



Universidad Pontificia de Comillas: ICADE Business School.

*Blockchain: Decentralizing the financial system. Comparative analysis of different use purposes.*

Autor: Carlos García Pérez

Director: Luís Garvía Vega

Madrid  
Junio, 2019

*Blockchain: Decentralizing the financial system. Comparative analysis of different use purposes.*



Carlos  
García  
Pérez

I would like to thank my Thesis Director, Dr. Luís Garvía Vega, for guiding and supporting me over this Thesis. You have set an example of excellence as a professor, mentor, instructor and role model. Thanks for all the time invested in me.

I would also like to thank my fellow graduate students, who contributed to this research, I am thankful for having had you during the confection of this Thesis. I would like to highlight here the support of Beatriz not only during the process of writing this thesis but also during the whole Master. You have been the greatest pillar I could ask for leaning on.

I would especially like to thank my family for the love and constant support I have gotten over the years. In particular, my parents, my brother, my sister and my niece Vera, for giving me the strength needed in tough moments. You are the salt of the earth, and I undoubtedly could not have done this without you.

Finally, I would like to thank and dedicate this thesis to my grandfather, Antonio. You contributed in my infancy and adolescence and helped me settle and understand the values that make me the man I am today. Although it has been years since you have passed, I still take your lessons with me, every day.

## Index

<b>Chapter 1. Introduction</b> .....	6
<b>1.1 General Objectives</b> .....	6
<b>1.2 Motivations of this Thesis</b> .....	6
<b>1.3 Methodology</b> .....	7
<b>1.4 Structure of the Thesis</b> .....	7
<b>Chapter 2. Conceptual framework.</b> .....	8
<b>2.1 The origin of the currency.</b> .....	8
<b>2.2 The destruction of the currency</b> .....	9
<b>2.3 Loss of value (devaluation)</b> .....	9
<b>2.4 The appearance of coins</b> .....	10
<b>2.5 The appearance of the notes</b> .....	10
<b>2.6 The Gold Standard</b> .....	10
<b>2.7 Origin of the Gold Standard and transition to the Gold Exchange Standard</b> .....	11
<b>2.8 FIAT Money</b> .....	12
<b>2.9 Creation of money</b> .....	13
<b>2.10 Inflation</b> .....	13
<b>2.11 Deflation</b> .....	15
<b>2.12 Fractional Reserve Banking</b> .....	16
<b>2.13 Money and debt</b> .....	17
<b>2.14 Digital Currency (Electronic Money).</b> .....	19
<b>Chapter 3. Understanding Blockchain.</b> .....	20
<b>3.1 Centralization VS Decentralization</b> .....	20
<b>3.2 ARCHITECTURE OF THE BLOCKCHAIN</b> .....	22
3.2.1 Timestamp.....	22
3.2.2 Mining .....	<b>¡Error! Marcador no definido.</b>
3.2.3 The difficulty and the hashrate .....	23
<b>3.3 Use Cases of Blockchain</b> .....	24
<b>3.4 The 3 stages of Blockchain</b> .....	26
3.4.1 Blockchain 1.0: Currency .....	27
3.4.2 Blockchain 2.0: Contracts .....	29
3.4.3 Blockchain 3.0: Application in other fields beside currency, financial markets and business. 35	
<b>3.5 Impact of blockchain in the financial sector.</b> .....	39
3.5.1 Continuous rise of banking disintermediation.....	40
3.5.2 DLT's impact on digital economy and e-commerce.....	40

3.5.3	<i>Why DLT is almost impossible to ignore?</i> .....	41
<b>4.</b>	<b>Conclusions</b> .....	<b>43</b>
<b>5</b>	<b>Bibliography</b> .....	<b>44</b>

## **Chapter 1. Introduction**

### **1.1 General Objectives**

After the revolution generated on the media by the new technology Blockchain and all the attention it is dragging, the objective of this Master Thesis is analyzing which factors and elements are significant in the process of building a project with Blockchain or if it is pointless to use this technology.

In order to reach the mentioned objective, we have taken into account 2 main subobjectives:

- a. Understanding the Blockchain technology.
- b. Analyzing and understanding successful cases.

Even though we might be at the dawn of a new revolution<sup>1</sup> (Melanie Swan, 2015), we cannot let emotions lead our decisions and try to deploy Blockchain over everything. Blockchain is a new technology, a technology with a lot of potential and use cases, but every situation has to be analyzed in order to find out if it is worth or not using Blockchain.

### **1.2 Motivations of this Thesis**

Life is changing. Fast. Really Fast. We are evolving at an undeniably accelerated pace. The generational jump is huge. The difference between our grandparents, parents and us is huge. This Christmas I was hanging out with my dad and Blockchain popped in the conversation. I had clear in my mind that my Master Thesis was going to be about Blockchain, but I had it even more clearly that day.

Adapt and survive. A good teacher of my Master used to tell all the class that. Because swimming upstream forever is impossible. Like Industrial Revolution, Newton with the printing or Internet, nowadays we are standing in front of something that might change the world as we know it. We are facing a new game-changer player; some scholars call it the Fourth Industrial Revolution (Bloem, J., Van Doorn, M., 2014 and Schwab, K., 2017). This game-changer is called Blockchain.

We would like to have better cars, better houses, better cell phones, better suits, but never or just few times have we thought we could have a better currency... and could we? Is it possible and desirable to have a currency of quality? Here comes into stage the cryptocurrencies.

---

<sup>1</sup> This revolution started with Internet, followed by Bitcoin in 2008. Bitcoin was the issuance of a new currency, an alternative one called to be the new digital currency. A new currency which was not issued by a central authority and controlled by everyone with the implying technology called Blockchain.

Some years ago, I read a paper that claimed a new Electronic Peer-to-Peer cash system was rising (Nakamoto, S., 2008.), and Bitcoin was in the epicenter. I started reading about the main goals of the electronic currency and cryptocurrencies. The entry barrier was huge, nor banks nor governments wanted to change things. Allow a currency created by the people flow into the economy? No way.

However, people underestimate the power of Internet and people that works on it (Us), and Blockchain and cryptocurrencies have arrived and are planning to stay.

### **1.3 Methodology**

Once the Thesis main topic was chosen, the methodology chosen in order to carry out this TFM was Gantt Chart in terms of planning. The main goal pursued with this was to distribute time according to the weight of the topics inside the Thesis, giving less time to those topics that are less importance dragging and giving more time to the ones we want to get deep on. In this direction, the conceptual framework (understanding the historical perspective to understand the importance on the media of the Blockchain nowadays) and analyzing use cases captured most of the time.

### **1.4 Structure of the Thesis**

With the objective previously described, which is to analyze which factors and elements are significant in the process of building a project with Blockchain or if it is pointless to use this technology, we have followed the next steps in terms of structure:

- a. Review of the conceptual framework so we can contextualize the importance and the potential of Blockchain nowadays.
- b. Analyzing use cases. When Blockchain can be deployed and when it is pointless.

In this way, the first half of the TFM is dedicated to the conceptual framework, and the second half is dedicated to understand Blockchain and to analyze the use cases.

## **Chapter 2. Conceptual framework.**

### **2.1 The origin of the currency.**

Let us start from the beginning. The origin of the currency is almost the same age as the own civilization, and it appeared in the Neolithic times in a steady and gradual pace. It evolved as the relation between humans and the transactions they did among them became more and more complex. Currency appeared to make our life easier and to improve our relationships.

In the Neolithic there was no currency as we know it. The way they did business was based on the exchange or barter. It was more than enough at the beginning, but there was the need of matching 2 same necessity.

For example, I might be an Eskimo, I have leather, and I want vegetables. There is a farmer that has vegetables, but in that precise moment, he is not interested in leather. If I do not find a farmer with vegetables that needs leather, I cannot exchange my leather for vegetables. So this is 2-need matching.

In this silly example, we can see a set of problems that are:

- A. The exchange or barter depended of the demand of every individual in a specific moment. Therefore, it cannot match the emergencies (I want vegetables NOW) and the process might be slow.
- B. There is a problem of fair value matching. All in all, how many vegetables can I get for a leather? What is the value of my leather?
- C. Not all goods are as easy to exchange. Vegetables are easy to carry but maybe for carrying leather you need a more complex transportation.

Society evolved, and relationships got more complex. Due to the factors mentioned above, the exchange or barter could not work. It did not disappear overnight, but it was slowly substituted by the currency we know (more or less). Every little community might have developed its own type of currency (stones, salt, cocoa, etc) and it extended across borders. But how? Let's get back to our silly example:

Our Eskimo has its leather, but the farmer does not need leather but needs clay. A third party appears, and is in the need of leather but he does not have vegetables. We have 2 possibilities here:

-The Eskimo exchange the leather for clay with the third party, and carries it to the farmer, in order to exchange it for vegetables. The transportation is on the Eskimo now, with all its risks (losing it, squandering it, dropping it...).

-The other possibility is the Eskimo getting something from the third party (a piece of paper, a piece of wood, something) which is easier to carry than the own clay, and that something is worth a posterior exchange for clay. Therefore, the Eskimo gives the leather and obtains that something from the third which gives it to the farmer for vegetables, and the farmer can use that something to exchange it for clay with the third-party.

Barter appears as the engine for the evolution of economies (Caroline Humphrey and Stephen Hugh-Jones, 1992) but at the same time as something self-oriented or even selfish. Seems obvious that this “something” will end up becoming into the currency we know today. But let’s see how the society ended up there.

## **2.2 The destruction of the currency**

It can happen by many causes, but the mere pass of time might deteriorate that “something”. Alternatively, it can be lost and never be found. Nowadays, the notes are changed from time to time as well in order to avoid falsification or print new ones because there are many notes damaged.

