Dipartimento di Economia e Finanza

Cattedra Money and Banking

The rise of cryptocurrencies: a monetary and financial analysis on Bitcoin

RELATORE Prof. Paesani Paolo

CANDIDATO Lucrezia Masi

Matricola 188721

ANNO ACCADEMICO

2016/2017

INDEX

INTRODUCTION:

"Multum egerunt qui ante nos fuerunt, sed non peregerunt" (Seneca, Epistulae ad Lucilium,7,64)

The people who came before us did much, but other things are yet to come"

Looking back at the history of human beings, technological progress has always covered a key role in fostering people's welfare and economic development. From the πολυτρόπος(polytropos) Ulysses, clever and ingenious, to many inventors and scientists that have followed him throughout history, men have always tried to achieve an improved status through the use of enhanced instruments and methods never losing their knowledge-seeking approach. This has allowed us to live in a moment of history where technology and improvements are hectic and change is always next door.

In Economics, we know that the main drivers for economic growth are: accumulation of capital stock, increase in labor inputs, and technological advancement, the most important for a sustainable progress in the long run.

Recent innovations in information technology have taken the major role in the changes we are observing in our environment and the most powerful of these innovations is of course the Internet. Internet can be thought as the basis which from its "birth" every other invention and advance leans on. It has impacted particularly financial services, where it can be thought of as a "transactional agora": FinTech is its main outcome.

Fintech is a *portmanteau* of financial technology describing all technological progress in the financial sector that has appeared since the last decades of the 20th century, including a very broad range of innovations.

Innovation in financial services, in short FinTech, has brought both excitement and hype because the entrance of newly developed technologies could disrupt or at least impact the whole current financial and subsequently economic system. The three main categories of technological innovations that are changing the financial and economic environment, and to some extent society as well, are the cellphones and smartphones, the artificial intelligence and big data analytics, and distributed ledger technology (DLT) and blockchain, invented in 2008 together with "Bitcoin" concept.

The possible impacts FinTech could have on financial services are the unbundling and restructuring, the globalizing, customizing, virtualizing of the services and new issues regarding payment, settlement and financial stability. FinTech has the potential to redistribute financial tasks among different companies so as to prevent a risky multiple engagement in diverse activities (i.e. most commercial banks take deposits, in such a way they are involved both in processing payments and making loans and this makes commercial banks possible preys to bank runs because of the

unbalanced financial structure in terms of different maturities between loans and deposits). Financial inclusion is enhanced and stimulated, giving innovative opportunities for business expansions or economic transactions through the internet, smartphones or DLT systems.
The financial industry has a long history dating back from Renaissance in some countries like ours; its main infrastructures (i.e. money and ledgers) had conceptually stayed the same since their establishment up to a recent past where they have started being challenged by upcoming inventions, driven by Avant-guard creations and developments. The payment system, which partly consists of money and ledgers, has been challenged by what can described as the "Blockchain revolution" of decentralized digital currencies.

This thesis has undertaken the following path: we have started by investigating the characteristics of a payment system and how they have been modified in their history by the upcoming improvements, especially by the distributed ledger technology. We decided to study the development of money from its early stages to the most innovative forms of digital currencies. Among them, we have concentrated our research on decentralized currencies' taxonomy, properties and industry. Then, we put our focus on the most illustrative case for cryptocurrencies: Bitcoin. This, due to its hybrid nature, have been analyzed in its features either as a currency or as an investment, through the examination of its properties as a currency and a model of its returns to make predictions.

The question this work aims at answering is about how the financial system, looked at through the investigation of payment systems and monetary systems, has been already impacted by Fintech, and above all, which is the result of such an impact by the most notorious exemplary of this technological innovation, Bitcoin, on the financial system. Our ambition is to try to identify the nature of this cryptocurrency and to analyze, by exploring its key functions and properties either as a currency in the traditional sense or as 'pure' financial asset, what can be the future of this first experiment of a decentralized currency. Most people concern is about the total disruption of the financial system as we know it nowadays. The questions that people have on the topic are many. Could cryptocurrencies represent a feasible alternative to currency issued by Central Banks? Could the financial markets survive without any intermediary? Could a peer-to-peer system made up by all possible users on the Internet substitute the job of banks and other financial intermediaries? This paper aims at discussing the disruption of this new type of currency, its functions in comparison with the traditional types, and the possible evolution of the panorama for the future of money and of the payment system.

The thesis is structured in two main chapters and a final one for the conclusion. Its focus follows the shape of a funnel from the general features describing the payment system and digital money to a detailed analysis of Bitcoin. Chapter 1 starts with the description of the payment system and the requirements it has to fulfill in order to be considered efficient. These criteria will be then checked for the innovative payment system brought to life by digital currencies. Afterwards, an excursus of money from its origins to the recent times is given, together with a comparison of the traditional forms and functions linked to money with digital currencies. Those are in-depth analyzed in their taxonomy, structure and main properties. Virtual currency schemes as described by many reports will be studied in their advantages and potential risks. Our attention will then focus on decentralized digital currencies, on their differences compared to other digital currencies and their internal division. We would examine the factors which influence their development and the legal and regulatory aspects concerning them. Finally, we would enter into cryptocurrencies' industry and sectors to better understand the foundation of the entire infrastructure of decentralized currencies and the distributed ledgers, whose technology represents one of the most important discoveries of the last century.

Chapter 2 deals with Bitcoin in all its facets: we have defined all the elements which constitute Bitcoin system looking at its four basic components: the protocol, the network, the currency and the open source project. We explored the main constituting technologies and above all the Blockchain, which represents the most important contribution of Bitcoin to the financial system. After we considered all attributes and properties on Hash functions, public-key cryptography and digital signature, the peer-to-peer (P2P) system and the Proof of Work, we decided to take two analysis paths on Bitcoin: a monetary analysis and a financial analysis. The former investigated whether bitcoin, the currency, could be considered as money by looking at the main traditional functions attributed to it, such as medium of exchange, store of value and unit of account, in a Bitcoin's perspective, examining all advantages and drawbacks of the cryptocurrency with respect to the functions. The latter involves the study of Bitcoin as an investment through the analysis of its returns. We have looked at any correlation with some indicators to understand the behavior of the returns over time, then we have decided to estimate two models. The first model is an autoregressive model, for which we have explored the main properties. We have searched for volatility clustering and conditional heteroskedasticity, using statistical tools such as the Test Ljung-Box, and we tested the stationarity of the model through the Augmented Dickey Fuller test. Once we have estimated the autoregressive model, we have decided to try to estimate a structural model using the returns of other currencies' exchange rates: the EUR/USD and the JPY/USD

crosses. We have opted for these currencies due to their soundness, surely from a historical perspective, and popularity in the economic system.

Our research ended with the discussion of the outputs from the two regressions. The quantitative analysis of the returns and volatility is interpreted and studied through summary statistics evaluated by means of the program Microsoft Excel, and some final considerations on potential future scenarios about the evolution of Bitcoin and in general of cryptocurrencies are drawn.

At the end of the conclusion, there is an appendix with tables of data estimated on Excel, which have been useful for the investigation of the structural model for Bitcoin returns.

CHAPTER 1: MONEY IN THE DIGITAL ERA: the rise of cryptocurrencies

1.1 DIGITAL PAYMENT SYSTEMS

1.1.1 Five criteria for an efficient payment system

A payment system is "any financial system supporting transfer of funds from suppliers, savers, to users, borrowers, and from payers to the payees, usually through exchange of debits and credits among financial institutions" (Businessdictionary.com). It mainly consists of two mechanisms: a paper-based one for handling checks and drafts, and a paperless mechanism for managing electronic commerce transactions. Traditional forms of payment have three components: cash, bank-based payments, and card payments. Electronic payment systems have more components and have many requirements to accomplish, above all for what concerns the security. The security apprehension has to solve problems related to authorization, data confidentiality and authenticity, availability and reliability of the infrastructure, and most importantly privacy, anonymity and untraceability. For a payment system to work smoothly and properly it must be efficient.
The criteria that should serve as guiding principles for assessing the efficiency of a payment system, according to Mr Erkki Liikanen, Governor of the Bank of Finland, are the following: technical efficiency, accessibility and non-discrimination, efficient and cost-based pricing, operational stability with contingency plans in case of problems, and international compatibility. This will allow us at the end of this chapter to identify whether the most recent disruptive technologies applied to the financial system, cryptocurrencies and the distributed ledger technologies, could be the basis on which fund an innovative, but still efficient and sustainable, payment system.
Technical efficiency is achieved by a payment system when the payment methods providers are able to take full advantage of the available technical innovations so as to make the process faster, cheaper and safer either for users or for the providers themselves. Innovation is the main driver for the new payment solutions and digitalization is its main instrument.
The second criterion establishes that all different kinds of users shall have access to the payment infrastructure without disproportions in costs or use inconvenience. A basic right, as well as a necessity, in our society is the ability to make and receive payments, therefore financial inclusion and access to appropriate means of payment is crucial. Accessibility allows the payment system to be spread and so achieved by critical mass, enabling the system to achieve a more efficient and cheaper status since the costs related to transactions could be borne by many instead of a few. Factors affecting accessibility and attraction of users are essentially reputation and trust. Subsequently security and credibility, together with their breaches drive the success or fail of a new payment method diffusion.

Efficient and cost-based pricing entails transparency in the pricing of the payment methods, that should truly reflect the cost of producing the services. Competition boosts efficiency, but when we lack a multitude of alternatives in a market, economies of scale (linked to the accessibility criterion) play a major role in providing pricing effective solutions. In the payment infrastructure, there exist a competition-cooperation tie since payment methods constitute a network, it is important to recognize the cooperation role in defining the payment standards and building the underlying framework. Operational stability in the payment system is at the core of all the economic activity. The systems must be reliable and run smoothly. Providers of different payment methods face a trilemma between usability, costs, and security. In the digitalized world, cyber threats are the main challenge for future payment systems. Thus, cyber resilience must be a central feature in all future payment systems; security is not only about the technological structure, but also on the involved people, processes and communication. Central banks usually have a leading role in raising awareness of cybersecurity, setting the basic requirements and enabling the smooth flow in operations from one payment service operator to another. International cooperation is required to promote cybersecurity development and fulfilment.

Eventually international compatibility defines the common standards and rules needed in payment systems to promote harmonization and to guarantee interoperability of different payment methods either among themselves or with laws and regulations. Technical innovation may cause a rise in fragmentation in payment methods, challenging coordination and consequently compatibility, hence a common ground should be prepared in terms of guidelines before the shattering actually takes place.

Although FinTech and digitalization is bringing to life many different forms of payment methods, these five criteria should so far be considered in the development of new systems. The challenge for developers is how to find a solution to the trilemma between the payment method usability, costs and security. The competition-cooperation tie in the financial industry should be used to enable faster adaptation and usage diffusion of innovative solutions without compromising security, but still maintaining competition so as to achieve the most cost-efficient solution.

1.1.2 An introduction on the distributed ledger technology

Along with the payment system stand both the clearing and settlement systems, which have been affected in the last decades by the new waves of innovation that has crashed against the entire financial organism. An example of a disruptive technological innovation related to the financial world is the distributed ledger technology. It was introduced for the transfer and record-keeping of Bitcoin and other digital currencies and it is a consensually shared databased, synchronized across

the network available across several sites and institutions. The ledger records any transaction or contract that are maintained in a decentralized form: this eradicates the necessary presence of a central authority to check for manipulation and digitally arising problems such as double spending. Security and accuracy of information is guaranteed through cryptography, related keys and signatures represent the instruments through which information can be accessed. Once information is on the network, it cannot be challenged or modified.

