies are put into circulation through the mining process.

DIFFERENCES

- Creation → Bitcoin was created in 2008, but it was not until 2009 that took place the first transaction. It is also important to highlight that its founder is still unknown. On the other hand, Ethereum was created on December 2013 and its first transaction was on July 2015. In this case, as I have just mentioned, the inventor was Vitalik Buterin.

• Principal function →Bitcoin was designed to act as a decentralized, secure and fast payment system. While, Ethereum was created for being a platform that executes **smart contracts** between two or more parties and **decentralized apps**, applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

• Divisions → Bitcoin only have 8 decimals (Satoshi unit), whereas Ethereum has 18 (Wei).

• Limit → As we know, there are just 21 million BTC. Ethereum does not have a maximum total number of Ether, nor a specific date to end its creation. However, it limits the amount created every year to 18 million. Therefore, ETH tends to be inflationary.

• Miners' reward → We have seen that Bitcoin miners' reward is reduced every 210.000 blocks, and that nowadays is 12,5 BTC. At the beginning Ethereum reward was 5 ETH per block, currently is 3 ETH.

• Transactions speed→ In Bitcoin, each block is generated in an average of 10 minutes. Ethereum is given every 16 seconds.

There are many things that make Bitcoin and Ethereum different from each other. They can coexist to the extent that they work for different goals, so we can say that they are compatibles but not replaceable. Today, 1st June 2018, 1 ETH is equivalent to 575$.

7.2 Ripple

Even though Ripple characteristics are totally different from Bitcoin ones, it is considerate it the third more popular cryptocurrency in the world. It is named "the cryptocurrency of banks" and now we will see why.

23. Ripple's logo

SIMILARITIES

• Limit → Both currencies have a maximum, meaning that no more currencies will be created. There is a total of 100 billion Ripples, of which 60 billion are owned by Ripple's company.

DIFFERENCES

- Creation → The idea came up in 2004, but it was not until 2012 that Chris Larsen and Jed McCaleb founded the corporation. The first difference with Bitcoin is that there are three parts of Ripple: the parent company Ripple Labs, the RippleNet that is the payment network used and the coin itself "Ripple", the XRP.

- Principal function → Ripple is a "decentralized" payment network for banks and financial institutions that allows them to send and receive money and liquidate transactions more quickly and economically than their existing backup systems. The large number of banking partners that have this company, such as American Express, Santander, USB, has made its value considerably rise during the last two years.

- Divisions → A Ripple can be split it until 6 decimals (Drop). So, 1.000.000 Drops is the same as 1 Ripple.

- Miners' reward → Ripple does not have mining operations like the Bitcoin blockchain, where more Bitcoins are created each time a miner loads transaction data. In its case, Ripple's transactions are verified by several parties to achieve consensus. Therefore, since there are no miners, there are no rewards.

- Transactions speed→ XRP transaction confirmations take between 5 and 10 seconds, much faster in comparison to Bitcoins.

If we compare Ripple with Bitcoin and even with Ethereum, we can observe that it lacks two main characteristics. The first one is that, it is not a totally decentralized coin since it is created by a company. At the same time, this give more security to its users, as XRP price is directly related with the firm's situation. Its actual value, on 1st June, is 1 RXP for 0,642$. The second one is that it cannot be mined, an unthinkable concept for BTC and ETH.

7.3 Litecoin

Litecoin is based on Bitcoin, so it is virtually identical in most of its technical aspects. This is why many people compare the "new" cryptocurrency Litecoin with silver and Bitcoin with gold. As we will see differences between them are few, the structure is the same, but its content varies a little.

24. Litecoin's logo

SIMILARITIES

- Both are considerate it decentralized cryptocurrencies. Litecoin acronym is LTC.

- They are based on blockchain technology.

- Both currencies are put into circulation through the mining process. Nevertheless, mining Litecoins is easier, as they use scrypt[18] instead of hash. The first benefit of this change is that it makes any PC able to engage in mining

- Limit → Litecoin also has a maximum. However, it is bigger than the Bitcoin one, 84 million Litecoins. Thus, we can also say that is a deflationary cryptocurrency, as it follows a path similar to that of Bitcoin. Nowadays, there are 67,65% of the total Litecoins mined.

- Principal function → As Bitcoin, its main function is to be used as a global mean of payment.

DIFFERENCES

- Creation → It was created on October 2011 by Charles Lee, a Google employee. He has always assured that he does not want to compete with Bitcoin, but rather to be a complement.

- Miners' reward → Litecoin miners' reward is halved every 840.000 blocks. At the beginning, the reward was 50 LTC per block, currently is 25 LTC.

