UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO

CORSO DI LAUREA MAGISTRALE IN ECONOMICS AND FINANCE

TESI DI LAUREA

"CRYPTO-CURRENCY AND BLOCKCHAIN: THE REVOLUTION OF THE WORLD ECONOMIC SYSTEM AND DIGITAL IDENTITIES"

RELATORE:

CH.MO PROF. ALBERTO LUPOI

LAUREANDO: VALERIO DECARO

MATRICOLA N. 1104252

ANNO ACCADEMICO 2016 – 2017

Il candidato dichiara che il presente lavoro è originale e non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere.
Il candidato dichiara altresì che tutti i materiali utilizzati durante la preparazione dell'elaborato sono stati indicati nel testo e nella sezione "Riferimenti bibliografici" e che le eventuali citazioni testuali sono individuabili attraverso l'esplicito richiamo alla pubblicazione originale.

Firma dello studente

_____

Contents

List of Figures

1 Introduction

Since I was a child, I have always been fascinated by the power of money and how simple pieces of metal or printed paper could heavily affect relationships between people.
Growing up I began to realize that this power went beyond simple retail trading, money was, and it is still, able to change the political forces that move an entire country.
During university studies I was able to feed my curiosity by trying to deepen the knowledge in the political and macro-economic fields, studying the role played by central banks and credit institutions in general, but above all trying to find out what in the centuries had shaped the concept we have in today's currency.
Then, at the end of the previous academic year, before the summer, by accident I read an article in a magazine that talks about a "new" concept of currency, without physicality that can give tangible proof of existence, without authority to govern its operation, simply relying on computer and math algorithms. When I went deeper in details I realized that much of what I had learned was about to change and that I had just fallen in love with Bitcoin.
Across centuries humans optimized every aspect of our lives, from caves to the penthouse of a skyscraper, wheel, roads, from the handcart to the Ferrari, etc. but also different types of money, like the barter, or gold paper, or coins minted by increasingly sophisticated techniques, checks, bills of exchange, bank transfers, credit cards, ATMs; optimizing everyday tools and objects and making them increasingly efficient and with the sole purpose of making our life simpler.
Looking at the cell phone we have in our pockets, we are no longer amazed at what we can do comfortably in the palm of a hand and how this technology concentration can connect with someone on the opposite side of the Earth within a few milliseconds; however, it may surprise us that, up to 10 years ago there was no iPhone in circulation, the first model was introduced June 29, 2007. The evolution of multimedia players, the possibility to connect almost with anyone and everywhere in the world, the speed at which we can connect among each other, all these evolutions /innovations can be grouped together as Exponential Technologies, and I think that means of payment are evolving in the same way, moreover I think money can be digital too.
One of the major questions I will try to answer in this thesis is: "what about the future of money?" But obviously there will not be a real solution, at the end of the work I will simply expose some possible future frameworks of this context and according to my interpretation.

Starting from a synthetic historical reconstruction of money from its origins, *between myth and reality*, I will then sketch out what is currently the landscape of the means of payment, increasingly dematerialized. Then, in Chapter 4 that contains the most technical part, I will try to analyse in detail, but not too much, how Bitcoin works and what is hidden behind its algorithms.
Technologies like Bitcoin, in its underlying framework the blockchain, are fundamentally weave themselves into the fabric of our society.
From the beginning, the 'bitcoin is for criminals' narrative had to be fiction. Its value and its volume are now demonstrably independent from its greatest suspected criminal use. The legality of bitcoin depends on who you are, and what you're doing with it.
An important challenge for this new set of technologies is communication of its significance to policymakers and to the public, and maybe this is one of the important motivation that led me to write this thesis.
Bitcoin creates suspicion and fear, most of the time, amongst citizens and government policymakers because of its association with criminal transactions and "dark web" trading sites. But digital cryptocurrencies are of interest to central banks and government finance departments around the world which are studying them with great interest. This is because the electronic distribution of digital cash offers potential efficiencies and, unlike physical cash, it brings with it a ledger of transactions that is absent from physical cash.
Without the presumption of wanting to change the idea that everyone has on this subject, in this thesis I have tried to represent in an objective way what is happening today in the rest of the world; although sometimes I have included some of my personal reflection, thoughts and opinions developed during these months of studies and research on Bitcoin, I hope that this elaborate is of the liking of the reader.

2 Origin and Evolution of Money: Unit of Account, Medium of Exchange and Store of Value

In his book *The Wealth of Nations*, published in 1776, Adam Smith notes that human nature has "a propensity to truck, barter and exchange" which is "to be found in no other race of animals" [1]. Smith describes as a particular tendency of humans to trade among each other (just think that, the origin of writing arose from the need to keep accounts of the grain and other commodities deposited in royal palaces and temples)[1]. Then, at some point in the development of ancient societies, as different people specialise in different skills and jobs and careers, they begin to recognise that simple bartering can be cumbersome and slow. They needed some special things which would be accepted at any time in exchange for any article, that would make the process easier and quicker. That special thing would be money and such part of human nature, that makes money come into existence, allowed to meet the need for a more efficient means of exchange than barter.

Over the centuries, money has reflected changes in politics and government, in economic life and power, in science and technology, in religious and other cultural beliefs, in family and neighbour-hood life, and in other aspects of how we live. And it has not just reflected those changes, it has al-so helped to bring them about[2].

2.1 Money: its role and definition

If we have to define money we can say that it can be whatever people will generally accept in exchange for other things, and let me pose attention to the verb I used because, as we will frequently see later on in this work, the coin (in the strict sense) is that thing issued by the State on a specified historical period and it is part of the money until it is accepted by the market: the currency out of circulation and devalued currencies are no longer money, since no one accepts it.

If we want to try understand the role played by money throughout centuries, until nowadays, we cannot avoid to mention the enormous contributions left to the cause by Sir John Hicks, the father of the *IS-LM* model. He defined money as the *numéraire* of the economy and, more importantly, the medium of exchange used to meet future payments. More deeply, he saw, in the money of mature economies, two main features: (1) money has no intrinsic value, and (2)

[1] A. Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, London, March 9, 1776, Ch. 2, p.18
[2] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 2-6. Available online.

it is universally accepted for trading good and services. But this is not enough.[3] We have to consider money also like an asset and, as such, it should be treated as a component of a general theory of portfolio choice, otherwise, assuming a simultaneous general equilibrium world, where the date and the amount of future payments are certain, it is not possible to have demand for money as a means of payment. Its role as a store of wealth then became the distinguishing feature of money, whereas its function as a means of payment and a unit of account were neglected [2].

There was and still there is an inherent difficulty in fitting the complex nature of money into the models available. Hicks therefore started an extensive search for methods of dynamic analysis (see, for example, Hicks J. 1982C [1956]. Methods of dynamic analysis in Hicks, J. (ed.), *Money, Interest and Wages, Collected Essays on Economic Theory*, vol. 2, Oxford, Basil Blackwell). In particular, Sir John tried to find a mode of process analysis that would retain the role of money as store of value but would also consider money's role as means of payment. He proposed to approach monetary theory from a non-Walrasian perspective (since he soon realized that, in a Walrasian system of interconnected markets, there was no analytical role for money). The aphorism he never tired of using was that: "Monetary theory is in 'history'".[4]

Hicks proposed an economics that describes the chain of historical sequences that characterise modern economic systems. He recommends explanations that run in terms of sequential causation, in particular, he explained the different roles that money plays in a single-period theory and in a continuation theory [3]. Money is a flow of means of payment that is naturally created during the economic process (especially but not exclusively the production process) and used for the circulation of commodities. Furthermore, in a world of uncertainty, money is also a stock, a store of wealth to meet unforeseeable payments. [2]

Monetary theory cannot be ahistorical. The nature and origin of money can be properly interpreted only in terms of an economy moving through time. In Hicks's optic, the analysis of a single period is an essential first step to the full description of the process.[5] Thus, after this first merely introductive part we will see how the role of money changed in time, depending on the evolving time-frameworks.

[3] G. Fontana, *Hicks on monetary theory and history: money as endogenous money*, in *Cambridge Journal of economics*, 2004, Vol. 28, n.1, pp. 73-88

[4] G. Fontana, *Hicks on monetary theory and history: money as endogenous money*, in *Cambridge Journal of economics*, 2004, Vol. 28, n.1, pp. 73-88

[5] G. Fontana, *Hicks on monetary theory and history: money as endogenous money*, in *Cambridge Journal of economics*, 2004, Vol. 28, n.1, pp. 73-88

2.2 Money across centuries: Why was money so important from the beginning?

In the medieval tradition, since the time of Carlo Magno, the right to coin money was one of the usually reserved and jealously guarded rights to tax authorities, and one of the most important cities claim, obtained after lengthy and not always easy negotiation. The royal resistance is partly determined by the fact that the currency is seen as a symbol of sovereignty, but also, and perhaps to a greater extent, by the fact that the mint is a vital source of legal financial revenue, for the so-called "law of lordship"[6], and illegal financial revenue, for the gain that the tax authorities can obtain by entering in the market increasingly poor coins, of which, however, maintains the legal value unchanged.

Before metal coins were invented, ways to pay for things took many forms, i.e. hundreds of objects were used as money. As opposed to what we might believe, the barter economy, except for some very specific and exceptional circumstances, has never existed as a system. Such opinion is confirmed by an anthropologist as David Graeber, in his book *Debt: The First 5000 Years* [4] where he shows that never existed economies based on barter. The reason lies in the fact that bartering always leave someone unhappy, given the difficulty to match the values of the objects exchanged, and often the deal took on unexpectedly violent traits. Moreover, if money had been simply a continuation of other instruments, we would face an economy that could not reach the levels that today are there for all to see, in particular, if money did nothing more than replace the barter, the amount of money in circulation could never exceed the amount of goods. On the contrary, as it is well known, the money has been a growth engine of the economy over the centuries.

To address trade, the men immediately sought to obtain a certain quantity of goods or any other object that had the characteristics to be accepted by others in exchange for their products. In ancient societies of the Mediterranean and Near Est areas they included wheat and barley and cattle. Cowrie shells and bronze and copper copies of them have been used more widely and for longer than any other form of money, from 1600 BC in China to the 20th Century AD in Africa. The fundamental feature, in a society in which men live next to each other, is that the members of the community have confidence in this commodity, in its role as unit of account and means of exchange. Thus, the money was born with the mark of the collective confidence about its ability to pay the debts resulting from the exchange, it is born almost in parallel to the development of trade and civilization.[7]

[6] Nobel Prize winner Paul R. Krugman, in the international economic text written with Maurice Obstfeld, defines the law of lordship, or seigniorage, as the flow of "real resources a government spend on goods and services when printing money ". [103]

[7] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 11-49

2.3 An interesting case study: Island of Yap

An interesting and unusual form of money is that developed on the island of Yap, a piece of land of Micronesia, in the Pacific, including the Philippines and Hawaii, where the anthropologist and traveller, William Henry Furness, in 1903, discovered that the currency of that community was represented by giant stone wheels, known as Rai, or Fei. In this island remained primitive, excluded from contact with modern civilization, the economy was very rudimentary; however, contrary to what you might believe, the Yap families had invented a very sophisticated payment technology, which Keynes himself, in 1915, found much more logical than the currencies anchored to gold in vogue in those days of gold standard [5]. These people had entrusted the task of units of account to large stone wheels that could not be moved, except with great difficulty. In fact, each remained in place, but the community knew well to who it belonged to each boulder: when a transaction occurred they merely recorded collectively that a stone, or part of it, had changed hands. The indifference to the physical custody of the stone was such that some of these, sunk in the sea during a transport operation, but they still maintained its function as a unit of account and changed owner remaining in place [6]. Without spoiling too much, this reminds quite accurately how does the Block chain works, that is the pillar of the most common crypto-currency now in circulation, the bitcoin.

The keystone of the payment system developed in the island of Yap, the trust, still remains the foundation of modern monetary systems. It is interesting how the inhabitants had caught, in the unit of account and in the credit and debits compensation system, the essence of money. Of course such a system - which, however, marks the origins of the money - requires a total mutual trust and a very tiring annotation mechanism. For this reason, at some stage in history, the community has begun to look at objects that for their symbolic value, religious value, rarity, intrinsic value or utility, were able to guarantee the ability to transfer the receivable due as a result of a trade.[8]

2.4 From etymology to numismatics

History, literature, ethnology and mythology help us to detect early experiments. In the sixth book of the Iliad, Homer tells the story of the hero named Glaucous who exchanges his golden armour, worth a hundred oxen, with that of Diomede, made of bronze, that is worth only nine. The etymology of the word "capital", from the Latin *caput* (unit of cattle), or the word "pecuniary" (from the Latin *pecus*, sheep) and even rupee (which derives from the herd) are directly related to a use of the cattle as the local currency in an economy that had just took the road of farming, livestock and agriculture. [5]

[8] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 11-49

2.5 How coins are made and why these material have been chosen

There are countless other examples, such as salt cut into small cubes, in the upper Senegal, cotton canvas as a measure of the slave price, cowries mounted in wires and garlands, in Asia and Africa, small carved cylinders squeezed into rosary, used by Native Americans, etc. all of these solutions, while giving assurances of solvency plan, they presented many practical drawbacks (i.e. risked the salt to melt after the first rain, the cotton squares became cumbersome, and in general they were all subject to deterioration and exposed to disastrous losses). The time was ripe for the choice of new techniques and payment practices.

At this point, it is natural to wonder why the precious metals were chosen. There is no denying that suggestion played a role in convincing the men of that time, as we cannot refuse the idea that their intrinsic value and their scarcity has contributed to the choice. However, in hindsight, the reasons that led to prefer precious metals, were at least four, all of a practical nature: (1) the precious metal encloses a great value in a limited volume and therefore can be transported, stored and eventually easily hidden; (2) precious metals are indestructible and unalterable - in particular gold - and therefore may defy the years and bad weather with fewer losses than any other material; (3) gold and silver are divisible, malleable and reassembled, therefore, can be cut, coined, stamped in a variety of shapes or dimensions; furthermore, (4) they are a medium of exchange having the characteristic of value reserve, precautionary reason, sought after by man in times of economic uncertainty.[9]

But gold and silver, despite their undoubted qualities, they will never succeed alone to play the role of money. You will need State intervention.

2.6 From the first minting to the disintegration of the Roman Empire

The first proper money, as we think of it now, was the gold and silver coins of the 6th century BC. These were produced by the Greeks in Ionia, in the Western part of modern Turkey, not very far from the city of Ephesus. In ancient myth and Greek history, two kings, Midas e Croesus, were famous for their gold and riches.

The coinage by Croesus is the symbol of a crucial step that will mark the history of money up to the present day: the combined role of the State and the market. In first place, in fact, the transition from rods to the coins, guaranteed in weight and quality, allowed the exchanges to act in a framework of trust and to gain time, since the new coins could easily count and weighed.

[9] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 52-97

In the Aegean trades occurred a revolution, thanks to the concrete guarantee of the proper weight of the currency and the price of the metal by the State. Moreover, the State had a working capital available to pay the troops and collect taxes. This gave legal force to the coin.[10]

In a deeper study of ancient coins, Greek and Roman, we can realize that the collective security function is crucial. Greek and Roman coins were minted with the name of the monetary magistrates responsible for the emission, i.e. on the coin there were no figures corresponding to the weight or value and everything was regulated by a decree of the State [5].

In the same period, 5th century BC, in Athens, we see what illustrious names have defined the first monetary reform in history made by Solon, archon of Athens, remained legendary in the stories of Aristotle and Plutarch. Solon in addition to a series of measures and revolutionary reforms brought to completion at least two significant legal and monetary policy actions: on the one hand, he abolished the debt bondage, imposed by law; on the other, he devalued the drachma, silver coin minted with the precious metal from the nearby mines of Laurion. With the devaluation, which was implemented by simply reducing the weight of the coins, the city of Athens obtained three results: more liquidity, a reduction of the state debts and the debts lightening for the weakest sectors of the population. An operation that became known as *seisachtheia*, or "discharge of weights".

Certainly the devaluation of Solon demonstrates the narrow link between money and the needs and State policy since the debut of the first civil and organized syndicates. Moreover, with this reform he built a parallel with the policy of the American president of the New Deal, 2500 years later, in order to lighten the burden of debts of farmers in the Midwest. The story did not go unnoticed by John Maynard Keynes who devoted to the reform of the Greek legislator an essay where he loved another crucial move of the Athens monetary strategy: the imposition of some kind of legal tender in the State currency. The law of Solon in fact reserved to the Prince and the State the right to grant permission to import and export or the right to print money [5].

With regard to the Roman currency, the *aes grave*, it came to the first minting much later than in Greece (between 289-275 BC), the same period when the mint was located in Rome at the temple of Juno Moneta on the Capitoline Hill[11]; hence the name *moneta*, that still is used in many Western languages (money, monnaie etc.)[12].

[10] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 52-97

[11] *Campidoglio*, between the Forum and the Campus Martius, is one of the Seven Hills of Rome.

[12] the temple was located on Capitol Hill and was built to honour the goddess Juno, who, according to tradition, would cause the geese, animals sacred to her, to sound the alarm, in 390 BC, when Gauls penetrated into the city. Hence the definition of cautionary and since the mint was placed near the temple, by extension the name of "moneta" (derived from Latin *monēre* which means to remind, to warn, or to instruct) [12].

Also the Romans resorted to devaluation, and such operations continued in the era of the emperors, starting with Emperor Octavian and following. Later on, when the disintegration of the Empire took place, with the disorderly management of the coins the inflation swept throughout the Mediterranean. The expenses for the maintenance of the huge territory and the birth out of control of peripheral mints did the rest. The last Roman coin now ready to be bequeathed to the Middle Ages was the *golden solidus*, minted during the reign of Constantine in 309 AD.

2.7 Middle Ages: two separate functions of money

Throughout history, for many centuries, from the Middle Ages to the eighteenth century, the two main functions of money, unit of account and means of payment, co-existed separately. In order to better understand this statement, it is necessary first to clarify each of the two functions. As a unit of account, the currency is a unit of measurement which makes it comparable to the value of the goods, therefore in this case it should not materially exist to be used, you can simply use an accounting system. On the other hand, when we mean the currency as a medium of payment, we refer to it in a material and effective sense, it can be any object with a liberating power, i.e. that delivers from each obligation, and that, normally, must be imposed by law.

Roberto Petrini, in his book, expressed the essence of what you may think about this situation "It seems paradoxical, but men have first learned to count and then to pay".[13] The first need was to compare the values using a unit of measurement which was combined with the propensity to exchange and followed - only immediately after - by the need to share and indicate a means of payment. One proof of the fact that the function of unit of account was the mainly consists of the names of European currencies, which have dominated the last centuries, derived from the so-called system of weights (the French livre, the Italian lira and the British pound, derive directly from the Latin *libbra*, from the Greek *litra* or "balance").

For ages the accounting system moved away from the real weights of precious metals due to the repeated devaluations for state intervention and Princes. We must also consider that the old coins were usually minted without any written indication of their nominal value, there was no number indicating the value, only symbols or the effigy of the sovereign: hence the value of the coins was set out by edicts issued by the Prince [7]. This means the Attic talent and Roman pound gradually lost the link to their original weight, up to the point where they remained mere unit of account, intangible. The process was gradual: the weight that corresponded to the units of account was reduced and thus the number of actual coins of silver or bronze to make the exchange (or to pay a contract signed in units of account) diminished. These steps lightened the burden of debtor classes or, as we will see later, the debts of the Crown.

[13] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 52-97

Insisting on the separation of the money functions, unit of account and means of payment, and putting the emphasis on the former, as evidenced by history, it allows to point out that money from the very beginning is something that is subject to social conventions and it is administered by the State. It is a sign-money, overnight it can change value even in spite of the weight and of value of gold of which it is composed. It is not, instead, a commodity-money that travels independently on the market, which belongs only to businesses, and indeed it did not even need the intervention of central banks as proposed in nineteenth and twentieth centuries by the hyper-liberal theories.[14]

However, something was left out of the State control, outside its enormous prerogatives. It was the market value of the material with which ware made the coins, copper, silver or gold: a circumstance which in later centuries would be the decisive point of the European issue. In fact, the shortage of precious metals made chronically restricted the money supply.

The shortage of money showed up first between the X and XIII century, when the population grew from 5,000,000 to 12,500,000 and the GDP quadruples [5]. The whole continent was moving: the new city-centers were a driving force for development and this generated the need for a new and plentiful money. The solution was quickly found, if there is demand for money, we have to coin it. Thus ticks multiplied exponentially. The situation was quite chaotic: who could take advantage of it attempted to make profits.

The proliferation of ticks, created to deal with the hunger for money, had the effect of loosening the state's stranglehold on currency, it disappeared what had been one of the main features of the system since the Greeks and Roman times up to the reform of Charlemagne.[15]

He did not last long. It is obvious that such a "private" system did not facilitate exchanges and gave no guarantee on the quality of the coins, so the State intervened again. The anarchist galaxy of ticks, after such sporadic private experience, gradually came under the strict control of public authorities of the Republics, feudal barons, Kings or Princes.

As mentioned earlier, the precious metal was scarce on the Continent, and this generated many hardships. Carlo Cipolla, in listing the answers they gave the economy around the thirteenth century to the supply of money that could not keep up with demand, he explains that "we must admit that back in those days we can find the early developments of anonymous archaic practices which then turn into institutions and banking and credit organizations" [8].

If the Credit multiplies money when the economy requires, to personify and give legs and brains to the new phenomenon, there was a new category of enterprising characters, called Lombard and Cahors (appellations linked to regions of provenance), that scatter throughout Europe and

[14] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 52-97
[15] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 52-97

everywhere they lent money gaining an interest and taking to guarantee a pledge.[16] They proliferate, and when they were chased away from one country, they simply land in another. In Florence they were fined, but at the same time they were left free to continue their operations: thus the license fee became a sanction. They are not persecuted like the Jews of that time but they do not make a quiet life. Alongside these two figures, in the fourteenth century, Money-changers come out. Modern and sharper, they had a wider and structured operating range: they often stationed on the road, with a work bench as ordinary craftsmen; they are accredited in history as the ancestors of modern bankers. This is a critical step in the history of money, the function of these work benches began unequivocally to be a monetary function, i.e. the creation of money on the basis of cash deposits. It born so, for all practical purposes, the bank money.

It was realized that in addition to lack of cash, there was another very significant problem to solve: if trades are far apart, the physical movement of money is dangerous and expensive and, to deal with this problem, the deposit banks (mainly local banks) are not enough. In fact, in this fast-paced world where economic entities change form and substance, the horizon of these operators is no longer just local, but it is a European horizon. The bill of exchange is the most extraordinary technology of the fourteenth century that allows to multiply and facilitate trade and to put legs to the money. If the bill of exchange is the newest means of payment, the fairs of Champagne are the places where this instrument exploits its potential.[17] Such fairs are the maximum financial organization products of those times. Every three months, when a fair was held, bills of exchange were brought into a clearing union, clearing house of debts and credits, where an officer proceeded to the validation of debits and credits, to the cancellation of balanced items and to the compensation of mismatches.

Only when, in 1545, the conquistadors discovered the silver reserves of Potosi, in the Andes, the hunger for money in Europe subsided for at least a couple of centuries. However, the silver dripping blood. The human and moral costs of that epic deeds were high: the workforce was made up of Indios substantially treated as slaves and a lot of them died there.

The Spanish silver flooded Europe, but did not benefit Spain, which was engaged in war with the Dutch provinces. Moreover, between 1500 and 1620, again in Europe, it took place what has been called the "price revolution", caused by population growth and demand for consumer goods. The increase in working capital and the demand for goods were integrated with each other giving rise to a development, which characterized the whole seventeenth century [5].

If the market could be satisfied with silver arrival and enjoy the most working capital available, it cannot be said for kings and princes, also engaged, between the sixteenth and seventeenth

[16] C. M. Cipolla, *Le avventure della Lira*, Il Mulino, Bologna, 2001, pp. 51-78
[17] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 52-97

centuries, in endless wars. These had to borrow money directly from the bankers, as did Edward III with the Bardi and Peruzzi families, or "make money" from the coin: seigniorage receivable and devaluations to ease the cost of sovereign debt. In fact, the reduction of the metal content of coins was the characteristic feature of the entire sixteenth and seventeenth century, throughout Europe, with the exception perhaps of England.[18]

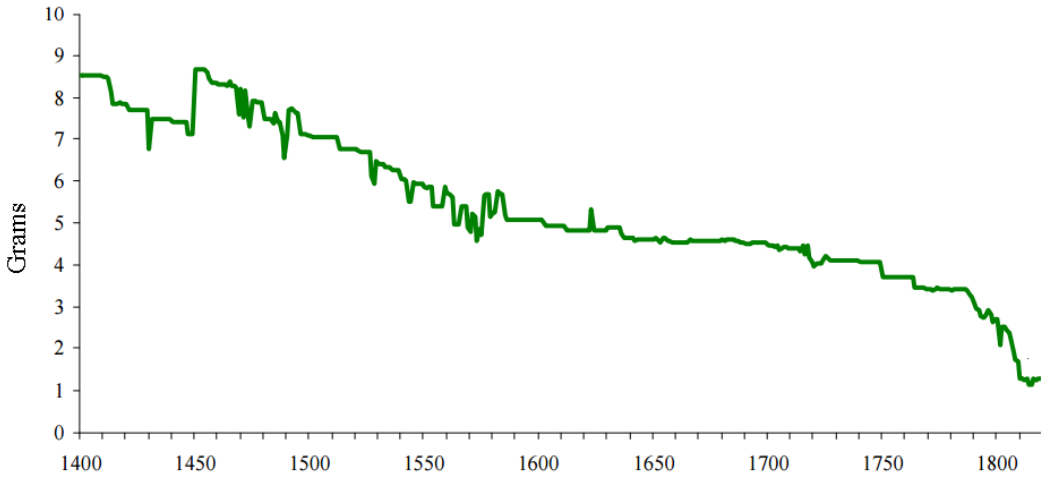


Figure 1 - Europe 1400-1850, Average Silver Content (in grams) of 10 Currencies (Reinhart & Rogoff, 2008)

The reason why they reduced the intrinsic value, devaluing the currency and causing inflation, were always the same: the debts of the State and the need to increase the monetary base at a time when, despite the American silver, the working capital remained scarce. However, there was no lack rulers who tried without success the way of appreciation and of a strong currency, as in the episode of Elizabeth of England.

Coming back to the separation of money functions, the system of the old money, which may seem paradoxical and counterintuitive, was on two levels. the first, as I said, was that of jingling coins, effective, minted in silver or gold, and the second was that of the unit of account, imaginary or virtual coins, which only served to count or rather, to conclude contracts. The best expression remains to Luigi Einaudi when he explains that *"si contrattava in lire e si pagava in scudi"* [9] (from Italian: "trading took place in *lire* but the payment was made in shields"[19]). This system, in one way or another, remained in force until the eighteenth century, in many European States, in which many hundreds of different coins circulated and a table indicated their respective value in *lire* or other units of account. Cipolla suggests that, the reason for which this system was created and then kept alive for so long, lies just in a comfort factor:

[18] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 52-97

[19] The scudo (pl. scudi) was the name for a number of coins used in Italy until the 19th century. The name, like that of the French écu and the Spanish and Portuguese escudo, was derived from the Latin scutum ("shield"). From the 16th century, the name was used in Italy for large silver coins. Sizes varied depending on the issuing country. Source Wikipedia: https://en.wikipedia.org/wiki/Italian_scudo

people, in order to avoid handling large numbers, began to express transaction terms in *lire*[20]. Instead of saying "2163 denier", it was faster to say 9 *lire* and 3 deniers[21]. Another explanation comes from Fernand Braudel, he argued that the virtual money allows to unhook the coins from gold and silver values: this system allows to have room for manoeuvre for a rudimentary monetary policy, in case you intend to devalue [5].

2.8 From the 17th to the beginning of the 20th century: the first central banks and the gold standard

If we move forward in time by few decades, precisely in the year 1637, we encounter another important stage in the history of money. The bubble of tulip bulbs is another phenomenon that marks the era of transition that will lead, albeit in embryonic form, to the institutionalization of a system of payments, to the creation of a body of law, and to address the problem of the need to control them. Someone wanted to see as early as the concept of the bulb, or incubation of a future asset, the first signs of the financial revolution: the bulb is already a *future*, or a *future contract* on the tulip.

By tracing the main stages of the history of money you cannot avoid mentioning the story of John Law (1671-1729), of which wrote the best authors and the best minds of the eighteenth century and beyond, from Voltaire to Smith, from Galiani to Gleeson. In fact, it is thanks to Law that in 1716 we witnessed the birth of the first central bank, the *Banque Générale*, although that was an attempt failed miserably.

Law devised a way to solve the debt problem of France: it was possible to subscribe the capital of the *Banque Générale* giving in exchange government bonds, thus helping to remove from circulation the huge amount of *billet d'Etat* that weighed on the public purse. The other prerogative of the institution was to be able to issue banknotes, genuine paper currency, transferable and payable to the bearer; for this purpose, Law made two crucial steps: tax collectors were forced to pay in paper money the taxes collected, establishing an embryonic legal tender; and then, he ordered the Banque Générale to discount bills and change foreign currency, pushing up the circulation of its currency.

To permanently solve the problem of public debt, John Law began an itinerary that soon would give birth to a conglomerate which included a State bank, the *Banque Royale*, and a new holding company to the head of production activities in the Louisiana colony, the Mississippi Company [5].

[20] C. M. Cipolla, *Tre storie extra vaganti*, Il Mulino Bologna, 1994
[21] C. M. Cipolla, *Le avventure della lira*, Il Mulino, Bologna, 2001, 51-78

Banque Royale and the Company assumed the role of a sort of central bank but with the genetic defect of being in the hands of the government and not independent: the combination of Law had as collateral the issuance of paper money, the production activities of the Mississippi and the trend of the real economy, unlike the Bank of England (created a few years earlier) that had as collateral gold and government bonds.[22]

Weaknesses aside, "thanks to John Law", in a short time Paris became the financial capital of Europe, they were expected imaginary and extraordinary gains. However, if the exchange of Government Securities/Shares could withstand systemically, the financing of purchases made by printed paper money was more problematic and created conditions for a huge financial bubble. In fact, everything went ahead on a fragile balance until the day in which Law realized that the loans from the Banque Royale were climbing too much. At that precise moment he pulled the brake violently, causing the collapse of the stock and a run to the conversion of notes. As a consequence of the disaster, France was fallen down, the rampant inflation was pushing many people to beg and to look for food on the streets. Inside the banks the queues became uncontrollable and in these catastrophic hardship Law was forced to flee and died in poverty in Venice where he is now buried in the Church of San Moise [10].