This kind of technology has been firstly introduced by Satoshi Nakamoto, the Bitcoin creator, as the rationale behind the blockchain technology at the heart of Bitcoin. It is a solution to the disappearance of third parties in this peer-to-peer payment system based on cryptographic proof rather than on trust, given the disappearance of intermediaries, perceived by the public as "trusted third-parties". More on this topic will be investigated in the next chapter, where its main form, the Blockchain, is examined. The most important point to make while dealing with distributed ledger technology is that it has great potential as one of the most disruptive examples of innovation that could be used in the financial sector. It could update the way in which most institutions, governments and corporations operate (i.e. tax collection, record land registries, etc.).

The decentralization of such a technology, that represents the most innovative and disrupting feature, is at the origin of the rise of cryptocurrencies, whose creation has been catalyzed by the desire to use a currency that could not be controlled, and to some extent manipulated, by central authorities. Cryptocurrencies aim at reaching the status of currency in a broader sense while maintaining their independence in control. Cryptocurrencies are one of the faces of the diamond of digital money.

1.2 VIRTUAL CURRENCIES

1.2.1 Historical background and current representation of money

Money and payment systems mirror the societies they operate for. Therefore, as well as societies, they have been thrilled and renovated by technology. As a matter of fact, innovation has recently qualified alternatives to traditional currency instruments. Due to cryptographic and computational progresses, development of digital alternatives to traditional forms of money have been possible that share and combine the main characteristics of each form of traditional money: "*peer-to-peer as cash, convenient as debit cards, and potentially cheaper to use and safer than deposits*." (Camera,2017). [1]

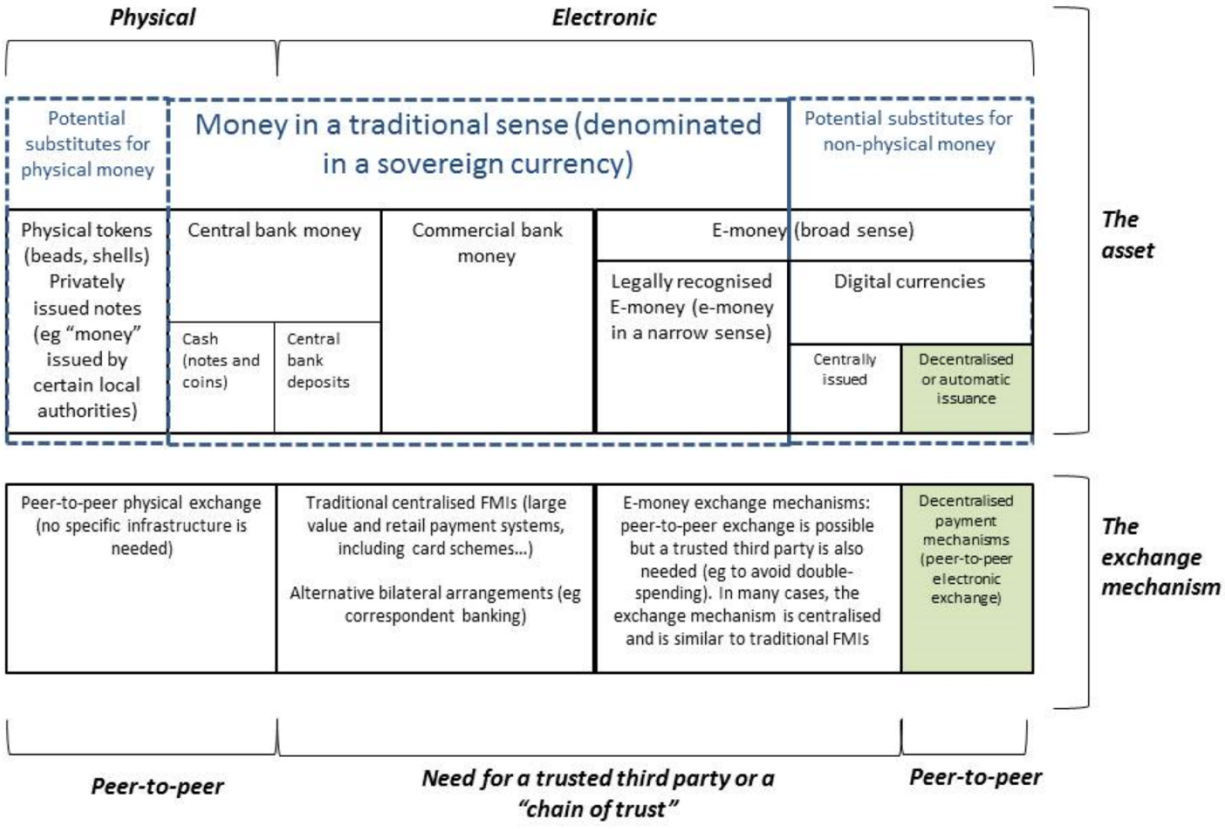
1: "A perspective on electronic alternatives to traditional currencies" (Camera, 2017, Sveriges Riksbank Economic Review 2017:1, 126-148

Money rationale is the social convention emerged to build trust among unknown parties in economic transactions. Symbolic objects become money as individuals start believing they could be used in the near future in exchange for goods and services and as a means of payment, both with formal and informal "quid pro quo" trading pattern.

As Aristotle believed that "*When the inhabitants of one country became more dependent on those of another, and they imported what they needed, and exported what they had too much of, money necessarily came into use*" ("Politics" Aristotle, translated by Benjamin Jowett, 1994-2009, Book 1 Part 1), when people satisfied the main needs and refined their way of living, division of labor created supply and demand of goods and services that required the use of a medium common to allow for market operations.

The firstly-appeared type of money was commodity money: objects with an intrinsic value, usually precious metals, acquired a value in their use of money. Coins from time to time replaced the use of commodities because of their peculiar characteristics of durability, portability, divisibility, difficult counterfeiting, general acceptance and value over time. Coinage was the first attempt of a central institution to put control on money and thus on the entire payment system. Coins are representative

Taxonomy of money and exchange mechanisms Figure 1



Source: CPMI report on digital currencies, November 2015, Bank for International Settlements

money because there are backed by precious metals (i.e. silver or gold) but usually their intrinsic value is less than their value in use. During the early Renaissance in the Western World the first type of fiat currency appeared initially in the form of trade bills of exchange, that constituted the buyer's promise to make a payment at a specified date in the future, and then as paper money: fiat money is a currency with no intrinsic value established as money by government regulation or law.

Later on, other types of currencies have been introduced: scriptural money, electronic money and virtual/digital currencies. Scriptural money is held by a bank in current accounts, where funds are recorded as money-units as part of a bank's record system. This facilitates transactions to the extent that there is no more need for a real exchange of paper notes, they take place only through an exchange of information between different accounts. Non-cash options of money appeared with the advent/arrival of debit and credit cards, always linked to use of bank accounts. Innovative electronic payment methods are coming up to fill the gap that the lack of accessible banking services around the world left: the broad definition of electronic money states that it is money which exists only in banking computer systems and is not held in any physical form. A narrower definition distinguishes between two kinds of e-money: sovereign digital money (which we will refer to as e-money) and non-sovereign digital money (abstract or cryptocurrencies). Monetary instruments in use today could be classified according to two basic dimensions as explained in Figure 1:

- The main features of the asset: the type of the currency (whether it is physical or electronic), and the denomination of the currency instrument — either a sovereign reference unit or not
- The exchange mechanism behind the asset: peer-to-peer or in need for an intermediary as a trusted third party

Legally recognized e-money is an electronic representation of physical sovereign currency. The main forms of e-money are commercial bank reserves with the central bank and the money created by commercial banks when they make loans. E-money can generate revenue for the issuer, which roughly corresponds to the spread between the yields on securities bought and liabilities issued; [2] the owner of e-money has a claim on the issuer's funds, while e-money represents a liability for the issuer.

Though e-money does not necessarily imply a legal right to a physical currency, it has so far typically implied, or is taken to imply, that owners of e-money can exchange the instrument at par for the underlying physical currency without restriction (e.g. demand deposits). This characteristic is behaviorally important because it may boost confidence in the currency system in periods of

uncertainty, since individuals can disintermediate their savings and independently store value by physically hoarding the instrument.

Broadly speaking, every financial institution participates in partly maintaining the ledger associated with an e-money system. This ledger is not public. Settlement relies on several layers of trusted institutions (banks, courts, central banks, etc.) and is ultimately accomplished by adjusting the reserves of commercial banks with the central bank. In this sense, the system is centralized and likely more expensive compared to systems that grant some decentralization. During the past fifteen years we have been seeing the creation of a new class of digital instruments that are not issued by a sovereign institution or commercial bank, are not denominated in a sovereign unit, and do not have a physical counterpart. Since these instruments may be used as a currency, they are variously labeled "electronic cash," "digital currency," "virtual currency," "altcoins," or "cryptocurrencies."[3]