- Divisions → A Litecoin can be divided it until 3 decimals (Lites). Hence, 1000 Lites is the same as having 1 Litecoin.

- Transactions speed→ Litecoin transactions are validated more quickly. The chain produces a new block after every two and a half minutes. This is similar to 4 times the speed at which Bitcoin chains create a new block.

As we can prove, Litecoin and Bitcoin features are alike. Nevertheless, Litecoin capitalization cannot be compared with the Bitcoin one. Today, on 1st June, 1LTC is equivalent to 123,92$.

[18] Script: Are programs, usually small or simple, to perform and very specific tasks.

VIII. CONCLUSION

In order to conclude this study on Bitcoin, I can assert that I have learned many new things and enjoyed a lot. I have to say that I have always had in mind the main objective, that is, knowing Bitcoin, its characteristics and also its current situation in society. Especially, I was very pleased to see how my current knowledge of this currency has evolved compared to the beginning.

The reasons why I decided to choose this title "*Bitcoin: two sides of the same coin*" are the following. First of all, because when I selected the theme I had only heard and read positive news from Bitcoin. The information I had, was that it was a completely safe and almost instantaneous means of payment and that the number of Bitcoins available was limited. Many called it "the Electronic Gold", since its price was higher every day, to the point of turning young people of my age into millionaires. However, as I expanded my knowledge, I realized that not everything was so fantastic, but there was also a "darker" part that was hidden behind the great success.

We know that thanks to the P2P network and the blockchain, it is an anonymous payment method, in which no intermediary is required to send or receive money from anywhere in the world. As we have seen, this feature has sparked the interest of many cybercriminals, such as "Silk Road" case or frauds, as authorities have no control over Bitcoin. Fact that has risen concerns in many countries for regulating its use. On the one hand, regulations would have positive effects. Considering restrictions on the easiest way to access the financial world that Bitcoin supposes, security would increase in the network, and illegal transactions would be reduced. On the other hand, with regulations, Bitcoin would lose its anonymous appeal, which could cause its price to drop even more than nowadays. That is why I consider that a Bitcoin regulation should not occur, as it was specifically set up so that no government could have control. Additionally, cybercriminals would never be eliminated altogether, and new ones would emerge.

Another negative aspect of the study that surprised me the most is the great volatility to which Bitcoin is exposed. As being a decentralized currency, there is no authority that limits the rise and price drop, are the users themselves who, through trust, value the currency. Therefore, the higher the demand, the higher the prices and vice versa; the lower the demand, the lower the value. This is demonstrated by the different charts in section 4.5. The data do not show a linear or stable behavior of the price, but quite the contrary, they are constantly varying. Therefore, I can affirm that due to the great volatility presented by Bitcoin, the investment risk associated with this currency is really high. Anyone would never be able

to know for sure when the value will increase or decrease. The most impressive graph is that found in Figure 16. As we have seen previously, bitcoin's history has been punctuated by three stunning bubbles. By the end of 2017, Bitcoin reached the highest peak ever, but for months its price began to fall, and it has not recovered yet. This great decline made me think of the possibility of a “Fourth Bitcoin Bubble”. A thought, which many experts also contemplate. From my point of view, we are clearly in front of it, as it presents the same characteristics as the three previous ones. In all four cases, the price rises sharply in less than one month, then it is reduced by more than 50% in a matter of days and remains low for months until it goes up again.

I have observed that the great volatility of this currency creates the following doubt in society: is Bitcoin a currency or a speculative asset? Originally, Bitcoin was designed as a virtual currency or payment method. It is true that today the number of transactions carried out as a means of payment, meaning, for the purchase of goods and services, is low, and that is mainly used as an investment. In addition, in section 2 of the paper, we present the three crucial characteristics that all currencies share. Bitcoin prevents the fulfillment of two of them: unit of account and store of value. Due to its volatility and for being a decentralized currency, it is impossible to calculate its value. Therefore, we could consider that due to the lack of these two characteristics, together with the uncertainty of the risk and the benefits it entails, Bitcoin is currently becoming a speculative asset rather than a currency. However, I think that if population increase its awareness of the use of electronic commerce, Bitcoin could play an important role as a means of payment.

It is true that Bitcoin has many aspects against it and it is difficult to think that it could be the only currency of the future. It should be stressed that, apart from its position as a currency, the volatility and legality that put into question the destiny of Bitcoin, the technology it offers is very attractive for society. More and more companies are considering this cryptocurrency as a business opportunity to invest; however, I believe that it is still in full development and needs time to mature. I hope this work brings a grain of sand to the world of Bitcoin, helping to make known its nature and the implications that it represents today.