In the Age of Enlightenment, with the Industrial Revolution at the gates, and the Scientific and Technological revolutions now in place and with new ideas about the organization of the State, a renewed reflection on the currency was needed. The new middle class that took power soon needed stability of exchange rates and security for trade. It is thanks to Jean-François Melon (1675-1738), who worked with John Law, with his paper *Essay politique sur le commerce* [5], that money enters fully into the public debate and between the State prerogatives. Moreover, through the currency and the mechanism of write-downs, they were also looking for the key to redistribute income and alleviate the suffering of the weakest.

Money begins to have a significant as the prerequisite for development: it starts to be seen as "capital" whose role is crucial to set in motion the production process. To definitively affirm the bank note on silver and gold, an event that will materialize massively in the second half of the nineteenth century, the State will (1) require all to accept payment in paper currency, that is, you will have to impose legal tender, which means that the banknote circulates exclusively on national territory; (2) provide that the note has a large (if not absolute) liberating power against any debt contracted with any entity, with the private sector or the State; (3) finally, since the banknotes must be able to pass from hand to hand without any problems and revocation,

[22] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 99-156

they shall be payable to the bearer, without the possibility of disputes, although, paradoxically, it is money coming from a theft[23].

Behind the evolution of technologies in payment systems, however, there is a real credit and financial revolution caused by the need to increase the circulating money and credit, and at the same time to keep intact the guarantees and trust in the mediums of exchange.[24] The advent of paper money coincided with the abandonment of a payment system based on the intrinsic value of the metal, where the only task of the State was to manage the mint and to put in place complicated and lengthy standing monetary policy in favour of a much more sophisticated payment system; this new system has two main protagonists: (1) the new central bank, or something like that (as seen before with the experience of John Law), which simultaneously with the issue of paper money was capable of guaranteeing the value of circulating money; (2) and the creation of a credit bank system that "multiply" the presence of banknotes in the market by making loans based on the money deposited by account holders and that prevent this money remains unused in their coffers [5].

The financial revolution, cited above, has been one of the engines of the industrial revolution of the eighteenth century and will allow Britain to economically dominate the world until World War II. The creation of the Bank of England opens the door to the new monetary framework, but to bring to an end the transitional process they had to liquidate the old banking system, based on the silver coins, and make definitely affirm the new paper notes by linking them to a solid anchor; the research consisted of finding a counter value more robust than silver that was too abundant on planet. Such equivalent will be identified in gold.[25]

1717 is the year in which Isaac Newton (1642-1727), the author of the theory of universal gravitation at the head of the Royal Mint in London since 1696, anchored the printed pound sterling to the price of gold. About 60 years later, in 1774, the silver was completely removed from the currency in circulation in favour of gold and banknotes. Thus leading to the *gold standard*, a strong currency anchored to gold, of which Britain was the leader in the nineteenth century.

The currency - coins or their corresponding paper - takes upon itself two functions that were previously separate, unit of account and means of payment, making it independent from government decisions. This autonomy, enjoyed by coins, and by the paper money which is simply its reflected image, transforms it into a commodity, namely an object whose value is determined by supply and demand, at least according to the standards of that time.

---

[23] A passage that is worth mentioning is that of portability, in which the protagonist was the judge Mansfield in 1758, when, following a robbery of a Bank of England note, promptly denounced by a British citizen, the bank refused the collection of the unfortunate which found the ticket in his pocket as last [5].

[24] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 99-156

[25] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 99-156

In 1833, the Chancellor of the Exchequer, Lord Althorp, announced in Parliament the great British compromise: from that moment the Bank of England is entrusted with the monopoly of ticket printing and local banks is instead prohibited the issuance. In exchange, the latter would be able to enjoy the ability to collect deposits from savers and to decide how much money put back into circulation (bank multiplier), an activity that was prohibited to the Bank of England. With the new banking regulations, it is recognized the legal tender of banknotes. This gave way to the banknotes to impose itself with respect to the coins, but they acquired the nature of fiduciary-money or bank-money, consequently, the other issue that will arise, with the advent of the new credit-money system, will concern the solvency of banks that began to proliferate throughout Europe.

It was in France that born a totally alternative idea of payment systems, in the role of the State, and in the option on precious metals. The novelty, that put France in a separate position from England is that the Banking Act of 1803 embraced bimetallism, without a value of gold and silver determined by the law, but simply a rule, ensuring greater flexibility, that would have a fixed ratio between the two metals.

A few years later, because of his influence in Europe due to the Napoleonic invasion, France was followed in the bimetallic system by Piemonte (and then the whole Italy), Belgium, Greece and Switzerland.

However, the bimetallic system had many negative aspects, first of all the international market of gold and silver: the discovery of new mines increases the price of a metal and decreased the price of the other, forcing the State intervention in order to stabilize prices by selling and buying gold or silver on the international markets, but when speculators began to understand this practice they jumped on the bandwagon for a nice profit [5].

The bimetallic system, with its problems and with a strong monometallic market as rivals, led by Britain, was not lucky and was forced to give way before the end of the century: the decisive move that provoked a domino effect was played by Prussia in 1871. In fact, after the French victory, the peace of Frankfurt obliged Germans to a compensation of 5 billion francs; in this framework they took the opportunity to snap up the yellow metal on the international market by selling large silver quantitative, minting new coins' gold and convert to the gold standard. Reducing the price of silver, it put in crisis the Latin Union[26] systems that were likely to see gold disappear from their circulation and to exhaust its reserves.

[26] The Latin Union is a defunct international organization of nations that use Romance languages, with the aim of protecting, projecting, and promoting the common cultural heritage of Latin peoples and unifying identities of the Latin, and Latin-influenced, world. It was created in 1954 in Madrid, Spain, and existed as a functional institution from 1983 to 2012. In the history of currency, the Latin Union played an important role when in 1865 the

The German-area countries, Denmark, Netherlands, Norway and Sweden, they immediately conformed to the gold standard and were followed, soon after, by countries of the Latin Union, France, Italy and Belgium in 1878, Austria-Hungary in 1892 and then Russia and Japan in 1897.[27]

The gold standard provided for the engagement of all the currencies to the value of gold, it was a guarantee of stability of the exchange ratios and it included, by its nature, the free movement of capital: all these elements were necessary for the development what now goes under the name of the first globalization of the late nineteenth century. London was becoming the most important square in the capital sorting and therefore being able to ensure a strong currency was a means to encourage investment in England.

Until the point in which monetary stability could be considered more important than the social issues and the common good, the system worked in some aspects and the aim to maintain the level of gold reserves was achieved. The price of this architecture was the British hegemony on the international economy, in fact, someone has already defined it a sterling standard system: Bank of England could assume the role of a conductor because other countries were willing to hold their reserves as deposits in London.

2.9 The world changes during World Wars

The shots fired in Sarajevo, on June 28, 1914, frightened the markets. The rush to liquidity was immediate: Vienna Stock Exchange collapsed. The world of credit suffered the backlash. In a short time, most countries abandoned the gold standard: it was necessary to be able to print money not redeemable in gold on demand for the production of armaments. World War I left on the field nearly 10 million deaths and devastated economies. The public debt from 1913 to 1921 had exploded, especially in the defeated countries, prices were multiplied causing a complete loss of value of paper money [11].

The manoeuvres for the return of the gold standard in the post-World War I model, began with the Genoa Conference of 1922, sponsored by the League of Nations and carefully prepared by the British diplomacy that did not worry about the profound change undergone in the world and that their hegemony was quickly giving way to the US.

They opted for a return to the traditional way of the gold standard, with its rigor, trying to moderate the system with the ability to use as reserves, in addition to the traditional gold, even sterling. The gold standard ran to what was later called the *gold exchange standard*. However,

signatory states - Belgium, France, Italy, Switzerland and Greece - decided to uniquely determine the fineness of the silver coins to 83.5 percent, following a dispute between the various states.
The fineness of a precious metal object (coin, bar, jewellery, etc.) represents the weight of fine metal therein. [105]

[27] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 99-156

the return to the old system was tougher than expected and came through deflationary pressures and heavy economic manoeuvres.[28]

The US economy was running like the wind, but the domestic market was soon saturated, and took the form of a classic situation of overproduction. The only outlet to the American economy was the exports, financed with abundant loans granted to European and South America countries. The Americans Roaring Twenties had created an immense mass of profits that they could not address to new investments and so they veered blithely toward the Exchange [5]. Wall Street began to grow. The demand for shares and exhilaration were so sustained that the rates that banks practiced to brokers for speculation were two digits, so much higher than the discount rate. The high indebtedness of the private was beginning to be a time bomb. The Fed's monetary policy was decisive for the bubble to burst and cause the collapse.[29]

After October 24, 1929, the "Black Thursday", the US credit system wrapped her credit sweaters and also those of the market, this circumstance caused the collapse of more than 20 percent prices. The fall in prices was added to a cost reduction, due to new technologies and increased productivity, and it was crucial in bringing the crisis spread worldwide.

The economic shock was soon to turn into deep recession. Governments were faced with the alternative of defending the gold standard, or having to deal with huge unemployment.

At the beginning of 1932 you could begin to take inventory of rubble: almost twenty countries had abandoned the gold standard. And so, until the outbreak of World War II, in 1939, they entered in a period of great turbulence and of an unusually severe money disaster: freely floating exchange rates, competitive and currency devaluations, trade protectionism. In the period between the two Wars, the USA replaced Britain as the world's financial superpower.

2.10 From the beginning of globalization to the present day

In July 1944, when the second World War was nearly over, there was an international met at Bretton Woods, in the USA, to decide how the post-war international money system could avoid repeating the disasters of the inter-war years.

The idea that inspired the Americans for the revival of the international system after World War II was the free market development. However, since the early years such a "free trade" scheme proved that cannot work, mainly because of the great disparity between the US and Europe. Initially, America was not aware of this situation and insisted in proceeding to the free convertibility of currencies at official rates by each country. US was especially focused on Britain, and when they finally surrendered to the pressure, the results were disastrous: British convertibility,

[28] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 99-156
[29] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 99-156

introduced in 1947, lasted only six weeks and caused a massive outflow of capital, which imposed a returning to the control of its currency. The story of Britain finally convinced the US to change course.

Moreover, Bretton Woods Agreement resulted in setting up the International Monetary Fund (IMF) and the World Bank, and much later the World Trade Organization (WTO). These bodies are controlled by USA and other rich and powerful countries as separate organizations from the United States itself. It was envisaged the equality of all currencies and settled a system of exchange rates, fixed or minimally fluctuating. In the last version of the Agreement, shortly before the signing, it appeared the following critical marginal note: "*The parity of the currency of each member shall be expressed in relation to gold as a common denominator, or in dollar* [...] *terms in force since the 1st July, 1944*" [5].

Keynes argued that a proper international currency was needed, which would not belong to any single nation.[30] The Americans said No. They wanted to be the top financial superpower, with the US dollar replacing the Britain's pound as the main international currency. The other countries, bankrupted by the costs of the war, had to agree [12].

The first two years after the WWII were characterized by humanitarian aid policy. The disorganizations and chaos gradually overcome. The year 1947 was particularly dynamic in the reconstruction effort. Even collective action normalized and European countries were able to hold election and to set up a new political map. The same year, the Foreign Minister of the USA, George C. Marshall announced his final proposal to solve the European problem, the European Recovery Program (ERP), which will go down in history as the Marshall Plan. They were made available to European countries US $ 13 billion which contributed greatly to the recovery of the Old Continent.

Meanwhile trade liberalization continued at an increasingly speeds. In 1947, the GATT agreement to reduce trade barriers, was signed by twenty-three countries. However, Europe was still hobbled in 1949, so Britain and 23 other countries decided to devalue without asking permission to the IMF, as stated by the agreements of Bretton Woods. Only thanks to this move were able to breathe a sigh of relief.

As a backdrop to the European post-war development there was the European Payments Union. It was a clearing house in which all surplus countries negotiated their return with other Union partners and were thus induced to liberalize trade and to move towards a squaring. Only after 1958, when the European economies were settled in and many trade barriers were torn down,

[30] Keynes' plan was even deeper and contained a revolution with the creation of an International Clearing Union and the issue of a new accounting currency, the *Bancor.* Actually, even before Bretton Woods, he did not have chances. He published his ideas in *The International Clearing Union (Not Utopia, but Eutopia)*, but the latter part of the title disappeared in the next version [5]

we can talk about a real implementation of the Bretton Woods agreements: so the Europeans declared their convertibility against the dollar[31].

The Bretton Woods system established that exchange rates between other countries' currencies and the US dollar were fixed, and the USA was obliged to meet requests from other countries to give them gold at a price of $35 an ounce in exchange for US dollars which they had earned in international trade. A link was kept between the world's money and gold until 1971 when the USA under President Nixon found it could no longer repay other countries with gold for all the dollars they were now earning, and the remaining link between the world's money and gold was scrapped. From that moment national currencies "float" against one another in value [12].

As a consequence of the Marshall Plan, the world and Europe were full of dollars and central banks were continuing to buy dollars to their reserves: the deficit of the balance of the US assured the international cash payments. The United States was a kind of locomotive in the world. However, the abundance of dollars made them fear an imminent depreciation of the dollar and began to spread the rumours that Britain and France had plans to convert into gold all dollar they hold.

The situation worsened on August 15, 1971, when President Nixon, engaged in the war in Vietnam, closed the gold door, suspended the convertibility of the dollar into gold and sanctioned the fluctuation of the dollar against other currencies, as well as a duty on imports. Thus, this episode marked the end of the Bretton Woods agreements.

The post Bretton Woods-new globalization scenery is presented as totally new. The exchange rates are fluctuating anarchically, capital movements are free, finance is deregulated. The architecture of the dollar standard is definitively shelved. Gold was formally eliminated as a reserve asset, central banks began to hold in their vaults other currencies, alongside the dollar; reserves were created addressing the capital market: it’s the market that solves the problem of liquidity that had plagued previous systems, but opening the door to immense risks especially for European countries.

In April 1972 in Basel it was born the "European monetary snake", involving France, Germany, Italy, Belgium and Holland, who established a trading band for the European currencies but that lasted only seven years because of the strength of speculation. On the ashes of the "snake", in March 1979, they gave birth to the EMS, the European Monetary System, with the same aim of avoiding competition of the dollar and hold together the European currencies around the mark. Only in 1989, it was sketched for the first time the project of a real monetary union, by the commission headed by the Socialist exponent Jacques Delors.[32]

[31] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 193-261
[32] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 193-261

The 1st G6 summit, that took place on November 1975, in Rambouillet, France, can be considered the starting point of globalization. The idea, attributed to Henry Kissinger, at the time US foreign minister, was to break the stalemate that could last much longer between OPEC, a cartel that was hurting the Western countries, raising oil prices, and South of the world[33] promoting the rapid development of the latter [13]. In this scenario, since the eighties, with the election of Ronald Reagan in the US, and Margaret Thatcher in Britain, many countries began to implement in-house deregulation, liberalization and anti-inflationary policies. Another significant element of the picture was the rise of a regulatory revolution whose aim was the deregulation of markets and financial products, which reached its peak in the nineties. A huge amount of securities and derivatives products have flooded the markets, to the point that some people began to talk about "private money" which escapes the control and replaces the public one. The phenomenon is based on innovations that improve liquidity as well as market instability. The most significant changes were the mechanism of securitization, whereby lending operations related to the real economy become negotiable instruments on the financial market, and derivatives, i.e. tools that enable a separate risk management and make liquid assets that otherwise would not. Finally, the globalizing world opens a new scenario that had remained in the shadows until the outbreak of the 2009-2012 crisis, the sovereign debts increase and become matters of trade and speculation.[34]

The German reunification[35] acted as accelerator to the euro process: as early as December 1989, the European Council decided to convene an intergovernmental conference, by 1990, with the task of developing the final stages of the European Monetary Union. The Conference met in 1991 and predispose the text of the new Treaty which was signed in Maastricht on 7 February 1992.

In a matter of about six years, Europe was able to give rise an operation happened a few times in history: to baptize a new currency, the euro, and to retire the old currencies, physically destroying them (the mark, the lira, the franc, etc.). The path proceeded in forced stages, in the belief that monetary union would trawl political union. It was imposed a path of convergence of public finances and inflation, to the countries interested in participating, which, after an admission test, gave birth on January 1, 1999 to an irrevocable system of fixed exchange rates

[33] Composed by Brazil, India and South East Asia

[34] R. Petrini, *Controstoria della moneta*, Reggio Emilia, Imprimatur, 2014, pp. 193-261

[35] The German reunification was the process in 1990 in which the German Democratic Republic joined the Federal Republic of Germany to form the reunited nation of Germany, and when Berlin reunited into a single city. The end of the unification process is officially referred to as German unity, celebrated on 3 October (German Unity Day). Following German reunification, Berlin was once again designated as the capital of united Germany [106]

between eleven eligible countries (Austria, Belgium, Finland, France, Germany, Ireland, Portugal, Italy, Luxembourg, and Spain). At the same time the ECB, the European Central bank, began to operate; it was built on the model of the Bundesbank, based in Frankfurt, which is responsible to issue the euro and manage the monetary policy.

Since the euro came into existence in 2002 some people have suggested it should capture a good share of the profit now enjoyed by the US dollar for providing the world's main international currency. But perhaps a genuinely international currency, belonging to all the world's people would be a more efficient and fairer way to meet our international trading and investment needs, as was suggested but rejected at Bretton Woods over sixty years ago. That idea will probably grow stronger in the coming years [12].

3 Mobile Payment and Crypto-Currencies

In a world that is dematerializing many aspects of everyday life, possessing digital good has become natural and greatly simplified. Photos, music, movies, books: everything is taking on so complex aspects that very soon the separation between digital and material will be almost indistinguishable.

This passage is already in place for money; much of the wealth is digitally stored: from cash, increasingly replaced by credit cards and home banking tools, we also find loans, stock exchanges, acts and even digitally signed notarial documents. Central banks themselves nowadays dispense with this securities and coins system, leveraging the enormous advantage of the IT age: any digital asset can be replicated and copied countless times, each identical to its original [14].

Anyway, the banking system built around fiat currencies, despite the adjustment in progress, doesn't fit to the new digital framework defined by internet, first of all, by mobile communication and social networks. Only twenty percent of humans currently have access to the banking system. It's a system that was developed in the Renaissance age, as we already saw, and it hasn't really change that much, with trusts clearing houses in the middle and very high transaction costs, at least much higher than the poor of the world could afford, or that even be making economic sense for micro-transaction that we will see more among the sharing economy, for example in the IoT world[36].

What people need today concerns to the possibility to transfer instantly and securely across the globe the equivalent of few cents or millions of dollars, when they want, without the necessity of a third party in the trade; people need a whole efficient, pocket and fair monetary, financial, and banking system [15].

As suggested in 2007 by the Bitcoin inventor, Satoshi Nakamoto, the main mission of this crypto-currency is exactly what corresponds to people needs, *a purely peer-to-peer version of electronic cash* [that] *would allow online payments to be sent directly from one party to another without going through a financial institution* [16].

[36] The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "the infrastructure of the information society." The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention [110].

Both mobile payments and Bitcoin heralded a new era of digital payment. Both developments open new avenues and yet give rise to new challenges. If on the one hand mobile payments represent, in a certain sense, the natural evolution that fits into the conceptual framework storyline of the payment mechanism and intermediary institutions role and architecture, on the contrary, Bitcoin and cryptocurrencies in general provide for a totally revolutionary type of money, a true conceptual revolution which may require more than adaption of existing laws.[37]

Bitcoin is not the first private money, not the first digital currency, and not even the first currency based on cryptography. Moreover, before the introduction of Bitcoin, online payments already existed and relied on financial institutions that act as trusted third parties to facilitate electronic payments.

3.1 Peer-to-Peer Revolution like the Internet Revolution

I'm old enough to remember the time in which the internet just started and all the serious discussion about the future changes that would lead, e.g. there were discussions about the internet impact of mail service organizations, about to replace or reduce the amount of mail that is going to be sent, etc., but nobody thought about shopping, entertainment or finance, and if we think at the mobile banking, a phenomenon that would transform all of our lives on a day-to-day base, it seems impossible that no-one at that time was worried about that issues.

We today have over 7 billion people in the world, approximately 3 billion own a toothbrush but nearly all of them have an access to a cell phone. We have over 6 billion cell phone and, as well known, this tremendously transformed the access of information globally to the electronic exchanges and communication channels around the world.[38]

In the last decades, development of networking from the centralized old-school computing, but also from a business perspective, has reached unpredictable levels; we have topped own organizational structures, we have most technology wise and business and organizational voice who distributed decentralized and eventually peer-to-peer networking, as well as organizational structures and business relationship; it really changed computing and businesses over the last twenty years, dramatically.

[37] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 6-14. Available online

[38] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

Peer-to-peer networking today is everywhere. When one started to talk about technology in the late 90s and the world was concerned about Nectar[39] and file-sharing[40] nobody thought about IP communications with skype for example or, maybe a better example for the money world, if we look at WeChat[41] case in China that has taken over, within 2-3 years, nearly the complete population and change the process of how people exchange value, communicate, collaborate and that really changed the banking system: today there is no need for credit card in China if you have a mobile phone.

All these things are coming together and accelerating with each other and making completely new scenarios possible.

3.2 Behind or beside Bitcoin: Blockchain

As mentioned earlier, Bitcoin is a peer-to-peer payment network while bitcoin is the digital currency based on an open source protocol, which makes us of a public transaction log. In making a payment, the payer requests an update to the public transaction log, the so called Blockchain, a master list of all transactions that shows who owns what bitcoins, currently and in the past. It is maintained by a decentralized network that verifies and timestamps payment using a proof-of-work system.

Thus we can say that Blockchain is basically a digital ledger that contains the payment history of each circulation of the bitcoin unit [17], but in reality Blockchain technology is much more, in fact it is also one of those topics that is really going to transform the world (I will explain in detail in the fifth chapter what is and how the blockchain works).

Looking at blockchain technology today it feels exactly the same or maybe even stronger than the internet. We are just scratching the surface of what is possible and the first impression is that tomorrow is going to be very different, this is going to change the world, and it is going to be changing faster and faster; it is important for all of us, individuals but also for organizations

[39] Nectar is a loyalty card scheme in the United Kingdom, run by Aimia. The scheme is the largest in the United Kingdom, and comprises a number of partner companies including Sainsbury's and BP. It launched in 2002 with initially four partner companies, and by 2010 had grown to include over 14 companies and over 400 online retailers [117].

[40] Peer-to-peer file sharing is based on the peer-to-peer (P2P) application architecture. Shared files on the computers of other users are indexed on directory servers. P2P technology was used by popular services like Napster, Spotify, and Infinit. The most popular protocol for P2P sharing is BitTorrent.

[41] WeChat is a social media (instant messaging, commerce and payment services) application developed by Tencent. It was first released in 2011 and by 2016 it was one of the largest standalone messaging apps by monthly active users, with over 889 million active users. However, as of 2017, WeChat has not been successful in penetrating international markets outside of China.
In China, users who have provided bank account information may use the app to pay bills, order goods and services, transfer money to other users, and pay in stores if the stores have WeChat payment option.
WeChat Pay is a digital wallet service incorporated into WeChat, which allows users to perform mobile payments and send money between contacts [116]

to be agile and adjusting to the change that is happening in the innovation economy as quickly as possible.[42]

However, emerging technology like blockchain will be a game changer, only if they achieve a network effect, which means we need to work together to establish standards and communities: come together and work together.

3.3 The route of Fintech Investment

When we talk about FinTech we use to refer to that sector composed by companies that use technologic innovations to make more efficient the financial system, however, this definition even if correct it is not enough exhaustive.

Within Fintech framework we have crowdfunding companies, peer-to-peer lending organizations, robo-advisors[43], and even those authorities which deal with payment systems, credit-scoring, exchange rates, data collection, and, obviously, digital and crypto-currencies.

There are some key areas of fintech were the Blockchain technology is applied, of course there is remittances, lending, insurances, mortgages, investment and peer-to-peer environment where blockchain technology start-ups are playing a role right now.

FinTech is actually changing how large organizations do business, but not only, this is also changing what kind of people will make business decisions going forward, it is really the IT leaders, all the people that have a clear understanding on what technology can do, that are going to be much more prominent and leadership positions outside of the traditional IT field.

We have been a tremendous amount of increase of global fintech investment over the last few years, from 2.4 billion dollars' investment in 2012 to 19 billion dollars' investment in 2016, and this trend is not going definitely to slow down sharply. However, as we can see in the Figure below, KPMG International in *The Pulse of Fintech Q1 2017* [18] observed that the investor sentiment tide turns, probably due to growing geopolitical and macroeconomic uncertainty or maybe because investors seeming to want more proof that innovative solutions can be scaled and commercialized.

[42] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

[43] Robo-advisors are a class of financial adviser that provide financial advice or portfolio management online with minimal human intervention. They provide digital financial advice based on mathematical rules or algorithms. These algorithms are executed by software and thus financial advice do not require a human advisor. The software utilizes its algorithms to automatically allocate, manage and optimize clients' assets. [121]

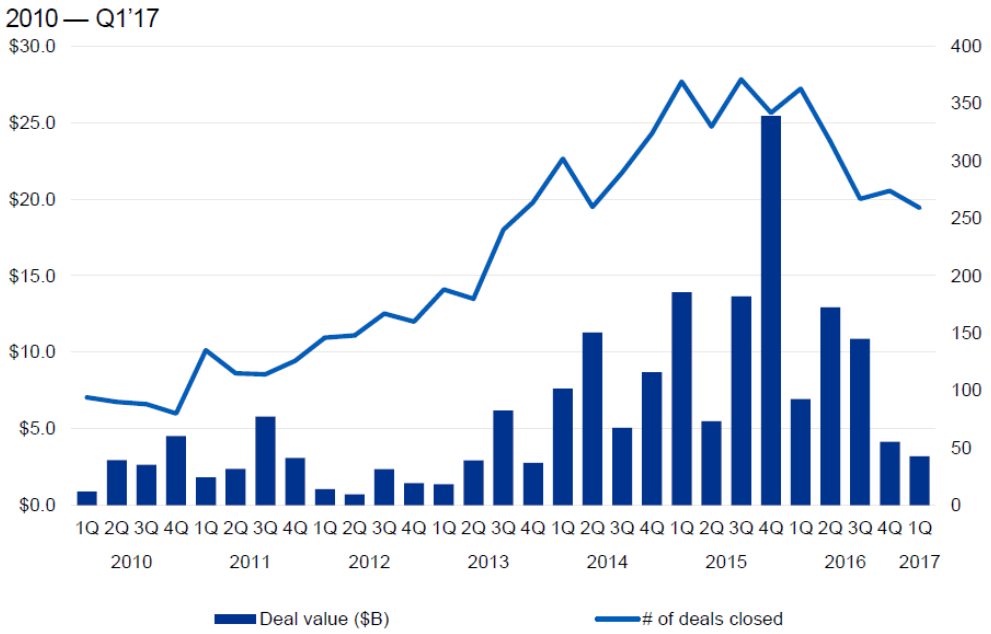


Figure 2 - Global investment activity (VC, PE and M&A) in fintech companies [18]

Of course every time you talk about money and new technologies there is risk involved because some things never change, when there is value or money some people try to steal it and get profits.

2017 is expected to be the year that clarify the potential of FinTech industry, given the Payment Service Directive 2 (PSD2) entry in force in Europe[44] and the various commitment to open-banking by other governments and regulators. This spotlight will likely bring increased investor interest in complementary technologies, such as data and analytics, but also Artificial Intelligence will likely be a hot area among corporate investors.

Most banks are keenly interested in finding ways to reduce costs and AI as a key mechanism to achieve this objective. Moreover, Global tech sector giants are also expected to become more engaged in fintech opportunities. Already, companies like China-based Alibaba Group are targeting promising fintech companies as a means to expand globally. [18]

3.4 Where will we end?

It is likely that every system inefficiency will be removed sooner or later by technology and those efficiencies will go back to either the consumers or the owners of the capital.

About Cryptocurrencies, OKCoin[45]'s Duan said: "talking about the impact of digital money now is like trying to predict how the internet would transform lives in the 1980s… we know

[44] https://www.eba.europa.eu/documents/10180/87703/EBA+Mandates+PSD2.pdf/5c2493a4-ef26-4434-8338-736895bd423f

[45] OKCoin is a Bitcoin company in China with core product lines of a Bitcoin exchange, and a mobile consumer payment and lending app [120].

it's going to be huge. It has the potential to change the entire economic infrastructure. We're just not sure about when and how" [17].

We will see new business models coming up, e.g. the Sharing Economy (Uber[46] / Didi[47]; AirBNB[48]) that has already shown over the last five years how start-ups, coming out of nowhere with a new model, can transform completely the existing industries that have not changed for hundred-plus years; or the Peer-to-Peer Financing (LendingClub[49]; Kiva[50]), bridging gap of organization internationally that has been thought to be undividable before, or connecting people directly makes an impact.

Blockchain Technology allows old and new players to offer new services to their existing customers. As we saw earlier, inefficiencies will be removed sooner or later; in the traditional transaction business, that today it is managing twenty percent of the people. We have more than a trillion and a half of "inefficiencies" in nowadays environments, and those are opportunities for existing players or start-ups to completely revolutionary transactions, not only the banking system.[51]

---

[46] Uber Technologies Inc. is a transportation network company headquartered in San Francisco, California, United States, operating in 570 cities worldwide. It develops, markets and operates the Uber car transportation and food delivery mobile apps. Uber drivers use their own cars, although drivers can rent a car to drive with Uber.
The name "Uber" is a reference to the common (and somewhat slangy) word "uber", meaning "topmost" or "super", and having its origins in the German word über, meaning "above".
Uber has been a pioneer in the sharing economy and the changes in industries as a result of the sharing economy have been referred to as "Uberification" or "Uberisation". Uber has also been the subject of protests and legal actions [111].

[47] Didi Chuxing, formerly Didi Kuaidi, is a major ride-sharing company, providing transportation services for close to 400 million users across over 400 cities in China. Its headquarters is located in Beijing. It provides services including taxi hailing, private car hailing, Hitch (social ride-sharing), DiDi Chauffeur, DiDi Bus, DiDi Test Drive, DiDi Car Rental and DiDi Enterprise Solutions to users in China via a smartphone application.
DiDi announced that it acquired Uber's China unit on August 1, 2016. Following this acquisition, Didi Chuxing is estimated to be worth US$35 billion and it is the only company to have all of China's three Internet giants - Alibaba, Tencent, and Baidu - as its investors [112].