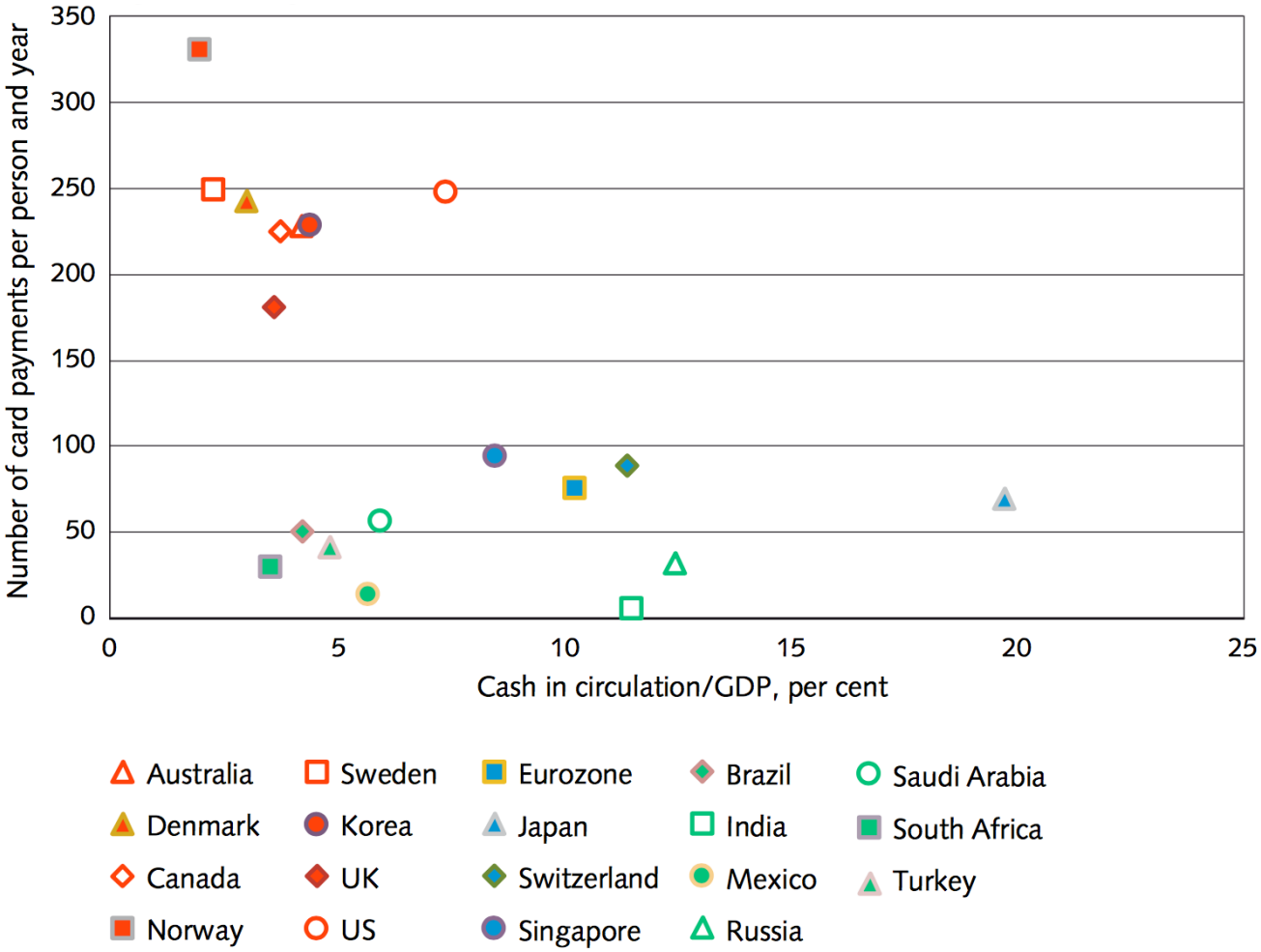
Among digital currencies we can individualize two different categories: centrally issued and decentralized. The former exchange mechanism is similar to the traditional FMIs because of its centralization, still based on a trusted third party even in peer-to-peer exchanges. The latter is completely decentralized and it is defined as "peer-to-peer electronic exchange". Current researches have highlighted the trend on the use of different kinds of money: the need for physical currency has declined as more and more citizens use electronic alternatives to cash. The use of cash is rapidly diminishing in some countries (Segendorf and Wretman, 2015). Figure 2, extracted by a research made by the Swedish Central Bank, shows the usage of cards and cash in a selection of countries in 2013. Different colors denote different patterns in the payment system according to the kind of monetary instrument used compared to the value of cash in circulation as percentage of GDP. The further up in the left- hand corner a country is, the more efficient this part of the payment market is considered to be. Correspondingly, this part of the country's payment market is considered to be less effective the further down towards the right-hand corner the country is.

2 In the case of central bank money, this is called seigniorage. It roughly corresponds to the interest income earned from the assets on its balance sheet (Haslag (1998)). A way to empirically calculate it is to take the product between the yield on an appropriately chosen portfolio of securities (typically, government bonds) and base money deflated by the CPI. As the choice of portfolio is somewhat arbitrary, empirical work often measures seigniorage as the change in monetary base normalized by CPI or GDP (Klein and Neumann (1990)). Extract from Camera,2017.

3 The architect of Bitcoin called it "electronic cash" (Nakamoto (2008)). The European Banking Authority (2014) and European Central Bank (2015a) call the instruments based on blockchain technology "virtual currencies". Some prefer "digital currency" (Broadbent (2016), Ali et al. (2014), Bank for International Settlements (2015)). Others use the words "cryptocurrencies" or "altcoins" (Bitcoin Magazine (2016), Danezis and Meiklejohn (2016)), (Camera,2017.)

The first group of countries are depicted in red and have the "card intensive" payment system, are industrialized and mostly well-developed. The ones painted in blue are still industrialized countries characterized by high cash usage and comparatively low card usage. Finally, the green faction is made up of developing countries with low card usage, due to recovering financial structural defects.

Figure 2:

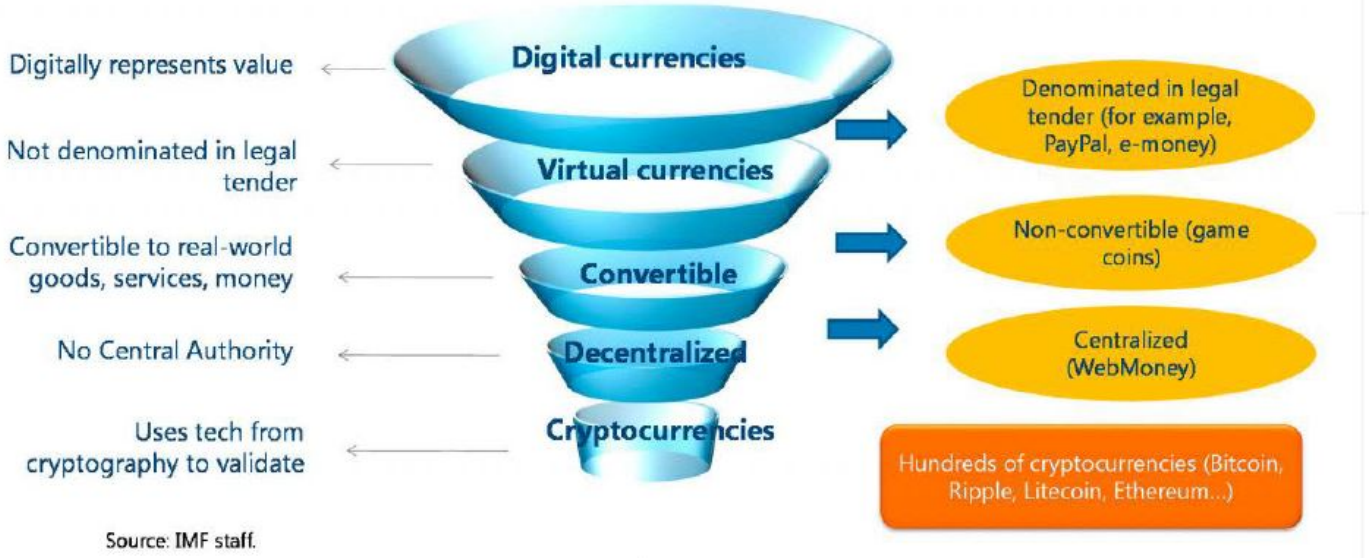


Sources: CPMI (2014b), ECB Statistical Warehouse and Norges Bank

Moreover, a significant portion of payments is typically executed by exchanging demand deposits, instruments that are risky and therefore costly to insure, but most of all based on intermediaries which have demonstrated all their pitfalls in the latest crisis that had shocked and modified the infrastructure of the entire financial system and probably of the society in its entirety. For this reason, an increasingly prominent movement took place since 1998 that had as its primary objective to exacerbate from central institutions the power to issue and thus control money. Cryptocurrencies have represented a collective action, they had their first public "release" in the early days of the crisis, right after the Lehman Brothers collapse in 2008.

1.2.2 In-depth taxonomy on virtual currencies

Virtual currency is a digital representation [4] of value that can be digitally traded and functions (at least in principle) as medium of exchange; and/or store of value; and/or unit of account, but does not enjoy legal tender status, while digital currency is referred to as a digital representation of either electronic money (fiat) or virtual currency (non-fiat). Virtual currency is neither issued nor guaranteed by any jurisdiction, and fulfills the functions usually given to money only by agreement within the community of their users. Figure 3



There exist two main basic types of virtual currencies: convertible and non-convertible. Convertibility in the case of virtual currency is not interpreted as "ex officio" as in the case of gold standard, but it is inferred as "de facto": the currency is convertible as long as a market of private participants making and accepting offers exist, and it is not guaranteed by law. A "convertible" or "open" virtual currency has an exchange value with a real currency for which it can be exchanged back-and-forth. A "non-convertible" or "closed" virtual currency is specific to a particular virtual domain, very popular for multiplayer online games such as World of Warcraft. It can never be exchanged for fiat currency since their validity remains within the specific virtual environment: sanctions would be applied to those in search for exchange opportunities in a secondary black market.

Still, if a robust secondary market exists, the currency characterization may change from non-convertible to convertible. These are the main Virtual Currency Schemes, that will be deeply studied in the next section of this chapter.

4 Digital representation is a representation of something in the form of digital data—i.e., computerized data that is represented using discrete (discontinuous) values to embody information, as contrasted with continuous, or analog signals that behave in a continuous manner or represent information using a continuous function.

Another aspect to look at while dealing with virtual currency is centralization vs non-centralization characteristic.

Centralized Virtual currencies are both open and closed, whereas decentralized can only be open. Closed virtual currencies are centralized by definition as they are issued by a central authority or administrator establishing rules that make them non-convertible. Open Centralized Virtual Currencies have a single third party controlling the system and working as administrating authority. The administrator issues the currency, establishes the use rules and maintains a central payment ledger. The exchange rate may be either floating, so determined by market demand and supply of the virtual currency, or pegged, fixed by the single authority at a value measure in fiat currency or another "real" store of value (i.e. gold or a basket of currencies). The administrator has the authority to redeem the currency at any time.

Decentralized virtual currencies (a.k.a. crypto-currencies) are defined as "distributed, open-source, math-based peer-to-peer virtual currencies" with no central administrating or monitoring authority. A cryptocurrency is protected by cryptography, that is to say it incorporates standards of cryptography to implement a decentralized, distributed, secure information economy. It relies on private and public keys made to transfer value from one individual or entity to another: each time it is transferred it must be cryptographically signed. A network of mutually distrustful parties, in Bitcoin called "miners", ensure the security, integrity and balance of the ledgers. These parties protect the network in exchange for the prospect of a randomly distributed fee, in Bitcoin called "block reward" (i.e. a small amount of newly created bitcoins), and some transaction fees users pay as an incentive for the parties to include their transactions in the next block. The first specimen of a cryptocurrency is Bitcoin: it uses a proof-of-work system to validate transactions and maintain the "blockchain", the most powerful discovery impacting on the financial system. More efficient proof methods as proof-of-stake systems came afterwards and implemented the model created by Bitcoin from the creation of alternative cryptocurrencies to Bitcoin, officially recognized as the first mover but much work had been done for decades before its appearance.

1.2.3 Virtual currencies history

The pursuit of an independent digital currency really got started in 1992.At that time Timothy May, a retired Intel physicist, invited a group of friends over to his house in California to discuss two important issues that would have hardly impacted the world in the next years: privacy and the nascent Internet. In the 80's, cryptographic tools, such as the first public-key encryption and "Pretty Good Privacy" by Phil Zimmermann, proved their usefulness for controlling the identity of who could access digital messages. The incoming works and inventions scared governments around the

world about a sudden shift in power and information control, therefore, access to cryptographic protocols had begun to be restricted.
The group meeting in California took the name of "cypherpunks"—and gave them the superhero-like task of defending privacy across the digital world. A cofounder Eric Hughes in a week wrote a program to receive encrypted e-mails, and send them back out to a list of subscribers who wanted to join this anarchic group. Each subscriber got this message:

"Cypherpunks assume privacy is a good thing and wish there were more of it. Cypherpunks acknowledge that those who want privacy must create it for themselves and not expect governments, corporations, or other large, faceless organizations to grant them privacy out of beneficence."(Williams,2017) [5]

The main concern from cypherpunks was about the security and privacy of people's private transactions, spending habits and further about the control on issuance of money by governing authorities. For this reason, a new system should have been created to democratically give back to people to power and the freedom they were about to lose in this upcoming world of Internet and technology.