Even with Bitcoin happened this event. At the beginning of Bitcoin, where people started mining it (we will see later what this is), some of the first miners lost their wallets loaded with Bitcoins because they lost the private key for accessing it. It is probable that those miners when Bitcoin hit the value of 19.000\$ in late 2007 teared their hair out of their skin.

## **2.3 Loss of value (devaluation)**

Devaluation affects that “something” in the sense that the third party and the Eskimo agreed that that “something” was worth 5 buckets full of clay. Now, 5 buckets full of clay might be too much to exchange for that paper.

We have to take into account that in the society there were as well monarchs and kings that probably exchanged something of higher value like precious metals (gold and silver), and probably because of this, they were the first to get universal acceptance.

With this fact, we turn up to use coins worth X quantity of gold and silver instead of using that “something”.

#### **2.4 *The appearance of coins***

The appearance of coins was a step ahead to the use of money for the society. Coins had inherent advantages such as the facility of transportation and its durability. The coins were created out of a base metal (used to be copper and not iron because iron can easily rust) and they were added a little quantity of gold and silver to add them value. Even though, it was frequent to find coins made of only gold or silver.

To ensure that a coin had a certain amount of precious metal, minting appeared. It was something like certifying the coin from a well-known and respected entity (like a reign) that endorsed the weight and the quantity of precious metal it had. This minting just added a trademark to the coin (like a symbol of an animal or of the king), that was easily recognized by the all society (let us not forget that most of the society in that times were illiterate).

For example, in some Greek coins we could see ears of wheat minted on the coins or the face of some Roman emperors in the roman denarius.

#### **2.5 *The appearance of the notes***

The origin of the notes is probably in the Chinese society, during the Tang dynasty (845 bC). The use of coins implied carrying something heavy, so they decided to create something lighter, although it was created out of something with less value like paper, but with the same value by government decree. The ones in charge of emitting notes were private banks by the order of the monarchs.

At the end of the XVIII century, private banks were substituted by central banks as issuers and in the XIX century there was established an international standard, the gold standard that we are about to get a general knowledge about.

#### **2.6 *The Gold Standard***

The Gold Standard is a monetary system that accepts gold as a standard of value. The currency issuer assures that the one who possesses the currency may switch it to gold at any time. During the Gold Standard validity, the inflows and outflows of gold regulated the quantity of money of

a country since it was convertible to currency, and the supply of money of an economy did have to preserve a ratio of 100% with the reserves of gold of the central bank.

The Gold Standard has not been the only Standard used along the history, there has also been the Silver Standard or the Bimetallic Standard, in which the currency was backed up by a quantity of gold and a quantity of silver.

## **2.7 Origin of the Gold Standard and transition to the Gold Exchange Standard**

The Gold Standard started being used in the XVIII century, but it was in the XIX century when it was extended globally financially speaking. Some economists find it the engine that made possible the Industrial Revolution, because it brought stability and prosperity to the financial system (at least until the First World War) and provided the framework for domestic and international monetary relations (BJ Eichengreen, 1996).

During the late XVIII century, the outlines of the standard would be set in order for it to function. The official starting date was in 1821. It was not until 1850 when England, that was a world power, proved that the implementation of the gold standard enhanced the industrialization, the modernization and the growth of a society. Pursuing England, the Standard become a popular system that was gradually implemented worldwide.

England, Germany, France and United States are considered the core of the Gold Standard, because they were the testers and, as a result, the main beneficiaries of the system.

*How does it function?* The currency had its equivalent in gold inside a range. If a country has a deficit, there were an outflow of gold outside the country and a contraction of the money supply. With the contraction, there were a drop in the prices in the internal market. This drop in the prices is an incentive that facilitates the exports and reduces the imports, which origins an inflow of gold in the opposite way, so the economy regulates.

This situation ended when at the end of the First World War, there were cases of countries that printed more money than they could back up with gold in order to be able to cover all the expenses that war originated. Against this background, they prohibited individuals to directly exchange the currency of the country for gold, and they changed the Gold Standard to the Gold Exchange Standard (Genève, 1922), fact that was the starting point for the Roaring Twenties, a period of time of industrial growing and prosperity that ends with the Wall Street Crash of 1929.

The Gold Exchange Standard stated that instead of being able to change straight a currency for gold, you needed to exchange first your currency to a set currency, and from that currency, you

could exchange it to gold. The Set Currencies used for this Standard were the British Pound and the United States Dollar.

Linking it to Set Currencies implied that those currencies could never be put into question, and it happened in 1971 and the Vietnam War. Vietnam War meant a problem for the United States, especially an economic one, because there was the sensation that there were abundance of dollars in the market and the feeling was similar to the one we just mentioned above during the First World War (too much dollars in order to back them all with gold), so the European Central Banks started converting all the reserves they had in USD into gold, compromising the situation of United States.

In 1971 the situation turned unsustainable, and Richard Nixon suspended the convertibility of the USD into gold for individuals, and devaluated a 10% the currency. It proved to be insufficient and Nixon ended up suspending the convertibility of USD into gold for governments and central banks as well. This situation is known as the **Nixon Shock** and heralded the end of the American Century (that began with the end of World War II) together with the first oil crises (Thomas W. Zeiler, 2003). They both punished consumers and real income for workers went steadily in decline.

## **2.8 FIAT Money**

Fiat money is a currency with no intrinsic value that has been established as money by a government. Fiat money's value is purely based on the confidence people has on the issuer. It can or cannot be backed by a precious metal, but the main currencies on earth like dollar or euro have no such backup. It may be shocking, but fiat money is fiat money because a government says so and the rest of us believe it and use it to exchange goods and services, otherwise it would just be paper.

Broadly speaking, if there is confidence on the system we are fine, if there is not we have a real problem.

Your mind might be popping some questions already, and we are about to introduce a new character in this TFM. An important one. But we need to go through some other concepts first.

## 2.9 Creation of money

You might have heard the phrase “printing money machine” somewhere. Central Banks tend to use it when things go wrong.

Because all the money we use nowadays (on paper) is fiat, the central banks can print as much as they want. They only have to press the button of printing and since we trust ECB, USA, European Union, FMI, etc., no matter the reserves of gold they have. Doing so, it happens to appear a new friend whose name is inflation.

On top of that, we have the fractional reserve banking<sup>2</sup>. Lending creates deposits. Commercial banks create money by making new loans out of the deposits. When a bank gives a mortgage, it does not give to the client all money in cash, but it credits their bank account with a deposit of the size of the mortgage. At that moment, money is created. Some economists have referred to bank deposits as “fountain pen money”, created at the stroke of bankers’ pens when they approve loans<sup>3</sup>.

## 2.10 Inflation

The definition is simple:

*“The sustained increase in the general price level of goods and services in an economy over a period of time”*

The inflation has to be with the capability of a currency to buy a good or a service. If inflation rises, the purchasing power of a currency decreases, which is an impoverishment. Which is logical: if prices rise, it implies we are going to be able to buy less things with every coin we have. Or to buy the same quantity or products, we are going to need more coins. Put it the way you want.

That is why inflation data is so important, and it is normally linked with indicators. In our case, the **CPI (Consumer Price Index)**.

---

<sup>2</sup> It is the common practice by commercial banks of accepting deposits and creating credit, while holding reserves at least equal to a fraction of the bank’s deposit liabilities.

<sup>3</sup> Fountain pen money is discussed in Tobin (1963), who mentions it in the context of making an argument that banks cannot create unlimited amounts of money in practice.

There are 2 factors that drive the CPI:

- Demand: If demand rises and the market cannot produce as fast as that increase, means that there are going to be more buyers for the same quantity of products. That is going to make prices rise.
- Cost: If an increase in cost of a production process happens, it is going to translate to the prices of the products. It can happen by:
  - o Increase in wages.
  - o Increase in the price of raw materials.

There are several types of inflation according to its magnitude:

1. *Moderate inflation*: Should be around 2% or 3% annual. The rise in prices happens in a slowly way. When this happens, we assume the value of my money is going to maintain constant through time and I can leave my money in a current account (in a normal macroeconomic situation).
2. *Tendency inflation*: In this case the CPI is continuous and perpetual. The values range from 3% to 20% annual.
3. *Galloping inflation*: We consider this case when the CPI surpasses the 30% annual. A CPI at this level would imply big changes in the economy. Our currency is losing value way quicker than expected.
4. *Hyperinflation*: If the galloping inflation is not controlled and there is not deep changes in the economy, we happen to have this inflation. This is a critical situation and the currency loses its value so fast. Population tend to get rid of it and buy things before its value is close to 0.

Hyperinflation usually happens in countries suffering a strong economic crisis due to the uncontrolled printout of money with a poor regulation between revenues and expenditures of a government.

So, having reached this point, the inflation is good or bad? It depends how the tale is told.

- General Impact: As we have said, a general increase of prices implies a decrease in the purchasing power of the currency. That is, when the general level of prices rise, we are going to be able to buy less quantity of goods and services for every coin we have. The inflation effect is not distributed evenly across the economy. For example, for those individuals that possess assets, such as property or stocks, will benefit from

the price/value of their holdings going up, when the individuals that want to acquire will need to pay more.

- Negative Impact: As mentioned above as well, high inflation rates are harmful for the economy. They add inefficiencies in the market and make difficult the act of forecasting in the long run.

The **European Central Bank (ECB)** has the main goal of maintaining an official inflation target of 2%, and the principal tool to achieve this goal is through interest rates, which is the price of money.

When ECB decreases interest rate, there is supposed to be growth in the economy, due to the fact that debt is cheaper and companies and individuals will borrow money to expand and to expend. If there is expansion and consumption, there will be job creation, which will bring wages to people and those will expend more (demand for products will rise). If demand rises, prices will rise as well, so inflation will increase. When inflation is at a level of 2%, ECB rises interest rate. Companies do not borrow money anymore and individuals neither. There is less money to expend so the consumption drops and prices drop with it as well. Companies do not need to produce that much products, so they start firing people. Less wages means less consumption, and the wheel keeps rolling. It is like a snake biting its own tale.