[48] Airbnb is an online marketplace and hospitality service, enabling people to lease or rent short-term lodging including vacation rentals, apartment rentals, homestays, hostel beds, or hotel rooms. The company does not own any lodging; it is merely a broker and receives percentage service fees (commissions) from both guests and hosts in conjunction with every booking. It has over 3,000,000 lodging listings in 65,000 cities and 191 countries, and the cost of lodging is set by the host. Like all hospitality services, Airbnb is a form of collaborative consumption and sharing [113].

[49] Lending Club is a US peer-to-peer lending company, headquartered in San Francisco, California. It was the first peer-to-peer lender to register its offerings as securities with the Securities and Exchange Commission (SEC), and to offer loan trading on a secondary market. Lending Club operates an online lending platform that enables borrowers to obtain a loan, and investors to purchase notes backed by payments made on loans. Lending Club is the world's largest peer-to-peer lending platform. The company claims that $15.98 billion in loans had been originated through its platform up to 31 December 2015 [114].

[50] Kiva Microfunds (commonly known by its domain name, Kiva.org) is a non-profit organization that allows people to lend money via the Internet to low-income entrepreneurs and students in over 80 countries. Kiva's mission is "to connect people through lending to alleviate poverty."
Since 2005, Kiva has crowd-funded more than a million loans, totalling nearly $950 million, with a repayment rate of between 98 and 99 percent. As of November 2013, Kiva was raising about $1 million every three days. The Kiva platform has attracted a community of well over a million lenders from around the world [115].

[51] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

Records of estates, Records of shares, any financial transaction, even voting in the democratic process could be benefitting from blockchain technology, the whole area of IP management, but also messaging Central Trust relevant for a lot of IoT applications could be benefiting from such technology.

Smart contracts represent another application of decentralized public ledger technology that is beginning to garner attention. Smart contracts can be thought of as self-executing transactions, or as "automated programs that transfer digital assets within the block-chain upon certain triggering conditions.

In my opinion agile organizations will create completely new ways of collaboration transactions and I think all of us need to keep looking at what is happening in the East and in China because they are innovating so much especially around this Blockchain technology, we need to make sure we are aware of what is happening.

I think this is a revolution but also a great opportunity, it doesn't matter where we are today, if we are able to unlock the potential of this fundamental change of business, technology processes structures and people. Those people that are participating, that are on top of that and the organizations that spent resources on this, they will be the ones that are rising and being able to drive that transformation. Technology and customer oriented leaders are positioned to drive and realize the vision and image of the future.

4 Bitcoin and how it became the first crypto-currency in the world

Today bitcoin is the most common successful decentralized digital currency because it is based on Bitcoin[52] which has been the first protocol relying on peer-to-peer network decentralization to avoid *double spending*, i.e. the effective impossibility in spending multiple times the same given amount of money.

A bitcoin does not represent a claim to a physical object or to a physical currency, it aims to be in itself a currency, a fiduciary currency. As it has no intrinsic value it is not a commodity-based currency.

Bitcoin is a cryptocurrency because it uses public-key cryptography to control the creation and transfer of the computer file which purports to be "money".

The Bitcoin protocol regulates issue of bitcoins and defeats counterfeiting and double spending ensuring the safe transfer; it does all that without relying on a single authority.

Tracking the flow of bitcoins through transactions recorded in the Blockchain can give clues as to who the owner is.[53]

Participants known as miners verify and timestamp transactions into a shared public database, the blockchain, for which they are rewarded with transaction fees and newly "minted" bitcoins. A new block of aggregated transactions will only be added to the ledger after "the computers on the network reach consensus as to the validity of the transaction." [16] The method for reaching consensus is referred to as *mining*, a process of solving complex mathematical problems to validate the block.[54]

4.1 A brief but intense story

Since one began to speak in the cypherpunk mailing lists, many virtual currency projects were born. One was that of Chinese Wei Dai, who in 1998 had proposed *B-money* to promote e-commerce. Opposed by banks and governments, every subsequent attempt to "monetize" and use electronic money had failed until the appearance of bitcoin.

In October 2008, Satoshi Nakamoto[55] published a paper on The Cryptography Mailing list at metzdowd.com describing the bitcoin digital currency. It was titled *Bitcoin: A Peer-to-Peer Electronic Cash System* [16], and this was the first time we heard about Bitcoin.

---

[52] Bitcoin consists of the Bitcoin protocol and the bitcoin (BTC) currency (note that by convention the protocol name is written with uppercase B and is singular, while the currency name is written with lowercase b and may be plural.

[53] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

[54] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 10-21, Available online.

[55] Satoshi Nakamoto is the pseudonym that lies behind the mysterious creator of blockchain technology, we do not know yet if it was a male, a female, or even a single person. Its traces were lost in 2010 after the publication

Nakamoto was also the first miner, in fact, in order to demonstrate the method to online observers, the first 50 bitcoins were mined by himself, but for the first real wold transaction we had to wait two years when, in May 2010, Lazlo Hanyecz sent 10,000 BTC to a volunteer in the United Kingdom, who then ordered two pizzas for Haneyecz, which cost him 25 USD. On May 25, 2017, 10,000 BTC have value of over 26 million USD.

The interest in Bitcoin led to the creation of Mt. Gox, the first bitcoin exchange which allowed users to buy bitcoins in exchange for fiat currencies. Prior to the creation of Mt. Gox, users could only "mine" their own bitcoins.

On the first day of trading Mt. Gox sold 20 BTC and offered one BTC for the rate of 4.96 cents.[56]

On February 9, 2011, Bitcoin briefly reached parity with USD on Mt. Gox and this is also the year in which Bitcoin started to become more widely utilized, also thanks to one of the first mainstream articles describing the digital currency by the Time magazine and the first conference about Bitcoin in New York City, Prague and Czech Republic. Its popularity was sparked because Bitcoin is global, anonymous, has low transaction costs, account cannot be frozen, and there are no prerequisites or arbitrary limits. At the beginning it was a perfect option to use as a donation system, however, its anonymity also started attracting illegal activities including black markets that sold illegal goods online.

In 2012, several Bitcoin startups began to form with the main aim of assisting nontechnical users in becoming familiarized with using Bitcoin (such as Coinbase[57]). In May 2017, there were more than seven-hundreds startups all over the world and in 2016 they gathered about $ 550 million [19].

Moreover, by the end of 2012, it was born the first bitcoin exchange to operate in the framework of European regulation as a bank, Bitcoin-Central. [20].

The first "regulation", if so can be defined, came in 2013, by the Financial Crimes Enforcement Network (FinCEN)[58], which established regulatory guidelines for "decentralized virtual currencies" classifying Bitcoin miners and exchanges in U.S. as Money Services Businesses (MSB). Due to legal requirements involved in this step, Mt. Gox started dealing with serious legal issues

---

of the white paper that theorized the mechanism behind the system and the release of the first software dedicated to transaction management (The software was released on Sourceforge on 9 January 2009 - version 0.1 was compiled using Microsoft Visual Studio).
Satoshi Nakamoto, before disappearing, had delivered the witness to Gavin Andresen, who handled the project's management and development until 2014. In turn, Gavin left his software development role to concentrate on his work with the Bitcoin Foundation (founded by Gavin himself in 2012, to support and nurture the development of the currency).

[56] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

[57] https://www.coinbase.com/

[58] https://www.fincen.gov/

and when these difficulties become apparent, more and more people tried to withdraw their funds, resulting in a digital bank run and the plummeting of bitcoin price. Towards the end of February 2014, Mt. Gox announced that the company filed for bankruptcy protection.

The first Bitcoin ATM was launched in Vancouver in 2013, and from that moment customers can withdraw their bitcoins and deposits fiat currency which are quickly converted to their Bitcoin Wallets. On May 2017, there were more than 1200 Bitcoin ATMs in 59 Countries all over the world[59]. Additionally, several retailers began accepting Bitcoin as a means of payment, already in 2015 there were 160,000 merchants accepting bitcoins and at the time of writing they are thousands more all over the world. Someone forecasted that by summer 2017, bitcoin will be accepted at more than 260,000 stores only in Japan. As a matter of fact, its extension is already enormous.

In 2014, the FBI shot down "Silk Road", a darknet marketplace which created a nightmare for the agency because it was virtually impossible to track the illegal transactions. However, there are now several replacements for Silk Road, which still use Bitcoin as a payment system.[60]

Despite the tempted attacks and media that constantly try to discredit Bitcoin, today their value has reached unbeaten peaks and the network continues to grow and spread uncontrollably in the eyes of everyone. We cannot foresee the future and understand what Bitcoin will become tomorrow, but it has certainly left a mark in the history of the world economy.

4.2 Basic Cryptography Background

In order to better understand why Bitcoin reached such level of notoriety we must know what there is behind. So we need to introduce some Cryptography Background, also in order to be more confident when we talk about its uses in the real world.

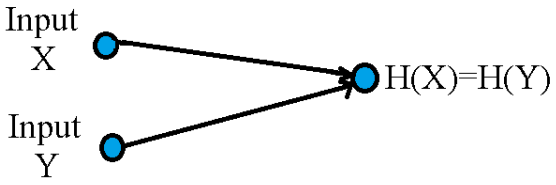
A cryptographic hash function is a mathematical function and it has three main attributes: (1) it can take any strings of any size as input, (2) it produces a fixed-size output (in the Bitcoin case it produces 256 bits output) and (3) it is efficiently computable, i.e. giving a string, in a reasonable length of time you can figure out what the output is.

Since we are talking about money and value, we need to make this hash function cryptographically secure. Cryptographic functions are complicated topics in general; a simple way to understand what we are talking about is to focus just on three properties of cryptographic functions which are important for our analysis: (1) collision-free property, (2) hiding property and (3) puzzle-friendly.

[59] https://coinatmradar.com/

[60] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

Collision-free property concerns the possibility that for two different and separate inputs we will get the same output as results of the hash function, so collision do exist.



Thus the question that arise spontaneously is: are there collision that are findable by regular people using regular computers? No, it is impossible, or it is better to say that the probability is infinitesimally small, as small as the probability that the earth will be destroyed by a giant meteor in the next two seconds. The explanation relies on the fact that in order to find a collision we are going to pick 2^{130} randomly chosen inputs and there is a 99.8% chance that two of them will collide, it works no matter what the hash function is, but the problem is that it takes a very long time to do, i.e. you have to compute the hash function 2^{130} times in order to have the high probability, and that's of course is a very huge number. [61]

However, for some possible values of hash functions of course there are faster way to find a collision but for others we don't know.[62] The most interesting things is that there is no hash function in existence which has been proved to be collision-free, people tried really hard to find collisions and haven't succeeded, so we chose to believe for simplicity that all of them are collision free and as a consequence we can use that hash function as a *message digest*[63], i.e. if we know that two inputs have the same hash then it is safe to assume that these two inputs were different.

The hiding property concerns the fact that, given the output of the hash function, there is no feasible way to figure out what the input was. The problem is that this property does not exactly hold, e. g. if we make an experiment of flipping a coin and results was heads we are going to return the hash of the string "heads", on the contrary, if the results was tails we are going to return the hash of the string "tails". Let's assume that now we are going to ask someone, who did not see the coin flip but only saw the hash output, to figure out what the string was that hashed that. Of course, in this scenario is very easy to find what the string was, you simply compute the hash of the string "heads" and the hash of the string "tails" and you see which one you got. The reason of the failure of this experiment concern the fact that there were only a couple of possible input value.

---

[61] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

[62] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 10-21. Available online

[63] A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula, it is an algorithmic number.

Thus, if we have range of input that is very spread out (like the a random 256-bit value), that has *high min-entropy*[64], and there are no values that are relatively more likely than others, then given the hash function it is infeasible to find the input and the hiding property can hold.

The third security property that we are going to need is that they are puzzle-friendly, which implies that no solving strategy is much better than trying random values of the solution.

In fact, if someone want to target the hash function, if they want it to come out to some particular output, that is there is part of the input that is chosen in a suitably randomized way that is very difficult to find another value that hits exactly that target.

4.3 SHA-256, Hash pointers and Data Structure

There a lot of hash functions in existence but I'm going to focus just on one of these, the so called *SHA-256 hash function*, which is the one that Bitcoin uses. In Figure 3 we have a simplified scheme about how it works.

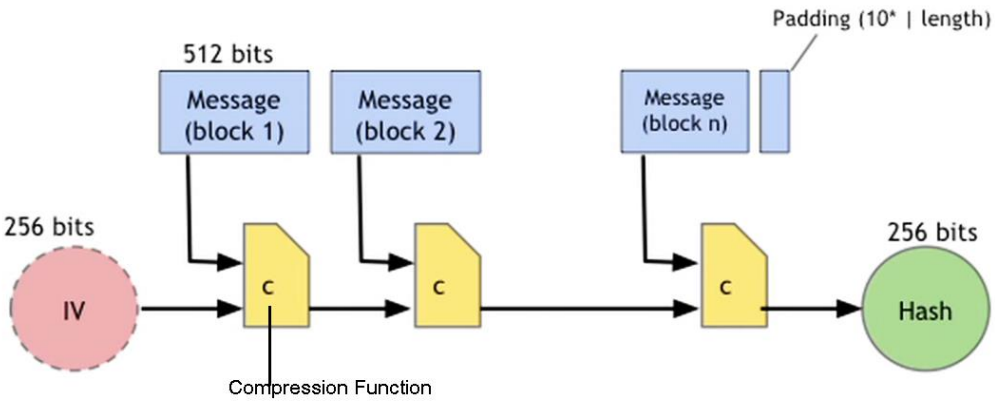


Figure 3 - SHA-256 Hash Function

Basically SHA-256 takes the message that you are hashing and it breaks it up into blocks that are 512-bits in size. Since the message size is not going to be necessarily a multiple of the block size (512-bits), we are going to add some padding at the end, and the padding is going to consists of a certain size length field, which is the length of the message in bits, so this comes out exactly to the end of a block.

Once you have padded the message, i.e. its length is exactly a multiple of the 512-bits block size, you then chop it up into blocks and execute this computation, you start with 256-bits value, called the Initialization Vector (IV)[65], that you look up in a standards document, and then you

[64] High min-entropy means that the distribution is "very spread out", so that no particular value is chosen with more than negligible probability.

[65] In cryptography, an initialization vector (IV) or starting variable (SV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. This number, also called a nonce, is employed only one time in any session.
The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding

take the IV and the first block of the message, you take those 768 total bits and you run them through this special function "c", the compression function[66], and outcomes 256 bits, then again you take that with the next 512 bits of the message run it through "c" and you keep going each iteration of "c" crunches in another 512 bits block of the message and mixes it into the result.[67] When you get to the very end and you have consumed all the block of the message plus the padding, the result is the hash, a 256-bits value for which is easy to show that if this compression function "c" is collision-free, then the SHA-256, the entire hash function is collision-free.

Hash pointer is a kind of data structure that turns out to be used a lot in the systems that we are talking about, it is a pointer to where some information is stored together with the (cryptographic) hash of such information. If we have a hash pointer, we can ask to have the information back but we can also verify that it hasn't changed.

With hash pointers we can build all kinds of data structure, the key idea here is: take any data structure, linked list or binary search tree and implement it with hash pointers.

More generally, we can use hash pointers in any pointer-based data structure that has no cycles, because if there are cycles in the data structure then we won't be able to make all the hashes match up. Graphically it is common use to represent a series of hash pointers like in the Figure below.

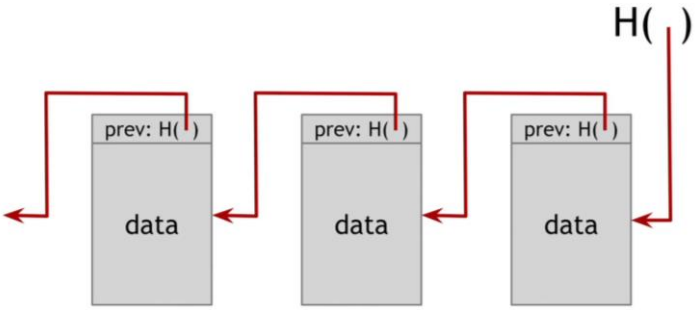


Figure 4 - Blockchain is an example of linked list data structure built with hash pointers

The blockchain is a linked list built with hash pointers and it is the data structure used in Bitcoin, as I already mentioned. It has a series of blocks and each block has data, as well as a pointer to the previous block in the list, here the previous block pointer will be replaced with the hash pointer, each hash pointers says where the block is in the chain and which was the value of the

sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.

[66] A compression function takes a fixed length input and returns a shorter, fixed-length output. Then a hash function can be defined by means of repeated applications of the compression function until the entire message has been processed. In this process, a message of arbitrary length is broken into blocks of a certain length which depends on the compression function, and "padded" (for security reasons) so that the size of the message is a multiple of the block size. The blocks are then processed sequentially, taking as input the result of the hash so far and the current message block, with the final output being the hash value for the message.

[67] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available online: https://bitcoin.org/bitcoin.pdf

previous block, as well as we are going to remember the head of the list, just like a regular hash pointer. Each block once recorded cannot be lost.

A use case for a blockchain is the temper-evident log, i.e. if we want to build a log data structure that stores a bunch of data, we can add data onto the end of the log but if somebody goes later and messes with data (that is earlier in the log) we are going to detect it, e. g. if and adversary want to temper with a block in the middle of the chain trying to change the data contents in such block, and therefore the hash of the entire block, it is not going to match up because the hash function is collision-free, it must be the case that the hash of this block is now different and so we could detect the inconsistency between this data and the hash pointer that we remembered before or we could do that unless the adversary also tempers with hash pointers, in this case these two match up but now he has changed the contents of the subsequent block and if we hash such contents it is not going to match the hash that we remembered before because the contents of the block has changed and so on.[68]

Thus, the upshot of this is that if the adversary wants to tamper with data anywhere in this entire chain in order to keep the story consistent he is going to have to tamper with hash pointers all the way back to the so called *genesis* block (the beginning of the list), and he is ultimately going to run into a roadblock because he won't be able to temper with the head of the list.

Another useful data structure that we can build using hash pointers is a binary three, and this is called in the jargon a "Merkle tree", after Ralph Merkle who invented it.

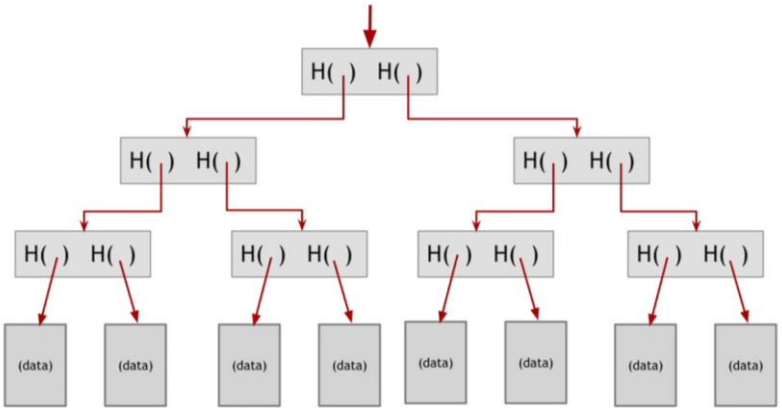


Figure 5 - "Merkle tree" is another example of data structure

As we can see in the figure above, we can imagine a Merkle tree like a set of branches where at the bottom there is bunch of data-blocks, and taking consecutive pairs of this data-blocks we can built a data-structure upon these with two hash pointers, one to each of these blocks, and similarly all the way across we will then add another level up building another data-structure

[68] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available online: https://bitcoin.org/bitcoin.pdf

that will contain two hash pointers of both the previous hash pointers, and so on all the way back up to the root of tree.

Then, like in the other example, we are going to remember just the hash pointer at the head of the tree and if we want we can traverse down through the hash pointers to any point in the list and we can make sure that the data hasn't been tempered with because, as in the blockchain case, if an adversary tempered with some data-blocks at the bottom, it will cause the mismatch with the hash point that is one level up and so he will have to temper with this block, and with the hash pointer one level up from there, and so on, until he'll get up to the top where he won't be able to temper with.

4.4 Digital Signatures and Digital Identities

A digital signature is supposed to be like a normal signature[69] on paper but in digital form with cryptography.

If we have to define a digital signatures API[70], first of all we need to be able to generate keys and define the key size. This process in the first step produces two keys: a secret signing key (sk), this is information you keep secret that you use for making your signature; and a public verification key (pk), that you are going to give to everybody and that anybody can use to verify your signature when they see it.

Then, in the digital signature scheme, after creating your signature we have other two algorithms/operations to check and verify the correct creation of your signature: the sign operations and validity operations.[71]

The two main requirements that we want for our signature concern: (1) a "valid signatures verify", i.e. a valid signature verifies if another signature is valid by using the pk and the message, which was signed with sk; (2) the "impossibility to forge signature", e. g. an adversary who knows your pk and gets to see signatures on some other messages, cannot forge your signature on some messages that he wants to forge it on.[72]

There is a bunch of practical things that we need to do to turn that algorithmic idea into a more practically implementable signature mechanism, e.g. the algorithms are randomized, or the fact that there is limit on message size that you are able to sign and, by the way, it's more secure to use the hash of the message as the input to the digital signature (rather than the message) which

[69] A normal signature is made only by you but everyone can verify the validity. It cannot be cut-and-pasted to another documents.

[70] In general terms an Application Programming Interface (API) is a set of clearly defined methods of communication between various software components. In computer programming it is a set of subroutine definition, protocols and tools for building application software.

[71] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available online: https://bitcoin.org/bitcoin.pdf

[72] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

will be only 256 bits; moreover, it is also possible to sign a hash pointer, in this way the signature "covers" the whole structure, not just the hash pointer.

Bitcoin uses a particular digital signature scheme that is called Elliptic Curve Digital Signature Algorithm (ECDSA) and it is a US Government standard that relies on extremely hairy math. ECDSA has good randomness essay and it is essential because otherwise in generating your keys or in the signing process you probably leaked your private key, so we need to be especially careful about this in practice.

A useful trick, to take a public verification key from a digital signature scheme and equate that to an identity of a person or an actor in a system, is whether or not the signature verifies correctly, i.e. if you can verify with someone's public key a signature on a particular message, then you can think of that pk as a person or an actor or a party in a system and that such public key can make statements by signing those statements.[73]

In practice, with your secret key you are making statements on behalf of that specific public key and this means that there is an identity in the system that everybody can see and which only you can speak for and that is what you want such identity to be.

One of the positive aspects of treating public keys as identities concerns the possibility to make a new identity whenever you want, you have just to create a new random key pair, sk and pk, by doing the generate keys operation in our digital signature scheme.

Pk is the public "name", but in general better to use the hash of pk, i. e. what you use to talk about the identity, while sk is the information that lets the person who generated this identity speak for the identity. Thus, you control the identity, because only you know secret key, and if you generate this in such a way that the public key looks random then nobody needs to know who you are, you can generate a fresh identity that looks random, like a face in the crowd, that only you can control. This bring us to the idea of decentralized identity management, i.e. rather than having a central place that you have to go in order to register as a user in a system, you don't need to get a username, you don't need to inform someone that you're going to be using a particular name, if you want a new identity just make a new one.[74]

Anybody can make a new identity at any time and you can make as many as you want. If you prefer to be known by five different names there are no problems, just make five identities. If you want to be somewhat anonymous for a while, you can make a new identity and use it just for a little while, then throw it away. All these things are possible with decentralized identity

[73] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

[74] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available online: https://bitcoin.org/bitcoin.pdf

management and there is no central point of control, so you do not need anyone who is in charge of it, the system operates in an entirely decentralized way.

The decentralized identity management is the way Bitcoin actually does identities, called addresses in Bitcoin jargon, and so when we heard talking about addresses we must remember that they are just public key or a hash of a public key, and it is an identity that someone made up.

At this point one can ask how much privacy there is in this process and if there is privacy or not. Technically speaking, addresses made up in this way is not connected to real-world identity, you can execute a randomized algorithm that will make some kind of pk that looks kind of random and nothing exists to connect that to who you are. On the other hand, if that address or identity is making a series of statements over time, if it is engaging in a series of acts, e. g. a pattern of behaviour of an address over time that people can see, observers can link together these things over time, they can start to connect the dots and make inferences.[75]

4.5 From cryptography to cryptocurrency

In analysing cryptocurrency, it is better to start with a simplified case and make it more complicated one step at time in order to give us ideas about how systems like Bitcoin works.

Let's assume a girl called Alice decides to create her own cryptocurrency called Alice-coin, and it is the simplest cryptocurrency we can imagine.

As a rule of the game, Alice can create new coins whenever she wants and, when she makes a new coin, it belongs to her, so the data structure when she creates a new coin appears like in Table 1 below, where there is a unique coin ID that Alice generated and a digital signature that was put on it by Alice, which anyone can verify that is valid.

Table 1 - New Minting Data Structure

Signed by pk_{Alice}
CreateCoin [uniqueCoinID]

Whoever owns a coin can pass it to someone else, they can spend it, so in this way with subsequent transactions users are generating a blockchain that take a hash pointer to that coin generated before.

However, in such a structured ecosystem, a problem of *double spending* may arise. Let's assume that through an Alice's statement, that says pay a specific coin to public key "Bob", the coin that is represented by this hash pointer also signed by Alice goes under Bob's ownership.

[75] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

Now Bob owns the coin and he can prove it by the data structure signed by the previous owner Alice.

Bob can move on and he can spend the coin as well, and you can verify the validity of a coin by simply following the chain checking all of the signature along the way.

Let's assume that after Alice paid the coin to Bob, he decided to pay this coin to Carol but at the same time Bob makes another data structure in which pays to Dom the very same coin. Graphically we can imagine the situation like in the scheme of Figure 6.

If Dom does not know the whole framework he thinks that the data structure in which he is involved is perfectly valid and now he is the owner of the coin, so Dom has a valid claim to be the owner of this coin as well as Carol. That is a big security problem with Alice-coin.

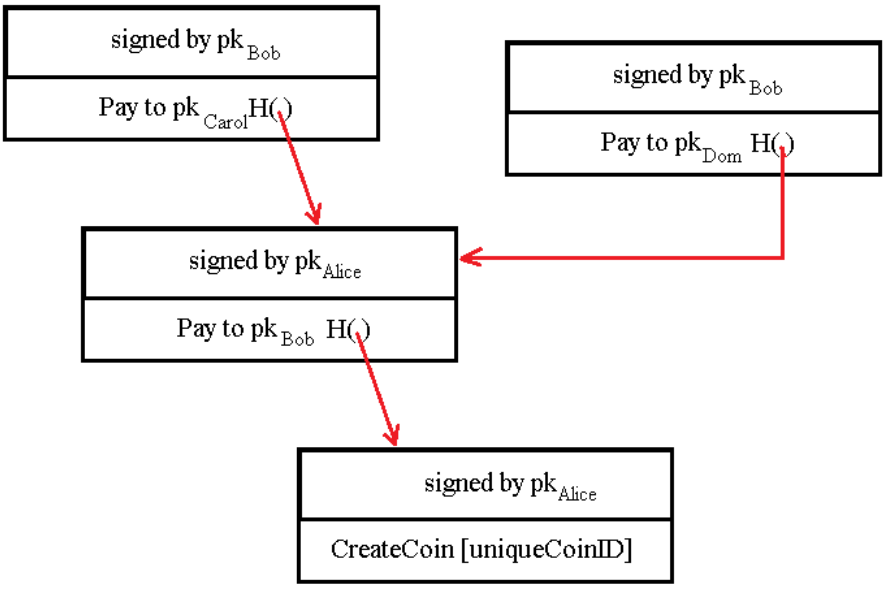


Figure 6 - Double Spending Attempting

This is called *double-spending attack*, because Bob is spending the same coin twice, and this is one of the key problems that a cryptocurrency has to solve, in other words this is the main design challenge that we face in designing a cryptocurrency, and since Alice-coin doesn't prevent the double-spending attack, therefore Alice coin is not secure.

You can overcome this kind of problem and in order to make it works Alice-coin needs to be improved: Alice can solve the double-spending problem by publishing a history of all the transaction that have happened and this will shape a blockchain data structure digitally signed by Alice.

If Alice will digitally sign the hash pointers which represents an entire structure and publish them, anybody can verify that Alice really signed this hash pointer and then they can follow this chain all the way back and see what is the entire history of all the transaction in Alice-coin. The history published by Alice allows us to detect double spending attacks.

In this renewed framework, we distinguish among two types of transaction: (1) the new minting made by Alice and (2) the PayCoins transaction.

Let's start with the Create-Coin operation. A CreateCoin transaction is always valid because Alice said (they call it Alice-coin for a reason). If she signs and puts such transaction into the history then it is valid by definition. We do not need to worry about whether Alice is entitled to create coins, the rules of the system which was created simply say that if she wants to make coins then that is valid, so anything she puts in the history its valid.

The second kind of operation consists of a PayCoins transaction which consumes some coins, destroys them and creates new coins of the same total value but which might belong to different people.

Alice stated that a PayCoins transaction is valid if (1) the consumed coins are valid, i.e. they really were created in previous transactions; if (2) the consumed coins were not already consumed in some previous transaction (no double-spending); (3) the total value that comes out of this transactions is equal to the total value that went in; and, finally, the transaction is validly if (4) signed by the owner(s) of all consumed coins.

One thing that should be notice in this framework is that coins are immutable, they never changed or subdivided or combined, they are just created in one transaction and later consumed in some other transaction, anyway, the effect is the same by using transactions.

It seems that the renewed Alice coins work very well and in a transparent manner, but there is still a problem with this, and it is Alice.

Even if she declares that is honest if Alice starts misbehaving or if she starts to get bored of the whole Alice-coin scheme and stops doing the things that she is supposed to do then the system won't operate anymore.

The problem with Alice coin is centralization, so the technical challenge that we need to solve in order to improve on Alice-coin concerns the possibility to get rid of that centralized Alice figure; in order to get a crypto-currency that operates without any central trusted authority we need to figure out a system where everyone can agree on a single published blockchain (the agreed-upon history of which transaction have happened), we need to figure out how people can agree and which transaction are valid as well as the way to assign IDs to things in a decentralized way. If we can solve all these problems, then we can build a currency that is very much like Bitcoin scheme.