The first publication on cryptocurrencies dates back to 1998, when Wei Dai provided the description of "b-money": an anonymous, distributed electronic cash system.[5]
Thereafter there has been the creation by Nick Szabo, a computer scientist, of "Bit Gold", a first attempt to imagine a new digital currency. Bit gold scheme is considered as the basis on which Bitcoin has been developed, nevertheless no emphasis was given to privacy in this experiment. Indeed his primary goal was to transform the binary code intrinsic to the virtual world into something valuable over time by people. He thought about the analogy between difficult-to-solve problems and the difficulty of mining gold, for every solution provided to the puzzle solved, since it took time and energy and so it deserves value, a reward could be given in form of a digital coin. In bit gold scheme, a participant would dedicate computer power to solving cryptographic equations producing a specific binary string assigned by the system.
In the network solved equations would be sent to the community which either accept or reject them. If accepted, the work had to be credited to the solver and it becomes part of the next challenge, creating a growing chain of new property. This feature of the system provided a clever way for the

5 "Cryptocurrency compendium: A Reference for Digital Currencies" – Devin Williams, 2017, sec. History

network to verify and time-stamp new coins, because unless a majority of the parties agreed to accept new solutions, the next equation could not be started.
The problem when attempting to design transactions with a digital coin is the "double-spending" issue because once data have been created, their reproduction is a simple matter of copying and pasting data. Some e-cash scenarios have solved this problem by relinquishing some of the control to a central authority, keeping track of the balance of each account (e.g. DigiCash, a prototypic form of digital money, handing the oversight task to banks). Bit gold provided a decentralized solution to this problem, creating a network-based consensus for the acceptance of transactions. Many problems continued to afflict the system as the proper value assignment to different strings of data not equally difficult to make or more importantly the nature of the system controlling the transfer of currency.

After b-money and bit gold failure, many years passed until a new type of augmented cryptocurrency has been created. In 2008, an individual or a group of people under the name of "Satoshi Nakamoto" wrote a proposal for Bitcoin. The starting idea is a chain of data similar to bit gold but rather than creating a chain of digital property, the working system of Bitcoin records a chain of transactions. Bitcoin can be thought of as a digital ledger book. The ledger records how many bitcoins each user has at a given time and the balance of each account, by necessity, is public information. Every transfer has to be announced publicly and the entire network of users appends the transaction to the ledger, which they all need to agree on. In this kind of system, money can still exist only in digital form but cannot be spend twice (i.e. solving the double-spending problem threatening previous cryptocurrency systems). The basic working of Bitcoin, that will be furtherly analyzed in the following chapter, is based on participants who are spread across a global peer-to-peer network, and on transactions taking place between addresses on the network. Address ownership is verified through public-key cryptography, without publicly revealing who the owner is.

After the increase in awareness and interest about cryptocurrencies, many other cryptocurrency systems have been launched either with little innovations with respect to Bitcoin, it is the case of the so-called "Altcoins", or with cryptocurrency and Blockchain innovations. Bitcoin first operation is recorded in January 2009 and the second cryptocurrency, Namecoin, emerged in April 2011. Nowadays, hundreds of cryptocurrencies are being traded since then.

1.2.4 Virtual Currency Schemes advantages and potential risks

Virtual currency schemes (VCS), as highlighted in the "Virtual Currency Schemes" from the ECB document published in February 2015, could represent from the user's perspective, either for payers or payees, and from the payment system at a general level some advantages and risks. From users' point of view, the payer benefit from a shorter time for the payment transaction to be verified and settled. This would the case not only for decentralized VCS but mostly for centralized VCS, whose process is instantaneous. Another pro of this scheme is of course that the speed at which the process takes place does not depend on the geographical locations of the parties involved. The costs associated with VCS are usually perceived as low if compared to the traditional systems: there are no account-holding fess when using a wallet to store the token, and transaction fees can be seen as negligible. Both the payee and the payer benefit from the absence of direct foreign exchange cost, although they are exposed to exchange rate risk if they want to keep an amount of virtual currencies to be used in the future.

Due to its global scale, transactions are not restricted by geographical or logistic problems. From the general perspective, decentralized VCS allow for the processing cost distribution over several subjects involved in the mining activity. This allows the network to reach reasonable computing power without requiring any large single investment. A strong scalability is granted to the network, as long as people participate to the system.

A network-related advantage is the fact the developments of the software is taken by users on a voluntary basis due to the open source nature of the system.

Thus, advantages are related to usage possibilities, costs, speed, and development of alternative payment solutions, that could pose a challenge to traditional payment and settlement system.

Looking at the other side of the coin, risks are relevant and lies beneath the nature of VCS. The most significant risks are the following:

- Lack of transparency due to technical infrastructure difficulties and limited availability of information. This failure can be used for fraudulent activities.
- Absence or unclarity of legal status due to the lack of legal obligations for each entity involved. Even the taxation regime in some countries is not well defined, adding costs to users. Furthermore, users are exposed to risks resulting from frauds as in case of the default of Mt. Gox exchange in 2014.
- Lack of continuity and potential illiquidity since decentralized digital currencies do not have any intrinsic value. If their market collapses, users will be left with valueless units.

Continuity of the business could be additionally affected by bankruptcy or lack of profitability.

- High IT and network dependency due to the digital nature of the schemes. In this sense, risks stem from technical failures in the mechanism to hacking, that could take place both at an individual level and on a wider scale
- High volatility, which represents the most severe drawback for users. This topic will be addressed in the next chapter when we would examine the possibility for the most important cryptocurrency in the market, Bitcoin, to be thought of as a currency in a broader sense.

Anonymity or "pseudonymity" feature stands in the middle: some users, not only fraudulent or criminal, are concerned with the protection of their privacy and their sensitive data, but this arrangement does not allow to put in place mechanisms enabling the resolution of mistaken or criminal transactions.

Related risks associated with cryptocurrencies may be: potential AML/CFT (aka anti-money laundering and counter-terrorist financing) risk, and anonymity risks.

Money laundering and terrorist financing[6] may be enhanced by the greater degree of anonymity provided by these VCS compared to traditional non-cash payment methods. This is what Min Zhu, the Deputy Managing Director of the IMF, thinks about the role of effective AML/CFT standards: "Effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse."

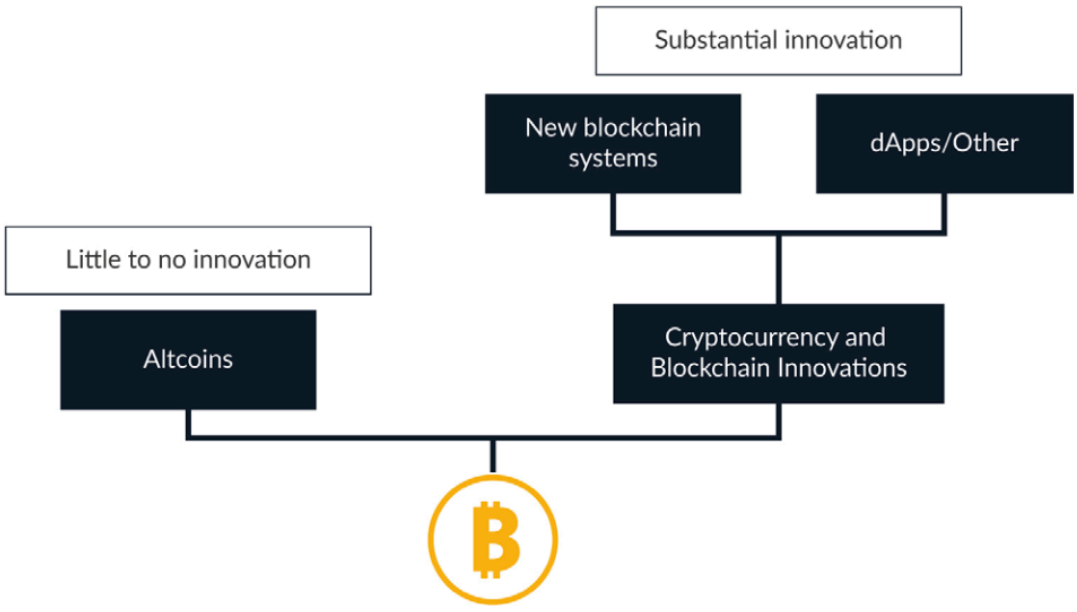
6: The reasons behind the abuse of money laundering and terrorist financing are identified in the 2013 NPPS Guidance. Money laundering requires an underlying, primary, profit-making crime (such as corruption, drug trafficking, market manipulation, fraud, tax evasion), along with the intent to conceal the proceeds of the crime or to further the criminal enterprise. These activities generate financial flows that involve the diversion of resources away from economically- and socially-productive uses—and these diversions can have negative impacts on the financial sector and external stability of member states. They also have a corrosive, corrupting effect on society and the economic system as a whole. Because of the negative consequences of these forms of financial abuses on our members' economies and financial systems, the IMF has been very active for over ten years in the AML/CFT area. - IMF.org

1.3 CRYPTOCURRENCIES

1.3.1 Cryptocurrency organization

All cryptocurrencies present the common elements of the public ledger (aka Blockchain) which is shared among the participants in the network and of the use of native tokens as incentive to participants to run the network in the absence of a central authority granting safety and control. The difference among cryptocurrencies stands within the level of innovation displayed. As Figure 4 describes, Bitcoin represent the starting point for cryptocurrencies which have been created since 2011. There exist two paths for the development of cryptocurrencies: Altcoins, which are largely clones of bitcoin and simply feature different parameter values (e.g. different currency supply, issuance scheme and/or block time) as in the case of Dogecoin and Ethereum Classic; and more innovative cryptocurrencies, providing novel and enhanced features to the ones offered by Bitcoin, such as the introduction of new consensus mechanisms, from proof-of-work to proof-of-stake, and decentralized computing platforms with capabilities for "smart contracts", that allow for non-monetary use cases.

Figure 4



Source: Global Cryptocurrency Benchmarking Study, Dr Garrick Hileman & Michel Rauchs, 2017

Among these emerging cryptocurrencies we can distinguish between two categories: new public blockchain systems and dApps /Other[7]. The former group features their own blockchain, and their

7 dApp stands for decentralized application.

most well-known examples in the market are Ethereum, Peercoin and Zcash. The latter exists on additional layers constructed on top of the existing blockchain system, such as Counterparty or Augur. DApps have the potential to surpass the world's largest software corporations in utility, user-base, and network valuation because of their superior characteristics: incentive-based structure, flexibility, resiliency, transparency, and distributed nature.

Bitcoin represents the standard to which other cryptocurrencies refer to. It is the first "peer-to-peer electronic cash system", as the White Paper from Satoshi Nakamoto states, based on the following characteristics:

- It enables direct transactions with no need for a trusted third party;
- Transactions enabled by the system are non-reversible;
- Credit cost in small casual transactions are reduced;
- Transaction fees are reduced;
- Unlike previous cryptocurrencies, double-spending is prevented.

The largest after Bitcoin cryptocurrencies, represented according to a market cap share ranking, are the following:

- ETHEREUM (ETH) – "a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference" [8]. It has its own programming language (Turing- complete) [9] running on a blockchain that helps developers to build and publish distributed applications. It has been officially launched in 2015, although a previous native cryptocurrency, "ether", was already in the market. Scripts and contracts that are run and signed by every participating node are recorded on the blockchain.
- DASH – a cryptocurrency launched in 2014 whose primary focus is on privacy. It is open source, peer-to-peer and it offers the same features as Bitcoin with advanced capabilities (i.e. instant transactions – InstantSend-, private transactions - PrivateSend, and decentralized governance – DGBB). The decentralized governance associated with a decentralized budgeting systems sorts it as the first decentralized autonomous organization.