All in all, low and stable inflation is important for market-driven growth, and monetary policy is the most direct determinant of inflation (Ben S. Bernanke, Thomas Laubach, Frederic S. Mishkin and Adam S. Poscn, 2018).

### **2.11 Deflation**

If the inflation value is negative, it is defined as deflation. Deflation is the general and prolonged drop in prices (at least 2 semesters). This concept should not be misunderstood by disinflation, which is a deceleration in prices, but still positive.

Deflation tend to have worse consequences than inflation due to **The Ricardo Effect**, which asserts that in conditions of full employment an increase in the demand for consumer goods will produce a decrease of investment and vice versa (FA Hayek, 1942).

Yes, people will be happier if prices go down. Everything is cheaper, and the money we have seems to be more than we had before, because we can buy more things with the same amount of money. But when deflation happens for too long, companies' profits begin to decline. Economic environment force companies to sell their products even cheaper and continually,

reduce production costs, cut employees' wages, fire personnel or even close facilities. At this point, you all can guess that unemployment will increase; the economy cannot grow anymore because people is not spending and the future become uncertain.

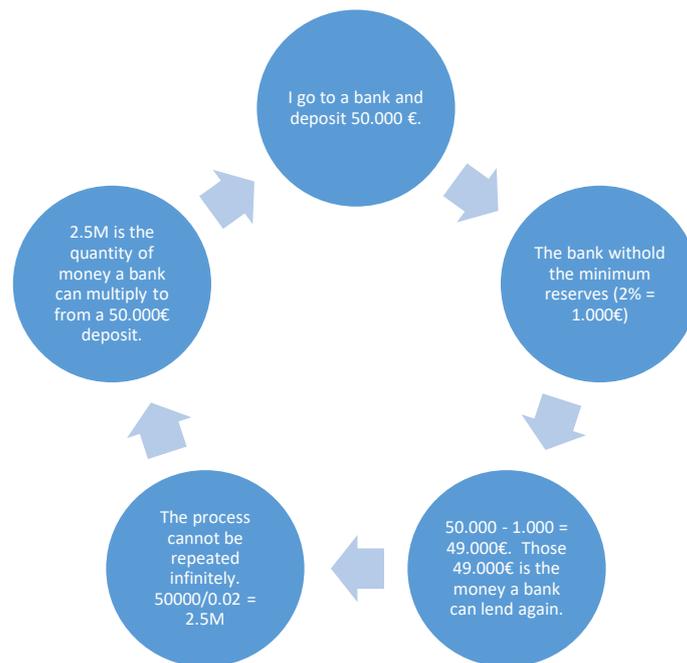
When there is inflation, government reduce spending and encourage saving by increasing interest rates. On the other hand, as governments do the opposite to encourage spending during deflation, they cannot decrease the interest rates to a negative level.

### **2.12 Fractional Reserve Banking**

What we have to have clear is that the printing machine belongs to the Central Banks. European Central Bank in the case of Europe. Let us have a look on what is this process.

Because the currency we use nowadays is fiat money, central banks can print as much as they want without having assets backing it up. We are adding another actor scene, national banks. Banks whose business is basically deposits. This activity is really important for the economy, because they capture deposits from individuals that have a surplus of money to lend it to individuals with a deficit of money. Taking this in consideration, we need to have in mind that these banks cannot lend all the money depositors have in their accounts. They must keep a percentage of all to face liquidity problems they may have (like runs). The amount they must keep is calculated through the **minimum reserves coefficient**, and since 1999 is fixed by the ECB on 2%.

Let us see an example on how it works:



**Figure 1 Example of fractional reserve banking way of functioning.**

That is called the banking multiplier and that is how banks do magic. I think that is clear why banks are trying capturing new deposits at all time. Therefore, ECB can create money whenever he wants and as much as he wants, and national banks can multiply it. However, creating money as a loan, needs debtors in the economy. People that want to get debt, and those exist. That is basically what happened in the crisis of 2008. Banks lend money to people that knew would not be able to pay beforehand. If we lend money and the debt is not paid back, system collapses, confidence on the system is lost, we join into mayhem, and the situation becomes unmanageable. Not even the States were able to pay their own debt. Yes, you can say it. Holy Moly. There is more. Let us check next chapter.

### **2.13 Money and debt**

So far, we are at this point:

We have refused Gold Standard in order to print as much money as we want. Through the pattern just explained, we can multiply the money printed through loans and on top of it, bank wants to earn money through interests. So not only we have to pay the principal back, but also have to pay interests.

If all the money supply circulating in an economy is because has been generated through debt, we can consider that the money supply of an economy is the quantity of its debt. There is no money if there is no debt. Let us not forget that not only we have to pay back that money, but we have to pay interests as well. We have to pay back more money than it really exist.

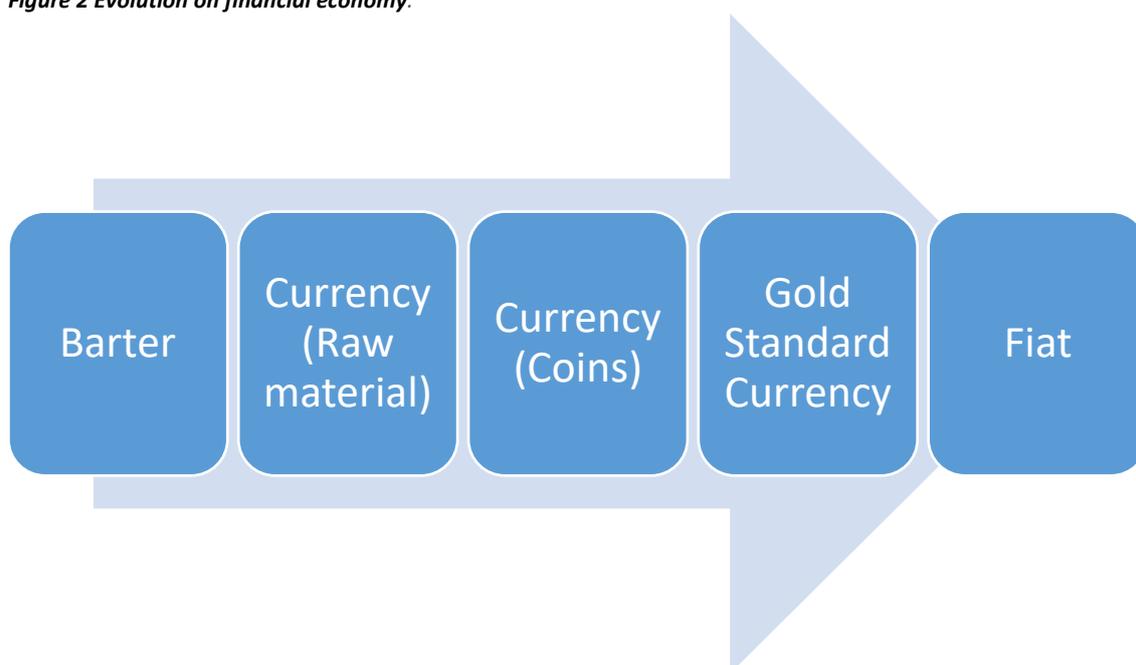
If the 50.000€ of the example of the chapter before were the money supply of a entire economy, there would be only 50.000€. Who is going to pay my interests? Exactly, other debts.

So the actual system does not permit the payment of its whole quantity of debts, and it is a problem growing exponentially. They can making it up how they want to and explain it to you upside down, but we are just patching the economy as problems pop instead of fixing it up.

Is there place in our finite world, for infinite growth?

In this TFM we have been through this stages in the economy:

*Figure 2 Evolution on financial economy.*



Currency has been evolving during all history. Is this the time to evolve again? We are. We are evolving to **digital currency (or electronic money)**.

### **2.14 Digital Currency (Electronic Money).**

Electronic money is the electronic store of value in an electronic device that may be used to make payments to individuals worldwide through electronic systems. Its value is backed by fiat currency and it can be exchanged into physical form whenever the individual wants. The concept of fiat electronic money is rather ambiguous. In the fiat electronic money perspective, bank payment card and internet banking are not electronic money, as these systems simply allow operations with real money held in bank accounts. In other words, these products only provide means of access to real money (Huerta de Soto, J. 2008; Allegret et al., 2016; Boldeanu and Tache, 2016; Fetai, 2015; Glavina, 2015). This is evolution. We can see all the transition from the barter, through precious metals and ending up into notes. Anyway, that electronic money is backed still with something physical, physical and real money backs the electronic one, so one can exchange it whenever he/she wants. The problem is somewhat complicated by the fact that all modern banking system uses the principle (as we have already gone through before) of the fractional reserve funds that were deposited, that, in fact, is a fraud (Arslan-Ayaydin et al., 2014; Grima et al., 2016; Suryanto, 2016; Thalassinou et al., 2013; Thalassinou et al., 2015). The use of this principle leads to the fact that banking system is using a mean of acting that is impracticable, with impractical liabilities and reaching volumes that far exceed not only the quantity of cash available in the banking system, but the entire amount of real money in the monetary base of the economy (AV Vlasov, 2017; Rothbard, 2003; Hamid and Won Kie, 2016; Tcvetkov et al., 2015). Our society is, nowadays, debt. All the money supply circulating is debt, because it is emitted by a central authority and it needs to be paid back. On top of that, since the gold standard pattern was abolished, the only value behind those notes is the trust we have in the institutions they emit it. It is paper, but our trust in those institutions make that paper something value or, at least, those institutions make us think that is valuable.

Electronic money is backed by the central bank system, which makes it different from **cryptocurrencies**. What did you just say? Cryptocurrencies? We have seen already the problems of the financial system and of the fiat currency, so let us give a look to this new concept I have just mentioned: cryptocurrencies.