4.6 How Bitcoin achieves Decentralization

Almost all of the decentralized systems are not purely decentralized. A good example of this is E-Mail, which is fundamentally a decentralized system based on standard spaces, in which, especially over the last decade, we saw a dominance of a few different webmail institutions

which are a sort of centralized service providers, and this might be a good model for understanding what might be happening to Bitcoin.

The way in which Bitcoin achieves decentralization is not purely technical but it is a combination of technical and clever incentive engineering.[76]

First of all, we have to focus on the Bitcoin peer-to-peer network, thanks to this anybody can run a bitcoin node: there is fairly low barrier entry, you can go online, download a Bitcoin client to yourself and run that on your laptop or your PC and this really resembles a P2P decentralized system. But that is not the only component of Bitcoin, there is also Bitcoin mining which is technically also open to anyone, even if it requires a very high capital cost due to how the system happens to have evolved, so by the way I do not know if we can consider this as real decentralized aspect of Bitcoin.

A third aspects that really can help us in understanding how decentralized is Bitcoin concerns updates to software, how and when the rules of the system change. One can conceptually imagine that everybody running a Bitcoin node will look at the Bitcoin specification, maybe even create their own software and achieves a decentralized system, but again it doesn't work exactly like this, in practice, the core developers are really trusted by the community and they have a lot of power in determining what Bitcoin software each of these nodes will run on their computer.[77]

At the technical level the key challenge of decentralization that you have to solve to build a distributed e-cash system is the so called *distributed consensus*, a class of protocol that have been studied for decades in the computer science literature. The traditional motivation application concerns reliability in distributed systems but also because a distributed key-value store enables various application like DSN, public key director, stock trades, etc. which are useful to achieve different goals than the Bitcoin one.

In technical terms, a Distributed Consensus is what we get when a consensus protocol is terminated, i.e. the value that has been proposed at least by one valid node at the beginning of the consensus protocol and which has been decided to be chosen by all valid nodes at the end of this. We talk about valid nodes because as we saw earlier there can be invalid nodes, or nodes that can be faulty.

[76] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 10-21. Available online

[77] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

In the Bitcoin context, the Distributed Consensus implies that when a user, Mr. A wants to pay another user, Mr. B, he simply broadcasts the transaction[78] to all of the Bitcoin nodes that comprise the P2P network.

If Mr. B wants to be notified that this transaction did in fact happen and that he got paid, he might want to run a Bitcoin P2P node in order to listen in on the network and to be sure that he received that transaction. However, but his listening is not necessary for him to receive the funds.

Given that a variety of users are broadcasting transactions like these to the network, where everybody wants to reach consensus on, at any given point in time all of these nodes on the P2P network would have a sequence of blocks that they have already agreed upon and each node would then have a set of outstanding transactions (for which consensus has not yet happened) that it's heard about.

Even if the decentralization problem is not solved in a general sense with distributed consensus, Bitcoin protocol introduces a further tool which consists in incentives, and this is only possible in Bitcoin context because it is a currency and you can use that to remunerate the participants for acting honestly.

Moreover, Bitcoin really embraces the notion of randomness, i.e. it does away with the notion of a specific starting-point and ending-point for consensus, instead it happens over a long period of time, about an hour in the practical system, but even at the end of that period you are not 100% sure that a transaction or a block that you are interested in has made into the consensus blockchain but as time goes on your probability goes up higher and higher.[79]

Differently to how traditional distribute consensus algorithm operated, the Bitcoin consensus algorithm does all of its jobs without nodes having any persistent long-term identities which would make things a lot easier, especially from a security point of view. All these aspects make the Bitcoin consensus protocol a bit harder than other protocols.

There are a couple of reason why Bitcoin has not identities. First of all, pseudonymity is a goal of Bitcoin, furthermore, in a P2P decentralized model like this there is no central authority to give identities to nodes and verify that they are not creating new nodes or Sybil attack[80].

It is spontaneous to wonder if a malicious adversary can try to subvert this process, and in fact, there are three main kinds of attack that a malicious user Mr. A can try to do: (1) he can simply

[78] The transaction will contain the signature of Mr. A and the hash pointers, together with the private key of Mr. B.

[79] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available online: https://bitcoin.org/bitcoin.pdf

[80] The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder [122].

try to steal bitcoins belonging to another user at a different address that he doesn't control, but since he cannot forge the signature of another user, as long as the underlying crypto is solid, he is not able to simply steal bitcoins; (2) if Mr. A really hates Mr. B, he can decide that he will simply not include any transaction originating from Mr. B address in any block that Mr. A proposes to get onto the blockchain, in other words he is denying service to Mr. B, so this is a valid attack that he can try to mount but it is not so efficacious because Mr. B will just wait until an honest node gets the chance to propose a block and then its transaction will get into that block.

A third typology of attack concerns the possibility to do (3) a double spending attack. Let's suppose that Mr. A broadcasts a transaction (the green transaction in Figure 7) to Pay Mr. B and that an honest node includes this transaction in a new block to the chain. This block contains the hash pointers to the previous block and the data structure of the transaction, which contains Mr. A signature together with an instruction to pay to Mr. B public key and also a hash which represents a pointer to a transaction included in some previous block in the consensus chain where Mr. A actually received that coin from somebody else.

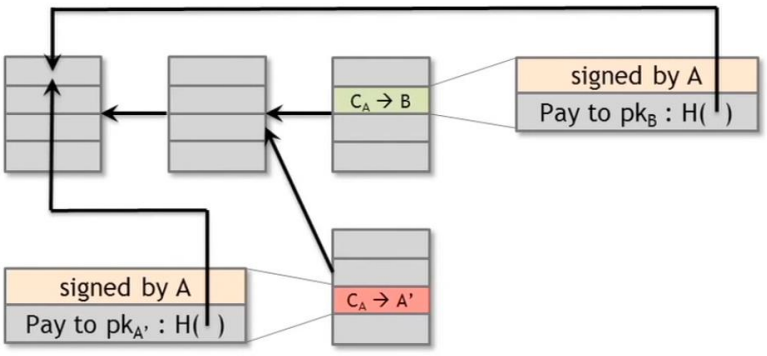


Figure 7 - Double Spending Attack

Now let's assume that the next block is the malicious one controlled by Mr. A, which ignores the valid block created by the honest node and contains a hash pointer to the previous block, furthermore, it is going to contain a transfer of coins from Mr. A to another address A' that is also controlled by Mr. A.

In order to know if the double-spending attempt is going to succeed or not we have to look whether the green or the red transaction is going to ultimately end up in the long-term consensus chain[81]. Moreover, nodes often follow a heuristic of extending the block that they first heard about on the P2P network but it is not a solid rule, also because of network latency.

[81] As a rule of the thumb, the long term consensus chain is determined by the fact that honest nodes are always following the policy of extending the longest valid branch of the chain.

Despite this, we might consider that there is at least some chance that the next node gets to propose a block extending the malicious block, or simply Mr. A can try to subvert the process in a variety of ways.

If the double-spending succeeded and the malicious block ends up in the long-term consensus chain, the block ignored by the network take the name of *orphan block.*

From the point of view of Mr. B there is something that he can do in order to protect himself against invalid transaction (in our case against double-spending) and it is enforced by consensus, cryptography has nothing to say about this because a true transaction that represent a double spending attempt looks identical from the perspective of signature and other features, but it is the consensus that determines which one will end up on the long-term consensus chain.

As I mentioned earlier, you are never 100% sure that a transaction you are interested in is one the consensus branch, but there is an exponentially probability that guarantees pretty good after six transactions[82], in practice, there is virtually no chance that you are going to go wrong.

4.7 Incentives and new minting

In order to give an incentive for behaving honestly, Bitcoin protocol does not penalize the node that created malicious block, instead, it rewards nodes that did end-up on the long-term consensus chain.

Since we have no identities in the blockchain, the protocol can't mail cash to their home address, in fact, it uses bitcoins in order to incentivize the honest nodes.

There are two different kind of incentive, actually the main one is called *block reward* and, according to the rules of Bitcoin, consists in the fact that the node which creates a new valid block gets to include a special transaction in that block, a coin-creation transaction, and this node can also choose the recipient address of this transaction (which typically is an address belonging to the node, thereby paying itself). So it is a sort of payment in exchange for the service of creating that block to go onto the consensus chain.[83]

The value of the coin-creation transaction for block reward has an interesting property, it is critically fixed and actually it halves every four years (see Figure 8). In the first period of bitcoin existence, the reward was fixed at 50 bitcoins; we are now in the third period[84] and it is fixed

[82] In general, the more confirmation your transaction gets the higher the probability that it is going to end up on the long-term consensus chain, since the honest nodes behaviour will always extend the longest valid branch that they see. In the most common heuristic that is used in the Bitcoin ecosystem, you wait for six confirmations. There is nothing special about the number six, it is just a good trade-off between the amount of time you have to wait and your guarantee that the transaction you are interested in ends up on the consensus blockchain.

[83] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available online: https://bitcoin.org/bitcoin.pdf

[84] The second Bitcoin *Halving* took place in July 9, 2016.

at 12.5 bitcoins, but it is going to keep halving [21] (there is also an appositely-created web-site with constantly monitors the "bitcoin halving countdown"[85]).

The other face of the medal of the Halving process is that, halving every four years[86] and since the block reward is the only way new bitcoins are released, it will asymptotically approach to zero, i.e. the block reward size and schedule specify the fully automatic, non-discretionary bitcoin monetary policy which has an inelastic fixed supply [15].

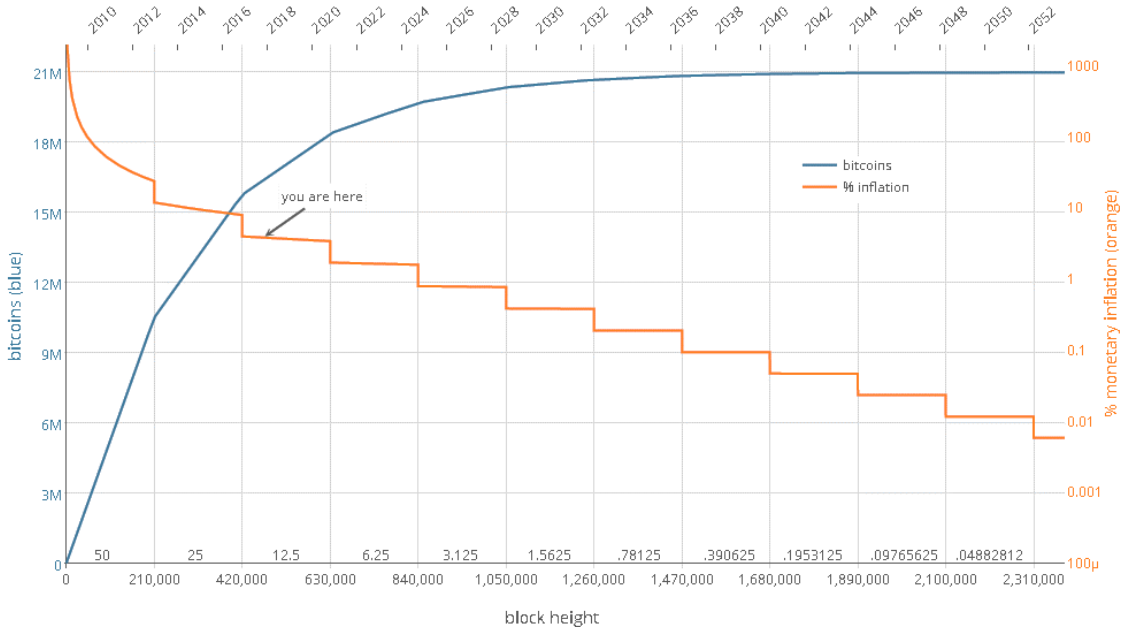


Figure 8 - Bitcoin Monetary Inflation[87] *[22]*

The total finite supply of Bitcoin, based on the rate of new block creation, is 21 million and this new block-creation reward is actually going to run out in 2040, as things stand now[88]. This means that the system will stop working in 2040 and it seems that becomes insecure because at that date nodes no longer have the incentive to behave honestly, but it is not totally true, in fact, here comes in place the other incentive mechanism.[89]

The second incentive mechanism, called *transaction fees*, concerns the fact that the creator of any transaction can choose to make the output value of that coin less than the input value, and the way that all the nodes interpret this difference, according to the rules of Bitcoin, is that it is

[85] http://www.thehalvening.com/

[86] The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years. The result is that the number of bitcoins in existence is not expected to exceed 21 million [123].

[87] $Inflation = coinbase * \frac{blocksPerYear}{existingCoins}$

[88] It is supposed that the decreasing-supply algorithm was chosen by Nakamoto because it approximates the rate at which commodities like gold are mined, but in reality Satoshi has never really justified or explained many of these constants.

[89] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 10-21. Available online

a transaction fee and whoever creates the block that first puts that transaction into the block-chain gets to collect that transaction fee. Of course, this transaction fee is purely voluntary, like a tip, but we can expect that it will become more and more important as the block reward starts to run out, or even mandatory for nodes to put a transaction fee into their transactions in order to get a reasonable quality of service. This is evolving precisely how the system is evolving and it is an interesting area of open research on Bitcoin.

4.8 Bitcoin Proof-of-work: The Hash Puzzle

In a nascent eco-system like Bitcoin, users' confidence is essential for the engine of system in order to expand and grow more and more. For this reason, the process of selecting nodes must depend on a resource that nobody can monopolize, if that resource that we are talking about is computing power we will select nodes in proportion to their computing power and this is the so called proof-of-work; furthermore, the resource can be alternatively the proportion to owner-ship of the currency and this is a legitimate model used in a lot of other alternative cryptocur-rencies to Bitcoin, that is called proof-of-stake.

In the proof-of-work mechanism, selecting nodes in proportion to computing powers means that we are allowing nodes to compete with each other by using their computer power and that will result in nodes automatically being picked in that proportion. There is also an alternative way of seeing this: making moderately hard the proof-of-work to create new identities is a sort of obstacle to attack on identity creation and on the Sybil attack.[90]

The exact proof-of-work system used in Bitcoin is called Hash Puzzle: in order to create a block, the nodes that proposes that block is required to find a number, a *nonce*, such that to predict which combination of bits will result in the right hash, many different nonce values are tried, and the hash is recomputed for each value until a hash containing the required number of zero bits is found. The number of zero bits required is set by the difficulty. The resulting hash has to be a value less than the current difficulty (target space) and so will have to have a certain number of leading zero bits to be less than that. As this iterative calculation requires time and resources, the presentation of the block with the correct nonce value constitutes proof of work.

The idea was to make moderately difficult to find a nonce that satisfies this required property, which is hashing the whole block together including that nonce is going to result in a particular type of output; if the hash function is secure then the only way to succeed in solving this hash puzzle is just to try enough nonces, one by one, until you get lucky[91].

[90] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

[91] If the target space is just 1% of the overall output space you would have to try about hundred nonces before you got lucky and if this hash function were to behave essentially randomly, only one in a hundreds nonces will result in an output that falls within this target space. The computational problem that a node is required to solve in order to produce the block is essentially this.

This notion of hash puzzle in proof-of-work completely does away with the requirement for somebody somehow to pick a random node, instead nodes are simply all the time independently competing to solve these hash puzzles and once in a while one of them will get lucky and will find a random nonce that satisfies this property, that node then gets to propose the next block.
There are three essential properties of this proof-of-work function: (1) it needs to be quite difficult to compute: today the hash power of the network is over four-hundreds Petahash per second, as we can see in Figure 9, and because of this only some nodes even bother to compete in this block creation process, and this is what is known as Bitcoin mining, i.e. the process of repeatedly trying and solving these hash puzzles. From this we can also understand in part the reason why nodes are called miners and because, even though technically, anybody can be a miner.
Just to have an idea about how fast the computation power needed is growing we can consider the fact that, in 2009, an individual with a personal laptop could "mine" 200 BTC in a few days but in 2014, it would take about 98 years to "mine" just one bitcoin on a personal computer. Today, in 2017, mining is four hundred-times harder than in 2014 [23].

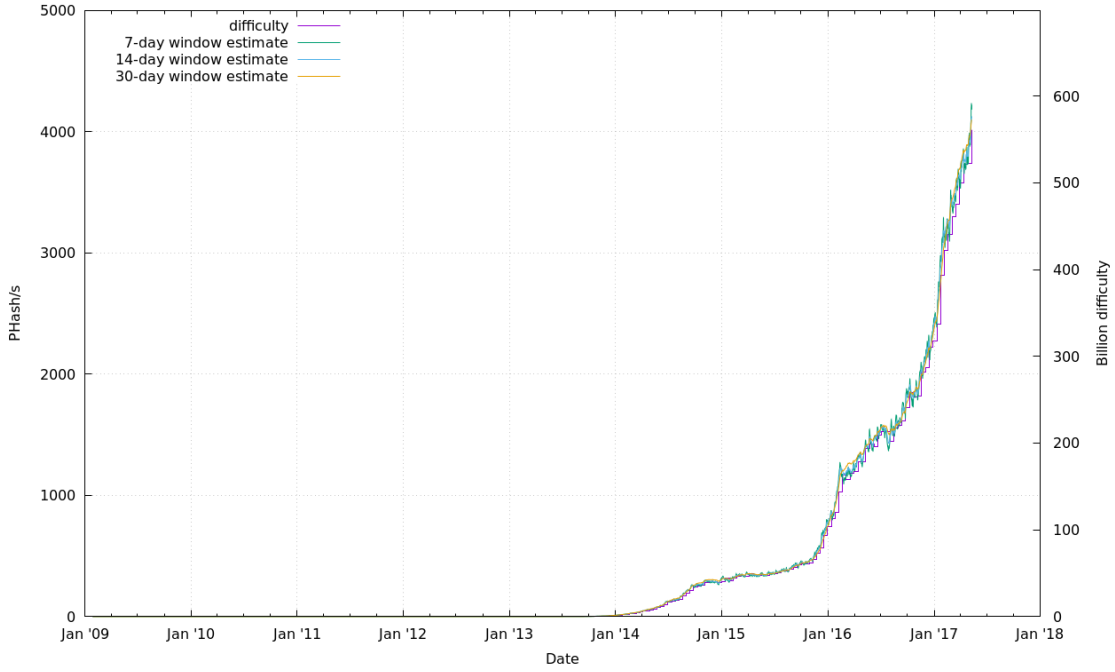


Figure 9 - Bitcoin Network total computation speed

The second property is related to (2) the cost of mining. It must be parameterizable, it is not a cost that is fixed over all time: all the nodes in the P2P network every two weeks will automatically recalculate the target, i.e. the size target of the space as a fraction of the output space in

such a way that they maintain the average time between any two successive blocks produced in the overall Bitcoin network, which is about 10 minutes.[92]

If you are a miner and you have invested a certain fixed amount of hardware into Bitcoin mining, the rate at which you find blocks is actually dependent upon what others miners are doing, i.e. the probability that a miner has to win the next block equals the fraction of global hash power that he controls. Since the overall mining ecosystem is constantly growing, more miners are coming in, or they are deploying faster and faster hardware, in a two-weeks period slightly more blocks are going to be found and expected and so nodes will automatically readjust the target and so the amount of work that you have to do to be able to create a new block is going to increase.

The reason why they want maintain this ten minutes invariant is simple and relies on the fact that if new block creation occurs very frequently there would be a lot of inefficiency and we would lose the optimization benefits of being able to check out a lot of transaction, as it currently stands several hundred transactions in a single block.

Because of the way in which proof-of-work is set up, it allows us to reformulate our security assumption, instead of saying that the majority of nodes are honest in a context where nodes don't even have identities, we can now state that a lot of attack on bitcoin are infeasible if the majority of miners, weighted by hash powers, are following the protocol (because of the competition for proposing the next block) or simply because they are honest.[93]

The third property of the proof-of-work function concerns the fact that (3) it is actually trivial to verify that a node has computed proof-of-work correctly, i.e. even if you find a nonce that succeed on average one to twenty tries, that nonce must be published on that new block so it is trivial for any other miner to look at the block contents, hash them all together and verify that the output is less than the target. This is an important property because once again it allows you to get rid of centralization to verify that miners are doing their job correctly.

4.9 Mining economics, Confidence and Bitcoin Bootstrapping

Bitcoin mining is the process of earning bitcoins in exchange for running the verification to validate bitcoin transactions. These operations provide security for the Bitcoin network which in turn compensates miners by giving them bitcoins. Miners can profit if the price of bitcoins exceeds the cost to mine.

Of course, there are several factors that determine whether bitcoin mining is a profitable venture. The main two factors involve the cost of the electricity to power the computer system (cost

[92] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 10-21. Available online

[93] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

of electricity), the availability and price of the computer system, and the difficulty in providing the services, so we can simplify the profit equation like in Figure 10.

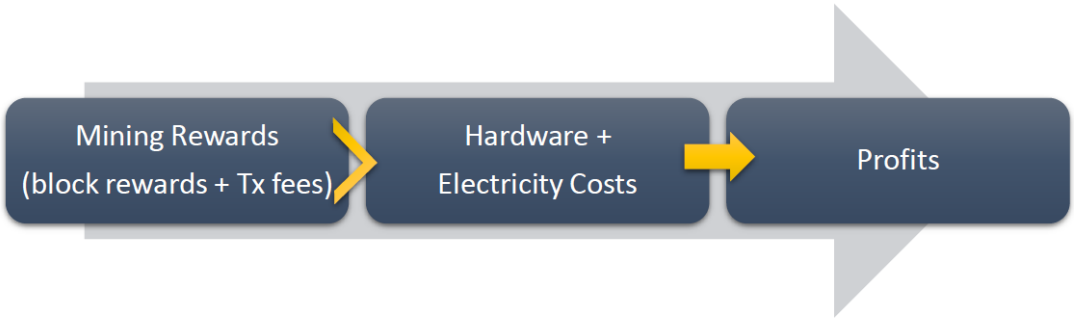


Figure 10 - Mining Economics, a simplified profit equation

Bitcoin mining is in fact very expensive in terms of electricity and it becomes a significant portion of the cost.

However, there are some complication to this simple equation, in fact, the hardware cost is a fixed cost (upfront cost) while the electricity cost is a variable cost that is incurred over time.

Another complication depends on the fact that rewards are correlated with the rate at which miners find blocks, which depends not only on the power of their hardware but also in the ratio of the power of their hardware as a fraction of the total global hash rate.

Moreover, the fact that the cost in which miners incur is expressed in dollars or other fiat currency whereas they are rewarded in terms of bitcoins can be a problem for nodes, so this simple equation is really going to depend on what the exchange rate actually is.

There is a concept that goes beyond, but at the same time incorporates the mere logic of profit, to explain why a miner is coming in or continuing to operate in this eco-system. This concept is called Bitcoin Bootstrapping is the tricky interplay between three pillar in the Bitcoin eco-system.

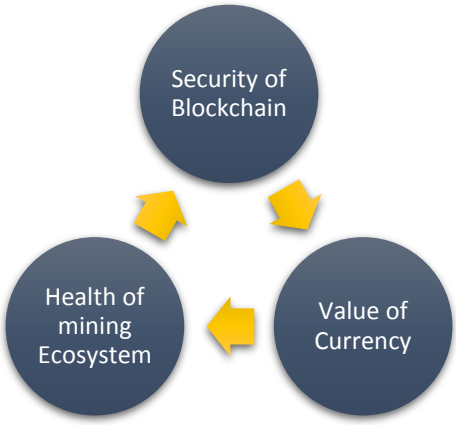


Figure 11 - Bitcoin Bootstrapping

Obviously we want the blockchain to be secure for bitcoin to be a viable currency, for the blockchain to be secure we need that an adversary shouldn't be able to overwhelm the consensus process, e.g. he shouldn't be able to create a lot of nodes and take over 50% or more of the new block creation. The prerequisite for that is a healthy mining ecosystem, made up of largely honest protocol-following nodes.[94]

We will be sure that a large part of miners will put a lot of computing power into this hash-puzzle solving-competition only if the exchange rate of bitcoin is pretty high, i.e. the more the value of the currency goes up the more incentivized these miners are going to be. Again, a high and stable value of the currency is ensured by the trust of users in the security of the blockchain.

4.10 A weakness of Bitcoin: 51%-Attacker

Over 80% of all Bitcoin mining today is already happening in China, the leading manufacturer of chips for Bitcoin, Bitmain[95], is based out of Beijing and it was the first among Bitcoin.

As already mentioned above, the high computing power needed and the large investments required in Hardware created a scenario consisting of a not too large number of miners participating in the network (see Figure 10), where agglomerations with greater hash power do not exceed 17% of total power.

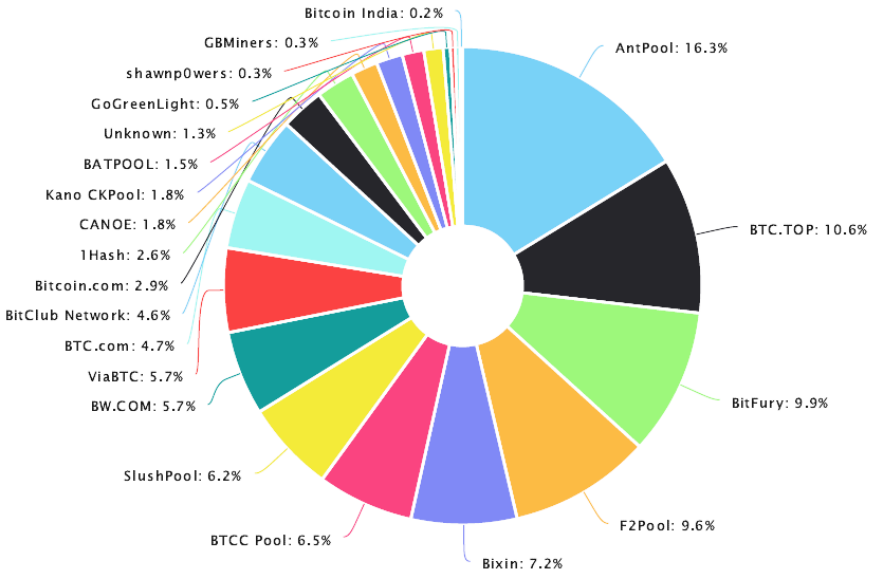


Figure 12 - An estimation of hashrate distribution amongst the largest mining pools on May 14, 2017 [24]

[94] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available online: https://bitcoin.org/bitcoin.pdf

[95] Founded in 2013, Bitmain Technologies, described as the world's most valuable bitcoin company, was established to develop and sell the world's leading bitcoin miners using Bitmain's ASIC chip technology. Starting with the Antminer S1, their task continuously became more difficult as bitcoin's "difficulty level" kept rising. In May of 2016 they released the Antminer S9, the world's first consumer-grade bitcoin miner based on a 16nm process ASIC chip. This is also the world's most power-efficient bitcoin miner, taking that title away from its predecessor, the Antminer S7 [119].

In a context like that of the Bitcoin network, where we have seen that healthy competition between the nodes is needed, it is spontaneous to wonder what would happen if that competition was to fail.[96] In other words, we are wondering what would happen to the system if a node could control more than half of the hash power and thus prevail over the other nodes, but above all it is interesting to know how the system would react in such a situation. To better understand what we are talking about, it might be useful to hypothesize scenarios of possible attacks.

We already saw that stealing coins from an existing address is not possible and even if you subvert the cryptography it is not enough to subvert the consensus process.

Let's say that this 51%-Attacker creates an invalid block that contains an invalid transaction that represents stealing bitcoins from an existing address that the attacker doesn't control and transferring them to his own address, now this attacker can pretend that this is a valid transaction and that's a valid block.

Even if the 51%-attacker keeps building upon this block and even succeed in making that the longest branch, the other honest nodes are simply not going to accept this invalid block and are going to keep mining based on the last valid block that they found on the network, so that situation represents what is called a *fork in the chain*.

Imagine this from the point of view of the attacker trying to spend this invalid coins and trying to spend it to some merchant and buy something in exchange. If the merchant is presumably running a Bitcoin node himself and that will be an honest node which is going to recognize that, even if it is the longest branch, it is not valid because it contains an invalid transaction since the signature doesn't check out and so he is going to simply ignore it has longest branch. Subverting consensus is not enough if you want to accomplish a successful attack you have to subvert cryptography to steal coins from an existing address, so we conclude that this attack is not possible for a 51%-attacker.[97]

By the way, we are talking just in theoretical terms, in fact, if there would be a 51%-node, developers will notice this and they will try to react to it updating the Bitcoin software and we might expect that the rules of the p2p network might change to make this attack more difficult to launch. Anyway, we cannot predict that so, we are working in a simplified model where 51%-attack happens but other than that there are no changes or tweaks to the rules of the system.

If there were a variety of double-spend attempts and the behaviour of not extending the longest valid branch and/or others had attempted to attack, then people are going to look at this and decide that bitcoin is no longer acting as a decentralized ledger that they can trust and so people

[96] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

[97] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, available online: https://bitcoin.org/bitcoin.pdf

will simply lose confidence in the currency and we might expect that the exchange rate of bitcoin is going to plummet. In fact, if there is a 51%-Attacker and this is known, even if the attacker is not necessarily trying to launch any attacks it is possible that this might happen, so we can classify this as not only possible but in fact likely and a 51%-Attack of any sort will simply destroy confidence in the currency and this is in fact the main practical threat if a 51%-Attack were ever to materialize.

Finally, considering the amount of expenditure that the adversary would have to put into attacking Bitcoin, achieving a 51% majority really makes sense from a financial point of view to try any kind of attacks.

An analogue case is that in which the leading mining pools decide to cooperate, assuming that they would have more than 51% of Bitcoin's mining power combined, and they could theoretically alter the original code and make macroeconomics decisions similar to the central banks. However, again, such operation in unlikely to be formed because Bitcoin's users would stop using the altered version of Bitcoin in favour of the older version and the so created conglomeration would lose all the profits. Any alteration of Bitcoin's code would result in a fork, i.e. the network would split into two separate Bitcoin networks. At the time of writing this has yet to occur, but it is a possibility in the future.

4.11 Bitcoin price, Wallets and Keys

Mining is an example of a proof-of-work consensus model. A proof-of-work consensus model "requires the client requesting the service prove that some work has been done" in order to process the request [16]. Each block requires tons of cpu power to be minted. It is same for everyone even the developers.

We saw also that the total amount of bitcoins is capped at 21 million and as a scarce resource with no government-affixed price, the value of an individual bitcoin is set by market forces.

It's likely that until today we are in a speculative bubble of the exchange rate between bitcoin and US dollar (see Figure 13), which contributes to spread out the idea that a cryptocurrency is mainly a financial enrichment tool, dangerous, which is uncontrollable by States and banks.