8 Ethereum.org definition

9 In computability theory, a system of data-manipulation rules (such as a computer's instruction set, a programming language, or a cellular automaton) is said to be Turing complete or computationally universal if it can be used to simulate any Turing machine. It is a mathematical model of computation that defines an abstract machine which manipulates symbols on a strip of tape according to a table of rules (Wikipedia)

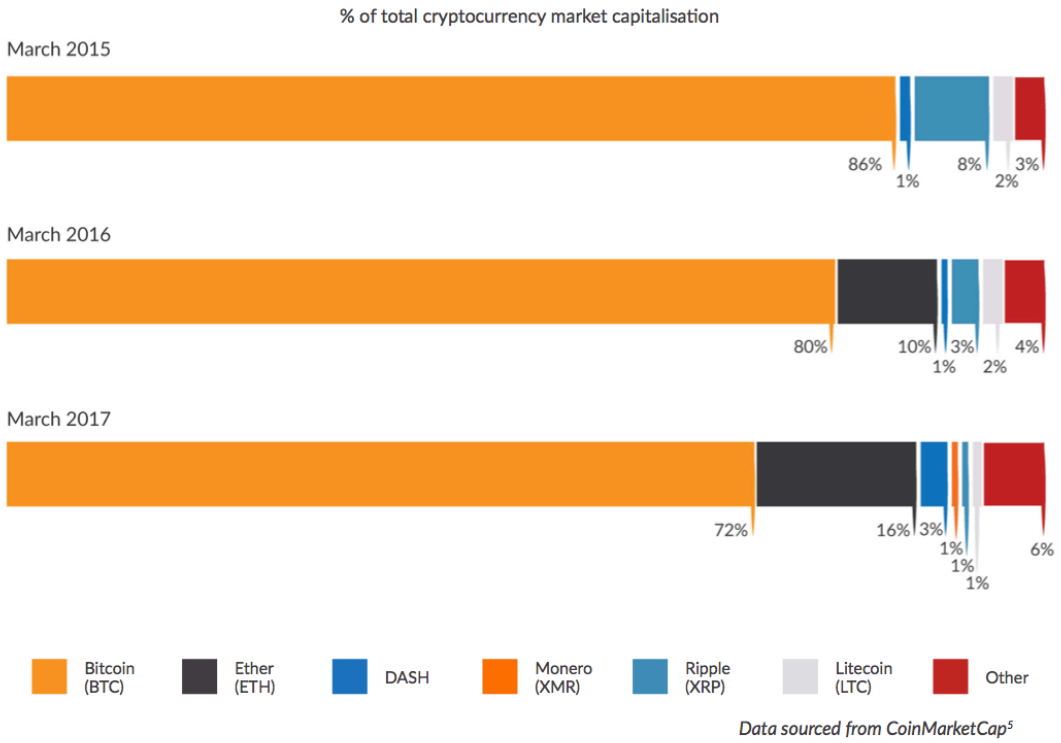
- MONERO (XMR) – a cryptocurrency system aiming at providing completely anonymous digital cash. To obfuscate the origin, transaction amount and destination of transacted coins the currency uses ring signatures, confidential transactions and secrecy addresses. It is decentralized but it is considered as digital cash.
- RIPPLE (XRP) - a technology working either as a cryptocurrency or as a digital payment network for financial transactions. Ripple operates more as a digital payment protocol used by institutional actors such as money service businesses and large banks. It does not have a blockchain, it is based on a "global consensus ledger". [10] Two of the functions of the native token (XRP) are to be a bridge currency between national currency pairs rarely traded, and to avoid spam attack.
- LITECOIN (LTC) – launched in 2011, it is the cryptocurrency which is more similar to Bitcoin. It is based on an open source global payment network not controlled by any central authority. The key differences with Bitcoin stand in the block generation rate, the use of Scrypt' as a proof of work scheme, and the more copious total supply of 84 million LTC.

Bitcoin remains the dominant cryptocurrency in terms of market capitalization, nonetheless other competitors are increasingly cutting into its historically dominant market cap share. It is still dominant for the average number of daily transactions, where it is by far the most widely used cryptocurrency. ETH has established itself as the second-largest cryptocurrency, furthermore privacy-focus cryptocurrencies, DASH and XMR, are increasing their popularity, now constituting a combined 4% of the total cryptocurrency market capitalization. The current situation is described in figure 5.

Decentralized Applications or dApps can be classified into three categories according to the complexity of the system, based on the criterion on whether the application has its own blockchain or it uses the block chain of another dApp:

10 The XRP Ledger is a shared, global ledger that is open to all. Individual participants can trust the integrity of the ledger without having to trust any single institution to manage it. The rippled server software accomplishes this by managing a ledger database that can only be updated according to very specific rules. Each instance of rippled keeps a full copy of the ledger, and the peer-to-peer network of rippled servers distributes candidate transactions among themselves. The consensus process determines which transactions get applied to each new version of the ledger (ripple.com)

Figure 5:



- Type I dApps have their own blockchain (e.g. Bitcoin, Litecoin and other "Altcoins")
- Type II dApps use the blockchain of a Type I dApp. They are protocols and necessarily use tokens for their function (e.g. Omni Protocol)
- Type III dApps use the protocol of a Type II dApp. They work with the same principle as Type II dApps since they are protocols and necessarily use tokens for their function (e.g. SAFE Network using the Omni Protocol with the purpose of issuing "safecoins", that can be used to acquire distributed file storage)

Because of this structure, due to network effects and the ecosystem around each decentralized application, there are few type I dApps, more type II dApps and much more type III dApps. Bitcoin itself is considered a type I dApp besides it effectively solves the problems arising from a trust-less and scalable electronic cash system through the use of a peer-to-peer distributed ledger, known as the Bitcoin blockchain. It is an application with which users can interact through computer software. It is a dApp because all its software applications are open-source, with open and public record of transactions and no control by any outsider entity; it generates the tokens, necessary for Bitcoin to function, with an algorithm that cannot be changed; any change to the system must be approved by a majority consensus of the user with the proof-of-work mechanism.

In this regard, there exist two mechanisms to establish consensus in decentralized applications: proof-of-work, POW, and proof-of-stake, POS, mechanisms. These schemes are referred to as "timestamping schemes", used to avoid the need for a trusted third party to govern the system.
The former prescribes that decisions about changes in a dApp are made according to the amount to work that each user contributes to the operation of the application. This is the approach used by Bitcoin for transactions, and it is generally called "mining".
The latter stipulates that decisions about changes in a dApp are made according to the percent ownership (aka the holding ratio) each user has over the application. The scheme is essentially dependent on the token and there is no standard form of it.
These mechanisms can be used in parallel and this combination allows a dApp to operate with less energy consumption than POW alone needs, and allows the structure to be more resistant to attacks.

Another important element in dApps is the mechanism to distribute tokens. They are three: the mining mechanism, where tokens are distributed to the users who contribute the most to the operation of the dApp, as for Bitcoin; the fund-raising mechanism, where tokens are distributed to the funders of the initial development of the dApp; and the development mechanism, where tokens are generated through a predefined apparatus and are available only for the development of the decentralized application. The first mechanism pertains to POW consensus system, while the other two to POS consensus systems.

1.3.2 Key cryptocurrency properties

In so far, we had a first glance/foretaste about what the cryptocurrency world is about and which are its main components, looking at the differences standing behind each system. However, all cryptocurrencies result from a combination of multiple accomplishments in several disciplines including computer science, through the peer-to-peer (P2P) networking; cryptography, either through cryptographic hash functions or digital signatures; and economics due to its intrinsic structure that could be essentially represented using game theory.
A cryptocurrency can be described as a digital token existing within a specific system, which generally consists of a P2P network, a consensus mechanism and a public key infrastructure. All network participants, called "nodes", enforce the rules governing the system. The rules stem from the definition of validity for a transaction to the specification of the total supply and the issuance scheme of the digital token. This role represents one of the most important innovations of these systems insomuch it was originally entrusted with a central authority, now essentially deprived, at least in principle, of the financial control over these new types of money.

Every transaction in the transaction history can be independently verified by nodes since a copy of the shared ledger is possessed by each of them. The shared ledger that in general takes the form of a chain of blocks comprised of transactions (aka blockchain), is updated in a constant manner through the "mining process" with which new units of the cryptocurrency are created. Joining is free and completely inclusive (i.e. no discrimination is made throughout the system, at least among people who have access to Internet, which nowadays represent the vast majority of the population even in developing countries, surely more inclusive than the banking system) and there is no contract ruling exit times and procedures. No identity is attached to users.

There are three key properties for cryptocurrencies: digital bearer asset feature, integrated payment network, and, for some currencies only, additional properties and functionalities enabling non-monetary use cases.

The native token must constitute a "censorship-resistant, digital bearer asset"* for the digital currency to be considered decentralized: a bearer asset in the sense that the person in control of the respective private key controls the specific amount of cryptocurrency associated to the corresponding public key; censorship-resistant in the sense that nobody neither can freeze or confiscate funds denominated in cryptocurrency nor repress transactions performed on the payment network.

The payment network, on its side, has to be integrated: it has a global reach and it can be used to transfer funds in a short period of time with no geographic limitations. No particular location or jurisdiction indeed can bound the system. This payment system allows for cost-effective micropayments: transaction fees are significantly lower than those charged by traditional payment network operators and do not depend on the amount transferred, rather on the transaction size measured in bytes. Significant advantages for merchants is posed by the irreversibility of the payments once confirmations on funds transfer and receipt are enough. Privacy about sensible data such as contract details, credit card numbers and passwords do not have to be stored on the server, users are identifiable only by their cryptocurrency address derived from the public key: "pseudonymity", and in some cases anonymity, is granted.

Therefore, this integrated payment system possesses, at least in principle, four out of five criteria for an efficient payment system:

- ✓ Technical efficiency through the distributed ledger technology, although some problems may arise in the mining process costs and integrity
- ✓ Accessibility and non-discrimination since it can be accessed by anyone at any place in the world

- ✓ Efficient pricing as it is lower than the traditional payment systems, although it is not cost-based, but it is based on the amount of work behind the involved transaction
- ✓ International compatibility because it is the same in all countries
- Operational stability with contingency plans in case of problems is subjective to the different cryptocurrency systems

The property enabling non-monetary uses beyond the digital assets and currencies is projected to have a big impact on the future of the whole financial system. By now, Bitcoin can be used as an undisputable data store: specific metadata in form of hashes is embedded into transactions carrying special meaning outside of the cryptocurrency network. Moreover, it can work as a decentralized timestamping service (this topic will be analyzed in the next section together with other topics concerning cryptocurrencies). This kind of mechanism supports the creation of "overlay networks" or "embedded consensus systems", built on top of the core network with different functionalities and use cases (aka dApps). Some systems have been created even with the aim of enabling specific non-monetary use cases, as in the case of decentralized computing platforms, and they use the native token only as an incentive for participants to preserve the running of the system.