I read somewhere in the net that these four technologies would be the disruptive technologies of the XXI century:

- Mobile development.
- Big Data.
- Cloud Computing.
- Everything related with social media.

In my opinion, the author of the article missed a huge one (and another one is implied with it) that is going to shake some things up:

- Cryptocurrencies (and decentralization).

A cryptocurrency is a digital asset that is meant to work as currency between individuals. It is a digital mean of exchange that uses the cryptography in order to ensure the transactions, control the creation of additional units and verifying the exchange of assets itself. They are an alternative and digital currency. Cryptocurrencies have a decentralized control (the opposite of fiat currency) and work on a pioneer technology called **blockchain**.

### **Chapter 3. Understanding Blockchain.**

Blockchain is a technology that allows society to make processes that some years ago would take days or even months, do them instantaneously. At the speed of internet.

Blockchain is a decentralized public accounting system. It allows us to count without cheating. Every transaction is written in the chain after the verification of it by consensus of a majority of the participants in the system, they are then pooled in blocks and those blocks have metadata (information that provides data about other data) of the last block of the chain. Doing so every individual helps creating the general or public ledger, the Blockchain, that contains a certain and verifiable record of every single transaction ever made.

Blockchain was conceptualized in 2008. Closely after, it was used to enable payment system for the Bitcoin Cryptocurrency. Bitcoin is the most popular example using Blockchain nowadays (Crosby, M., Nachiappan, Pattanayak, P., Verma, S., Kalyanaraman, V., 2016).

#### **3.1 Centralization VS Decentralization**

Centralization and decentralization are two types of structures that can be found nowadays in plenty of fields (organizations, management, government, purchasing, information...). However, what is the difference between those 2 concepts?

A. *Centralization*: It refers to the process in which the decision-making and planning is located in a specific individual. For example, in a centralized organization, the decision-making voice recurs in the executive.

Similarly, in a centralized government structure, the power belongs to the top of the organization structure.

B. *Decentralization*: It is, on the other hand, the process by which the activities of decision-making and planning of an organization are delegated away from a central figure to a group of people. It is, basically, the dissemination of authority and responsibility.

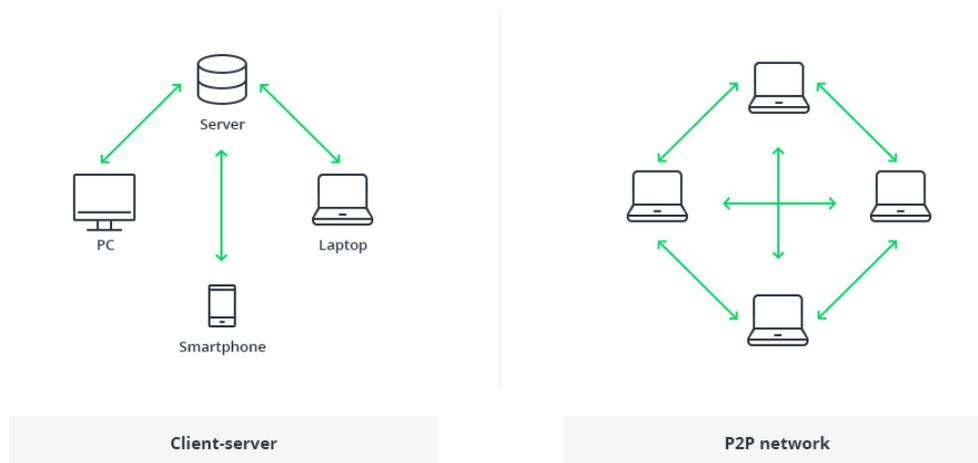
Another clear example of centralization or decentralization would be (speaking now about information system) how the information system worked 30 years ago compared on how it works now.

If someone wanted to look for something 30 years ago, he/she would do it in an encyclopedia that families used to have in the bookshelf. Nowadays and thanks to internet, we have a decentralized system of information. Does Wikipedia rings a bell?

The real difference between Larousse encyclopedia and Wikipedia recurs on how the content is created. With the encyclopedia, Larousse would hire 4000 contributors, they would create the content and they would go out and sell it, but only the people that bought the encyclopedia would have access to that information. With Wikipedia, it is all decentralized. Anybody can contribute with Wikipedia, anybody can read Wikipedia. Wikipedia has almost 300000 monthly editors.

That is how Internet decentralized the systems of information. Well, the Blockchain can potentially decentralize anything else. Why? Again, let us get deeper.

As we said before, the systems we are used to are centralized. That is a client-server traditional network. In this system, the server keeps all the information required in one side and a number of people or administrators that have the permission for it controls that server. In a DLT (Decentralized Ledger Technology) or Blockchain Architecture, each participant of the network participates and updates the system. It is not controlled only by several different individuals, but by everyone within the blockchain network. Each participant double check that all transactions are in order and correct, which results in an increase of security and proof of validation.



**Figure 3 Differences between client-server structure and p2p structure**

### **3.2 ARCHITECTURE OF THE BLOCKCHAIN**

#### **3.2.1 Timestamp**

Blockchain uses timestamp-systems in order to “prove” the authenticity of the transactions added to the chain, without the need of a third-party proving system. Trusted timestamping is a procedure for verifying the existence of unaltered digital data at a specific point in time. The action of attaching timestamp to physical documents was the way to assure the integrity of a document at a specific time. Historically, public notaries, governments or other third-party entities that need to double-check the authenticity of documents. However, this approach has the deficiency of timestamps being vulnerable to a central vouching party (Gipp, B., Kosti, J., Breiting, C., 2016).

The first time-stamp system was the “proof of work system” (PoW). It is SHA-256 algorithm based and most of the most used time-stamp system are based in SHA-256 or *script*.

The Secure Hash Algorithms (SHA) are a group of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) and the US Federal Information Processing Standard (FIPS). The main SHA hash functions are:

- SHA-0: it had a major flaw and was replaced by the SHA-1 revised version.
- SHA-1: It is a 160-bit hash function and from 2010 on, it was no longer used due to cryptographic weaknesses discovered. It was replaced by SHA-2.
- SHA-2: We have here the SHA-256 and the SHA-512, depending on the word size. The first one uses a 32-bit word while SHA-512 uses a 64-bit word.

- SHA-3: Developed by public competition among non-NSA designers. It was formerly called *Keccak* and it supports the same hash lengths than SHA-2, but the internal structure is completely different from the SHA group.

### 3.2.2 Mining

In the cryptocurrencies world, the mining is a system of validation of the transactions. For this effort, the validation, miners receive a reward. Because cryptocurrencies are a decentralized system, we need something that allows us to check all the operations carried out and avoid someone use at the same time the same quantity of Cryptocurrency, or avoid someone trying to add fake currencies into the system. So mining's mission is certifying that no one is using same coins twice or no one is creating and adding fake coins to the system.

What miners do basically (as stated before) is double check transactions and pooling them in a block. All those blocks together are known as Blockchain (DLT). Those blocks are completed by the PoW system, which is like solving a math problem by brute force. The more computational power you have, the easier is solving that math problem in order to create a block, adding it to the chain and receive the reward. Inside the BTC code, for instance, it is stated that for every block validated (every math problem solved) the miner receive a reward. By the time this TFM is written, the reward is at 12.5BTC per block validated. According to the forecast, in the middle 2020 (precisely 23<sup>rd</sup> of May at 6:29AM) that reward is going to be reduced to the half. That event is known as "halving". Every 210.000 blocks, a halving happens so the reward is reduced to the half.

*What do we need to mine?* What we needed in the beginning was just a computer processor due to the fact that only a few were mining. The more people joined the mining world, the more difficult was mining Bitcoins. Nowadays, in order to get chances to be able to mine and get rewards, we would need a high computational power. Why is now like that and in the beginning you did not need that much? We are going deeper in that in the next topic.

### 3.2.3 The difficulty and the hash rate

The more computers mining, the higher the computational power, but the higher the computational power, the higher the difficulty in order to solve the block. That difficulty of solving the block is the calculation needed to guarantee that the blocks are solved every 10 minutes. If 2016 blocks in a row are solved in less than 10 minutes, the Bitcoin protocol will

readjust the difficulty in order to raise the difficulty of the block solving system. If 2016 blocks in a row are solved in more than 10 minutes, it will happen exactly the opposite thing.

The *hash rate* is the processing capacity of the system. It is the unit whereby all the processing capacity of the system is measured. The hash rate is the speed at which a computer is completing an operation in the Bitcoin code. The higher the hash rate the better the opportunity for mining the next block and receive the reward.

High computational power has its controversy as well. Blockchain is susceptible to attacks of colluding selfish miners. Generally, it is known that nodes with over 51% of computing power can reverse the blockchain and reverse the happened transactions. However, recent studies have shown that even nodes with a percentage close to 51 are still dangerous (Zheng, Z., Xie, S., Dai, H-N., Chen, X., Wang, H., 2017).

### **3.3 Use Cases of Blockchain**

Backed by the success of using Blockchain as a payment method, people started raising interest in the capacity to extrapolate Blockchain to other use application. This technology enables a new design approach for distributed database using a peer-to-peer communication. Blockchain is meant to meet these services:

- A. Authenticity of transactions (Preventing duplicate transactions).
- B. Ensuring traceability of data by enabling transparency (It makes falsification difficult).
- C. Security of the system against attacks without a central authority.

Blockchain is a revolution in systems of record. It is the first permanent, decentralized, global, trustless ledger of record of the history. The manner blockchain works has imaginations running wild, because this system can now be applied to any need for a trustworthy record (Foroglou, G., Tsilidou, A-L., 2015).

Blockchain as a system of record:

- i) Digital identity: blockchain is going to be usable to form digital relationships between individuals. Blockchain opens the door to digital identity, because it is not

based on accounts and third-party permissions. The ownership of the private key is the one owning the digital asset and so to manage the identity.