At the time of writing, the latest media attack on the Bitcoin image occurred on the day after the WannaCry virus spread. When the US National Security Agency found flaws in Microsoft software (using taxpayers' money), instead of alerting Microsoft for a fix, NSA preferred to keep these vulnerabilities secret and leverage them to spy on "enemies." It turns out NSA is not even good at keeping the secrecy and a group of hackers made them public. So, criminals take advantage of the vulnerabilities and attack, bringing home the bitcoin booty.

This story became just another chance at demonizing bitcoin, whose only fault is to work perfectly and imperturbably, without any glitch or problem, without vulnerabilities and being transparent (with its code and transactions) to anyone [25].

The increase in price of the virtual currency is largely thanks to policy changes in Japan and China which let people trade in bitcoin more easily, according to the BBC, for some others the main cause is the ongoing demonization in India, others point to Brexit and Trump's election as central motives [26].

It seems unrealistic but if I had purchased a bitcoin in October 2016, when I suggested the argument of this thesis to Professor Lupoi the exchange rate was 608.21 USD, I would have already earned $ 1557.92 today, since at the time of writing (May 23, 2017) the exchange rate exceeded $ 2000 and is around $ 2166.13. Within about 7 months the value of bitcoins multiplied by more than 3.5 times, and this is nothing if compared to the fact that at the time of its birth a bitcoin could be purchased for only 4.96 cents.

Figure 13 - Market Price (USD), Average USD market price across major bitcoin exchanges [27]

Anyway, we cannot consider bitcoin just like a deregulated, decentralized and highly speculative currency, on the contrary, it is the beginning of a new technologic era that on one hand brings, for the first time, the rarity and uniqueness of a digital good, and on the other hand, bitcoin can rid the economy from social and political cages in which individuals, by nature, can be trapped.

Bitcoin can also be used for remittances especially because of the low fees associated with sending bitcoins across different countries. A report by Goldman Sachs from 2014 measured the cost of sending remittance using Bitcoin, which ended up being 1% on average, while with traditional methods is 7.7% on average.

Overall, Bitcoin works best as a medium of exchange when both parties are willing to negotiate in Bitcoin rather than just using Bitcoin as an intermediary to convert their fiat currencies from

and then immediately afterwards. The reason why there are not more parties willing to do that is because of Bitcoin's volatility, which makes trading ineffective and risky.

However, since transactions in Bitcoins are cheap, reliable, and transparent, and infrastructure has certainly been improving these two issues are motivating more merchants to begin accepting bitcoins as a payment. It is not that difficult today to use the technology, there are tools like iPayYou[98] which make it very simple to actually transfer bitcoin back into the real world and buy a coffee at Starbucks or gift card at Amazon.

It is happening all around us, we are not sure which one was in but they are definitely a lot of usage scenarios that make unravelling so much easier, you probably heard the news that going forward this coin can be used in Japan for a lot of more payment environment there as well.

All over the word, the ways in which you can get your bitcoins are evolving, and the institutions that provide such services are spreading and multiplying like wildfire.

Since the bitcoin network is in direct competition with PayPal, and PayPal does not like (or at least did not like) bitcoin you could not directly buy Bitcoin using PayPal, in fact they banned accounts that have anything to do with Bitcoins, and freeze their balance, until 2016, when they allowed users to buy bitcoins through the creation of a virtual card called E-coin [28].

On the contrary, with your credit card it is very simple to buy bitcoins, there exist platforms, like Cubits[99], VirWox[100] or CoinMama[101], that allow users to buy and sell bitcoin instantly with 17 supported currencies and Visa and MasterCard are accepted in almost all of them, but sometimes this service is not available in specific countries [29].

In this moment it is possible to buy bitcoins through Bank Transfer almost everywhere. There are already a lot of platforms that allow users to connect their account number to an appositely created account, e.g. Coinbase[102], expresscoin.com[103], Bittylicious[104], Kraken[105], BitQuick.co[106], and so on.

Since there is substantially less risk involved for exchanges when people purchase Bitcoins with their bank account, the fees for such a process are significantly lower, but, on the other hand, bank transfer are usually more complex to execute and take a longer amount of time to

[98] iPayYou, a bitcoin wallet that allows users to send bitcoin to people who don't have bitcoin accounts, has introduced Pay-by-Twitter, enabling users to send bitcoin directly to Twitter accounts.
iPayYou becomes the first full-service wallet that enables peer-to-peer payments over the Twitter social media network. Users can send payments via email without the recipient having a pre-created bitcoin account [118].
[99] https://cubits.com/
[100] https://www.virwox.com/
[101] http://coin-mama.com/
[102] http://coinbase.com/
[103] http://www.expresscoin.com/
[104] https://bittylicious.com/
[105] https://kraken.com/
[106] https://www.bitquick.co/

process, since the transfer needs to clear several banks on its way to exchange. Nevertheless, this is probably the best way to go in order to get the best exchange rate possible [30].

As I already mentioned, in order to use bitcoin software, you'll need to set up a bitcoin wallet which will house your details that will be used to send your mining rewards to.

Popular bitcoin wallets include Mycelium[107], Electrum[108] and Copay Bitcoin wallet[109] and like bitcoin software, there are specific wallets depending on your platform, i.e. desktop, Android, iOS and web.[110]

Like mining bitcoin, you'll need to have a bitcoin wallet set up to store then, whether that's online, using a desktop wallet or one for iOS or Android. You'll just need to download it and set it up with your details and then you'll need to get in touch with a bitcoin exchange, a place where sellers and buyers of bitcoin can virtually meet. These sites will also support other cryptocurrencies and most exchanges will have the bitcoins in your account within a couple of hours.

Another option to get bitcoins is to sell things in return for bitcoin. You'll still have to set up a wallet, but if you want a relatively quick process to gain bitcoin, this could be it.

Specifically, a wallet is made of two mathematically related keys: a private key and a public key. The public key is the outward facing destination address of the wallet, like a bank account number or an email address. The private key functions as a PIN to a bank account or a password to an email address. To execute a transaction, bitcoin owners use

their private key to authorize the transfer of bitcoin to the public address representing the recipient's wallet.

4.12 Altcoins: Main Bitcoin Competitors

Some analysts have attributed some of Bitcoin's growth to that of the altcoins[111]; altcoins are usually bought and sold with bitcoin, requiring traders to buy bitcoin. This is exactly what happens in online market like TokenMarket[112] where everyone can launch a crowdsale for its own ICO project and give backers a tradeable digital asset.

There are countless examples of altcoins on the today-market and the great part of these are a mere copy of Bitcoin or other cryptocurrencies.

[107] https://wallet.mycelium.com/
[108] https://electrum.org/
[109] https://copay.io/
[110] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80
[111] Altcoins are the alternative cryptocurrencies launched after the success of Bitcoin. Generally, they project themselves as better substitutes to Bitcoin. "Altcoin" is a combination of two words: "alt" and "coin"; alt is short for alternative and coin signifies currency. Thus together they imply a category of cryptocurrency that is alternative to the digital currency Bitcoin.
[112] https://tokenmarket.net

One of the main valid alternative to Bitcoin is Ethereum[113] and the first mention of this cryptocurrency appeared in 2013 when Vitalik Buterin, a Russian programmer, and Gavin Wood described the technical details and rationale for Ethereum protocols in a white paper [31].

Ethereum is peer-to-peer network that uses a protocol inspired by Bitcoin in order to ensure the integrity of a global transactions ledger. In addition to what has already been done by Bitcoin, Ethereum provides an instrument and a formal language for writing *Smart Contract*.

Smart contracts are computer codes that can facilitate the exchange of money, property, content, or anything of value. Because these contracts run on the blockchain, they run just as they are planned without any possibility of downtime, censorship or fraud [32].

The fear of compromising security prompted, in design phase, to avoid complex encoding within a Bitcoin transaction, this is the reason why smart contracts do not exist on Bitcoin protocol. On the contrary Ethereum has decided to do that; in fact, its value proposition is to do what Bitcoin has decided not to do [33].

On May 2017, Ethereum's blockchain becomes the most secure out of all proof of work based blockchains, making Ethereum the very first platform to overcome bitcoin in this measurement. That is a significant development because a higher level of security means that a higher level of value can be stored due to an increased cost for a 51% attack, but that's just in proof of work (PoW). As a consequence of this, Ethereum intends to move to proof of stake (PoS) which will make the network even more secure while also providing users with confirmation times of as low as potentially 2 seconds, making it as good as instant and the fastest of any other public blockchain based currency [34].

Bitcoin has the biggest market capitalization today, the second cryptocurrency is Litecoin[114], created in 2011 by Charlie Lee and largely considered to be silver to Bitcoins gold. Litecoin uses a different mining algorithm than Bitcoin, which is called Scrypt.

Dogecoin[115], Omni[116], Blackcoin[117], Tether[118] and so on, are all valid alternative to Bitcoin which differ for some particular features or scopes, but they did not reach the same notoriety of the main competitor.

[113] https://ethereum.org/
[114] https://litecoin.org/
[115] http://dogecoin.com/
[116] http://www.omnilayer.org/
[117] http://blackcoin.co/
[118] https://tether.to/

5 Blockchain: Bitcoin Security System and its countless applications

Collaboration and knowledge sharing are essential to stay on top of what is happening in order to build the new world together, because we are, for very clearly, at the beginning, or after, the next big innovation economy revolution, where everything is going to change and it is happening much faster than the industrial revolutions before.

Bitcoin ledger really creates what we think it is called a completeness set of economics, where value and collaboration over the internet can happen outside of the traditional financial institutions and create a completely new model of how that collaboration is going to happen.

Any kind of transaction or information exchange could potentially benefit, or at least being touched by blockchain technology over the next years and it will be a radical transformation, and every time you have a revolution or dramatic change a lot of things, we thought are fixed and will never change, will change and it will happen faster than we can imagine, so it's important to all of us to understand what Charles Darwin suggested about two hundred years ago: "*it's not the strongest of the species that survive, nor the most intelligent, but the ones most responsive to change*".

When you start to look into blockchain technology uses it looks very clear how does it works on cryptocurrencies, but one of the thing that becomes very clear the deeper you see is that the huge scenarios of blockchain technology goes far beyond just the financial value itself. Bitcoin is (currently the best know) usage of blockchain technology and it really changed the game on how people were thinking and adopting the new technology. It's a strong playout with the usage of Bitcoin, but I think this is just the tip of the iceberg and, above all, we will see far more usage beyond the digital currency itself.

5.1 The Core of the revolution

What happened with the blockchain? We are moving from a central control and a central point of failure to a much more distributed environment where we have thousands and millions of nodes talking to each other, working with each other and being fault resistant to a degree that has been impossible to predict before. It is the same story with the internet, instead of having a central control, we have many distributed environment that allow to the survival of the internet even in catastrophic failure scenario. Blockchain technology really allowed to create distributed ledger versus a centrally managed ledger across international organization about boundaries.

The Blockchain Settlement process is very different from what we have used in traditional financial transaction. In the past, we had clearing houses, we had central exchanges (banks or

central banks) managing the transfer of value from one juridical identity to another; on the contrary, in the blockchain process we have true peer-to-peer networking, i. e. the value is transferred peer-to-peer directly from one person to another, everywhere in the world, and then the transaction is validated by the network of blockchain itself.

Thus, Blockchain Technology solves also a lot of practical and technical problem that the internet had from the beginning on, the most important of these is the so called *internet trap*: it solves the problem of transferring value between internet users without having to rely on a third party.

However, from the point of view of practical uses, the benefits of Blockchain secured distributed ledger go beyond the unneeded intermediary in transactions or the possibility of creating a negligible digital assets, in details they concern: (1) the fact that an information on blockchain can never be changed, in fact, one of the key that have made Bitcoin Blockchain so special is the high focus on the immutability, i.e. a record that has been written on the blockchain can never be changed, moreover, utilizing cryptography in this way, creating the blockchain technology, organizations will be independent in creating this new environment; (2) you can create a worldwide ledger, not only organizationally or local ledger, and it can be used for intellectual property, for lend titles, for art and so on, all of these things can now be created and managed across countries boundaries; (3) in the Bitcoin Blockchain there is full transparency for every transaction, who transacts with who, what is the value of the specific good and what have been paid for; last but not least, (4) every information is recorded forever, so we can go back along the chain and make sure that specific block has not been tampered with and we have a complete track of ownership of whatever has been recorded.

Thus, another revolutionary innovation of blockchain consists, as we have already seen, in preventing double spending. If you record a vocal message or take a picture on your smartphone you can share it with your friends, your neighbours, your colleagues, as many times as you want, and all of them can then continue to share that picture again and again, and none of these people sharing the picture are losing anything, so the digital copy is as good as the original, nobody loses value by sharing the digital asset of the picture. On the contrary, it is completely different if I'm attaching the information to a blockchain, in that moment, instead of copying a digital file, I'm creating a unique digital asset. By using the blockchain I'm transferring not only the picture but I'm actually transferring the access right to do anything with this picture, so in that moment I do not have access any more, I lose value.

We can argue that this particular file which has been transferred through the blockchain worth five euros but it has a unique value now because in transferring it, I am giving up access to this

particular digital effort and, like a picture, like a coin, I can really attach any digital asset to a blockchain.

So instead of just sending messages, or copying files, from Mr. A to Mr. B, it really creates a unique digital value in the internet, not a copy, and this create completely new economic models that were impossible before of the emergence of the most popular blockchain technology, the Bitcoin distributed ledger.

5.2 Classification, Security and other "Technical Stuff"

As I mentioned earlier, Blockchain Technology is a Peer-to-Peer network, secured by cryptography and proof-of-work, so that is the foundation. It can be generally divided in three different groups: right now there are (1) Public and Open Blockchains, there are (2) Private Blockchains and there are (3) Government (or Controlled/Fostered) Blockchain.

Bitcoin Ledger is an example of Public Blockchain that works with an incentive model where the miners are getting paid by cryptocurrency; similar with this there is Ethereum, earlier mentioned, which is focusing more about the creation of a smart contract platform going beyond just a value exchange.

If we look at the private use of blockchain technology, there are consortiums, e.g. the consortium R3[119], that is usually mostly driven by US banks (Microsoft is part of them), then we have organizations which are creating their own cryptocurrency, like Citibank who is creating the Citicoin [35], or Goldman Sachs, who is trying intensively to go to that area, or company like Disney that already implemented its own interoperable ledger, called Dragonchain[120]. In particular, Disney creates a blockchain mechanism for internal organizational transfer between organizations, film studios and suppliers, and they also use the Dragonchain technology to track with IoT the whole supply chain that goes to their crew strips; they are really tracking the end-to-end logistics range using the logistic chain through the blockchain technology. Dragonchain's multi-currency directive is probably the most interesting aspect. It's quite possible the firm could issue "Mickey Mouse" tokens, with additional interoperability with assets like Bitcoin. Additionally, the corporation could create loyalty points for patrons visiting Walt Disney resorts and theme parks. Or Disney could create blockchain-based programs for its fast lane

[119] R3 (R3CEV LLC) is a distributed database technology company. It was founded in 2014 by David E. Rutter and It is headquartered in New York City. It leads a consortium of more than 70 of the world biggest financial institutions in research and development of blockchain database usage in the financial system. The consortium's joint efforts have created an open-source distributed ledger platform called Corda [125] especially geared towards the financial world as it handles more complex transactions and restricts access to transaction data. Although it is inspired by blockchain databases, and is expected to have many of the benefits of blockchains, it is not a blockchain. [124]

[120] https://dragonchain.github.io/

feature within Disney theme parks. The platform could monitor ride times and the length of lines in order to create a more efficient process [36].

Finally, we have Government Blockchain. An example of this kind of network is e-Estonia[121], a movement by the government of Estonia to facilitate citizen interactions with the State through the use of electronic solutions. E-services created under this initiative include i-Voting, e-Tax Board, e-Business, e-Banking, e-Ticket, e-School, University via internet, the e-Governance Academy, as well as the release of several mobile applications.

Also the People's Bank of China[122], after assembling a research team in 2014, has done trial runs of its prototype cryptocurrency [37]. That's taking it a step closer to becoming one of the first major central banks to issue digital money that can be used for anything, from buying noodles to purchasing a car. On May 15, 2017, The People's Bank of China (PBoC) announced the establishment of a new FinTech committee. The purpose of the committee is to the augment future regulations and policies surrounding the Chinese FinTech industry [38].

Blockchains can increase security on three fronts: blocking identity theft, preventing data tampering, and stopping Denial of Service attacks. Hackers can shut down entire networks, tamper with data, lure unwary users into cybertraps, steal and spoof identities, and carry out other devious attacks by leveraging centralized repositories and single points of failure.

The blockchain's alternative approach to storing and sharing information provides a way out of this security mess. The same technology that has enabled secure transactions with cryptocurrencies such as Bitcoin and Ethereum could now serve as a tool to prevent cyberattacks and security incidents.

Over generations we have been clear that security is important, so protection has always been a key for anything of value. We can argue that the Blockchain, in a certain sense, is the security protocol of Bitcoin and it is ultimately about collaboration. There is a lot of discussions about incentive models, how to make this happen, but it is a collective effort that makes possible to achieve that goal and the broader the collective is, the more opportunities we will see in the blockchain environment as well.

Many commercial and government services are basically "databases" that are centrally owned and managed. The central database has a lot of advantages from a scalability perspective, from a security perspective and a control perspective, but it also has a single point of failure where people can do malicious actions, in fact, the transactions in a database are recorded in a "Ledger" and that principle hasn't really changed since the seventeenth century.

[121] https://e-estonia.com/
[122] http://www.pbc.gov.cn/

If you think about distributed ledger and blockchain we have unparalleled opportunities, paradigm shift and risk to the business, society and government. All of those we really need to understand slow down and decide what it actually means.

Cyber-currencies and cyber-technologies go hand in hand as the internet evolves, so what we need is clear models to have those conversations. One of these which I think deserves to be mentioned was developed by William Mougayar and looks at six different security levels that we need to consider in the blockchain environment (see Figure 14).

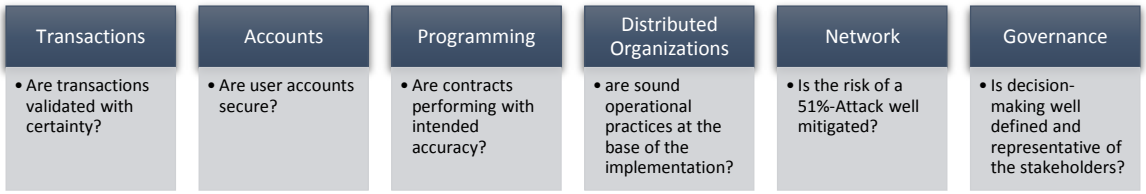


Figure 14 - Blockchain Security Levels [39]

The model looks at first the transaction labels, our transaction valid certainty, then it looks at the actual accounts that people own, how easy are they to protect and/or to break in to manipulate. As we go up to value chain and looking beyond just a few a cryptocurrency, like the Ethereum blockchain that is focusing on smart contracts, we see that programming become a challenge: how are those programs run? how are they controlled? How are they validated? Assuming we can even successful fix that level we have to look at the distributed organizations itself, the network and how decisions are made.

On the transaction level the minimum for a well-functioning blockchain it needs to validate transactions with certainty and predictability at the end of the consensus cycle, it is really important that a transaction is final and immutable, that is one of the big advantages we have with Bitcoin versus traditional transactions.

Many people do not know that if you accept a credit card today, the time it takes until you actually have the money on your account is about 90 days, that is the time it can take for people to dispute the transaction, for banks to validate it and so on; different if you use a blockchain or a Bitcoin transaction: the moment the projection is finalized, right now it can take from 10 to 60 minutes, then you have final proof and final evidence that the transaction is yours, you own it now and it is immutable, it cannot be reversed. The trust in a blockchain environments, that each transaction is immutable, is critical and Bitcoin today has made it as one of the cornerstones.[123]

[123] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 10-21. Available online

The second level is the Account level, where is my account? Is it on my cell phone? Is it on my pc? Is it in the cloud of the buyer? Is it provided by the service provider? How much do I trust that entity that is owning my account?

We have seen more and more hacks in that environment, in fact, one of the big challenge with Bitcoin upfront was really not with the technology itself (the underlying blockchain technology) but it was hacking into those account management providers, meaning that they did not make their account safe enough.

Now assuming we will figure out the account level what about programming?

I mentioned briefly that Ethereum is focusing on smart contracts, e. g. we are creating a business deal that if something specific happens, a payment, for example, is triggered and there is a computer program which at a specific clear date automatically decides if then the amount of payment is released or not released, but autonomy has its own risk, so how do we make sure that distributed organization that play here do not take over the external system?

There are different philosophies and different community approaches, Bitcoin and Ethereum are definitely good case studies there but I think we will see more technologies approaches that are looking at mitigating the challenges you have in a distributed organization.

Then we have of course network challenges. Since Blockchain is physically and virtually a peer-to-peer network, the challenges of networking become really critical; in details, a network that run on consensus method works well if you have only good players, but how many bad players can such a system actually tolerate and still function?

In the Bitcoin environment, as we saw earlier and as mentioned in Satoshi's Paper, we are basically saying that as long as 51% of hashing power in the Bitcoin blockchain are good players they will outperform and keep the system secure.[124]

Theoretically, an attacker can spend enough money in order to reach enough power to "hijack" a specific transaction and validate the process in his favour, but in that process he will destroy the trust into that environment and all the investments that had been done before, so the rest of the system is very motivated to prevent that fraud happening.

If you are going a little bit deeper you may actually find that the power-threshold potentially could be closer to 30%, and it is definitively a real issue. Of course, if you go to smaller blockchains, that are built on the same principle of Bitcoin blockchain, the amount of hashing power needed is much lower there, so they are much likely to be hacked or taken over by a bad player, at least in theory.

[124] F. M Ametrano, *Hayek Money: the Cryptocurrency Price Stability Solution*, August 13, 2016, pp. 10-21. Available online

Last but not least, we have to take care about the Governance Level: how do we actually manage the blockchain? How do we drive it? How do we make sure it stays intact?

It is interesting to see what is happening and how strategic position are taken on the specific blockchain. We have different approach today that we can observe: (1) Bitcoin with no central entity but a lot of discussion group of very passionate people, like Blockchain Education Network[125] and several others in the Bitcoin case, discussing key challenges, like performance costs at the actual block size at this point in time and many other more or less technical issues; on the other hand (2) we have blockchains like the Ethereum's one, also open source but with clear leadership, with a non-profit organization that is discussing and driving; and then we have (3) Private Blockchains centrally managed and controlled by private companies.

5.3 How "real" is Blockchain Technology?

Blockchain is still difficult to understand, it is difficult to use, it is not that easy to buy and today into the different cryptocurrencies' blockchain the perception of the risk by most media it is still like Blockchain is "illegal" and it is the shady business.

On the other hand, there are a studies stating that 20% of UK pounds, as well as many other fiat currencies, is actually used for illegal trading, so anywhere you have money challenges are rising and this should not be discouraging us from looking at the alternative way.

Individual from the broad masses have understood what email can do for them and Facebook as well, but they still do not understand which positive advantages Blockchain technology and cryptocurrencies can bring to them and how all these innovations can make their life easier right now, where that is happening adoptions happen quickly, just take a look at what Tencent[126] dishes in the last couple of years by completely changing how the economy is paying and trading by making easier and integrated into their social experience.

Microsoft was one of the first major IT companies to officially acknowledge the potential of Blockchain technology. They declared that "blockchain" is one of the key "must win" workload for their Azure[127] platform and business and they are investing heavily there.

---

[125] Originally founded as the College Cryptocurrency Network (CCN) in 2014, BEN began as a casual Facebook messenger group between bitcoin club leaders of MIT, Stanford, Michigan, Penn, and Delaware. After ballooning from a handful to over 40 student leaders over a few months, co-founders Jeremy Gardner and Daniel Bloch founded the organization and registered its status as a 501c3 Non-profit.
In 2015, the organization rebrands to the Blockchain Education Network as part of a larger effort to align with the changing direction of the industry. Today, BEN has thousands of members and fans all over the world, including myself.
BEN is made up of students and alumni across the world who are creating bitcoin and blockchain clubs on their academic campuses. By exploring this socioeconomic experiment within the safety of their peers, students build new expectations and innovations. In aggregate, the combined effort of all these clubs creates a rich web of interconnected blockchain hubs across the world. Impact global evolution through local your initiatives. Source: https://blockchainedu.org/

[126] https://www.tencent.com/en-us/index.html

[127] https://azure.microsoft.com/it-it/

Azure was designed to offer affordable solutions to companies that, due to their size, wouldn't have enough resources to launch their own software platforms.

Microsoft Azure already features a wide range of Blockchain solutions, including Ethereum, Chain Core[128], Corda[129], Nxt[130], Lisk[131], and Waves[132]. Together, they form an elaborate ecosystem known as Blockchain-as-a-Service (BaaS)[133], which supports the creation of all kinds of Blockchain projects for all kinds of purposes and for companies of any size [40].

As I mentioned earlier, Goldman Sachs Group Inc., publicly knowledge, invested more than $500 million just in the research of the technology itself, so it is very likely that they will develop their own blockchain and financial transaction mechanism independent from central banks going forward and, this could be one of the reasons why Goldman Sachs, before the end of 2016, has dropped out of the R3 CEV LLC blockchain group.

The R3 consortium of US banks is using the block chain technology in bond trading and it was the hottest topic at the financial innovation (FinTech) forum held in January 2017. On May 23, 2017, R3 has completed the first two of three tranches in its Series A fundraising round, securing USD 107 million in the world's largest distributed ledger technology (DLT) investment to date.

Today R3 is the largest consortium of global financial institutions collaborating to develop a platform and commercial applications for DLT.

At the beginning of June 2017, A number of major Japanese financial institutions have announced the successful completion of testing a blockchain prototype developed using Corda, the blockchain software platform developed by New York-based R3. The blockchain prototype was put to use during the negotiation of an ISDA Master Agreement and it was designed to remove the use of e-mails, in fact, ensuring agreed terms and conditions can be securely recorded and stored on the DLT platform in chronological order. That would make the data storing and management process simpler, while enhancing transparency in the overall process to ultimately benefit negotiations in a derivative transaction [41].

At the beginning of June 2017, The U.S. Department of State has launched Blockchain@State[134], a working group created to "research applications of Blockchain or distributed

[128] https://chain.com/technology/
[129] https://www.corda.net/
[130] https://nxt.org/
[131] https://lisk.io/
[132] https://wavesplatform.com/
[133] BaaS (Blockchain-as-a-Service) is a platform born in 2016 that provides a rapid, low-cost and low-risk platform for organisations to collaborate together by experimenting with new business processes, backed by a Cloud platform, appositely shaped for developers to build DApp (Decentralized Applications) quickly. So now rather than setting up your own Blockchain on Azure platform you can just launch the Blockchain with a click.
[134] https://vsfs.state.gov/projects/view/776

ledger technologies in U.S. foreign policy." The purpose of the project is to use this technology to improve and transform government functions such as international diplomacy.

According to the project proposal, the department recognizes that blockchain technology is a disruptive force that could benefit many industries. Like many private sector innovators, the creators of Blockchain@State believe that although the concept originated with bitcoin, its applications extend far beyond digital currency.

The United States is not the first government to seek to capitalize on the possibilities of the blockchain. Australia's chief scientific research organization recently released two reports[135] recommending increased research and development into trustworthy blockchains.

India is increasingly becoming a hotbed for blockchain development toward solutions both regionally and internationally. On 8 February 2017, the State Bank of India (SBI), India's largest bank, announced the creation of the BankChain[136] Consortium, a platform for banks for exploring, building and implementing blockchain solution, whose main goal is to enhance efficiency and bring transparency and security in the banking industry facilitating information sharing among the banking institutions.

At the beginning of June 2017, BankChain members, that include State Bank of India, ICICI Bank, DCB Bank, Kotak Mahindra Bank, Federal Bank, Deutsche Bank and UAE Exchange, completed their first project called "Clear-Chain", which is a platform to share customer data.

As a permissioned blockchain, Clear Chain will enable banking consortium members who join the ledger to share KYC, ALM and CFT (Know Your Customer, Anti Money Laundering and Countering the Financing of Terrorism) details. The current version of the blockchain facilitates sharing of suspicious transaction reports, investigation reports, KYC data and cross-border wire transfer details, according to the Times of India [42].

As well-known, India is the largest inward remittance recipient in the world and this is the major reason why the India's largest bank is also looking at blockchain technology for the better the receptive system [43].

On June 2017, the consortium has roped in Microsoft as its 'exclusive cloud partner' wherein its 20 member banks will use the Microsoft Azure Blockchain as their underlying blockchain platform. BankChain members and SBI's Collaborative Innovation Center (CIC) will specifically test and validate blockchain pilots on Microsoft's nodes via the Azure cloud. [44]

In the same period, June 2017, the chairman of the Russian government-owned Vnesheconombank (VEB) announced [45] they are planning to implement the blockchain tech regarding project management, which they will start to test this fall.

[135] http://www.data61.csiro.au/en/Our-expertise/Expertise-Strategic-insight/Blockchain
[136] http://www.bankchain.org.in/

This is not the first time that a Russian bank decides to make use of the blockchain technology in the financial sector, other prototypes had already been implemented in previous years and from the statements [46] made in February 2017 by Herman Gref, the CEO of Sberbank (Russia's largest bank) it would appear that other steps will be made in this direction, until arriving in 2019 to legalize and regulate completely blockchain technology, even for commercial applications [47].

In Korea, a pilot blockchain is already being implemented by Samsung SDS, Samsung's IT subsidiary and technology provider for electronic giants, which could revolutionize the Korean shipping industry, notoriously averse to change, as early as the end of 2017.

The main goal of the project will be to simplify the clearance of companies and save logistic costs by tracking imports, exports and the location of cargo shipments in real-time over a blockchain ledger [48]. Even China is moving its first steps in that direction, in fact, rules and standards have been formed for the adoption of the logistics industry.

One of the most revolutionary applications of blockchain technology is taking place in Gyeonggi-do, the most populous province of South Korea, where they developed an online voting system, supported by Blocko[137], a Korean FinTech startup [49]. Here, local residents took the opportunity to vote for community projects that would see funds awarded by the provincial government as a part of the "Ddabok Community Support Project". The success of the blockchain-based vote has already led to interest in the solution from other parties.

Moreover, in 2016, the securities exchange in Korea, Korea Exchange (KRX), launched a blockchain-based marketplace where equity in startup companies can be traded, called the Korean Startup Market (KSM), and also this solution is provided by Blocko Inc. [50].