1.3.3 Factors influencing the development of cryptocurrencies

Digital currencies based on the use of a distributed ledger have been driven in the rise and development by technology, which is considered to be the key enabling factor for innovations in the financial sector and specifically in the payment system.
Nevertheless, many other factors influence the development of digital currencies, especially associated to the decentralized attributes.
Among the factors we can classify two kinds of factors: supply side and demand side factors.
The supply side is mostly represented by private sector non-banks[11]. The factors influencing from the supply side are: fragmentation, scalability and efficiency, technical and security concerns, and business model sustainability. The system is fragmented because there are more than 600 digital currencies in circulation, presenting different protocols to process and confirm transactions. Even if the systems may be considered cost-efficient from the individual point of view, because transactional fees are lower, the industry is very capital-intensive. Incentives for certain actors, such as miners, to support the scheme are straightforwardly related to the currency issuance, that may be

11 "any entity involved in the provision of retail payment services whose main business is not related to taking deposits from the public and using these deposits to make loans": see CPMI, *Non-banks in retail payments*, September 2014.

capped, and to competing schemes with enhanced degrees of efficiency and security.

The demand side is based on the fact that end users must be incentivized with benefits over traditional services to increase the use and acceptance of the schemes. Demand side factors, which are significant both for the direct use of the digital tokens and for indirect use, the infrastructure, that might influence the future evolution of digital currencies are the following:

- Security breaches that might undermine users' confidence in the VCS, particularly critical in an environment with no trusted third-party;
- Cost is usually an appealing element to customers as the VCS may offer lower transaction fees and a viable alternative for cross-border payments. (Cross-border reach may be an advantage)
- Usability in the adoption of new methods and mechanisms must be intuitive, convenient, and easy to integrate;
- Volatility and risk of loss associated with price and liquidity risks due to the variability of exchange rates according to multiple factors difficult to predict.

1.3.4 Legality and regulation for cryptocurrencies

The legal status of cryptocurrencies varies across countries and many of them still not define it or are slowly changing their policy about it. A limited number of countries have taken an explicit position about the allowance of cryptocurrencies in their financial systems: some tolerate their use and trade, while others have restricted or banned it either for certain related activities or at all. By now the ECB and the IMF have decided to take an examiner role for cryptocurrencies and in general VCS through papers that analyze the potential relevance and risks for retail payments posed by these new infrastructures. The ECB recognized in its report in 2012 the main areas in which virtual currency schemes might affect the central bank's tasks, which are: price stability, financial stability, payment system stability, prudential supervision, and preserving of the financial system integrity.

Most of the concern is about Bitcoin, which is the most popular and so mostly used cryptocurrency all over the world. Bitcoin and many cryptocurrencies are in principle covered by regulations covering digital money, which might not cover all aspects of Bitcoin since they cover virtual goods. Regulations that cover financial instruments based on cryptocurrencies are still in the early stages.

1.4 CRYPTOCURRENCY INDUSTRY AND SECTORS

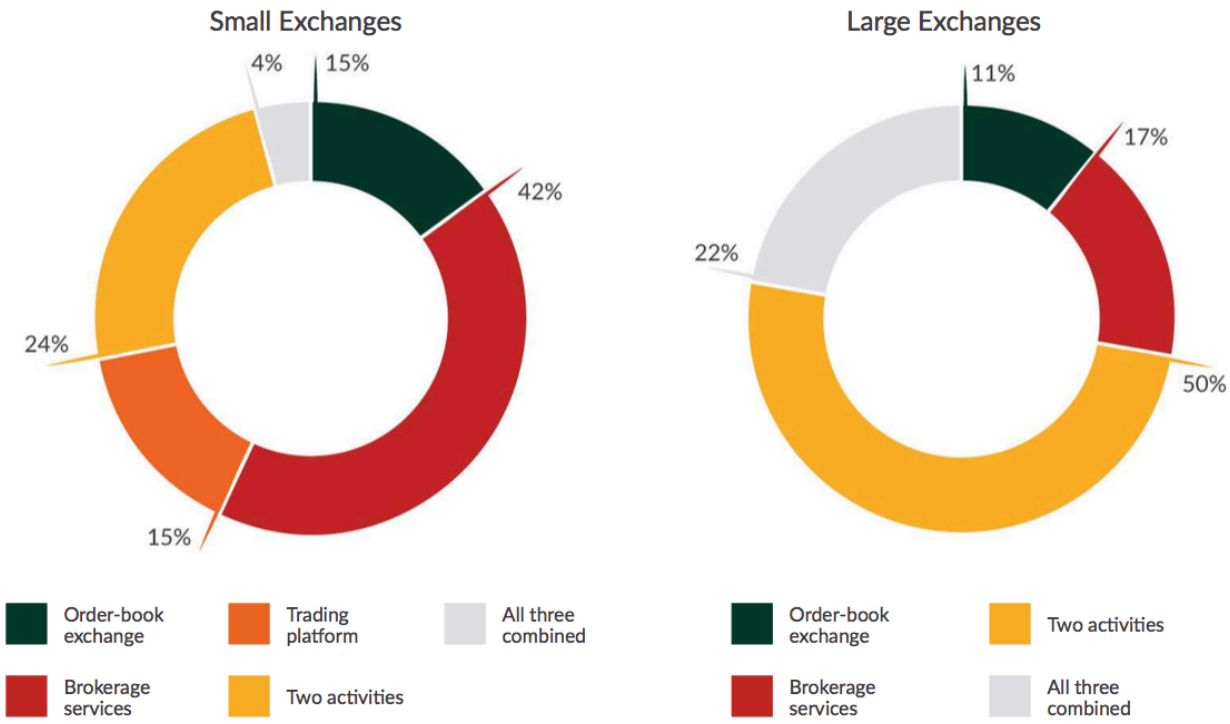
A multitude of companies and projects have been emerging in the last decade that provide services facilitating the use of cryptocurrencies. An ecosystem of diverse set of economic actors provide products, services and applications involving the use of cryptocurrency. Industry actors build interfaces between the multiple cryptocurrency systems, traditional finance and the global economy. Through these interfaces the value of cryptocurrencies is established and improved.
The process for participating to the network starts with users mining in order to earn the token, that can only be spent or sold within the same system. To counter this, exchanges are established for the trade of cryptocurrency either with other cryptocurrencies or with national currencies – this allows for the price determination, which give the tokens the status of digital assets with a certain value. Exchanges offer new users a way to join the system, thereby connecting the initially closed system to the traditional financial system. As the systems becomes more accessible and widely used, the cryptocurrency begins being accepted by merchants, hence making the currency a medium of exchange. Merchants are helped by payment companies providing tools to facilitate cryptocurrency payment and to reduce exposure to price volatility. In this way, the companies act as a gateway that bridges the cryptocurrency virtual world to the global economy.
Moreover, many actors developed supporting services: data service, with block explorers and market data sites; media and consulting. Other projects have arisen building a complex group of overlay networks on top of the existing cryptocurrency systems to expand the use of these systems to non-monetary use cases. These platforms have been launched to make the use of cryptocurrency available to mainstream users.

In detail, the key cryptocurrency industry sectors are four: exchanges, whose primary function is the purchase, sale, and trading of cryptocurrency; wallets, used for the storage; payments, facilitating payments via cryptocurrency; and mining, whose key role is that of securing the blockchain by computing an enormous amount of hash functions to find the validity of a block to add to the global ledger.

1.4.1 Exchanges

They offer liquidity as they offer a marketplace for trading and set a reference price for the cryptocurrency. It is the largest sector in the industry for the number of operating entities and employees involved. Large exchanges where the four most relevant national currencies are traded (USD, EUR, JPY and CNY) dominate global cryptocurrency trading volumes. USD is the most widely supported national currency on exchanges.

The services and activities made by an exchange fall into three categories: order-book exchange, a platform that uses a trading engine to match orders from users to buy and sell; brokerage service, a service that allows users to acquire and sell cryptocurrencies at a given price in a convenient way; and trading platform, that provides a single interface for the connection to other exchanges and delivers leveraged trading and cryptocurrency derivatives services. The most important division in this sector is although based on the size of the exchange: small exchanges specialize into one of the three listed services, while large exchanges provide multiple types of activities (as shown in figure 6 here below)



Source: Global Cryptocurrency Benchmarking Study, Hileman & Rauchs, 2017

The most important operational challenges and risk factors are the most sensitive concerns for exchanges as they continue to be popular targets for criminals. For small exchanges the highest risk factor are security breaches that could result in a loss of funds, while for large exchange is the second highest because they use a greater number of external security providers. Although it seems a paradox, a great challenge is posed on exchange by regulation, which represents one of the main problematic issue for large exchanges. Indeed, only 35% of large exchanges have a formal government license or authorization compared to 52% for small exchanges. Small exchanges have difficulties with obtaining and maintaining banking relationships and additionally much more concerns with respect to fraud, whose impact is more severe due to the limited scale of the

operations and budget.
Security measures adopted by exchanges may be external, through external security providers, or internal, as the use of multi-factor authentication for access control.

1.4.2 Wallets

They are software programs used to securely store, send and receive cryptocurrencies through the management of the cryptographic keys, both the public and the private key. Wallets provide a user interface to keep the balance of cryptocurrency holdings and automate specific functions, such as the cost of the fee related to transactions so as to achieve the desired confirmation time. Each cryptocurrency has a basic wallet functionality (e.g. Bitcoin Core for Bitcoin and Mist browser for Ethereum), but these reference implementation wallets have been usually substituted or at least assisted by several wallet providers, ranging from open-source projects by volunteer developers to projects backed by registered corporations, which represent the majority (85% of the wallets).
Wallets can be distinguished into three categories according to the control on access to user keys. Most of the wallets do not directly control access to user keys nor take custody of funds, in this case each user controls his/her own key. In other cases, the wallet provider controls keys or users have the option between the two previous control mechanisms.
The services are supported by multiple formats, from web to mobile, and allow to switch from one to another. More than half of the most popular wallet providers offer integrated currency exchange services and other additional features such as linked credit or debit card and insurance. Integrated currency exchange services are provided according to three different models: traditional, integrated third-party, and emerging models. The former, "the centralized exchange/brokerage service", implies a central exchange operator that takes deposits and offers a price for the sale/purchase of currencies, actively handling the exchange and acting as the counterparty to users. The middle model, the "integrated third-party exchange", integrate an independent exchange services within the wallet interface, where users can sell and purchase the currencies through a partnered third-party exchange. The latter, "P2P exchange or marketplace", enable users to make currency exchanges between each other with no need for a centralized exchange operator. The wallet interface acts a decentralized secure marketplace connecting buyers and sellers only through its infrastructure.

1.4.3 Payments

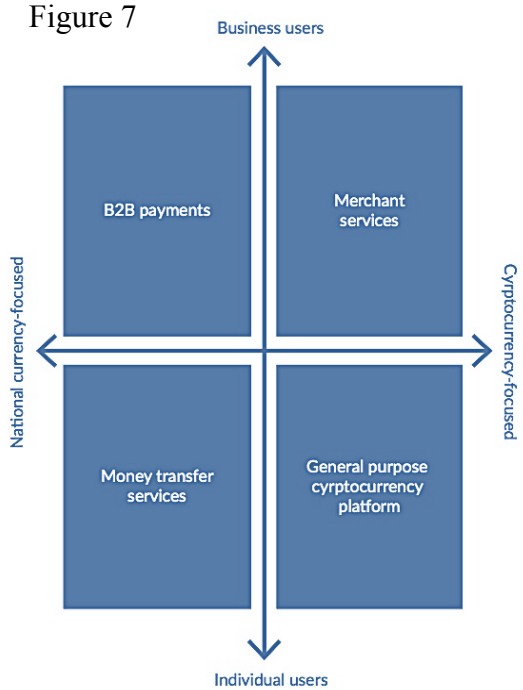
Companies operating in this sector act as channels connecting national currencies and cryptocurrencies. All cryptocurrency systems are equipped with an integrated payment network for

the process of transactions in cryptocurrency units. Although these networks are already provided by the systems, many users prefer services run by third-party payment service providers. The use they make of cryptocurrencies can be divided into two broad categories: payment rail and cryptocurrency payments. The former is defined as "national currency-focused", while the latter is "cryptocurrency focused".