- ii) Tokenization: the authenticity of physical assets could be controlled through blockchain. With tokenization you are binding the asset of the real world with the tokens themselves. It can be deployed in supply management, intellectual property, fraud detection...
- iii) For governments: Ownership of rights drag the attention of governments. They want to find out who is acting behind blockchain, that is why they are trying to regulate the transaction authorization.
- iv) Financial institutions: Banks prefer using an obsolete, complex and slow technology rather than using blockchain technology in cross-border transactions. Blockchain could be used to send money abroad faster, cheaper and more efficiently than it is being done nowadays.
- v) For audit trails: Banks are currently spending way too much money in keeping information secure. And same thing will happen with normal businesses. Blockchain offers security in all the senses. It identifies the subjects of the operations, it tracks the operations and you can check anything that happened at any moment.

#### Blockchain *as a platform*:

- i) Smart contracts: If transactions can be coded out, you can use smart contracts and the blockchain. You run a code, it is authorized or denied, and the transaction carries out or not.
- ii) Automated governance: Bitcoin is a DAO (Decentralized autonomous organization).
- iii) Markets: Stocks and bonds can be tokenized.
- iv) Streamlining of clearing and settlement: Nowadays we often hear the terms “T+2” or “T+3”. This means, when a trade is signed, it takes the trade (T), two (T+2) or three (T+3) days to execute. Of course there are ways to reduce this number, but not without compromising security and risk. With blockchain, you would not compromise security nor risk, and the transaction would be T+0.

The potential benefits of the Blockchain are just beyond from only the economical perspective, it can reach the political, humanitarian, social and every single area from life you can think of. Actually, its technological capability is already being used to face real-world problems. For instance, in political repressive regimes, blockchain can be used in a decentralized way in order

to do transactions that before needed to be checked or processed by the government in a centralized way. Blockchain was useful when the US government banned all the accounts of Wikileaks, they were able to receive donations in order to keep the wheel rolling. In these situations, public interest must prevail over governmental power and hierarchical power structures.

Blockchain brings some major useful features to the market:

- Coordination.
- Record keeping.
- Irrevocability of transactions.

Those features may bring forward progress in society. Blockchain could potentially be used for public records, registry of documents, events, identities and even assets. An interesting concept such as *smart property* is appearing, which at the end of the day is encoding every asset in the Blockchain in order to be traced, controlled and/or exchanged.

How can be assets encoded in the Blockchain? Intellectual Property is another field Blockchain can tackle. An algorithm is run over a file (any) and it is compressed into a hash, a 64-character hash. After the coding, the hash is included in a blockchain transaction, which adds timestamp, which is the prove digital asset is existing at the moment. That hash can be recalculated from the original file, which is stored in a computer, in order to confirm that the original contents have not changed.

### **3.4 The 3 stages of Blockchain**

The potential of Blockchain technology is extremely disruptive and it might be able to reset the way we carry out major things in our society. The different things we can carry out so far with Blockchain are divided into three main categories (Swan, M., 2015):

**Blockchain 1.0, currency:** Obviously, the implementation of the *distributed ledger technology (DLT)* led to its first obvious application: cryptocurrencies. It is also known as “the cash of internet”.

**Blockchain 2.0, smart contracts:** They are not smart nor contracts. They are small computer programs that live in the blockchain and execute automatically. There are conditions that are defined beforehand such as the facilitation, verification or enforcement of the performance of a contract. Advantages of this technology are the reduction of the cost of verification and execution.

**Blockchain 3.0, other applications:** It is referred here to other applications beyond the currency, finance and markets. Specifically in the areas of government, health, science, literacy, culture and art.

### 3.4.1 *Blockchain 1.0: Currency*

The word Bitcoin may lead to confusion, due to the fact that is used to refer 3 different things:

1. **Bitcoin, as the underlying blockchain technology platform.** It is the decentralized ledger that keeps the transaction record. Let us say it is the database that is shared by all the nodes, updated by miners and owned and controlled by no one.
2. **Bitcoin, as the protocol run by the blockchain.** The software system that transfers the money over the blockchain ledger.
3. **Bitcoin, as cryptocurrency and the largest of them.** It is also known as BTC.

The key things of all this put together is that it is the structure of any modern cryptocurrency: blockchain, protocol and currency.

#### *The double-spend and Byzantine Generals' computing problems*

Long before of the arrival of Blockchain, digital cash had a central server trusted third-party in order to prevent double spending. Bitcoin might be the solution to a major issue such as *the double-spend problem (Chaum, 1983)*<sup>4</sup>. Before the invention of Blockchain cryptography, digital assets were infinitely copiable, and there was no way to find out if a certain amount of digital cash had been already spend without the help of a centralized authority (or intermediary). We can say, for instance, that the 30€ that I have in my PayPal wallet do exist and have not been spent, because that third-party authority tells me so. Because PayPal is the one that records transactions and knows for a fact (not 100% sure) that money belongs to me. The same problem can be extrapolated into the war field, with the Byzantine Generals. They had the necessity to transmit information between each other but had the difficulty of not trusting 100% to each other.

---

<sup>4</sup> Chaum is credited with the first conceptualization framework for digital currencies; some of his ideas have been endorsed in the Cypherpunk's Manifesto.

Blockchain fixes that double-spending issue by the sum of BitTorrent p2p sharing method with public-key cryptography.

**“BitTorrent p2p<sup>5</sup> sharing method + Public key cryptography = Digital Money”.**

The owner of the digital money is recorded in the ledger and confirmed by cryptographic protocols and the miners. The user of the Blockchain does not need to trust the other party in the transaction; the user needs to trust the system, the Blockchain protocol software system. That is why Blockchain is trustless. The group of transactions in order of time are grouped in “blocks”, and those are registered in the ledger.

#### How does a Cryptocurrency function?

Cryptocurrency is also known as digital cash. We could say Bitcoin is digital cash, which is used to buy and sell products and things on the internet. There are some things that compose the bitcoin value chain: software developers, miners, exchanges, merchant processing services, web wallet companies and users.

From a consumer perspective, the important things here in order to carry out a transaction are the address, the private key and the wallet software. The address is where the counterparty is going to send the Bitcoins or cryptocurrencies to you, and the private key is the cryptographic secret by which you can send bitcoins to the counterparty. The wallet is where your cryptocurrencies are stored and where you manage them.

#### Adoption

At the time of the writing this Thesis, there are major exchanges where you can exchange FIAT to Bitcoin or other cryptocurrencies such Coinbase in the United States or Kraken and Coinify in Europe.

Even though the way of getting into the cryptocurrencies world is easier and easier for the consumer perspective, it is difficult for vendors, like a cafeteria, to run two different payment system, the FIAT and the Cryptocurrency. Mobile payment is a feature that is going to make things easier for both the consumer and the cafeteria perspective. A matter companies like

---

<sup>5</sup> P2P (Peer-To-Peer). This concept is created on the internet and it is based on sharing a product to a final client, erasing all kind of intermediation, establishing a peer-to-peer relationship, equal to equal relationship, between the distributor and the consumer. P2P has allowed other interesting concepts to be born like *crowdfunding*.

CoinBeyond are trying to solve. We have to remember that this technology is still walking with diapers. It needs time, like every other world-changing event, because the potential is there.

All in all, Blockchain is already a payment solution system, and it may change the way we see money nowadays. There has never been a real alternative to the currency we have ever dealt with. We want better cars, better clothes, better jobs...but what about better currency? Bitcoin itself brings payment fees reduction to below 1 percent in a market which has 514 billion international transfers. It is also direct, peer to peer, no intermediaries, that is people can exchange electronic cash in a decentralized way. ALL transactions since the origin of the Blockchain can be traced and tracked by every single user of the technology. It is quick, users can receive funds immediately in their wallets.

### Regulation

Government's regulation is probably one of the most discussed topics. Regulation might be the fact that might let this technology get into full-adoption in the financial world or not. There are plenty of countries that have prohibited the use of cryptocurrencies by users (Bangladesh, Bolivia, Ecuador, Iceland and Vietnam for instance. China banned back in 2013 financial institutions from using it. Germany and France have negative thoughts on Cryptocurrencies as well.

Even though the biggest economic powers of the world do not look in a good way to Cryptocurrencies, they are still deliberating and studying it. On the other hand, some countries like United Kingdom are treating cryptocurrencies like currency, so it is not subject to VAT. In the United States, the IRS is approaching Cryptocurrencies as financial assets (like stocks), not as money, so if a person has capital gains with it the taxation would be applied like it was stock.

#### *3.4.2 Blockchain 2.0: Contracts*

Blockchain 2.0 is the next big step in the Blockchain technology development. Since 2014, the activity in this area has skyrocketed. We can include here Smart Contracts, Smart Property, Decentralized Applications (DApps), Decentralized Autonomous Organizations (DAOs), and Decentralized Autonomous Corporations (DACs).

Just as Blockchain 1.0 is meant for the decentralization of currency and payments, Blockchain 2.0 is meant for the decentralization of markets. We can actually compare the Blockchain technology with the Internet with a simple analogy.

When Internet technology was deployed over the world, we could build platforms like Amazon or Netflix on top of it, and those platforms have been getting more complex with the pass of time. With Blockchain technology we can say the same: Once Blockchain 1.0 have been deployed, we are now able to construct Blockchain 2.0 protocols on top of it. The key concept of the matter here is understanding that the decentralized transaction ledger functionality of the blockchain might be used to register, confirm and transfer all manner of contracts and properties.

All financial transactions could be reinvented with Blockchain technology: stocks, private equity, crowdfunding, bonds, mutual funds, public records, land and property, business licenses, marriage and death certificates...you name it.