In Taiwan, Taipei-based OwlTing[138] is an e-commerce platform whose mission is to leverage the concept "from Farm-to-Table" to all industries. They are trying to help millions of small merchants/farmers to make more money and consumers pay fewer by building direct sales relationship. At the end of May 2017, OwlTing claimed to integrate an Ethereum-based blockchain technology solution to its supply chain infrastructure, as a means to improving food safety for consumers: in their opinion the food-provenance-blockchain aims to achieve better transparency, immutability and integrity for a new benchmark in food safety among various food supply chains as well as raising public awareness of the impact of rampant production on the ocean's resources.

[137] https://www.blocko.io/
[138] https://www.owlting.com/intro/home_en

OwlTing expects more vendors to join the platform. The goal is to collaborate on an open supply chain provenance system that provides complete transparency in the production and distribution process of a food supply chain [51].

Even Wal-Mart, the world's largest retailer, is trialling Blockchain for food safety. It is expected that a Blockchain-based accurate and updated record can help to identify the product, shipment and vendor, for instance when an outbreak happens, and in this way get the details on how and where food was grown and who inspected it. An accurate record could also make their supply chain more efficient when it comes to delivering food to stores faster and reducing spoilage and waste [52].

The Department for Work and Pensions in the UK have also trialled the use of blockchain technology for welfare payments. Here, citizens use their phones to receive and spend their benefit payments and, with their consent, their transactions are recorded on a distributed ledger. The aim of the initiative is to help people manage their finances and create a more secure and efficient welfare system, preventing fraud and enhancing trust between claimants and the government [53].

The blockchain technology revolution has brought its benefits to Africa as well. In an interview of Frisco d'Anconia, published on May 2017, Confidence Nyirenda, a Software Engineer that work with a Blockchain firm, said that in Africa there are many opportunities not yet exploited and that thanks to Bitcoin the political control will be limited to the barest minimum, because especially in Zimbabwe for so long government have used money to control inhabitants, since Bitcoin is a currency no one can control [54].

Moreover, it was born BitMari, a Zimbabwe-based organisation and the first black-owned Bitcoin startup founded by African-American Sinclair Skinner and it is making a great distinction in the lives of women farmers. Using Bitcoin, the organisation grants loans to rural women to raise crops, poultry and improve on farming methods. This is really changing the life of a lot of Africans, since before Bitcoin they did not have access to credit or even just a bank account, now they are being able to mechanise their operations in order to make farming activities commercial [55].

In generalized nausea that declares the magnificent and progressive fate of the blockchain, in Italy, notarization is one of the main non-monetary application of the technology used by bitcoin. Its underestimation comes from the confused understanding surrounding the real nature of Bitcoin.

Pioneer of this notarization technique known as timestamping is Peter Todd, one of the most well-known bitcoin developers, assisted by Riccardo Casatta, the Italian startupper who with

EternityWall[139] promotes the blockchain potentialities through multiple applications. Together they standardized the methodology in an open-source protocol called OpenTimestamps[140].
The latest application of this protocol was to "notarize" all the contents of archive.org, the non-profit internet store that catalogues and stores websites (as well as millions of books, videos, music files and software). Archive.org is a time machine for the web: it lets you see what a web page is like at any time in the past. It's like if all new pages published on the internet were automatically filed by an incorruptible notary every day.
In addition, Casatta and its EternityWall have recently helped Intesa Sanpaolo and Deloitte to notarize the bank's transactional database, reinforcing through this technique the satisfaction of the regulatory obligations regarding the preservation and immutability of those data [56].
Carlo Brezigia, Head of Information Security at Intesa Sanpaolo, explains that, with this Proof of Concept (PoC), data is processed to produce a unique identifier in the form of hash or digest so that it matches the input digital fingerprint. This block mark is linked to a Blockchain transaction that allows it to be recorded with Blockchain mode. In this way: the immutability guaranteed by the structure of Blockchain provides a solid and unmistakable timestamping that will always give proof of the existence of some data in its specific state and at a precise moment without any doubt [57].
The hundreds of pilots and proofs-of-concept currently in motion are but a tip of the iceberg when it comes to potential applications.
With regard to Italian excellence in blockchain, it is compulsory to mention Helperbit[141], an Italian platform launched in 2015 a few days after the earthquake in Nepal, aims to solve this problem. It is a peer-to-peer system, based on Bitcoin's Blockchain technology, which aims to monitor the flow of humanitarian aid around the world by making transparent individual cryptographic transactions.
The platform links peer-to-peer donors on the one hand, NGOs and people living in areas affected by natural disasters on the other. Whoever wants to make a donation is enrolled and chooses whether to pay a sum of money to a humanitarian organization or individual damaged users. Through a number of analytical services at various levels, such as graphs and geolocalizations, on the site you will see exactly how the money is allocated.
Helperbit uses only multisigned portfolios, so managers cannot directly access user funds. If the platform were to disappear, everyone could claim their money without any problems. It is

[139] https://eternitywall.it/
[140] https://opentimestamps.org/
[141] https://www.helperbit.com/#home

a system designed to be resilient and secure: this increases confidence, and as a result the contributions.

All of these features and the commitment to achieving goals in order to make the world in which we live a better place brought to Helperbit many important and honourable awards such as being selected by Block Chain Space[142], a focused startup accelerator for talented visionaries creating disruptive solutions to real-world problems using blockchain technology, and by the World Humanitarian Summit[143], which was held in Istanbul, in May 2016. They were also rewarded by Blockchain Hub for the Blockchain Startup Contest[144] and by the German Tech Entrepreneurship Center with the Community Prize[145]. Moreover, Helperbit won the European Competition for Natural Disaster Relief at the D10e contest in Amsterdam[146] and the first edition of the iBank Challenge[147], in December 2016.

Trentino Alto Adige is one of the most active regions that recently started to use Bitcoin and many shops based there accept Bitcoin thanks to the Inbitcoin[148] company. Inbitcoin is the first Italian company to allow merchants accepting Bitcoin in their store, both for B2B and B2C activities. Inbitcoin mainly operates in Trento, Rovereto, Pordenone and Milan but also works with innovative companies based in England, Luxemburg, Malta and Holland.

The main objective of the Trentino company is to create the *Inbitcoin Valley*, and nowadays the project seems to work quite well with more than 50 activities that use Inbitcoin products, people can make gas, eat, buy technology or simply do shopping. The success stories of these early pioneers, regular people and merchants, outside the circle of the first "cypherpunks" have had a quick cycle, thanks also to the Bitcoin growth during the last two years.

Is also thanks to Inbitcoin if Italy has begun to become more interested in this new world, in fact, they are often contacted by research institutions and universities, organizing speeches about Bitcoin and Blockchain across northern Italy [58].

Another Italian *first-mover* was BlockchainLAB[149], it was the first Italian effort that decided to gather the best Blockchain expertise within the Italian country with the main goal of doing research and organizing events related to the tech. It also publishes insightful researches and analysis related to the Blockchain world, allowing an easier access to new products and it also participates directly in venture investments in startups.

---

[142] http://blockchain.space/
[143] https://www.worldhumanitariansummit.org/
[144] http://blockchainstartupcontest.com/
[145] http://gtec.berlin/blockchaincontest/
[146] https://bitcoinmagazine.com/articles/helperbit-uses-blockchain-to-win-european-competition-for-natural-disaster-relief-1457369146/
[147] http://www.abilab.it/ibank-challenge
[148] https://inbitcoin.it/
[149] http://www.blockchainlab.it/

Another noteworthy initiative is the one promoted by Bitcoin Foundation Puglia[150], which aims at the preparation of Italian user guides, as well as the drafting of documents aimed at encouraging and developing a critical legal / economic matrix.

The foundation created at the beginning of 2016, is mainly composed of young boys and girls from Puglia who want to share the potential of this alternative world of payments (and not only) with as many interested parties as possible, collaborating also with the local Università degli Studi Aldo Moro [58].

Also the Italian Five Stars Movement leader Beppe Grillo seems to have found a new application for the distributed ledger [59]. At the end of 2016, in an interview Grillo said that the technology could help political party in expelling unwanted members, in particular, if a Parliament Member you voted for does not follow the program he/she would be automatically expelled, and this could be one of the highest expressions of the concept of direct democracy.

Of course, it was just a joke and nothing has been done at present, but all this makes us very hopeful that the Italian government in a not too long-term future can implement the technology under discussion to solve some political inefficiencies.

On 17 June 2016, during a conference held in Rome, organized by Blockchain Education Network Italia (BEN Italia), a project was proposed for the adoption of blockchain technology within the public administration. In particular, the law proposal (still in draft), also presented by Davide Barillari (at that time Lazio Region Counsellor), was accompanied by an illustration of the benefits that the distributed ledger had been able to bring to the entire political system and specifically to do transactions across Lazio Region, public entities and suppliers, to pay for public services, to certify contracts and documents, to carry out administrative checks, etc. [60]

Still in Rome, on March 30 and 31, 2017, the first Italian hackathon took place in order to promote the innovation of Public Administration services. The event was organized by EY, Microsoft and Digital Magics. At the heart of the battle between developers there was the use of blockchain, understood as an enabling technology that guarantees interoperability, transparency and security in procurement-related processes in the Public Administration.

The goal of these 48 hours of intensive innovation was to enable the PA to promote interaction between various public administrations in a non-institutional co-working space to foster a dialogue between ideas and focus the actual needs of those who will use the services, also providing a prototype solution in just two days, through the exchange of ideas between the experts of the identified subject and the technology experts, with the possibility of creating a contamination between different interlocutors that unlikely in an institutional framework they would have

[150] http://bitcoin-puglia.org/

been able to interact and gain knowledge from the outside context, bringing innovation to the solutions that are needed and actually feasible [61].

At the beginning of June 2017, the evolution of public digital services seems to have made a further step forward. In fact, Designers Italia[151], an Italian community of designers for public digital services, was born during the Digital Design Days[152], thanks to the collaboration between the Digital Transformation Team and Agenzia per L'Italia Digitale[153].

The goal of the community is to focus on the needs of citizens including their point of view in the process of technological change, to stimulate them to approach the digital tools and to link them to the changes introduced by digital transformation plan of the country [62].

Designers Italia is a further goal of joint collaboration between AgID and Digital Team, adding to Developers Italia[154] - the developer community that was born a few months earlier - with which projects will be launched to encourage collaboration between designers and developers. Developers Italia, created from the collaboration of AgID with the Digital Transformation Team, is the developers' community of Italian Digital Government services, a platform upon which to host all the major technology projects in the country. Among other services, it provides: (1) a space on GitHub[155] for hosting the source code and open-source libraries ready for use and integration; (2) an area based on ReadTheDocs[156] for rewriting structured and indexed documentation, designed and written for developers; (3) a newsletter and a space for news, where developers can be updated on new projects and activities; and also (4) an open forum based on Discourse, where developers can freely discuss with colleagues all over Italy and the world. [63]

In conjunction with the birth of Designers Italia, the design of the new portal of the Ministry of Education, University and Research (MIUR) changed with a new graphic identity, easy access to digital services, user centred design and entirely responsive. The new MIUR site[157] is implemented in accordance with the Design Guidelines for PA's web services[158] of the Italian Digital Agency [64].

Over the last few years, Italy now demonstrating how Bitcoin could be an easy and faster method of payment in a few sectors, for instance, booking a taxi, in fact, in Rome, taxis even

[151] https://designers.italia.it/
[152] http://www.ddd.it/it
[153] http://www.agid.gov.it/
[154] https://developers.italia.it/
[155] https://github.com/italia
[156] https://docs.developers.italia.it/
[157] http://www.miur.gov.it/web/guest/home
[158] https://design-italia.readthedocs.io/it/stable/

started to accept Bitcoin through a platform called Chainside which creates an invoice to be paid in Bitcoin by the final user [59].

Thanks to the BitTaxi[159] payment system, who buys a ride from the app or the it Taxi[160] site can choose Bitcoin's cryptographic currency as a mode of payment. Then the driver will receive the payment in euros.

The initiative started with the Cooperative Radiotaxi 3570 and are now they are trying to implement the bitcoin payment system also on POS on board the cars [65].

In the food sector, especially in the wine sector, surprisingly Italy is among the first in the world to implement the use of blockchain. EY[161] creates the Wine Blockchain with the goal of certifying and communicating the quality and geographical origin and production of wines made in Italy. Involved in this project also the EzLab[162] startup.

This is the first case of a digital relationship between the producer and final customer who - by using his/her own smartphone to scan the QR Code printed on the wine label - can read about the wine producer (identified by a digital signature), the entire process of cultivation, production and processing of wine maximizing the trust of the consumer.

The first tracked and certified product is the Falanghina Wine produced by Cantina Volpone[163], and it is already possible to buy it online.

This “digital ID card” is an opportunity to fight against the dumping in prices created by foreign products or "fake Italian" and to create a recognition and promotion mode for Made in Italy wines and not only; Blockchain's applications could go beyond the wine-growing sector as a digital product identity card could be useful to the whole Italian agri-food business, especially in the fight against dumping, the phenomenon of "false Italians" and counterfeiting.

In addition to that in the wine sector, Italy has another first place at the world level, but this time in the real estate sector. It is in fact in Italy, precisely in the San Lorenzo district in Rome, which you can buy 123 apartments with virtual currency.

The novelty is made possible by a resolution of the Agenzia delle Entrate of September 2016, which has recognized bitcoins as a foreign currency, making it possible to use it in a notarial act. The announcement was made on April 6, 2017 by a real estate company, the Barletta Group, which strongly believes in Bitcoin [66].

[159] http://www.bittaxi.it/
[160] https://www.ittaxi.it/
[161] http://www.ey.com/
[162] http://www.ezlab.it/
[163] http://www.cantinavolpone.com/

Blockchain-based systems have the potential to enhance the efficiency of procurement, logistics and payment processes, reduce manual processing of import/export documentation, ensure conformity and delivery of goods and prevent losses, thus generally reducing costs, improving safety and security, and minimising fraud. They can also provide the means to verify the authenticity, origin and ethical standards of goods and services. Transparent and traceable ownership histories would reveal any historical fraud, theft, use of forced labour, links to violence, drugs or arms trafficking or other dubious practices, improving the capacity to enforce the law and enabling more responsible consumption. However, there are reasons to be cautious. Trust between participants depends on trust in blockchain technology, but this is not completely free from vulnerabilities, including both accidental errors and malicious attacks. Automation will not guarantee the elimination of bugs, conflicts of interest or corruption in complex global supply chains.

5.4 Blockchain Technology in 2018 and beyond

I think blockchain technology is going to revolutionize the world economy, we will create completely different trust models through peer-to-peer mass collaboration creating new economic models over the next five years and sophisticated computer code rather than through central powerful institution (bank or government) will take over making the world more efficient and enable this new scenarios, exchanging transactions, finance, business, international collaborations and government's economic tools.

According to Nicolas Cary, Co-Founder and CEO of Blockchain, "Check it on the Blockchain" will be the phrase of the 21st century, an expression soon as banal as the today-phrase "I read it on Google".

Commentators often compare the technical development and stages of public adoption of bitcoin to the development of the Internet, in my opinion the development and adoption of the blockchain is akin to that of the Internet. Bitcoin is simply one application, a payments application of the blockchain technology on which it runs.

In an attempt to predict what benefits blockchain technology could bring in the future to the world we live in, a good starting point is to analyse its strengths that have made it one of the most extraordinary innovations of this era.

In its Decentralized Cloud function, blockchain also allows users to choose to "rent" their excess storage space, almost like the AirBNB style, enabling new markets to be created. In addition, this solution would significantly reduce the cost of storing data for businesses and private users.

Decentralized apps will come in different flavours, sizes, and complexity levels, so we must be prepared for that variety, and we must see beyond the bitcoin promise to be the Internet of

money, and into the blockchain's promise to become a new development environment, just as web development was the new paradigm back in 1996.

Blockchain as an immutable ledger of encrypted information could also lead to the end of patents: if we assume the case, for instance, of a company that would like to prove the creation of a specific technology at a given date without the filing of a public patent, when someone disputes the ownership of that technology, it could then be proved by internal documents linked to the transaction hash, existing at the date specified on Blockchain.

In fact, blockchains allow not only to trade, but to make economic relationships, collaboration agreements and professional relationships valid without requiring a third party to certify this validity. Thus one of the main collateral effect of a world based on blockchain could be the decreasing relevance of notaries, lawyers, accountants, and all those figures that place right now the agreements and transactions verification feature [67].

The automation of the vote count of cards is a breeze for the improvement of the cost, the time and accuracy. However, previous systems have been undermined by technical issues. The main problems are the inability to verify the accuracy of computers during the recapture of votes and their being the main targets for hackers. It is not strange, in fact, that political parties have already addressed Blockchain for their own domestic elections (we may think to what happened in Denmark in 2014 [68]) and not only, as we have already seen in the Korean case.

Since each block contains a hash value of its content, and the content also includes the hash of the previous block, any modification of a block inside the chain yields a change
of its hash, which would in turn require modification of all subsequent blocks, this means that changing a vote already in the chain requires millions of votes to be changed before another vote is cast. The network is protected by the simple fact that no hacker has enough computing power to rewrite so many votes so quickly.

As for the truth, Blockchain allows any vote to be publicly shared without identifying the voter. So any voter could check if his vote was counted from public registers. Moreover, this could someday eliminate electoral corruption in developing countries [69].

Blockchain forces to rethink the same bank transactions.

Of course, for each transaction that uses a distributed ledger instead of a traditional centralised system, the intermediaries and mediators are displaced, missing out on their usual source of power and income. For currencies these are the banks, for patents the patent office, for elections the electoral commissions, for smart contracts the executors, and for public services the state authorities. A significant level of growth in the use of blockchain technology, could see substantial change in the substance and, perhaps, quantity of 'white collar' work [70].

Another interesting point about the future of the blockchain is the legal aspects. The existence of public and private networks creates an unusual situation (for a technology) and therefore will need to use two different approaches. If on the one hand it will not be difficult to set up laws on the development of private blockchains, on the other hand, public blockchains according to their uses are not so easy given the international and open-source nature of their distribution.
Moreover, it is not even possible to apply the jurisdictional laws of the domicile of the creator, since no one knows the Satoshi Nakamoto provenance, neither of the domiciles of the apps creators, since they can be launched from anywhere, by anyone. Thus, the regulators have no choice but to let the market decide and simply assume the role of seal of confidence.
The EU appears to be following this path. Its innovation-first philosophy could end up supporting development from two angles: 1) encouraging the exploration of use cases to test impact and laws, and 2) giving entrepreneurs confidence that their 'approved' applications will be more trusted by their target markets [70].
This approach could end up making Europe a prime destination for blockchain development, as businesses choose the continent for their domicile and as talent flocks to the area.
Hopefully, the economic boost would inspire other areas to adopt similar measures. Shedding defensive regulation in favour of a more supportive approach could change the perception businesses and citizens have of their government [71].

6 Crypto-currency: work in progress and how they are transposed into national legal systems

In a few fields, such as that of study of money, a recent acceleration and a sudden change in the positions of doctrine and jurisprudence have been seen. Perhaps the reason is that this evolution has undergone the influence of new technologies in the field of digital data transmission and their speed of evolution.

Nevertheless, the resulting barriers to entry and climate of legal *stigma* are stifling the nascent decentralized technology industry and preventing further innovation. In response, the decentralized virtual currency industry and other businesses interested in exploring the potential uses of decentralized technologies in commerce call for self-regulation; notwithstanding, history intimates that the self-regulatory approach is unlikely to sufficiently resolve the market failures that will ultimately allow illicit and fraudulent uses of decentralized technologies to occur.[164]

From an economist point of view every restriction (and forced inefficiency) comes with a cost, so it is just a question about "who is carrying the cost?". Every time you make a restriction and regulation it comes to the cost to somebody and you just have to make sure the society would clear what it means and if we are willing to have that group pay that particular cost.

Due to the absence of intermediaries, virtual currency transactions can currently be achieved at lower costs than other means of payment, such as payment cards or bank transfers. This is partly due to the absence of any regulatory requirements that would guarantee the safety of those means.

Virtual currencies can also be less expensive for merchants as payees as well as for payers to whom transaction costs may be partially passed on.

Although reliable and independent data on the exact costs of virtual currency transactions is difficult to ascertain, some anecdotal suggestions have been made that average transaction fees on the Bitcoin network tend to be less than 0.0005 BTC, or 1% of the transaction amount. This compares with 2%-4% for traditional online payment systems or an estimated 8%-9% for remittance without involving bank accounts via money transmitters.

Transactions within or between virtual currency schemes are also not subject to the exchange fees applied to conversions for transactions with third countries, therefore providing further potential for cost savings, (although conversion fees would typically apply as and when virtual currency are exchanged against fiat currency or vice versa). The increase in competition for

[164] S. Pepe, *Investire Bitcoin*, November, 2014, Priulla, Palermo, pp.19-80

transaction services may also have a cost reducing effect on the costs of conventional transactions in fiat currency.

Almost all governments and organizations understood that there is essentially a digital value system beyond the nation-state, the central banks are very concerned about it, as soon as they start to understand it, and the question is only how is it going to happen? Is it going to be an open source environment? Is it going to be government controlled environment? Is it going to be one of those existing systems that are emerging, like Bitcoin or Ethereum? Is it maybe Goldman Sachs that is investing heavily into the blockchain technology already? Is it a mother of coin or technology that is just emerging right now? We cannot know it now, but I think this is what for sure we will see in the next years.

6.1 Is Bitcoin legal?

The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them.

While some countries have explicitly allowed its use and trade, others have banned or restricted it, in particular following the Mt. Gox disaster in 2014, and the reasons of ban are different from each other and sometimes seem counter-logical.

Right now, Bitcoin is still illegal in a few countries throughout the world, including Bolivia, Vietnam, Kyrgyzstan, and Bangladesh.

In Africa, the Central Bank of Nigeria (CBN) on January 2017, has passed a circular to inform all Nigerian banks that all transaction in bitcoin and other virtual currencies have been banned in Nigeria. [72] While, in December 2014 the Reserve Bank of South Africa issued a position paper on Virtual Currencies whereby it declared that virtual currency had "*no legal status or regulatory framework"*[165].

The Reserve Bank of Zimbabwe is sceptical about bitcoin and has not officially permitted its use. On 5 April 2017 however, BitMari, a Pan-African Blockchain platform got licensed, through its banking partner, AgriBank, to operate in the country, as I already mentioned in Chapter 5.

In North America, more precisely in Canada, Bitcoin would seem to be classified pursuant to the current provisions of the Personal Property Security Act simply as an "intangible" [73]. By the way, Bitcoin is regulated under anti-money laundering and counter-terrorist financing laws in Canada.

[165] South African Reserve Bank, National Payment System Department, *Position Paper on Virtual Currencies*, Position Paper N. 02/2014, December 3, 2014, p.2, Available at: http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf

In United States the situation is a little bit more complicated and there had been several upgrade of the legislative set of rules, which somehow influenced the history of Bitcoin and its evolution over time, as you will see later in this chapter.

For the time being, know that not all states were friendly and welcoming with digital currencies. At the moment, the U.S. has shown very little interest in legalizing bitcoin. This can be seen by the fact that in March 2017, the Securities and Exchange Commission (SEC) rejected the bitcoin exchange traded-fund (ETF), the first of its kind, proposed by the Winklevoss Twins[166]. [74]

If we move to Central and South America, we found Countries where since 2014Bitcoin has been banned by national authorities, like in Bolivia and Ecuador; this latter not only banned Bitcoin and all other cryptocurrencies, but it did so while establishing guidelines for the creation of their own virtual currency.

It is in fact not so long ago, precisely in May 2017, that the Bolivian Financial System Supervision Authority (ASFI) arrested 60 people for carrying out "training activities" related to the investment in virtual currencies such as bitcoin, according to Functional a press release [75] published by ASFI.

Furthermore, at the end of 2016, also the Latin American nation of Colombia has declared Bitcoin illegal. By doing so, the country has included itself into a list of handful nations that have taken such a step.

However, it is actually possible to trade Bitcoin in the other countries of this part of the world, even if sometimes it is not regulated at all.

Neither in Israel, nor in Lebanon, nor in Jordan the Bitcoins have been banned, but all the three nations of Western Asian issued a warning discouraging the use of bitcoin and other similar systems in 2014, as well as among the nations of southern Asia, except for Bangladesh that, since 2014, banned its use saying anybody caught using the virtual currency could be jailed under the country's strict anti-money laundering laws. [76]

Eastern Asia is one of the main supporters of the cryptocurrency with the booming investment culture in the region, where it is common to swap investment tips. According to a ranking by CoinMarketCap[167], China, Japan, and South Korea are home to several high traffic cryptocurrency exchanges.

As one of the largest economies in the world, China couldn't get aside of the Bitcoin legislation battle. While China is the centre of Bitcoin mining industry today, financial organisations such

[166] This was because the SEC did ‘not find the proposal to be consistent with Section 6(b)(5) of the Exchange Act, which requires, among other things, that the rules of a national securities exchange be designed to prevent fraudulent and manipulative acts.

[167] https://coinmarketcap.com/

as banks or hedge funds can't hold or transit bitcoins, while individual users in their turn are able to store, exchange and trade bitcoins freely.

It's clear that Bitcoin would be a part of the government financial regulation one day, but should almost never become a legit currency alongside Yuan in China, on the contrary, according to the current regulations, it's more likely for China to invent their own cryptocurrency based on the blockchain technology.

As of January 2017, Chinese government issued a statement that warns those to attempt to use Bitcoin of its potential risks [77]. Anyway, China is investing heavily and a tangible proof of that is Shenzhen: it is a city located immediately north of Hong Kong Special Administrative Region, 35 years ago it was an ordinary little village but today it is at least a 12-million-people-city creating a completely new development zone. It is focusing on digital currencies experimentation zone and a financial zone and all the key players are in that area, giants like Tencent (WeChat pay), Huawei (Cloud and Network) and The People's Bank of China, and they are really focusing on collaborating and creating the next version of the digital environment.

For a person who has not yet realized the innovative magnitude of digital currencies, it is a good start to really see what is happening on the other side of the Pacific and how much focus is happening on innovation there.

Regarding the People's Bank of China, after a process that began in 2014, the institute, in the first half of 2017, is taking a step closer to becoming the first major central bank to issue digital money, developing their own digital currency, and at the same time they are increasing scrutiny of bitcoin and other private digital tenders, in order to not cede the cryptocurrency space to companies they have no control over but also to foresee the likelihood of a bitcoin bubble to blow up. So if you can't beat them, join them [17].

In January 2016, the PBOC said it will have its own cryptocurrency "soon", but there has still been no formal start date announced [17]. Thus, it is likely that the use of digital currencies such as Bitcoin will be banned in the country and that the official digital currency developed by China's Central Bank will be used.

After a crackdown at China's Central Bank earlier this year, more investors in Japan and South Korea turned to the cryptocurrency. According to the media publication Reuters, the increased Japanese and Korean investment had an impact on bitcoin's surge in 2017. [99]

From April, 2017, Japan legalized bitcoin as a payment method through a text [97] released by country's Financial Services Agency. Virtual currency was described as having asset-like values, limited to items that are electronically recorded excluding Japanese currency, foreign currency and currency-like denominated assets. The fact that it is usable as payment, resulting in more bitcoin being bought with yen. In July, Japan will also stop imposing the 8% consumption

tax on bitcoin buying through exchanges. The move to end this taxation will almost certainly increase adoption and demand of bitcoin among adopters in what is already one of the world's top three bitcoin trading markets.

Moreover, the government of Japan has set a growth strategy for financial technologies (FinTech), one that aims to double the adoption rate of digital payments over the next decade in the country. In the development of the strategy were involved the Japan's Financial Services Agency (FSA), the country's financial regulator, and the Ministry of Economy, Trade and Industry (METI), and it was planned to be compiled before the end of June 2017.

Earlier in May, Japan's Peach Aviation, a budget international airline that flies to multiple countries in the region, became the first airline in Japan to accept bitcoin, a service that will enable travellers to buy air tickets with bitcoin by the end of the year. According to a report [97] by The Asahi Sumbun, Peach Aviation plans to install two-way (BTC/JPY) bitcoin ATMs near ticketing counters "at multiple airports".

Also the government of the Japanese city of Hirosaki is accepting bitcoin donations in its effort to preserve and maintain a popular cherry tree park. Donations will help preserve 2600 cherry trees of 50 different varieties and the 400 years-old Hirosaki castle at the park, by repairing its stone walls. [98]

South Korea is planning to introduce regulations on the digital currency in 2017, according to regional publication Korea Joongang Daily [100].

In Europe, the national legislative framework is very varied, however, at the time of writing, no country prohibits the use of Bitcoin, as well as in Oceania. Even in Russia, which had previously banned the use of Bitcoin, but as of November 2016 declared, bitcoins are "not illegal" according to the Federal Tax Service of Russia [78].

Also the Banca Naţională a României (BNR), the central bank of Romania, has ruled on the use of bitcoin as a payment instrument. In an official notice [79] in 2015 the Institute warned the public about risks in using digital currencies and still in June 2017, BNR has not changed its attitude, despite the developments on the subject, they have tightened its character against cryptocurrencies: "*The National Bank of Romania maintains its previously communicated views and continues to warn users of virtual currency risks that they face. Virtual currencies have a very high volatility and a low security relative to currencies issued by central banks and regulated transparent electronic currencies. Virtual currency holders have no guarantee that it can be used for buying goods and services in the future as legal tender*"[168].

[168] Banca Naţională a României, Bucharest, March 18, 2015, *Comunicat referitor la schemele de monedă virtuală*, 2015

6.2 Historical highlights of the bitcoin normative evolution in the world

Academics predict that the blockchain and similar technologies will revolutionize the way people order their affairs and conduct transactions through the evolution of smart contracts, decentralized autonomous organizations, distributed property registries, and distributed and secure data stores. Although similarly captivated by these developing technologies, governments, individual regulators, and various policy makers remain less optimistic that the good contributions of the technology will outweigh the way bad actors use the technology for illicit purposes. Over the years, from the time they are created until now, Bitcoin have been the focus of heated debate, especially legal and regulatory.

If on one hand, payment with bitcoin is assumed to be a transparent and neutral payment method, available everywhere with lower transaction fees and without the need to disclose a party's identity, on the other hand, it is spontaneous to have doubts about the efficiency of digital identities, about privacy and cyber-security, without mentioning the fact that the market value of bitcoin is highly volatile.