National-currency focused category is characterized by the use of cryptocurrencies as a channel for transfer of national currencies that becomes faster and cost-effective. The cryptocurrency is in this case a means for the transfer rather than the primary focus. This category is then divided into two narrower groups depending on the nature of the payment activity. The first is for money transfer services, such as cross-border payments, primarily provided to individual. They are denominated in national currencies and include traditional remittances and bill payment service. The second is for B2B(business-to-business) payments. In this case platforms provide payments, denominated in national currencies, for businesses usually across borders.

Cryptocurrency-focused category is on the other side characterized by the presence of a platform that facilitates and broadens the use of cryptocurrencies. Transfers can either be denominated in cryptocurrencies or in national currencies terms. Two more limited distinctive groups can be identified in this category. Merchant services process payments for merchants that accept cryptocurrencies. They may also be provided with additional merchant services. On the other hand, a "general-purpose cryptocurrency platform" performs a variety of cryptocurrency transfer services as instant payments to users on the same platform through cryptography. Here payments are denominated in cryptocurrencies but they can be easily exchanged for national currencies.

Figure 7



Source: Global Cryptocurrency Benchmarking Study, Hileman & Rauchs, 2017

A small taxonomy on the payment sector is depicted in figure y, where payment rail for cross-border transactions represent the majority of the operations.

The major challenges currently faced by cryptocurrency payment companies are ranked according to the urgency they pose on their operations. The most important risk factors for both broader categories are the difficulty of obtaining and maintaining banking and MTO * relationships, and high cost of regulatory compliance, especially for money transfer services platforms.

National currency-focused category is more challenged than the cryptocurrency-focused one by the exchange rate risk, better managed by the latter thanks to additional operations in a cryptocurrency exchange. Moreover, B2B payment platforms face customer acquisition costs and competition from FinTech firms.

1.4.4 Mining

A critical role in all cryptocurrency systems is performed by miners, responsible for unconfirmed transactions assemblage into new blocks and addition to the blockchain or global ledger. Their job is to provide the computing power necessary to secure the blockchain by computing a large number of hashes to find a valid block. Every valid block is then added by a miner to the blockchain and generates a reward for the miner.

Mining has grown from a simple activity performed by early adopters on ordinary hardware into a complex capital-intensive industry using custom hardware equipment. The value chain in mining industry works as follows:

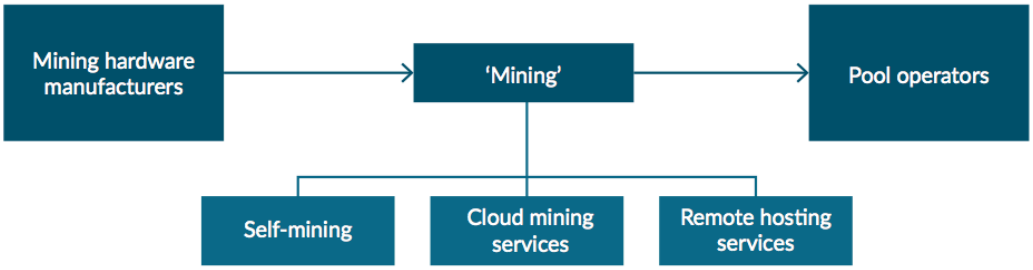


Figure 8, source: Global Cryptocurrency Benchmarking Study, Hileman & Rauchs, 2017

Few mining hardware manufacturers, organizations designing and building specialized equipment, supply the industry with the most innovative and efficient apparatus. Since not everyone can afford the equipment additional services of cloud mining and remote hosting have emerged to offer users the possibility to participate to the mining process. Large mining companies mine in their own mining facilities all over the world. Both individual and corporate miners "point their hashing power" towards multiple mining pools. They combine computational resources from several miners to increase the chance and frequency of finding new blocks and then distributing mining rewards among participants based on the proportion of contributed computational resources.

There are several legal and regulatory risk factors attached to the miner position, for which small miners are more threatened by. These are: a tighter regulation creating barriers to mining and thus to the cryptocurrency adoption and the possibility of an increased taxation on mining profits. Surprisingly miners, above all large ones, are not worried neither about a potential government ban on cryptocurrencies nor about the transformation of the mining activity into a money transmission service, requiring a money transmission license to be hold.

CHAPTER 2: CONSIDERATIONS ON BITCOIN: A monetary and financial analysis

2.1 INTRODUCTION TO BITCOIN

2.1.1 Main definitions

Bitcoin is an overfull world and there are many misconceptions about what this technology is and is not. The most general definition describes Bitcoin as a decentralized digital currency, where no individual or institution backs or control it, it is not backed by any physical good. It was created by Satoshi Nakamoto, whose identity is still unknown. He has never had the control on the system because the code is open source and thus it belongs to the public domain. Bitcoin most innovative feature is its decentralization: it operates through a peer-to-peer network of connected computers, called nodes. Bitcoin has created its own currency units, called bitcoin, whose creation is integral to how the system operates, serving two concurrent purposes: it serves to represent value; and issuance of new tokens is used as a reward to operators in the network working to secure the distributed ledger.

The spirit of the network is represented by the database, called ledger, holding the past transactions and the current fund holders. As a financial database that must be resilient against users trying to falsify and duplicate payments, Bitcoin has created technological mechanisms to protect the entire system, such as hash, public-key cryptography and digital signature.

Critics have argued that Bitcoin can be considered as a Ponzi scheme, but it is not. A Ponzi scheme is "a fraudulent investment operation where the operator generates returns for older investors through revenue paid by new investors, rather than from legitimate business activities or profit of financial trading." (Zuckoff, 2005, page 1). [12] In a Ponzi scheme there is a central operator that pays returns to current investors from new capital inflows. There are at least three reasons why Bitcoin cannot be considered so. First, in Bitcoin there is no central operator that can profit from the relocation of funds. Second, a mechanism to deflect funds from new investments to pay returns does not exist because the only funds Bitcoin protocol recognizes are the tokens and transfers are initiated by users at their will. Thus, the protocol autonomously cannot deflect funds from one user to another. Third, in Bitcoin a new investment is always matched with a disinvestment, since investors putting money into bitcoins operate usually through an exchange. Therefore, there is no new investment flowing into bitcoins.

12 Mitchell Zuckoff, Ponzi's Scheme: The True Story of a Financial Legend. Random House, New York, 2005.

Summing up, we can say that Bitcoin is mainly a computer program and inside its world we can distinguish four basic components:

- The protocol, which is the specification of how to construct the blockchain (the distributed database), and all the rules governing transactions (assemblage, validity, etc.)
- The network, that is peer-to-peer and where nodes(people) connect to exchange messages containing new blocks to add in the blockchain and new transactions published in the public ledger
- The currency, "bitcoin", that is a unit of the native currency of the Bitcoin network, with a fixed supply and with a 10^7 divisible pieces called satoshis.
- The open source project implementing the protocol, the project was recently branded as Bitcoin Core.

2.1.2 Main features and technologies constituting Bitcoin

Four are the most important features defining Bitcoin and altogether design the structure and the functioning of the entire system. These attributes represent the innovative and disruptive nature of Bitcoin, and they are the following:

- Decentralized
- Open source
- Technology
- Public asset ledger

Bitcoin's decentralized nature is in contrast to the structure of fiat currencies, which are the majority of the currencies in use today. For fiat currency systems, the currency is issued by the government and its supply is controlled and managed by the central bank. On the other side, Bitcoin, as it is based on a peer-to-peer network of computers running the software, has no central governing authority with a monetary policy task. In Bitcoin, the monetary policy follows a simple rule: the final monetary base is fixed at 21 million bitcoins, new tokens are minted at a planned schedule and paid to users helping to secure the network. The fixed supply and the creation mechanism serve the purposes of providing the currency with value due to scarcity and of incentivizing users to connect to the network and help secure it by offering computational power.
Control in this peer-to-peer network is subtler than in a centralized system, where it is generally concentrated in an institution and where changes are relatively straightforward to be decided and implemented. In Bitcoin changes have to be agreed by a majority of the peers, but the remaining minority can technically challenge the change so much that the network runs the risk of a split.

Consequently, one of the advantages of the decentralization of power is that changes contrary to the interests of the majority would be rejected.
Another advantage is the resilience of these decentralized systems because they are robust against attacks both by insiders and outsiders. Malicious participants in the peer-to-peer network, unless they do not control a majority of the network, are fought through the proof-of-work system used to implement the distributed timestamp server on a peer-to-peer basis, and this is what Satoshi Nakamoto in his declarative paper wrote about the strength of Bitcoin system on this topic:

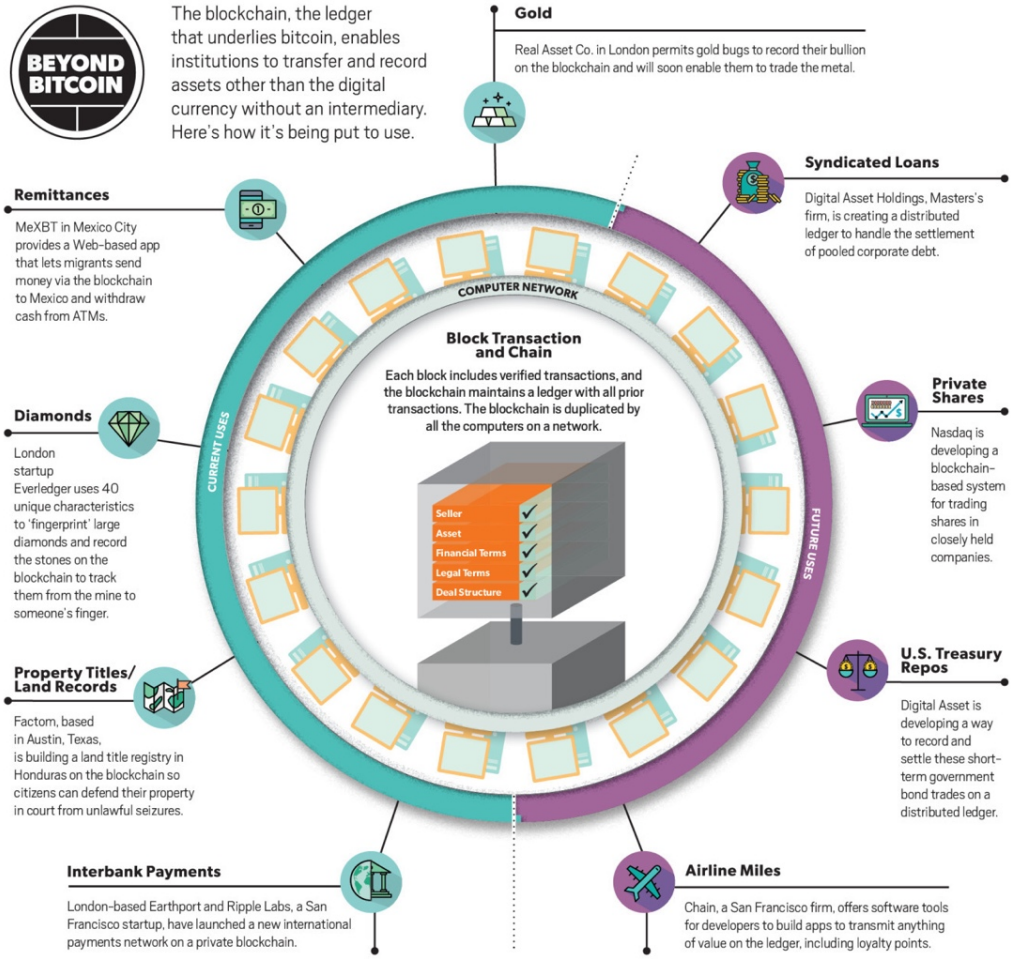
"*Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes."(Nakamoto, 2008,page 3)*

Outsiders' attacks and attempts to force down the system are really hard to realize since all individual users must be forced down in order to force down the system, and it is a much harder task to accomplish. This makes Bitcoin "censorship-resistant".