#### *3.4.2.1 Financial Services*

Blockchain is trying to link itself with the traditional banking and financial markets. We have a clear example like Ripple Labs, fighting for a spot in this market. Ripple uses Blockchain technology to reset the way of functioning of the banking business. It allows financial institutions to run their business more efficiently in the blockchain. The main advantage of Ripple system is that allow banks transferring funds from one to another in a direct way, without a third-party intermediary as is now required.

Another analogy with cryptocurrencies might be PayPal. At the beginning, PayPal was an innovative payment solution outside the traditional financial system, like Bitcoin, but with the pass of time it has become a formal business within the regulated industry, gathering personal information of its client. PayPal had always been known for being in the edge of financial innovation, now it is well known and used by most of population and corporations in the payment industry. Now, PayPal accepts cryptocurrencies as mean of payment with the strategic partnerships done with Coinbase, BitPay and GoCoin. Nowadays, PayPal also has a mobile payment provider that allows customers to pay in AirBnB and Uber with cryptocurrencies.

The concept of "BitBank" has also been a matter of discussion. The European cryptocurrency exchange Kraken, partnered with a Bank in order to provide regulated financial services related to Bitcoin. In the future, there might be the necessity of having Bitcoin saving accounts or lending services.

#### *3.4.2.2 Smart Property*

As stated before, onto the Blockchain can be encoded every type of asset, making possible the tracking, exchange and registration of the mentioned. We include here hard assets such as

physical property or intangible assets such as votes, patents, health data or any kind of information.

Using Blockchain technology in this area opens multiple doors of different use cases involving all segments of money-related-businesses and financial transactions. Blockchain encoded assets become smart property that can be exchanged via smart contracts. The idea behind smart contracts is the fact of transacting all property using blockchain models, and with property, we can refer to hard property assets like a house, a motorbike or a computer, or to intangible assets such as shares, bonds or patents. With *Swancoin* for instance, you can exchange 121 physical artworks, crafted in wood, via Blockchain. Whoever controls the private key controls the possession of the asset.

In short, the idea of smart property is having access to an asset and therefore to the ownership, by having it registered onto the blockchain and having access to the private key. Smartphones could be unlocked by confirming user's identity in the Blockchain, the doors of the vehicles or homes could be "smarter" as well and be embedded to Blockchain technology and anything you can imagine now, could be "smarter" and linked to Blockchain to make it function.

#### *3.4.2.3 Smart Contracts*

From Smart Property rises another interesting topic, which is Smart Contracts (William Cong, L., He, Z., 2018). In a simple way, contracts would be using Bitcoin to form agreements among people through the Blockchain. A contract, at the end of the day and in a traditional way, is an agreement between two parties to do something in exchange for something else. There has to be trust between the parties and every party must fulfill its obligation. Smart Contracts kind of function the same way, but they remove the trust part of the equation. That is because the smart contract is based on running a code. The Contract is defined by a code, run by the code and executed by the code. Actually, the basic characteristics of a smart contract are:

- A. **Autonomy:** once it is running, a contract and its creator do not need to be in contact anymore.
- B. **Self-Sufficiency:** it is code running. If its function is raising funds to deliver energy, if the funds are not raised, the energy is not released. It is all automated.
- C. **Decentralization:** they are not stored in one server; they are distributed across the nodes of the blockchain.

The classical example used in order to describe smart contracts is the example of a vending machine. A vending machine is based on an algorithm. Instructions set will be followed always in the cases they have to be followed. When a customer inserts the coin and chooses a product, the item is dropped. There is no possibility of the machine not dropping the item, the vending machine “has to fulfill with the contract” as well, because “code is law”.

Obviously, if cryptographically activated assets were to be the new way of functioning of our society, probably new body of law and regulation would need to be discussed. Parties involved in the contracted would need to choose a legal framework to be incorporated to the contract.

There are many Blockchain projects that can be gathered under the 2.0 protocol projects, although there might be some controversy around the categorization.

<b><u>Project Name</u></b>	<b><u>Description</u></b>	<b><u>Blockchain</u></b>
Ripple <a href="https://ripple.com">https://ripple.com</a>	Payment, exchange, remittance network; smart contract system -> Codius	Separate Blockchain.
Counterparty <a href="https://www.counterparty.co">https://www.counterparty.co</a>	Currency issuance and exchange	Bitcoin blockchain
Ethereum <a href="https://ethereum.org">https://ethereum.org</a>	General-purpose Turing-complete cryptocurrency platform.	Own blockchain (EVM)
Mastercoin <a href="http://www.mastercoin.org">http://www.mastercoin.org</a>	Financial derivatives	Bitcoin blockchain.
NXT <a href="http://www.nxtcommunity.org">http://www.nxtcommunity.org</a>	Alcoin mined with proof-of-stake consensus model	Bitcoin blockchain overlay.
BitShares <a href="https://bitshares.org">https://bitshares.org</a>	Decentralized crypto-equity share exchange.	Separate blockchain

**Table 1 Blockchain projects with different purposes**

**Wallet Development Projects**

With a tiny margin of error, we can say that probably the category to which developers are paying more attention to build atop the blockchain is wallets. Wallets are a core element for

cryptocurrencies, because they are the mechanism for the secure holding and transfer cryptocurrencies or any other asset. We have here projects like:

1. Chroma Wallet, open assets.
2. CoinSpark, open assets.
3. Melotic, it has the ability to trade curated digital assets with Bitcoin.
4. OneWallet, bitcoin marketplace and wallet

#### *3.4.2.4 Blockchain Development Platforms and APIs*

There are plenty of companies developing projects that offer tools to facilitate the task of application development in the Blockchain. There are Applications Programming Interfaces (APIs) for working with its ewallet software to make and/or receive payments. With *Chain* you can ask for the data available in certain nodes and ask for Bitcoin balances in certain addresses, as well as program notifications when there is movement in those addresses.

As the Blockchain world grows, there will be needed more APIs environments in order to respond to all parts of the Blockchain (Storage, messaging, wallet interactions, mobile payments, identity confirmation...). There is also room for cooperation between Blockchain and other areas like M2M (Machine to Machine) communication and IoT (Internet Of Things). An example of this cooperation would be an smartwatch that can interact with smart-city traffic-sensor data to automatically reserve and pay for a spot with a Bitcoin Smart Contract.

#### *3.4.2.5 Ethereum: Turing-Complete Virtual Machine.*

Back in 2008, in Satoshi Nakamoto's initial plan, there were 3 original steps (Nakamoto, S., 2008).

1. Blockchain: Decentralized Public ledger.
2. Bitcoin protocol: the transaction system with no third party.
3. Turing completeness: the ability to run any coin, protocol or blockchain.

One of the Blockchain projects that is oriented to be a Turing<sup>6</sup> complete platform is Ethereum.

Ethereum is a platform and a programming language in order to create and build applications.

Ethereum used Blockchain as starting point and wanted to cover a wider class of

---

<sup>6</sup> The Turing idea is 83 years old, originated in the mind of Alan M. Turing, the man who broke the unbreakable German Enigma code during the World War II. The Turing machine is an abstract idea of a machine capable of simulating any algorithm that can be logically constructed. What is that at the end of the day? He thought of a machine, which had the capacity to solve any problem as long as it could be coded out.

implementations. With Ethereum, you cannot only guarantee the financial transactions but literally any condition or agreement. In a daily basis we use the agreement principle “if...then” in everything, not only in the financial world. Main problem of these agreements is that no one can guarantee a final result, no one can guarantee the fulfillment of the agreement.

In order to avoid this kind of problems, businesses use contracts. That is hiring special people in order to design contracts with special words, signatures and papers with the goal of punishing the party not fulfilling the agreement. It is a boring football match where you must trust someone because the honesty he transmits to you. This problem is solved by Blockchain technology. Ethereum is the main author in this crime scene.

Ethereum is not a Blockchain, nor a protocol running over a blockchain. Ethereum is a complex infrastructure that can run all blockchains and protocols. Ethereum is a platform for application development to write smart contracts that can call multiple other blockchains, protocols and cryptocurrencies. It works through Ethereum Virtual Machine, which is like a giant computer where all transactions are executed. This giant computer is actually a network of different computers connected with each other. The main function of EVM is executing the Smart Contracts and every node runs a EVM.

The execution of those contracts has a cost (energetically speaking), that is why a reward needs to be established. The reward unit is GAS. The work capacity required for a transaction is measured by GAS. The reward therefore will be GAS. The cryptocurrency of the Ethereum network is Ether, and 1 Ether equals to 1.000.000.000 Gwei. The sentence “My gas cost for this transaction is 0.000000001” could be “My gas cost for this transaction is 1 gwei”.

The implementation of Smart Contracts is the principal feature brought by Ethereum to the Blockchain world. With those Smart Contracts, you can create over the Ethereum network practically anything exchangeable between two parties. You can create tokens that can function in the Ethereum network rather than creating a personal Blockchain for every token.

#### *3.4.2.6 DApps, DAOs, DACs and DASs.*

At this point, we can see now some projection of Blockchain. First of all is currency transaction, followed by all kind of financial transaction. Close enough is smart property, which can code hard assets and intangible assets into the Blockchain. Finally, we have seen smart contracts that can transact with all those assets that can be encoded. With time and usage, smart contracts could become more and more complex and autonomous. DApps, DAOs, DACs, DASs and

automatic markets would gain meaning in that stage. An example of a simple smart contract would be a bet between two parties about the weather of tomorrow. On the hour set in the contract, it would automatically read the temperature from an official database. The party closest to the temperature would win the bet, so smart contract would be executed so as the transaction implied from one account to another.

*DApps (Decentralized Applications), DAOs (Decentralized Autonomous Organizations), DACs (Decentralized Autonomous Corporations) and DASs (Decentralized Autonomous Societies)* will begin to gain sense when smart contracts are developed and complex enough that can become automated or self-contained entities, conducting preprogrammed and self-programmed operations in the Blockchain.

A DApp would be an application that runs on a network with participant information securely protected and operating in a decentralized manner across all the nodes.