All of these issues raise the question whether the use of bitcoin should be regulated and if so, to what extent?

The ways in which the various governments of the world are confronted with the question are varied, but above all, they changed and evolved over time and under varying circumstances, as it should happen in front of an innovative technology of this magnitude

The first official document about cryptocurrencies is perhaps that one issued in October 2010 by the Financial Action Task Force (FATF), an inter-governmental group based in Paris and whose purpose is to develop and promote policies to prevent money laundering and funding of terrorists. The report entitled *Money Laundering Using New Payment Methods* [80], warned consumers in using digital currencies like favourite instrument to finance terrorist groups. About a year after the publication of the report Silk Road opened for business, and soon became the most famous Bitcoin marketplace for illicit drug deals [81].

The same year of the birth of Silk Road, Bitcoin reaches the parity with US Dollar at Mt Gox (February 9, 2011), and passes the parity with Euro and the British Sterling Pound (April 2, 2011), while the value of Bitcoin money stock passes US $ 10 Million.

Europe seems to have been among the earliest continents, in fact, before the end of 2012, Bitcoin Central becomes the first bitcoin exchange to be licensed as a European bank, operating Within the European regulatory framework, as we saw in Chapter 4, while we have to wait until March 2013 to learn about the position of Financial Crimes Enforcement Network (FinCEN) about virtual currencies [82].

As early as April 2012, the FBI published a document [83] highlighting its fears around bitcoin. It voiced concerns that while US-based exchanges are regulated, offshore services may not be, and could be a haven for criminals to use bitcoin for illicit activities without being traced. In particular, in the dossier, the Agency stated that "*Bitcoin will likely continue to attract cyber-criminals* […] *if Bitcoin stabilizes and grows in popularity, it will become an increasingly useful tool for various illegal activities beyond cyber realm"*[169].

On July 23, 2013, furthermore, the U.S. Securities and Exchange Commission (SEC) published an article [84] on its website with the main aim to alert investors in using virtual currencies. The article, drawn up by the Office of Investor Education and Advocacy, was an investor alert to warn people about fraudulent investment schemes involving bitcoin. In particular, it warned of Ponzi schemes, after charging Texas resident Trendon T. Shavers (aka 'pirateat40'), founder and operator of "Bitcoin Savings and Trust", with allegedly raising 700,000 bitcoins by promising investors up to 7% weekly interest.

In addition to this article, until 2014, the Commission had not issued solid regulations on virtual currencies but the SEC case has forced the legislative branch of government to consider bitcoin's legal status.

The US Department of Homeland Security was the most worried about the criminal threat from illicit use of bitcoin, while the Department of Justice, the Federal Reserve and the Department of Justice all acknowledged the legitimate uses of virtual currencies. The SEC argued that "*any interests issued by entities owning virtual currencies or providing returns based on assets such as virtual currencies*" were considered securities and thus fell under its remit [85].

Each US State has their own financial regulators and laws and, as I mentioned earlier, each State approached bitcoin differently. In 2013, there were both more aggressive States, like California and New York, as well as States that preferred to wait and see how the situation had evolved, like New Mexico, South Carolina, and Montana.

In particular, the California's State Financial Regulator issued a (almost threatening) letter to the Bitcoin Foundation warning it that the Bitcoin's transactions may be understood as money transmission business, and threatening people there with potential fines and jail time, while, the New York Department of Financial Services, at first defensive, then decided to partner with 22 companies bitcoin-related, asking for a dialogue to develop appropriate regulatory guidelines for the digital currency industry[170].

[169] F.B.I., Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity, April 24th, 2012, Intelligence Assessment, pp.2-3

[170] Also the US private banks, at first reluctant, stopped accounts owned by people operating bitcoin exchanges.

Perhaps one of the most important stages in the "acceptance process" of Bitcoin dates back to August 6, 2013, when, in the proceedings [86] move by the SEC against Trendon Shavers, accused for allegedly running a Bitcoin Ponzi scheme through His Texas-Based "Bitcoin Saving & Trust", the Magistrate Judge Amos Mazzant of the Eastern District of Texas declared for the First time that "Bitcoin can be used as a money".

During the trial, Shavers had defended himself by saying that the SEC should not be able to prosecute him since Bitcoin was not money or part of anything regulated by the United States, but the judge sided with the SEC [87] and gave bitcoin his first stamp of approval as real world money as it is used to pay for individual living expenses.

In particular, there is a passage of the judgment in which the court clarifies all doubts about their use: "*It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money …"*[171].

In September 2013, virtual currencies emerged as one of the many innovations the EBA was monitoring at the time, and after three months of studies and analysis the EBA issued a public warning on 13 December 2013, making consumers aware that virtual currencies are not regulated and that the risks are unmitigated as a result.

More than 70 risks were identified across several categories, including risks to users or risks to financial integrity, such as money laundering and other financial crime. Risk that were confirmed in the months following the publication, as a market-leading exchange (Mt. Gox) had to close due to mismanagement, cyber-attacks and theft of a substantial amount of Bitcoins, etc.

To find a solution to the issue of whether virtual currencies can and ought to be regulated, the EBA carried out additional analysis during the first half of 2014 issuing a paper [83] in which they specified the potential benefits, such as transaction costs, transaction speed and financial inclusion outside of the EU, furthermore, the report continues also by identifying the main risks arising from virtual currencies.

At the beginning of 2016, after the terrorist attacks in Paris in November 2015, a Europol report [88] stated a review of EU member states and the Europol about Islamic State's operations. They did not found confirmed evidence that suggest Bitcoin is used for terrorism financing. Furthermore, the European Union's law enforcement agency stated that the sources of funding of ISIS operatives in the European Union "*are largely unknown*". An excerpt from the report

[171] United States District Court, Easter District of Texas, Sherman Division, August 6, 2013, case n. 4:13-CV-416, in *SEC vs. Trendon T. Shavers and Bitcoin Saving and Trust*, 2013, p. 3

read: "*Despite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement*"[172].
Also the HM Treasury Department of the UK government offered a deduction similar to the one established by Europol and EU member States through a report [89] issued on March 2015, where they confirmed no evidence of a link between bitcoin and terrorism financing[173].

6.3 What about Taxation?

Income that is earned through the exchange of services with another person, whether in the form of bitcoins, dollars, euros, or barter; is included in gross income, and would be subject to income tax at applicable rates. Also these bitcoins could be subject to self-employment tax. In some jurisdictions, income earned through the process of buying and selling bitcoins would also be included in gross income, but would be treated as capital gains. This interpretation is based on the assumption bitcoins are treated as a store of value such as gold, or other such commodity. If instead they are treated as a currency or debt, the full gain could be taxed based on market value at the end of each tax year.
In international standard, in particular with 3858 IRS ends Currency ETN advantage by simply putting the ETNs at a slight disadvantage for most investors. The IRS never considers currency a long-term investment. Consequently, if bitcoins are treated as a currency, you will be taxed the same as holding an account in any non-functional (foreign) currency.
In 2014 the Internal Revenue Service ("IRS") announced that it intended to treat convertible virtual currency – like Bitcoin – as property for tax purposes.
Notably, the IRS has taken the position that convertible virtual currency is considered property – not currency – for tax purposes. [90] As a result, the tax consequences from transactions involving Bitcoin turn on general principles applicable to the taxation of property transactions. The treatment of virtual currency as property rather than currency is important for a number of reasons, some of which are not readily apparent from the IRS Notice 2014-21[174], in fact, they cannot result in a foreign currency gain or loss for U.S. tax purposes. Moreover, when crypto-currency is sold in exchange for real currency the transaction should, presumably, be treated as the sale of intangible property rather than an exchange of currency, while it is exchanged for goods or services the transaction should, presumably, be treated as a barter transaction. [91]
Taxpayers must keep careful accounts of basis. Yet the Notice does not indicate what type of accounting method should be used with digital currency, Last-in, First-out, First-In, First-out,

[172] Europol Public Information, The Hague, January 18, 2016, *Changes in modus operandi of Islamic State terrorist attacks*, 2016, p.7
[173] HM Treasury Department of the UK government, London, March, 2015, *Digital currencies: response to the call for information*, 2015, p.11
[174] Available at: https://www.irs.gov/pub/irs-drop/n-14-21.pdf

or some other method, while mining equipment can still be deducted as a legitimate business expense. [92]

On June 2, 2017, U.S. Congressmen Jared Polis, a Colorado Democrat, and David Schweikert, an Arizona Republican have written a letter[175] to the Internal Revenue Service (IRS) Commissioner John Koskinen asking for additional guidance for reporting virtual currency transactions. They acknowledged the agency has offered taxpayers some virtual currency guidance in regard to taxation, but additional guidance is needed to assist businesses that accept virtual currency. [93]

What about taxation in Italy? a few months ago Italy decided to regulate Bitcoin as a currency, as the Italian tax agency, Agenzia delle Entrate, published a paper titled "Bitcoin and digital currencies buying and selling: clarification on the tax treatment" about the fiscal regulation of Bitcoin and how VAT would be applied to cryptocurrency transactions [59].

The Central Directorate of Agenzia delle Entrate, Resolution No. 72/E [94] in September 2, 2016, thus responded to a taxpayer's request for direct and indirect taxation relating to "bitcoin purchase / sale transactions". In particular, mentioning the principles expressed by the European Court of Justice (C-264/14), in terms of indirect taxes (VAT), the Agency specified that "*transactions consisting in the exchange of traditional currency against units of bitcoin* [...] *constitute provision of services on a fee-paying basis.*"[176]

In the light of Article 135 (1) (a) of Directive 2006/112 / EC, it is "*plain that the virtual bitcoin currency has no other purpose than that of a means of payment and that it is accepted for that purpose by some operators.*"[177], consequently, those transactions, as far as the VAT is concerned, are to be regarded as exempt (Article 10, paragraph 1, No 3, D.P.R. No 633/72). [95]

Therefore, the performance in comment is true that it does not fall into the category of so-called traditional coins, but will have to be classified into the cluster of currency-related financial transactions, so the activity will be VAT-free.

From a point of view of tax compliance as a tax substitute for natural persons, for the company operating in the field of the sale of bitcoin, currency (purchases and sales) activities "*do not stimulate taxable income due to the reason that it lacks speculative purposes*", while the same

[175] The letter is available at the following web-site:
https://polis.house.gov/uploadedfiles/060217_ltr_irs_digital_currency.pdf

[176] Agenzia delle Entrate, Direzione Centrale Normativa, *Trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali*, Risoluzione N.72/E, Roma, September 2, 2016, p. 3

[177] Council of the European Union, Official Journal of the European Union, *COUNCIL DIRECTIVE 2006/112/EC of 28 November 2006 on the common system of value added tax*, November 28, 2006, p.

company must comply with anti-money laundering requirements (Article 11 (2) (c) of Legislative Decree No. 231/2007[178]) by means of an "*adequate customer verification, registration and reporting*". [96]

The companies who are holding the Bitcoins, instead of the individuals, the Agenzia delle Entrate resolution indicates that the revenues from intermediation in the purchase and the sale of the Bitcoins are being subjected to the IRAS and also the IRAP, net of the related costs. This is a serious disadvantage for the companies who hold the Bitcoins for their certain activities and who will have to pay the taxes onto the profits not yet realized but only just estimated, since any of the unrealized capital gains and even the losses are arising from the difference between the purchase rate cost and the evaluation at the very end of the year will subject to the capital gain taxation.

6.4 Checks, Bank Transfers and Bitcoin

Over the years, the attention of scholars has focused on identifying the most common forms of currency alternative to cash in order to define its scope and to regulate its effects without ever having to estimate the extent to which they are positioned outside the payment system normally identified; on the contrary, that is exactly the opposite of what is happening with cryptocurrencies. In other words, the question raised concerns the definition of the possibility for the creditor to refuse payment of the monetary debt which the debtor intends to carry out rather than in circulation (banknotes or coins), otherwise by means of alternative means of payment (circular, bank account, wire transfer, or crypto currencies, as in our case).

As in the case of digital currencies, when large-scale innovation has to be implemented at the regulatory level in individual State systems, the institutions that deal with large agglomerations, as in the European case, are in great difficulty. Both because they are entering into uncharted legislative areas, but also because the directives will have to be homogeneously transposed by the various States that are part of the agglomeration and characterized by pre-existing inhomogeneous sets of laws.

In this part of the thesis, I will try to explain how an innovative payment system, specifically Bitcoin, can be transposed into the Italian system, starting with a more or less exhaustive explanation of the current regulatory framework in Italy regarding payment systems.

In Italy, is known a very clear position that sees a slavish identification between the expression "legal currency", contained in particular in the article 1277 of the civil code, and the physical currency, i. e. banknotes and coins. This statement has never been changed since its first writing in 1942, although this identification has already been overcome some decades ago with the

[178] http://www.gazzettaufficiale.it/eli/id/2007/12/14/007X0246/sg

widespread use of dematerialized currency for the fulfilment of pecuniary obligations; furthermore, these principles can claim to be acquired for the obvious practical use of alternative forms of money transmission in a context in which the distance purchases of goods and services are becoming the rule rather than the exception.

It should be observed that the monetary obligations are essentially characterized as currency debt because the debtor, since the rise of the mandatory report, will have to comply by paying a certain sum of money. Pecuniary obligations are governed by the nominal principle, according to which the fulfilment of the obligation occurs with the payment of the currency having legal tender in the state, in the amount originally established.

The business world has identified, as noted above, other non-cash payment instruments: think of the debt securities, to ATMs, credit and debit cards, the poste pay, etc. Although corresponding to different business logic, these assumptions are characterized by the payment function recognized by the legal system. By convention, therefore, a check is equal to the amount of money shown therein.

First of all, you need to assess whether the delivered check made by the debtor is liable to extinguish the original obligation in question in the contract, as is the delivery of cash. The execution of pecuniary obligations by means of payment other than money has been the subject of numerous judgments by Corte di Cassazione, which, since the first years of the entry into force of the Civil Code, provided an unambiguous interpretation of the aforementioned standards.

As regards the question arose, over the past years, a jurisprudential conflict, then settled in 2007 by the United Sections of the Supreme Court regulator, which have recognized the effectiveness *solutoria* of alternative means of payments that, such as checks, eliminate physical transfer of money [97].

Therefore, since the subject of the payment is not the currency with legal tender but the monetary value or the amount of money, the debtor's delivery of the bank check is thus not an alternative means of fulfilment falling within the schema of the *datio in solutum* ex art. 1197 civil code but a different mode of payment [98].

In particular, a 2012 update [99] specified that "*The extinction of the obbligation with the release effect of the debtor occurs* [...] *when the creditor concretely acquires the legal availability of the sum of money, falling on the debtor the risk of the inconvertibility of the check*"[179].

Once again, if we look at the current world of payments as a whole, one can only acknowledge that the traditional scheme that the fulfilment of the pecuniary obligation occurred through the

[179] Cfr. Corte di Cassazione, Sez. III Civile, 9 ottobre 2012, n. 17146

material transfer of cash, carried out by the debtor through the physics delivery of banknotes in the hands of the creditor, it is now inadequate to express the actual legal content of the pecuniary obligation.

With other forms of payment made through alternative means of payment, the pecuniary allocation is made through one or more contractual transactions but highly standardized and secure transactions which result in the creditor becoming a creditor of a pecuniary claim (most often to a bank), a credit to which the creditor may have the maximum autonomy as a means of payment to extinguish further pecuniary claims which in turn is obliged to be debtor in the evolving of economic relations, whose becoming is characterized by the succession of each economic operator as a creditor and a pecuniary debtor.

It is therefore a more complex situation than the purchase of banknotes due to the delivery by the debtor, since that attribution is the result of one or more negotiating transactions from which the creditor obtains the benefit of the translational effect of a credit claim relating to monetary units. With the consolidation of this translational effect, the creditor is entitled to further circulate the credit right on those monetary units attributed to him, by doing so with greater efficiency and security in all the dispositions he could have achieved with greater slowness and laboriousness and with constant risks of damaging losses in the use of cash.

The fulfilment of the pecuniary obligation through means other than money may in any case be considered effective and free of charge for the debtor only if it performs the same effects as the cash payment would have made. The payment made through means other than cash, achieves the satisfactory effect when the creditor is in the condition of freely disposing of the amount of money that the debtor has been attributed to him. This full power of disposition is not achieved through the fulfilment of a factual situation, but through the final consolidation of the creditor of a definitive right to have monetary units, towards third parties, mostly a bank.

Another issue that has arisen in the past was about to determine when the debtor is allowed to implement this form of payment through bank transfer.

Given the different needs that a modern payment system has to make, it does not seem to be an obstacle to the use of alternative means of payment. the fact that the place to which the debtor must direct the act of payment is not the creditor's own domicile but that of the subject which is technically suitable to receive payment for the creditor. This is because the concept of creditor’s domicile, rather than coinciding with his domicile subjectively attributable to the natural person, must be objectified and identified with the various places expressly or implicitly deputed depending on the nature of the service or the various circumstances in which the payment

is to be executed, as is otherwise provided for by art. 1282 c.c., which subordinates the determination of the place of performance to the indications deriving from the use or the nature of the benefit and the circumstances.

Likewise, it may be justified that, as a result of the use of an alternative means of payment, the moment at which the creditor actually obtains the availability of the sum due to him does not coincide with that in which the payment transaction is made. Intervention in the operation of a third party involves the usual variation of the availability dates according to needs (no matter in this case, to estimate how much is justified) of the third subject, the bank. The same subjects of the mandatory relationship will also have to strictly regulate these aspects.

In addition, given that the place of detention and provision of monetary liquidity can no longer be considered the domicile of the debtor, but it is the intermediary's one who is able to preserve the possession of the liquidity in the forms of scriptural record as well as to manage it efficiently and substantially without risk in any form of circulation, and which is legitimately considered to be the actual domicile of the pecuniary creditor.

Thus, the pecuniary debtor diligently and faithfully fulfils the necessary performance when, based on a proper assessment of the need for safety, efficiency, speed, compliance to industry payment practices or in relation to the nature and purpose of the performance, or the tools that are best suited to make that attribution of ideals monetary unit effective for the creditor (art.1176, c.c.).

Moreover, if the previous theories that attributed to the bank money the role of substitute of a different nature for the performance originally due are now definitely over and therefore the banking money is nothing more than a transmissive form of coin totally similar and equivalent to the State money, it makes no sense to talk about the public monopoly of currency as an absolute paradigm. The consequence of the gradual transition to a state of competition in the production and circulation of money coincides with its gradual dematerialization.

The idea of private money has so far been linked to the presence of the banking system, which plays a competitive role with respect to the State in the management of monetary policy. Now the problem is to ascertain the legal nature of Bitcoin, and more generally, of all cryptocurrencies.

On the question, it is good to start from the position officially expressed by the ECB, which has argued that virtual coins, as they have no legal framework that establishes their function as a means of fulfilling their pecuniary obligations (according to the mechanism provided for in art.1278 c.c.), would not be currency or perhaps it is better to say that they would be currency but only in the contractual sense, i.e. they are valid in the exchange mechanisms as there is an agreement between the parties.

Virtual coins, the ECB continues, would not be subject to the mechanisms set out in the Payment Services Directive (PSD2)[180].

A significant step in recognizing the value of Bitcoin as a currency was, however, accomplished by the European Court of Justice, with judgment of October 22, 2015 (Case C-264/14, Skatteverket vs. David Hedqvist). The Court has in fact established, with reference to Bitcoin, that "*non-traditional currencies, i.e. different from freely convertible currencies in one or more countries, constitute financial transactions, as these currencies have been accepted by the parties of a transaction as an alternative means of payment to the legal means of payment and have no other purpose other than that of a means of payment.* " In the judgment, in fact, the conversion of Bitcoin to legal tender was recognized as a traditional exchange rate transaction.

There are, in this regard, examples of countries in which we are going in the direction of fully integrating Bitcoin with the legal currency.

In Japan, on May 22, 2016, the Diet has approved a law regulating payment in virtual currencies, while in the United States the case of a judicial ruling that Bitcoin is a currency, not a commodity, is very know.

Indeed, the central concern of the central authorities is that the unstructured diffusion of Bitcoin could undermine the instruments of monetary policy control.

Once again, each country frames Bitcoin in its own order in a different way and rules and regulations in this area are constantly evolving.

6.5 Bitcoin and requirements to replace legal currencies

The reality of a currency controlled directly or indirectly by the State has never been the only option, economists have always distinguished a possible set of situations in which they can distinguish, in addition to national currencies, the currencies adopted (as in Case of Montenegro with the Euro), parallel coins, black market coins (not officially admitted but circulating in fact based on exchange rates other than the officer) and alternative coins. These last are accepted within a particular context and / or communities as in the case of crypto currencies. In this framework, Bitcoin is the alternative digital coin which achieves the highest level of accomplishment, openness and the highest degree of similarity to a real currency so far.

[180] The PSD2 is a data and technology-driven directive, which was introduced as a way to respond to the changes in the landscape of payment services since the introduction of the original directive in 2007, and to drive further improvements in payment services across Europe.
The revised version includes a number of changes and enhancements to the original paper, with the main goal of providing clarity, efficiency and ease-of-use of European payment services.
The directive significantly extends the scope of the original PSD regulations beyond Europe and revises the definition of a 'Payment Institution.'
Other features of the reform package include: new rules on access to payment accounts, liability allocation provisions, transparency requirements and customer authentication measures.

The unstoppable popularity and diffusion of Bitcoin led to a lively debate around the possible future replacement of the legal currency with the virtual one, in general and with Bitcoin in particular.

I believe that the proper way to respond, at least in part, to this question is to observe Bitcoin in the shoes of legal currency, in other words, trying to analyse Bitcoin from a point of view of the functions that the legal currency plays today in the various systems.

As already seen in Chapter 2 of this paper, one of the main functions of any currency is to serve as a means of exchange or payment instrument in the sale of goods and services and in other commercial transactions.

In this regard, it can be seen how Bitcoin as a means of exchange differs significantly from the standard currencies, in particular, since there is no central system to remunerate, Bitcoin's transaction costs must only cover the costs of offsetting the mining system and, without any physical support, they also relieve all items relating to the transfer of standard currencies such as storage, authentication, transport and security.

It is not surprising, therefore, that on average, the costs for a Bitcoin transaction oscillate between 0% and 1% of the value of the transaction (on July 6,2017 the fastest and cheapest transaction fee was 0.0000039 BTC/byte[181], which for the median transaction size of 226 bytes, this results in a fee of 0.0008814 BTC[182]), while those for a standard currency transaction reach a percentage from 2% to 5%.

Sifting of an official document of Banca Intesa San Paolo we can know all the rates of the foreign transfer. We note that the cost of a foreign bank transfer is from a minimum of € 1.2 to a maximum of € 10 in the worst cases.

Going to evaluate the rates of the most important Italian banks such as the BNL Group, Banca Monte dei Paschi di Siena and Unicredit, we can say the scissors between the minimum commission and the maximum fee increase and the cost of a foreign transfer can cost at worst even 20 €.

Currently, bitcoin users have to attach a fee of 420 satoshis/byte in order to have transaction confirmed relatively quickly. Since the median transaction size of bitcoin is 226 bytes, the 420 satoshis/byte recommended fee costs users over $2 per transaction. For most transactions, the recommended fee would climb up to $2.14 if users want to see their transactions confirmed faster than others. A few months ago, until March, the recommended fee for bitcoin transactions was 160 satoshis/byte.

[181] https://bitcoinfees.21.co/

[182] It's important to note that the total bitcoin amount of your transaction doesn't matter for the purposes of fee calculation! For example, if your transaction is 250 bytes, you'll have to pay the same fee whether you're transferring 0.001 bitcoins or 1 million bitcoins.

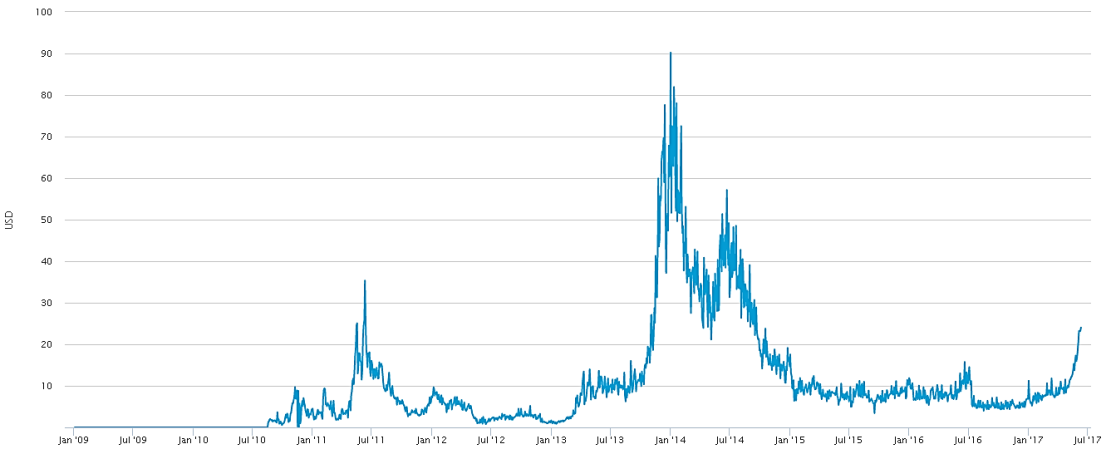


Figure 15 - Cost per transaction, Miners revenue by the number of transactions.

Source: blockchain.info [100]

The absence of a central system and physical media also translates into the ability of the Bitcoin system to process and execute transactions faster than traditional online payment systems, with an average of 10 to 60 minutes, as already exhaustively explained in Chapter 4, while, for example, in the case of a bank transfer, once the transaction is completed, usually the amount of money will be credited to the beneficiary's current account for a period ranging from 2 to 4 (maximum 5) working days. However, times vary from institute to institute. For an online wire transfer, credit times vary from case to case. For example, if the recipient is a customer of your own branch, will see the money after just one day. If he is a client of the same bank but of another branch, it will take about two days; If the banks are different, it can take up to three days. In this respect, therefore, convenience and speed are certainly elements in favour of Bitcoin with respect to standard payment systems.

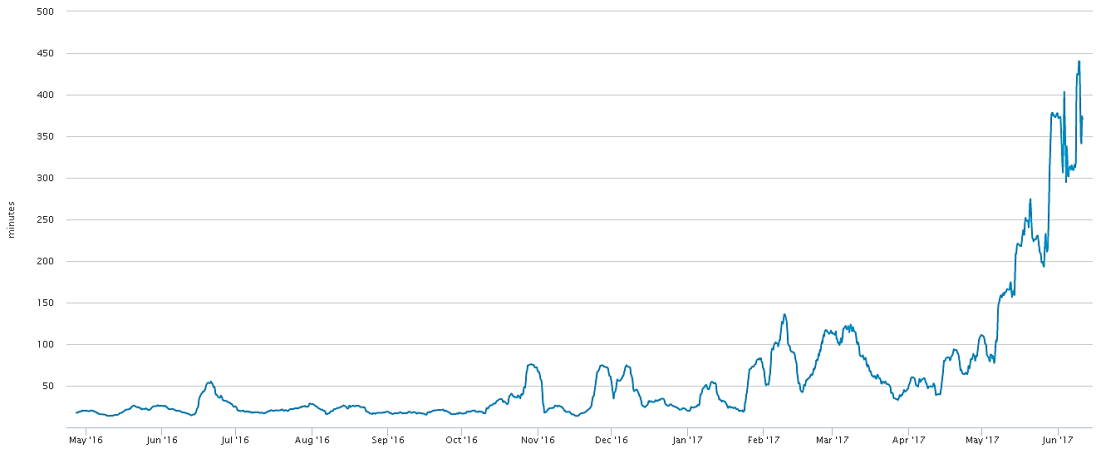


Figure 16 - Average Confirmation Time of a Bitcoin transaction. Source: blockchain.info [101]

It is useless to deny how good Bitcoin is to operate as a means of exchange in the field of illegal and criminal activities, although all Bitcoin payments are encrypted but have a story that can be tracked on Blockchain and freely visible, as I already mentioned in previous chapters. For

these reasons, anonymity and transparency are peculiar traits that can be admitted as ambivalent elements both in favour and against the use of Bitcoin compared to standard currencies.

Bitcoin is not a legal tender currency as opposed to standard currencies[183]. Its use as a means of exchange depends solely on the will of market players that are not legally bound to accept it as a means of payment [102]. In this respect, therefore, the fact that Bitcoin has not a legal tender can in fact be a disadvantageous factor in the generalized use of standard currencies.

Currently, no virtual currency has legal tender status in any jurisdiction, but it is theoretically possible that a virtual currency might be declared legal tender in some jurisdictions in the future. However, this is unlikely to happen in an EU/EEA member state, and if it was issued by a public authority, it would cease to be a decentralised virtual currency and would instead become a fiat currency backed by a central authority [102].

The legal tender status of euro banknotes and coins is laid down by Article 128 (ex-Article 106 of the EC Treaty) of the Treaty on the Functioning of the European Union (TFEU). Exclusive right to authorise the issue of banknotes and approve coin volume issuance within the European Union is given to the European Central Bank, as well known, so it would be necessary to amend the TFEU if a virtual currency were declared legal tender.

In addition to the lack of legal tender, strong initial investment is likely to be a barrier to the entry of potential users, and hence a constraint on the global spread of the currency.

In benchmarking with standard currencies, another peculiar feature of Bitcoin is related to the fact that the Bitcoin number in circulation is known and all Bitcoins live within Blockchain, so a person who wants to exercise Bitcoin's joint collection activity and granting credit in Bitcoin, can actually only lend it if he has obtained the entire private key from the depositor and will only be able to lend Bitcoin to the extent that he owns them.

To perform the unit of account function, Bitcoin should be able to measure the exchange and market value of goods and services as well as the value of all economic transactions.

If the Bitcoin’s almost infinite divisibility may seem like a plus for the currency, on the other hand the price difference expressed in many decimals may confuse consumers. Moreover, prices in Bitcoin are characterized by a short extremely high term volatility, resulting in indirect costs borne by the market players who are forced repeatedly to adjust prices, and thus compromising the ability of virtual currency to operate effectively as a unit of account.

Another feature that a payment instrument has absolutely to have is that of value reserve.

[183] Virtual currencies have no legal tender, which means the following features are not fulfilled: (a) mandatory acceptance, i.e. that the creditor of a payment obligation cannot refuse currency unless the parties have agreed on other means of payment; (b) acceptance at full face value, i.e. the monetary value is equal to the amount indicated; and (c) that the currency has the power to discharge debtors from their payment obligations.