IX. BIBLIOGRAPHY

Banking on Bitcoin, 2016. (consultation 28.2.2018) www.netflix.com

Bitcoin and Ethereum, 22 April 2017 (consulting 25.5.2018) https://altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

Bitcoin bubbles (consulting 17.5.2018) https://www.xataka.com/empresas-y-economia/las-tres-veces-que-hubo-una-burbuja-de-bitcoin-para-luego-hacer-crack

Bitcoin legality around the world (consulting 25.5.2018) https://howmuch.net/articles/bitcoin-legality-around-the-world

Bitcoin number of transactions (consulting 17.4.2018) https://www.quandl.com/data/BCHAIN/NTRAN-Bitcoin-Number-of-Transactions

BUCHKO, Steven. How many Bitcoins are left? (consultation 29.4. 2018) https://coincentral.com/how-many-bitcoins-are-left/

Curiosities of Bitcoin (consulting 29.5.2018) http://www.boomsbeat.com/articles/284059/20180123/100-interesting-facts-you-need-to-know-about-bitcoin.htm

DAVIS, Charlotte. "Bitcoin to come under EU regulation as Brussels plots to kill cryptocurrency anonymity" 24, January, 2018. https://www.express.co.uk/finance/city/909280/price-bitcoin-usd-news-value-btc-cryptocurrency-ripple-ethereum

El País Economia, 21 July 2017, Blockchain (consultation 22.4.2018) https://retina.elpais.com/retina/2017/07/13/tendencias/1499945987_724507.html

Ecomipedia: Gold Standard (consultation 16.3.2018) http://economipedia.com/definiciones/patron-oro.html

EU Parliament votes (consultation 20.5.2018) https://www.coindesk.com/eu-parliament-votes-for-closer-regulation-of-cryptocurrencies/

FRANCO. Pedro "*Understanding bitcoin: cryptography, engineering and economics*", 2014 (consulting 17.4.2018) https://books.google.es/books

Futurism, Bitcoin history and timeline (consultation: 19.4.2018) https://futurism.com/images/the-entire-history-of-bitcoin-in-a-single-infographic/

Genesis Block (consultation: 22. 4. 2018) https://www.oroyfinanzas.com/2015/01/que-es-bloque-genesis-bitcoin/

How to do Bitcoin transactions? (consultation: 21.4.2018) https://blockchain.info/es/

How Bitcoin price is determined? (consultation 10.5.2018)
https://bitcoinsgeeks.com/2018/01/como-determina-precio-de-bitcoin/

Investopedia, Altcoins (consultation 2.6.2018)
https://www.investopedia.com/terms/a/altcoin.asp

MAYNEZ, Natalia. ¿Qué son las criptomonedas y por qué deberian importarte?(consultation: 16.3.2018) https://blog.adext.com/es/que-son-las-criptomonedas-importancia

OECD: Glossary of Statitical Terms (consultation 15.4.2018)
http://stats.oecd.org/glossary/detail.asp?ID=5075

Price charts (consultation 10.5.2018) https://www.coindesk.com/price/

Ranking Bitcoin use in the World (consultation 18.5.2018)
https://criptotendencia.com/2018/02/09/ranking-de-los-paises-donde-mas-se-utiliza-bitcoin/

Ronald A.Gove: Fundamentals of Cryptography and Encryption 2007(consultation: 15.4.2018)
http://www.infosectoday.com/Understanding_Cryptography/Articles/Fundamentals_Cryptography_Encryption.pdf

SINGH. J Barter Exchange: Meaning and Problems of Barter Exchange (consultation: 16.3. 2018)http://www.economicsdiscussion.net/exchange/barter-exchange-meaning-and-problems-of-barter-exchange/595

The Statistics Portal (consultation: 19.4.2018)
https://www.statista.com/statistics/343127/number-bitcoin-atms/

Value Bitcoin (consultation: 10.5.2018) https://www.buybitcoinworldwide.com/es/precio/

What is Bitcoin? (consultation: 19.4.2018) https://bitcoin.org/en/faq

What is Bitcoin? 4 December 2017, (consultation: 2.5.2018)
http://www.historynet.com/bitcoin-history-works-pros-cons.htm

What is Bitcoin double spending? 23 June 2017 (consultation: 29.4.2018)
https://www.bitcoin.com/info/what-is-bitcoin-double-spending

¿What is mining Bitcoins? (consulting: 5.5.2018) https://blog.bit2me.com/es/que-es-minar-bitcoins/