DAOs and DACs is a more complex form of a DApp. To become an organization, a DApp would need to have a more complex functionality (such an organization), it would need to announce its governance publicly in the blockchain and it would need to have a mechanism for financing its operations, like issuing equity in a crowdfunding.

DAOs and DACs derive from artificial intelligence. A group of decentralized autonomous agents carries out tasks in a organizational manner but without any human component and under the control of a preset business rules.

One example of DAO model is *Storj*. It is a decentralized cloud storage platform automated with smart contracts. It raised almost 500.000\$ back in 2014. It uses Bitcoin blockchain technology and peer-to-peer protocols to provide secure, private and encrypted cloud storage. Through internal apps, users can rent free storage and store their files on the Storj Network. The rental transaction is executed thanks to Storj's token, which is Storjcoin X. It provides a method of storage, which is cheaper, more secure and more decentralized than Google or Dropbox.

As you can imagine, a DAS would be essentially an ecosystem of DAPPs, DAOs and DACs functioning automatically.

### *3.4.3 Blockchain 3.0: Application in other fields beside currency, financial markets and business.*

As stated before, Blockchain technology not only have the capability of reconfiguring the way of functioning of payments, financial markets, financial services and economics in general, but it

might also have the capability of reconfiguring all kind of industries or, even going beyond, all mankind efforts. Blockchain is the new way of doing the same activity we do nowadays but more efficiently and at much greater scale. It could also revolutionize the world due to the asset reallocation potential. Blockchain decentralized scope is universal, global and instantaneous, which was previously impossible. All kinds of human activity could be connected and coordinated by Blockchain and by requiring consensus to operate, the model could also have greater liberty and equality.

In order to reach the Blockchain 3.0 phase, there is an on-going topic on discussion: scalability. That one particular problem cannot be ignored. Blockchain 3.0 platforms need to meet the demands of large institutions and enterprise by offering a solution that is truly scalable for their business. Plenty of factors measure that, but a key one is *Transactions per seconds*. Visa's tps is able to handle from 1700tps to 24000tps. So the next logical step for Blockchain 3.0 would be to build on this features in order to meet the necessities of those entities and improve transactionality in terms of speed, cost and throughput.

*Metabase* is a project by Intrepid Ventures, a high-performance blockchain platform that allows entrepreneurs to build their own decentralized applications on. It aims to provide a blockchain protocol solution that offers robust programming capabilities designed with security, usability and scalability in mind.

3 potential use-cases of Metabase would be:

- Data Storage: all concerning data privacy and security. Businesses and governments need a more secure way of managing this kind of information. There are currently 2.5 quintillion bytes of data created each day. The solution that provides Metabase is a blockchain protocol that scales with adoption. Of course, to imagine a single blockchain running the storage of the whole world would be a dream.
- Healthcare: Currently, the infrastructure of the healthcare system struggles to track and record verifications, movement of assets, ownership and identity. Using blockchain in these areas could potentially save massive amounts of money of taxpayer funds.
- Supply chain: Tracking transactions is a complex task because many intermediaries are participating in the chain. As a result, the supply chain industry is largely and worldwide inefficient and susceptible to fraudulent activity. Blockchain would be an ideal solution tackling straight this problem. It would offer real-time tracking; it would enforce transparency and would add efficiency to the system.

#### *3.4.3.1 Blockchain Government*

The idea of using Blockchain to provide services that have been centralized for a lifetime also remains in the pocket. Actually, we could use it to provide in a decentralized manner services provided by nations and states, and more importantly, cheaper, more efficient and in a personalized manner.

Blockchain government could have an impact and could be a role switcher of the “one-size-fits-all model” to one that can be tailored to the needs of the citizens. An example of a blockchain government model could be one citizen that pays a higher waste removal service that includes composting while another is paying for a higher school package. Personalized government services instead of the current “one-size-fits-all” model could be scripted and directed by Blockchain.

It is clear that “putting a country or a state” in the blockchain is a picture more representative of democracy than anything else we have now. That would be rather than relying in humans agents or representatives, use smart contracts and DAC’s.

#### *3.4.3.2 The other side of the coin: Blockchain is not for every situation.*

Despite the potential and the power of Blockchain, one of the most important points for us in order to deploy Blockchain in our lives, is to spot and identify where it is and is not appropriate to use cryptocurrencies and Blockchain models. Not all processes need a decentralized system, or a peer-to-peer payment method, or a high security record keeping system. For example, it would make no sense to record every micro transaction carried out in a tipping vLog platform. It could function in a side-chain where one daily transaction is recorded.

There is a tension between centralization-decentralization and we need to find an equilibrium. Besides from the Internet, there have not been many large-scale decentralization systems that have been conceptualized and used worldwide in different cases of use. At the moment, Blockchain’s biggest advantage which is “decentralization” it is at the same time one of the main problems for its no-possibility of use for a lot of areas. Every transaction in the Blockchain needs from 2 to 10 minutes to be validated and confirmed by miners. Compared to the millisecond response time that needs the advertising area for instance, Blockchain is just too slow to be a tool for real-time fraud prevention and validation.

We can say Blockchain industry is in its infancy yet, so there are many situational and possible limitations. Those limitations are internal and external, including those related with the technology itself, thefts and scandals, regulation, governments and the adoption.

*Technical Challenges:*

- A. Performance and efficiency: As stated before, Blockchain network has a problem with the performance and efficiency. Today the Bitcoin network is restricted to 7tps. Though, developers say this limit can be raised when it is necessary doing so. VISA can process 2.000tps with a peak of 10.000tps, Twitter can process 5.000tps with a peak of 15.000tps, and advertising networks can typically process over 100.000tps.
- B. Latency: Right now, each Bitcoin block takes 10 minutes to process, meaning that it can take at least 10 minutes for your transaction to be confirmed. Again, and I apologize for the comparison, VISA takes seconds worst case scenario.
- C. Security: There are some security problems that might be tackled by a major Bitcoin entity. The most problematic one is a 51% attack, in which one mining entity could take control over the blockchain and double-spend coins already transacted into his own account.
- D. Wasted resources: Mining waste a lot of energy. The last estimation was 15M\$ per day, and those estimates keep rising. That wastefulness makes the blockchain trustable, but those resources spent mining have no other use rather than mining itself.

*Scandals and Public Perception*

One of the biggest public problems of Bitcoin is the idea people have that Bitcoin is only useful to money-laundering, drug-related business and other illegal activities. Silk Road scandal has been one of the biggest of Bitcoin history. Bitcoin and Blockchain itself are neutral, as anything else in the Earth, and they can be used for good or evil. Even though Blockchain can be used for evil purposes, the potential good ones just outweigh the evil. Perceptions can change over time, especially if adoption is constantly rising and people have more wallets and coins as time passes.

Blockchain models need to mature in order to have better safeguards ready to stabilize the industry and allow people (from both in and out sides) to recognize between good and bad players.

#### *3.4.3.3 Government Regulation*

This would be probably the highest risk surrounding Blockchain. How government regulation deploys over it might either rotten everything or make it flourish, especially when Blockchain is used in the financial area as currency.

The deliberations and early rules worldwide about the use of Bitcoin bring some interesting questions to the scene. One is taxation. It would not be possible to carry out taxation due to the fact of the decentralized environment of the technology. The usual tracking systems of consumption and spending could not be applied in the same way, so it would make impossible taxation system to the citizens. Another one speaks about the obsolescence of the governments and about not being able to keep up with their record-keeping functions and making data accessible to citizens. On this question, governments could become obsolete because they cannot fund themselves the traditional way (By raising taxes). Blockchain technology could potentially solve these problems, record properly and making it accessible to the society.

### **3.5 *Impact of blockchain in the financial sector.***

As we have been mentioned many times, blockchain will make able the transition from a centralized transactional model pattern, which until today it has been the model that has prevailed, to a decentralized transactional model pattern.

Two of the most discussed topics of the actual manner of functioning are: weakness and corruption. Nick Szabo, one of the pioneers of decentralized cryptocurrencies, stated “Trusting a third party is a nice-sounding synonym for a wide-open security whole that a designer chooses to overlook” (Szabo, 2001).

Nakamoto, back in 2008 also stated, “The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank” (Nakamoto, 2008). Actually, the idea of a distributed system emanates from computer scientist that thought that precisely a distributed system should be more robust and more reliable rather than a centralized authority, such as government.

<u>Standard</u>	<u>Model</u>	<u>Blockchain</u>
Trusted third-party / central coordinator	Paradigm	Trustless system / pseudonymous participants
Centralized server / many clients	Architecture	Peer-To-Peer network
Single copy	Database	Multiple copies
Controlled access / firewalls	Security	Cryptography
Intermediation	Price / Cost	Consensus / proof-of-work
<b>PRIVATE</b>		<b>PUBLIC</b>

**Table 2 Differences between standard-based and blockchain-based models**

We can sum up the key differences between the transactional model we have been having and the decentralized model that distributed ledger technology provides. The DLT together with blockchain technology put under discussion three potential deficiencies of the centralized ledger controlled by a third-party institution:

- i) The trust depository might not be that trustworthy and might be subject to bribes and corruption.
- ii) The controller of the centralized ledger might not be one hundred transparent with the content or market participants, censoring or rejecting some of them.
- iii) Centralized systems are not immune to loss of records.

Blockchain, with its decentralized consensus-reaching mechanism, its open-source approach, and the possibility of being able to see every single transaction executed, addresses those three main deficiencies brought by the centralized methods to the system.

### **3.5.1 Continuous rise of banking disintermediation.**

The trend of disintermediation is rising and rising. One pretty clear symptom is the growth of shadow banking. The traditional banking system is not the only source of financing anymore, and this trend is far from the end. Actually, there has been a rise of transactions in worlds known as *crowdfunding and peer-to-peer lending*, where individuals with necessity of financing can transact with individuals with super habit.