In the case of standard currencies, unlike Bitcoin, the stability of purchasing power lies in the guarantee provided by the anti-inflationary management of monetary policy by a central bank. Even in this case, price volatility plays a key role, which is added to the fact that during its short life Bitcoin has been subjected to numerous attacks by hackers, thus jeopardizing the ability to preserve its security system, which plays a key role in its future.

Of course, Bitcoin's extreme vulnerability from the point of view of IT security weakens its ability to function as a reserve of value and is a Bitcoin weakness compared to standard currencies, as it inhibits the widespread use of virtual currency by users who continue to perceive it as a risky tool.

Bitcoin's major advantage is that the system is entirely decentralized and there are no central banks with which the virtual currency is not subject to inflation or even the interference of monetary policies in either way. Indeed, since the total number of Bitcoin is limited, the digital currency is, on the contrary, exposed to deflationary pressures, or has a tendency to appreciate over time. However, on the one hand, this is an advantage especially for Bitcoin owners, who, in appreciating currency, will find themselves accumulating greater wealth at the same amount of possession. On the other hand, just waiting for this to happen, users might be forced to accumulate Bitcoin as if it were a form of speculative investment rather than spending them as a coin, reducing its presence, availability and consequently use in the reference markets.

7 Conclusion

The time is more than ripe to empower the monetary obligation fulfilment by obsolete and narrow mode of the material bestowal of banknotes and coins issued by the State.

I do not feel enough confident to say that banks and payment companies will totally disappears, but their role would definitively change, and it is very likely that such revolution is already in place.

Technological innovation could potentially lead to a diminished lending role from the traditional banking sector if phenomena such as peer-to-peer lending and cryptocurrencies become mainstream and grow.

So at this point in time, they have to start looking for their new role in the possible future payment ecosystem, if they have not already done so, and we will probably see some innovative business model in this sector.

In my opinion, thanks to Blockchain technology we will reach the highest ever level of transparency of economic activities, but not only, and in every corner in the world; Central Banks, if they will play still the same role, will have unprecedented knowledge of what is going on in the economy that leads to unprecedented level of precision to monetary management and control.

The money history is dense with clamorous and spectacular changes: from the metal coin that founded its trading value in its intrinsic value, to the convertibility of paper money, mere confidentially and forcible course. It is well foreseeable for the new millennium to see the definitive sunset of every corporeality, even coin-printed with a revolution substantially similar to that which characterized modern society with the advent of the electronic payment.

The infinite possibilities offered by electronic writing and computer manipulation through magnetic cards, microchips, passwords, etc. will soon lead to the definite sunset of the paper circulation of coin, which is now completely incompatible, as we saw in the previous Chapter, with the demands of order and efficiency and with the means offered and above all necessarily practiced by the digital society that shapes our relationship life.

As I explained in Chapter 5, distributed ledger technology provides the framework for government to reduce fraud, corruption, error and the cost of paper-intensive processes. It has the potential to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust. It has similar possibilities for the private sector. Moreover, distrib-

uted ledgers can provide new ways of assuring ownership and provenance for goods and intellectual property; it has the potential to reduce fraud and prevent “blood diamonds” from entering the market.

I think with the United States and the European Union being added to the ever-growing list of governments and corporations actively pursuing blockchain technology, the likelihood of cryptocurrency-based global solutions is increasing each day. As more governments turn to blockchain, it’s only a matter of time before the nations of Latin America, and the others that at this time still forbid the use of Bitcoin, do as well.

However, the other thing I believe in, but more difficult to realize, is that if the governments and banks don’t implement these changes, the people are in a position to do it themselves.

I consider decentralization the most important characteristic of Bitcoin. No central power controls bitcoin. However, it is true that central banks could indirectly manipulate cryptocurrencies by creating derivatives and exchange traded funds based on those cryptocurrencies, but this will not change bitcoin’s underlying store of value.

Encryption and decentralization make Bitcoin secure, in fact, it can be stored in cyber “vaults,” where owners keep a hard copy of the encryption cipher. While a bitcoin exchange and a computer can be hacked, bitcoin that is in a “vault” will not reside in the exchange or the computer, and only the owner has the code to access the stored bitcoin and no one can confiscate it. As well as the decentralized public ledger is more secure than centralized ledger.

As I explained at the end of Chapter 6, at the present state of things, I am partially in agreement with the forecast that sees in fact unlikely that bitcoin will be recognized as a currency by all governments to the point of replacing the fiat currency. The three functions that a legal coin is required to fulfil today are not exhaustively met by Bitcoin, and one of the main reasons is the high short term volatility, which continues to characterize the cryptocurrency.

Perhaps it would be more accurate to say that Bitcoin is a pilot project. Sometimes pilot projects do evolve to encompass users' needs, sometimes they don't. Let the best cryptocurrencies win. If this should be just Bitcoin out of all, let it be Bitcoin.

The only thing I can say with certainty about this whole thing is that we are witnessing something so unique that we have no past experience to draw back on. Bitcoin showed that things can be different.

Bibliography

[1] A. Smith, La Ricchezza delle Nazioni, A. e. T. Biagiotti, Ed., Novara: Utet, 2013.

[2] G. Fontana, «Hicks on monetary theory and history: money as endogenous money,» *Cambridge Journal of Economics*, vol. 28, n. 1, pp. 73-88, 2004.

[3] J. Hicks, *A Market Theory of Money*, Oxford Clarendon Press, 1989.

[4] D. R. Graeber, Debt: The First 5,000 Years, Brooklyn: Melville House, 2011.

[5] Petrini Roberto, Controstoria della moneta, Reggio Emilia: Imprimatur , 2014.

[6] F. Martin, *Money: the unauthorized biography*, Bodley Head, 2013.

[7] F. Galiani, «FERDINANDO GALIANI: "DELLA MONETA" (testo completo),» 1963. [Online]. Available: http://www.filosofico.net/galianidellamoneta.htm.

[8] C. M. Cipolla, Le avventure della lira, Bologna: Il Mulino, 2001.

[9] L. Einaudi, Teoria della moneta immaginaria nel tempo da Carlomagno alla Rivoluzione francese, Torino: Einaudi, 1936.

[10] Wikipedia, «John Law (economist),» 2017. [Online]. Available: https://en.wikipedia.org/wiki/John_Law_(economist).

[11] P. Massa, G. Bracco, A. Guenzi, J. A. Davis e A. Carreras, Dall'espansione allo sviluppo, una storia economica d'Europa, 3 a cura di, A. D. Vittorio, A cura di, Torino: G. Giappichelli, 2011.

[12] J. Robertson, "The History of Money, from its origin to our time," 2007. [Online]. Available: http://www.jamesrobertson.com/book/historyofmoney.pdf.

[13] Wikipedia, «1st G6 summit,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/1st_G6_summit.

[14] S. Pepe, Investire Bitcoin, Palermo: Dario Flaccovio, 2014.

[15] F. M. Ametrano, in *Hayek Money: The Cryptocurrency Price Stability Solution*, 2014.

[16] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[17] B. e Y. Zhao, «China Is Developing its Own Digital Currency,» Febbraio 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-02-23/pboc-is-going-digital-as-mobile-payments-boom-transforms-economy.

[18] K. I. «Pulse of Fintech Q1'17, Global Analysis of Investment in Fintech,» 27 Aprile 2017. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/pulse-of-fintech-q4-2016.pdf. [Consultato il giorno Maggio 2017].

[19] IlSole24Ore, «Bitcoin ai massimi ma per le startup della blockchain calano le operazioni di investimento,» 19 May 2017. [Online]. Available: http://www.infodata.ilsole24ore.com/2017/05/19/bitcoin-ai-massimi-le-startup-della-blockchain-calano-le-operazioni-investimento/.

[20] Bitcoinwiki, «Bitocoin-Central,» [Online]. Available: https://en.bitcoin.it/wiki/Bitcoin-Central. [Consultato il giorno 25 May 2017].

[21] http://www.bitcoinblockhalf.com/, "Bitcoin Block Reward Halving Countdown," 2017. [Online]. Available: http://www.bitcoinblockhalf.com/. [Accessed May 2017].

[22] «Bitcoin Monetary Inflation,» [Online]. Available: http://bashco.github.io/Bitcoin_Monetary_Inflation/. [Consultato il giorno May 2017].

[23] O. Beigel, «Is Bitcoin Mining Profitable in 2017?,» 16 February 2016. [Online]. Available: https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/. [Consultato il giorno 29 May 2017].

[24] B. L. S.A.R.L., «Bitcoin Hashrate Distribution,» [Online]. Available: https://blockchain.info/en/pools?timespan=4days. [Consultato il giorno 14 May 2017].

[25] F. M. Ametrano, «Cyber-crime blackmails hospitals and corporations demanding bitcoin ransom. Yes, but this is not the whole story.,» 13 May 2017. [Online]. Available: https://www.linkedin.com/pulse/cyber-crime-blackmails-hospitals-corporations-bitcoin-ametrano.

[26] NewMoney.it, «Criptovalute: mai così bene dal 2009. Merito di Brexit, Trump e India,» 14 December 2016. [Online]. Available: http://www.newmoney.it/criptovalute-mai-cosi-bene-dal-2009-merito-brexit-trump-india/.

[27] B. L. S. “BTC to USD: Bitcoin to US Dollars Market Price,” [Online]. Available: https://blockchain.info/en/charts/market-price?timespan=all. [Accessed 23 May 2017].

[28] P. Digitali, «Bitcoin, ora per comprarli basta PayPal,» 29 March 2016. [Online]. Available: https://www.pagamentidigitali.it/payment-innovation/bitcoin-ora-per-comprarli-basta-paypal/.

[29] bitcoinwiki, «Buying Bitcoins (the newbie version),» 2017. [Online]. Available: https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version).

[30] O. Beigel, «How to Buy Bitcoin with a Bank Account / Wire Transfer,» 2017. [Online]. Available: https://99bitcoins.com/how-to-buy-bitcoin-with-a-bank-account-deposit-wire-transfer/.

[31] G. Wood, «ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER,» 2013. [Online]. Available: http://gavwood.com/paper.pdf. [Consultato il giorno May 2017].

[32] I. Balina, «HACKING INVESTING – BITCOIN, ETHEREUM AND CRYPTOCURRENCIES COULD MAKE YOU A MILLIONAIRE,» [Online]. Available: http://ianbalina.com/hacking-investing-bitcoin-ethereum-cryptocurrencies-make-millionaire/. [Consultato il giorno May 2017].

[33] G. M. F. «Smart Contract, tutti ne parlano, ma cosa sono?,» Gennaio 2017. [Online]. Available: http://www.gagminingfarm.com/blog/smart-contract-cosa-sono.html#sthash.UnOVRkS8.dpbs.

[34] Trustnodes, «Ethereum is Now the Most Secure Public Blockchain, Overtaking Bitcoin,» 21 May 2017. [Online]. Available: http://www.trustnodes.com/2017/05/21/ethereum-now-secure-public-blockchain-overtaking-bitcoin.

[35] N. Menezes, «Citicoin – The Banking Cryptocurrency,» 8 July 2015. [Online]. Available: http://www.newsbtc.com/2015/07/08/citibank-is-interested-in-developing-their-own-cryptocurrency-citicoin/. [Consultato il giorno 30 May 2017].

[36] J. Redman, «Disney Reveals Dragonchain, an Interoperable Ledger,» 25 October 2016. [Online]. Available: https://news.bitcoin.com/disney-dragonchain-interoperable-ledger/. [Consultato il giorno 30 May 2017].

[37] Z. Huang, «China's central bank thinks digital currency can do one thing cash can't,» 27 March 2017. [Online]. Available: https://qz.com/942413/peoples-bank-of-china-pboc-wants-to-replace-cash-with-its-cryptocurrency-in-case-interest-rates-go-negative/.

[38] D. Cummings, «People's Bank Of China Establishes FinTech Committee,» 16 May 2017. [Online]. Available: https://www.ethnews.com/peoples-bank-of-china-establishes-fintech-committee.

[39] W. Mougayar, «Blockchain Security is Multi-Layered, Here are the 6 Most Important Levels,» 2017. [Online]. Available: http://startupmanagement.org/2016/08/08/blockchain-security-is-multi-layered-here-are-the-6-most-important-levels/.

[40] V. Smerkis, «Why Microsoft Azure Integrates Blockchain Crowdfunding Platform Waves,» 11 May 2017. [Online]. Available: https://cointelegraph.com/news/why-microsoft-azure-integrates-blockchain-crowdfunding-platform-waves.

[41] S. Das, «Japanese Banking Giants Complete R3 Blockchain Trial for Derivatives,» 2 June 2017. [Online]. Available: https://www.cryptocoinsnews.com/japanese-banking-giants-complete-r3-blockchain-trial-derivatives/.

[42] R. Ayyarl, «First blockchain project 'Clear-Chain' is underway,» 2017 March 30. [Online]. Available: http://timesofindia.indiatimes.com/business/india-business/first-blockchain-project-clear-chain-is-underway/articleshow/58901149.cms.

[43] S. Das, «India Sees KYC Blockchain Lift-Off via BankChain Consortium,» 2 June 2017. [Online]. Available: https://www.cryptocoinsnews.com/india-sees-kyc-blockchain-lift-off-via-bankchain-consortium/.

[44] J. Nagpal, «Microsoft Azure to accelerate Blockchain adoption in BFSI sector in India as the Exclusive Cloud Partner for BankChain,» 12 June 2017. [Online]. Available: https://news.microsoft.com/en-in/microsoft-azure-accelerate-blockchain-adoption-bfsi-sector-india-exclusive-cloud-partner-bankchain/#sm.00001gcxpa75hhe6jtq52dvt25s2g#GogioqSRRHrMM7sr.97.

[45] Sputnik, «Russia's VEB to Launch Blockchain Scheme Prototype Soon - Bank CEO,» 31 May 2017. [Online]. Available: https://sputniknews.com/russia/201705311054173891-russia-spief-blockchain-veb/.

[46] S. Das, «Blockchain Will Be Commercial in 2019, Says CEO of Russia's Largest Bank,» 21 February 2017. [Online]. Available: Blockchain Will Be Commercial in 2019, Says CEO of Russia's Largest Bank.

[47] B. Vitàris, «This Russian Bank Is Testing Blockchain for Project Management,» 3 June 2017. [Online]. Available: https://www.cryptocoinsnews.com/russian-bank-testing-blockchain-project-management/.

[48] S. Das, «Samsung SDS Puts Blockchain to Use for Korea's Shipping Industry,» 31 May 2017. [Online]. Available: https://www.cryptocoinsnews.com/samsung-sds-puts-blockchain-use-koreas-shipping-industry/.

[49] S. Das, «A South Korean Province Used Blockchain Tech for Resident Voting,» 8 March 2017. [Online]. Available: https://www.cryptocoinsnews.com/south-korean-province-used-blockchain-tech-resident-voting/.

[50] L. Parker, «Korean stock exchange launches Blockchain-based startup market,» 18 November 2016. [Online]. Available: https://bravenewcoin.com/news/korean-stock-exchange-launches-blockchain-based-startup-market/.

[51] S. Das, «Taiwan's OwlTing Launches Ethereum-based Blockchain for Food Safety,» 30 May 2017. [Online]. Available: https://www.cryptocoinsnews.com/taiwans-owlting-launches-ethereum-based-blockchain-for-food-safety/.

[52] o. Kharif, «Wal-Mart Tackles Food Safety With Trial of Blockchain,» 18 November 2016. [Online]. Available: https://www.bloomberg.com/news/articles/2016-11-18/wal-mart-tackles-food-safety-with-test-of-blockchain-technology.

[53] B. Sheng, «GovCoin Systems Implements Social Welfare Payments Distribution Trial for UK's Department for Work and Pensions,» 7 July 2016. [Online]. Available: http://www.businesswire.com/news/home/20160707005803/en/GovCoin-Systems-Implements-Social-Welfare-Payments-Distribution.

[54] F. d'Anconia, «The Future of Africa through the Eyes of Two Blockchain Devs,» 14 May 2017. [Online]. Available: https://www.cryptocoinsnews.com/future-africa-eyes-two-blockchain-devs/.

[55] F. d'Anconia, «Bitcoin is Improving Lives of Women Farmers in Zimbabwe,» 9 May 2017. [Online]. Available: https://www.cryptocoinsnews.com/bitcoin-is-improving-lives-of-women-farmers-in-zimbabwe/.

[56] F. Ametrano, «La blockchain dà il tempo al web,» 21 May 2017. [Online]. Available: http://nova.ilsole24ore.com/progetti/la-blockchain-da-il-tempo-al-web/.

[57] M. Bellini, «Intesa Sanpaolo, Deloitte con la start up Eternity Wall in un PoC per la notarizzazione dei dati grazie alla Blockchain,» 22 April 2017. [Online]. Available: http://www.blockchain4innovation.it/mercati/banche-e-finanza/intesa-sanpaolo-deloitte-la-start-eternity-wall-un-poc-la-notarizzazione-dei-dati-grazie-alla-blockchain/.

[58] A. Tomasicchio, «La Dolce Vita in Bitcoin: Cryptocurrencies Around the World, Italy,» 15 March 2017. [Online]. Available: https://cointelegraph.com/news/la-dolce-vita-in-bitcoin-cryptocurrencies-around-the-world-italy.

[59] A. Tomasicchio, «Beppe Grillo's Bitcoin Blockchain: Truth or Joke,» 30 December 2016. [Online]. Available: https://cointelegraph.com/news/beppe-grillos-bitcoin-blockchain-truth-or-joke.

[60] A. Tomasicchio, «Rome, Bari, Milan House 3 Top Bitcoin-Related Projects in Italy,» 21 October 2016. [Online]. Available: https://cointelegraph.com/news/rome-bari-milan-house-3-top-bitcoin-related-projects-in-italy.

[61] A. Frollà, «A Roma il primo hackathon per la PA digitale: in campo 100 sviluppatori,» 29 March 2017. [Online]. Available: http://www.corrierecomunicazioni.it/pa-digitale/46569_a-roma-il-primo-hackathon-per-la-pa-digitale-in-campo-100-sviluppatori.htm.

[62] A. p. l. D. «DesignPA: nasce la community designers.italia.it,» 1 June 2017. [Online].

[63] G. Bajo, «Developers Italia is born, the developers community of Italian digital government services,» 7 April 2017. [Online]. Available: https://medium.com/team-per-la-trasformazione-digitale/developers-italia-community-italian-digital-government-services-public-administration-2e56022096f1.

[64] A. p. l. D. «Linee guida DesignPA: online il nuovo portale del MIUR,» 29 May 2017. [Online]. Available: http://www.agid.gov.it/notizie/2017/05/29/linee-guida-designpa-online-il-nuovo-portale-del-miur.

[65] L. Garofalo, «Taxi, pagamenti in Bitcoin con il 3570 a Roma,» 15 November 2016. [Online]. Available: https://www.key4biz.it/taxi-pagamenti-bitcoin-3570-roma/173377/.

[66] L. Giannoni, «In Italia la casa si paga in bitcoin,» 6 April 2017. [Online]. Available: http://www.ansa.it/sito/notizie/tecnologia/hitech/2017/04/04/in-italia-la-casa-si-paga-in-bitcoin_6a5a9395-8871-4b85-91c5-b2d390ba6e76.html.

[67] B. D'Amico, «Le blockchain stanno già cambiando il mondo del lavoro?,» 27 April 2017. [Online]. Available: http://nuvola.corriere.it/2017/04/27/le-blockchain-stanno-gia-cambiando-il-mondo-del-lavoro/.

[68] J. Borchgrevink, «Blockchain Voting Used By Danish Political Party,» 23 April 2014. [Online]. Available: https://www.cryptocoinsnews.com/blockchain-voting-used-by-danish-political-party/.

[69] E. Ferreri, «4 modi in cui la Blockchain cambierà il mondo,» 30 April 2015. [Online]. Available: http://www.ruralhub.it/2015/04/30/4-modi-in-cui-la-blockchain-cambiera-il-mondo/.

[70] P. Boucher, «How blockchain technology could change our lives,» 2017.

[71] N. Acheson, «Blockchain Regulation: Is Europe Getting It Right?,» 15 May 2017. [Online]. Available: http://www.coindesk.com/blockchain-regulation-europe-getting-right/.

[72] A. Opeyemi, «Central Bank of Nigeria bans transaction in bitcoins, onecoin, others Read more: https://www.naij.com/1083244-central-bank-nigeria-bans-transaction-bitcoins-onecoin-others.html,» February 2017. [Online]. Available: https://www.naij.com/1083244-central-bank-nigeria-bans-transaction-bitcoins-onecoin-others.html.

[73] S. M. Appel, «Canada: Can You Take A Security Interest In Bitcoin?,» 13 June 2014. [Online]. Available: http://www.mondaq.com/canada/x/313572/securitization+structured+finance/Can+You+Take+A+Security++Interest+In+Bitcoin. [Consultato il giorno 13 June 2017].

[74] R. Campbell, “Report: Bitcoin Likely to Fuel Ransomware Growth Unless Governments Act,” 27 April 2017. [Online]. Available: https://www.cryptocoinsnews.com/bitcoin-likely-fuel-ransomware-growth-unless-governments-act/.

[75] Autoridad de Supervisión del Sistema Financiero (ASFI), «Nota de Prensa N°20/17,» Santa Cruz, 2017.

[76] The Telegraph, «Why Bangladesh will jail Bitcoin traders,» 15 September 2014. [Online]. Available: http://www.telegraph.co.uk/finance/currency/11097208/Why-Bangladesh-will-jail-Bitcoin-traders.html. [Consultato il giorno 14 June 2017].

[77] P. Rizzo, «China's Central Bank Issues Warnings to Major Bitcoin Exchanges,» 6 January 2017. [Online]. Available: http://www.coindesk.com/chinas-central-bank-issues-warnings-major-bitcoin-exchanges/.

[78] K. K, «Russian Tax Office Updates Legal Stance On Bitcoin,» 2 December 2016. [Online]. Available: https://news.bitcoin.com/russian-tax-office-legal-bitcoin/. [Consultato il giorno 13 June 2017].

[79] Banca Naţională a României, «Comunicat referitor la schemele de monedă virtuală,» Bucharest, 2015.

[80] F. S. «Money Laundering Using,» Paris, 2010.

[81] A. Greenber, «Black Market Drug Site 'Silk Road' Booming: $22 Million In Annual Sales,» 6 August 2012. [Online]. Available: https://www.forbes.com/sites/andygreenberg/2012/08/06/black-market-drug-site-silk-road-booming-22-million-in-annual-mostly-illegal-sales/#161160c65962.

[82] F. C. E. N. «Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,» 2013.

[83] F. B. o. I. «Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity,» 2012.

[84] S. O. o. I. E. a. A. «INVESTOR ALERT: PONZI SCHEMES USING VIRTUAL CURRENCIES,» 23 July 2013. [Online]. Available: https://investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-ponzi-schemes-using-virtual. [Consultato il giorno June 2017].

[85] J. Southurst, «Federal Agency Responses Reveal US Government Attitudes to Bitcoin,» 16 November 2013. [Online]. Available:

http://www.coindesk.com/federal-agency-responses-us-government-attitudes-bitcoin/.

[86] *SEC Complaint: Trendon T. Shavers and Bitcoin Savings and Trust*, 2013.

[87] U. S. a. E. Commission, «Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, Civil Action No. Civil Action No. 4:13-CV-416,» 22 September 2014. [Online]. Available: https://www.sec.gov/litigation/litreleases/2014/lr23090.htm.

[88] E. P. I. «Changes in modus operandi of Islamic State terrorist attacks,» The Hague, 2016.

[89] H. T. U. K. "Digital currencies: response to the call for information," London, 2015.

[90] Bitcoin Taxes, «Common Questions about Bitcoin and Taxes,» 22 February 2017. [Online]. Available: https://bitcoin.tax/blog/bitcoin-taxes-common-questions/.

[91] BitcoinTaxes, «Some Questions & Answers,» [Online]. Available: https://bitcoin.tax/faq. [Consultato il giorno 13 June 2017].

[92] E. R. Carter, «Taxation of Virtual Currency,» 16 January 2017. [Online]. Available: https://www.bna.com/taxation-virtual-currency-n73014449855/.

[93] Jared Polis - Press Releases, «Polis, Schweikert request tax guidance for virtual currencies,» 6 June 2017. [Online]. Available: https://polis.house.gov/news/documentsingle.aspx?DocumentID=398396.

[94] Agenzia delle Entrate, «Interpello ai sensi dell'art. 11, legge 27 luglio 2000, n. 212.,» Roma, 2016.

[95] F. Marrucci, «Bitcoin: le Entrate chiariscono il trattamento fiscale della moneta virtuale,» 28 September 2016. [Online]. Available: http://www.altalex.com/documents/news/2016/09/07/bitcoin-moneta-virtuale-risoluzione-agenzia-entrate.

[96] XMLGOLD, «Italy: Bitcoin as a Currency and Tax it,» 18 November 2016. [Online]. Available: https://www.xmlgold.eu/en/news/article/375/italy-bitcoin-as-a-currency-and-tax-it?utm_referrer=https%3a%2f%2fwww.google.it%2f&fa821dba_ipp_uid2=wkL4jYSYLgcCWtJk%2fTapowAalnzvKpX4GbV7Y%2fg%3d%3d&fa821dba_ipp_uid1=1497345433383&fa821dba_ipp_key=149734543338.

[97] *Obbligazioni, adempimento, pagamento con assegno, legittimità*, 2017.

[98] G. Potenza, «Obbligazioni pecuniarie: consegna dell'assegno bancario in sostituzione di pagamento in denaro. Rifiuto dell'adempimento da parte del creditore.,» 2010. [Online]. Available: http://www.percorsi.giuffre.it/psixsite/Esercitazioni/Pareri/Diritto%20civile/Obbligazioni%20e%20contratti/default.aspx?id=12793&vistaraw=yes.

[99] E. Crimi, «Obbligazioni pecuniarie, efficacia solutoria del pagamento effettuato mediante assegni circolari,» 23 January 2013. [Online]. Available: http://www.unioneavvocati.com/news/23/01/2013/obbligazioni-pecuniarie-efficacia-solutoria-del-pagamento-effettuato-mediante-assegni-circolari_1127.html.

[100] blockchain.info, «Cost per Transaction,» 11 June 2017. [Online]. Available: https://blockchain.info/charts/cost-per-transaction?timespan=all.

[101] blockchain.info, «Average Confirmation Time,» [Online]. Available: https://blockchain.info/it/charts/avg-confirmation-time?daysAverageString=7&timespan=all. [Consultato il giorno 11 June 2017].

[102] European Banking Authority, «EBA Opinion on 'virtual currencies',» London, 2014.

[103] M. O. M. J. M. Paul R. Krugman, International economics: theory & policy, 9 a cura di, Addison-Wesley, 2012.

[104] C. M. Reinhart e K. S. Rogoff, «THIS TIME IS DIFFERENT: A PANORAMIC VIEW OF EIGHT CENTURIES OF FINANCIAL CRISES,» *NBER WORKING PAPER SERIES*, 2008.

[105] Wikipedia, «Latin Monetary Union,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Latin_Monetary_Union.

[106] Wikipedia, «German reunification,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/German_reunification.

[107] Wikipedia, «Cypherpunk,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Cypherpunk.

[108] Wikipedia, «SourceForge,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/SourceForge.

[109] T. B. F. 2017. [Online]. Available: https://bitcoinfoundation.org/.

[110] Wikipedia, «Internet of things,» Aprile 2017. [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things.

[111] Wikipedia, «Uber (company),» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Uber_(company).

[112] Wikipedia, «Didi Chixing,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Didi_Chuxing.

[113] Wikipedia, «Airbnb,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Airbnb.

[114] Wikipedia, «Lending Club,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Lending_Club.

[115] Wikipedia, «Kiva (organization),» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Kiva_(organization).

[116] Wikipedia, «WeChat,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/WeChat.

[117] Wikipedia, «Nectar loyalty card,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Nectar_loyalty_card.

[118] BitcoinWiki, «iPayYou,» 2017. [Online]. Available: http://bitcoinwiki.co/ipayyou-allows-users-to-send-bitcoin-via-twitter/.

[119] Bitmain, «BITMAIN,» 2017. [Online]. Available: https://www.bitmain.com/about.

[120] Wikipedia, «OKCoin,» maggio 2017. [Online]. Available: https://en.wikipedia.org/wiki/OKCoin.

[121] Wikipedia, «Robo-advisor,» 2017. [Online]. Available: https://en.wikipedia.org/wiki/Robo-advisor.

[122] Wikipedia, "Sybil attack," May 2017. [Online]. Available: https://en.wikipedia.org/wiki/Sybil_attack. [Accessed May 2017].

[123] Bitcoinwiki, "Controlled Supply," [Online]. Available: https://en.bitcoin.it/wiki/Controlled_supply#Projected_Bitcoins_Short_Term. [Accessed May 2017].

[124] Wikipedia, «R3 (company),» [Online]. Available: https://en.wikipedia.org/wiki/R3_(company). [Consultato il giorno 30 May 2017].

[125] G. C. Visconti, «Blockchain Technology Inspires R3 To Improve Financial Industry With Distributed Ledger Technology Corda,» 3 April 2017. [Online].

Available: https://coinidol.com/blockchain-inspires-r3-to-improve-financial-industry/.

[126] T. Morita, «Peach Aviation plans first bitcoin service for air travelers,» The Asahi Shimbun, 7 June 2017. [Online]. Available: http://www.asahi.com/ajw/articles/AJ201706070011.html.

[127] Coincheck blog, «Hirosaki City Collects Bitcoin Donations to Preserve Cherry Blossoms with 100 Years of History,» 20 April 2017. [Online]. Available: https://coincheck.com/en/blog/3496.

[128] M. Funakoshi e J. Lee, «Fretting over savings, Mrs Watanabe turns to bitcoin,» 2 June 2017. [Online]. Available: https://www.reuters.com/article/us-bitcoin-asia-idUSKBN18T0K2.

[129] Korea JoongAng Daily, «Government to introduce regulations for Bitcoin,» 18 November 2016. [Online]. Available: http://koreajoongangdaily.joins.com/news/article/Article.aspx?aid=3026364.

[130] Japan Financial Service Agency, «About the result of public comment, etc. on "Cabinet Order etc. (draft) etc. revising part of enforcement orders of banking law etc.",» 24 Marzo 2017. [Online]. Available: http://www.fsa.go.jp/news/28/ginkou/20170324-1.html.