### **3.5.2 DLT's impact on digital economy and e-commerce.**

Blockchain is very prominent to have a huge impact on the digital commerce, precisely because of the decentralized model it advocates for. The base of users in the e-commerce market share has been growing since the creation of internet, but the way of managing transactions have

been centralized since then (Amazon or eBay are clear examples). If we look at recent successes enterprises of the digital age like Uber or AirBnB, we will find the same exact problem, centralized platforms.

There are some examples of Blockchain technology already decentralizing those kind of models, like *Arcade City* in the US or *La'Zooz* in Israel for transportation services and car sharing.

### *3.5.3 Why DLT is almost impossible to ignore?*

It is pure strategy financial institutions cannot ignore blockchain technology. Ignoring it would be a mistake in case it reaches full-adoption. Financial institutions need to anticipate and adapt in terms of new methodologies of doing things. In this dual vision of threat or opportunity, looks like the last one is anticipating and gaining advantage. Financial institutions would function better with the cost saving advantages that Blockchain offers.

#### **Blockchain technology and the potential for financial applications.**

- A. Payment systems
- B. Corporate finance and governance.
- C. Financial accounting, trade finance and supply chain management.
- D. Financial reporting and compliance.
- E. Crowd-funding and peer-to-peer (P2P) lending.

#### **The Possibility of a New Digital Economy**

Cryptocurrencies and Blockchain technology are usually linked with a massive reduction in two key costs:

- i) The cost of verifying the transaction.
- ii) The cost of networking.

For being able to operate in a market properly, you as an user (particular or company) need to be verified and/or audited before you can execute any transaction. It requires the implementation of a third party to ensure everything is in order (checked, verified and audited). This process is intensive in terms of effort and it can be done way cheaper and more efficiently with a DLT system. Nevertheless, the ability of time-stamp and immutability of transactions are not what make Blockchain a disruptive technology.

It is the architectural change brought to the market that makes this technology a disruptive one. It is the combination of incentivizing the growth, operations and securitization. Anyone can build something on top of the protocol without requiring permissions from anyone. Combined with the incentives, participants can use cryptocurrencies to reach consensus on a global scale. This drastically changes the scale and scope of what an online community or platform can achieve.

The ecosystems built on top of blockchain technology will be able to look for and award talent, ideas and capital at a scale previously unimaginable.

### **Emerging legal challenges in financial regulation**

There is some complex phenomena rising in the financial world that needs to be regulated somehow. The Fourth Industrial Revolution (Bayón, P.S., & Vega, L. G., 2018) we are living it, as some researchers call it, has some major actors that have specific needs due to their size, the different fields they cover and the fact they are working in the cyberspace. These major actors in the digital economy bring legal challenges that need to be readdressed from a regulatory point of view.

FinTech industry is not properly regulated nor in regulation or transparency. Large financial and technological companies must be more transparent in terms of generating profits through the collection of data and their weight in books. Nowadays, we can compare 2 industrial companies looking at their books but we cannot contrast information from 2 different fintech due to the lack of regulation and transparency. A specific regulation is needed in order to make FinTech companies disclose information about where do their cash flows come from and how business actions impact their books, customers and markets.

FinTech world is young, so many things surrounding it are, but given the systematic risk they can generate (because some financial institutions already do) legislators need to establish a basic criteria to analyze information and avoid potential price manipulation, bubbles or even financial crisis.

A step forward in terms of accounting law would be to consider data as an asset. With this, we would be able to value fintech companies more precisely and not only value them with cash flows and profit or turnover, which is how society values them nowadays.

Regarding tax law, it has been the only discipline that has approached digital economy in a direct and effective way. The OECD BEPS (Base Erosion and Profit Sharing) project has led to

recommendations that have already been developed in the European Union. The aim is that the value of the data and the services digitalization do not result in a detriment in the tax revenues of the countries.

Information is the key point of the Fourth Industrial Revolution. Digital technologies are on its task of revolutionizing the chain of information and the processing systems by a 2-staged process:

1. Quantitative change: Big Data, amount of information being transmitted.
2. Qualitative change: Use of that information and transformation into knowledge. We have here the rise of FinTech.

FinTech industry is changing the market structure through Blockchain (cryptocurrencies and smart contracts) and it is forcing regulators to intervene and set legal and legislative frameworks into the financial system, dealing with topics and actors they had never dealt before.

#### **4. Conclusions**

Before Internet, there were things regulated and OTC. In Spain, “Bolsas y Mercados” was the platform where regulated transactions were carried out. It was a platform with a CNMV license where you could connect and transact. Before that platform, there was “Mercado de corros”. It

was a physical place where a group of, for instance, apple providers met and negotiated prices for 15 minutes.

As we can see, evolution has been, is and will be key in everything. Mercado de corros evolved to Mercado continuo, a platform where individuals connect among them. Investment banks or banks carried out all OTC back then. They were regulated because:

- There was law on the field.
- There were platforms that offered the service in an organized manner.

What is happening with Blockchain? Transactions are happening through internet platforms that apparently are like the ones we have been using so far. Transactions are carried out with the same seriousness as the regulated ones, and the volume of transactions can be even higher than in a regulated one.

That is a victory of the informal against the formal. Some years ago, the strange thing was the OTC, it was a minority and it was for rich people. Blockchain allow the democratization of the OTC markets, making the “informal” more accessible. When you make so, when you democratize the informal, you end up standardizing and regulating. And OTC market that were not regulated nor standard before, end up naturally regulated and being standard.

When is using Blockchain useful?

1. When peer-to-peer prevail. In the BTC Blockchain, people who trade coins are equal. There is no hierarchy among them. Blockchain is being used in syndicated loans precisely because banks are equal entities. They need to create a distributed trust. Blockchain allows users to create that trust. Blockchain is useful for everything? Might be in the future. It is an efficient and effective tool for some fields, but it is not for some others.
2. When a lot of transactions are going to be carried out.
3. When the transaction are juridical and legally simple.

In regulated markets where monopolies prevail, it is pointless to use Blockchain. When the time comes and we have the possibility, for instance, to store energy and exchange it between individuals breaking with the monopoly of electric companies, then it would make sense to use Blockchain as a mean of exchange.

## **5 References and Bibliography**

Sanz Bayón, P., & Vega, L. G. (2018). “Automated Investment Advice: Legal Challenges and Regulatory Questions.”

- Bayón, P. S., & Vega, L. G. (2018). "An outlook on the role of Finance Regulation under the Fourth Industrial Revolution. *Archives of Business Research*, 6(10)."
- Nakamoto, S. (2008). "Bitcoin: A peer-to-peer electronic cash system."
- Catalini, C. (2017). "How blockchain Technology Will Impact the Digital Economy." *University of Oxford Faculty of Law Blog*, 24.
- Elsinger, H., Fessler, P., Feyrer, J., Richter, K., Silgoner, M. A., & Timel, A. (2018). "Digitalization in financial services and household finance: fintech, financial literacy and financial stability." *Financial Stability Report*, (35), 50-58.
- Altenhain, T., & Heinemann, C. (2018). "Fintech Hypes, but Wealthy Internet Savvy Investors Prefer to Stay Hybrid." In *Digital Marketplaces Unleashed* (pp. 343-357). Springer, Berlin, Heidelberg.
- William Cong, L., He, Z. (2018). "Blockchain Disruption and Smart Contracts."
- Chaum (1983). "Cypherpunk Manifesto."
- Swan, M. (2015). "Blockchain: Blueprint for a new economy."
- Foroglou, G., Tsilidou, A-L. (2015). "Further applications of the blockchain."
- Zheng, Z., Xie, S., Dai, H-N., Chen, X., Wang, H., (2017). "Blockchain Challenges and Opportunities: A Survey."
- Gipp, B., Kosti, J., Breitingner, C. (2016). "Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain."
- Crosby, M., Nachiappan, Pattanayak, P., Verma, S., Kalyanaraman, V. (2016). "Blockchain technology: Beyond Bitcoin."
- AV Vlasov (2017). "The evolution of E-Money. Rothbard, 2003; Hamid and Won Kie, 2016; Tcvetkov et al., 2015."
- Arslan-Ayaydin et al., 2014; Grima et al., 2016; Suryanto, 2016; Thalassinos et al., 2013; Thalassinos et al., 2015.
- Huerta de Soto, J. 2008; Allegret et al., 2016; Boldeanu and Tache, 2016; Fetai, 2015; Glavina, 2015.
- FA Hayek (1942). "Three elucidations of the Ricardo Effect."
- Ben S. Bernanke, Thomas Laubach, Frederic S. Mishkin and Adam S. Poscn (2018). "Inflation targeting: lessons from the international experience."
- Thomas W. Zeiler (2003). "Requiem for the Common Man: Class, the Nixon Economic Shock, and the Perils of Globalization."
- BJ Eichengreen (1996). "Golden fetters: the gold standard and the Great Depression, 1919-1939."
- Caroline Humphrey and Stephen Hugh-Jones (1992). "Barter, exchange and value: anthropological approach."

Nakamoto, S., (2008). "Bitcoin: A Peer-to-Peer Electronic Cash system."

Bloem, J., Van Doorn, M., et al. (2014). "The Fourth Industrial Revolution. Sogeti VINT; and Schwab, K. (2017). The Fourth Industrial Revolution, New York and the Fourth Industrial Revolution: what it means, how to respond. Foreign Affairs."

Iansiti, M., Lakhani, KR., (2017). "The truth about Blockchain".

Zyskind, G., Nathan, O. (2015). "Decentralizing privacy: Using blockchain to protect personal data."

Pilkington, M. (2016). "11 Blockchain technology principles and applications."

Kosba, A., Miller, A., Shi, E., Wen, Z. (2016). "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts."

Tapscott, D., Tapscott, A. (2016). "Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world."