Bitcoin is an open source software, which makes the source code available for anybody to use, modify and redistribute free of charge. The goal of open source is to increase the quality of the software that is developed using the best volunteering forces with no geographical, legal or contractual limitations to contributions. Compared to proprietary software, where ownership remains with the software publisher, for open source software only the copyright remains with the creator, but rights are transferred to users. Open source software is always distributed with a copy of the source code and the cryptographic software has the advantage to allow users to check that the code has not been modified and it does not contain backdoors or security vulnerabilities. This represents a strength of this kind of software because it is more difficult to include flaws in such programs due to a higher level of scrutiny, that allows for the discovery and repair in a smaller amount of time.
Bitcoin was released under the MIT license, which is one of the most known examples of the "permissive" licenses. Those impose few restrictions on the redistribution of the software, that therefore acquires a life of its own once it has been released. This kind of license legitimates the start of new independent software projects from a copy of the original project under a process which

is known as "forking". The threat of such a process can often keep the developers of an open source project honest because it can be seen as a kill switch preventing evolutions against the users. In this respect, Bitcoin has been forked many times and this has given rise to many alternative cryptocurrencies such as alt-coins.
A problem connected to the open source status of the software is the "tragedy of the commons": although many users may benefit from it, few may have the incentive to contribute to further developments because of the impossible appropriability of merits and the high funding costs of the research. We should keep in mind that any development is enacted on a voluntary base.

The protocol behind Bitcoin allows transferring value securely in a trust-less way as it is an open platform not only for money but for any digital asset. In the past, transferring value has usually been a slow process, but the technology applied to Bitcoin is cheaper and faster than traditional



alternatives, thus creating opportunities for new applications.

Figure 9, source: CREATIVE CONSTRUCTION | Digital Innovation - delivered. » Trends 2016: Von AI-Revolution bis Blockchain – The Automation of Trust » Trends 2016: Blockchain – Automation of Trust

This decentralized system can be used as an ideal test ground for new technologies linked to Bitcoin infrastructure (e.g. smart contracts and autonomous agents) as innovators do not need any approval from anybody: the decentralized system enables "permissionless innovation". [13] Bitcoin is an Application Programming Interface (aka API) for money, whose first application is the currency bitcoin. However, Bitcoin could be used as an open platform for the exchange of value in the same way as the Internet is an open platform for the exchange of information. Above all, Bitcoin could become an open platform for financial innovation.

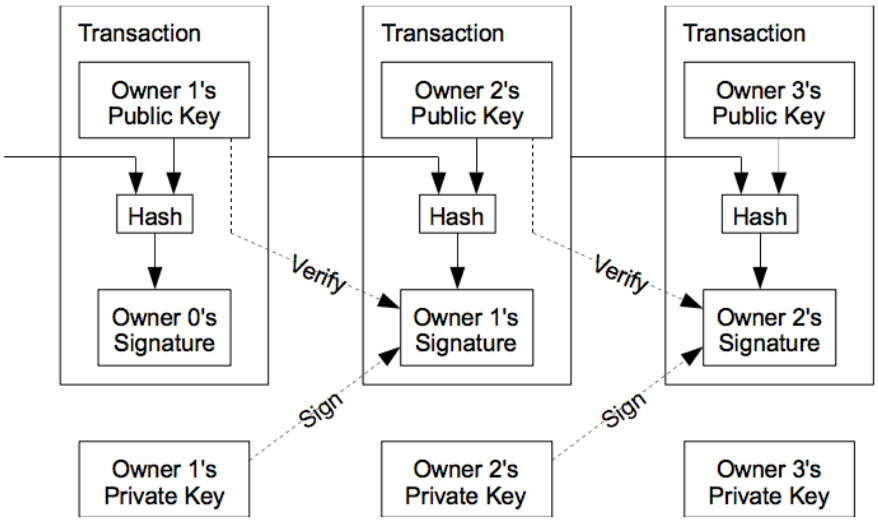
The adoption of smart contracts is enabled by the trust-less digital transfer of value. Smart contracts are math-based contracts not requiring neither human interpretation nor intervention to be completed, since their settlement is entirely run by a computer program. Through smart contracts, Bitcoin's technological invention gives the opportunity to lower the costs of entering and upholding contracts, making them more efficient and thus potentially changing the course of action of corporations and government toward more efficient processes. Another application is the autonomous agents, not to be confused with artificial intelligence, that are computer programs created for specific tasks. Those are just two examples, and many more innovative ideas are being devised through the new technology, the Blockchain, either for financial or non-financial uses, stemming from data storage, currency exchange and remittance, to election voting or patient records management. In figure 9 we can see the already implemented and upcoming uses of Blockchain technology.

The real innovation that stays at the heart of Bitcoin system is the distributed database holding a copy of the common asset ledger. It is distributed because each participant in the network (aka node) keeps a copy of it and each copy is consistent by design. Therefore, on the one hand all users are in control of the system, but on the other hand every user is in control of her own funds through a cryptographic private key, used to sign messages to start transactions. The electronic coin is defined by Nakamoto as a chain of digital signatures, which is transferred by each owner to the next "by digitally signing a hash of the previous transaction and the public key of the next owner and adding them to the end of the coin." Each transaction works in the way shown in figure 10. Indeed, the bitcoin wallet contains two keys: the private key, which is a randomly generated string of numbers and letters, allowing bitcoin to be spent, and which is always mathematically related to the

13 It refers to the notion that experimentation with new technologies and business models should generally be permitted by default. Unless a compelling case can be made that a new invention will bring serious harm to society, innovation should be allowed to continue unabated and problems, if they develop at all, can be addressed later. This concept is expressed in the preface to Adam Thierer's book "Permissionless innovation: The Continuing Case for Comprehensive Technological Freedom".

bitcoin wallet address; and the public key, which is used to ensure the ownership of an address that allows the receiving of funds and is mathematically derived from the private key but protected through a strong encryption code base.

Figure 10



Source: "Bitcoin: A Peer-to-Peer Electronic Cash System" paper by Satoshi Nakamoto, section 2

At this point, we have to enter deeply into the main technologies constituting Bitcoin that help the functioning of a system for electronic money without any central authority and are thought as means to prevent the falsification of data and the duplication of payments, as well as to ensure the security of the system against attacks. They are four:

- Hash
- Public-key cryptography and digital signature
- Peer-to-peer (P2P)
- Proof of Work

Once data are inputted into a hash function, the output of a hash value with a certain number of digits is created. The main characteristic of this mechanism is that small changes in the input, so in the data, cause extremely different results in the obtained output, resulting in a completely unalike hash value. Therefore, it is nearly impossible to infer the original data based on a hash value. This mechanism indeed is used for the detection of falsification of data, and specifically in Bitcoin for the verification and guarantee of the continuity of blockchain data and the creation of blockchains through Proof of Work using the computation of hash values.

Public-key cryptography and digital signatures are used in the Bitcoin system to identify the creator of data of a transaction and as an address[14] of a bitcoin wallet[15]. The public-key cryptography is a cryptographic method that uses different keys for encryption and decryption of data. The use of the cryptography for two different keys enables safe delivery and receipt of files only if the receiver prepares the pair of keys and delivers the public one to the sender in advance.
The digital signature is a mechanism employed to prove the authenticity of the data sent through the network and the pair of keys used in the public-key cryptography. It is made by encrypting the hash value of a file to be sent to receiver with the sender's private key and is sent to the receiver with the file. The receiver decrypts the digital signature with the public key and cross-checks it with the hash value of the file, thereby confirming the authenticity of the sender's digital signature if the created hash value and the obtained one are the same. This represents an important issue for what concerns privacy. It is still maintained by keeping anonymous the public keys related to publicly announced transactions. The public sees that a transaction between two parties is taking place without any information linking the transaction to a particular identity. This level of information is similar to the one released by stock exchanges, where the "tape", the time and size of individual trades, is made public without revealing the involved parties. The only risk is linked to the possibility that the owner of a key is revealed, leading to the revelation of other transactions belonging to the same owner.

P2P networking technology has contributed to the development of a base for a complete distributed network. In a P2P network, all "peers" (i.e. all participating nodes) hold data respectively and create an autonomous network in which data are requested and provided among the nodes on an equal balance. Compared to client-server networks, here roles of respective nodes as server or client are not fixed. Let's remind that a server is charged for the preservation and provision of data, while a client requests the server for data and gains access to them.
As we deal with a P2P network we have to consider two kinds of methods for search and data transmission. Search methods are used to manage locations of nodes and data, while data transmission methods are used to communicate data between nodes. The latter are divided into two subcategories: direct transmission between nodes and relayed transmission through another node.[16]

14 ID number designated as an address to deliver bitcoins
15 Software for managing bitcoins
16 Materials for the "Working Group on Ideal P2P Network, Network Neutrality Committee" (Computer Communications Division, Ministry of Internal Affairs and Communications)
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/network_churitsu/pdf/wg2_061129_1_si_1_2. pdf

In Bitcoin, the adopted search method is a P2P method, whereas the one adopted for data transmission relays the respective nodes. In Blockchain, all nodes participating to the P2P network and conducting mining activities are supposed to share the same data.

Bitcoin employs Proof of Work or PoW to create a mechanism to prevent falsification of data, duplication of payments and attacks against the system by malicious users. This tool avoids the need of a central authority maintaining and controlling the operations in the system. In Bitcoin, this work is called "mining": nodes calculate a hash value by adding a nonce (any given value) to the collection of data about transactions which are delivered, in case of relevant transactions, to the entirety of the P2P network. In calculations, it is required to obtain a value smaller than a certain value automatically set by the system, which has to be obtained by the participants' continued calculations using different nonces. When the relevant value is obtained, network participants mutually verify and affirm the correctness of the value. The collection of transaction data used for the calculations, once it is approved as official, becomes a new block. Thenceforth, tokens are granted as a reward to the successful miner. In the end, all nodes go on to the next mining using transaction data not included in the previous block together with newly created transaction data.

2.1.3 Blockchain achievements and related problems

A blockchain is a series of blocks created through PoW. Blocks assembling transaction data for a certain period of time, which last approximately ten minutes in case of Bitcoin, are linked into a chain and each of them contains technical data, previous block has, PoW target, nonce, and timestamp, in addition to transaction data.

A timestamp is a server that works by taking a hash of a block of items to be timestamped and widely publishing the hash. It proves that the data must have previously existed in order to get into the hash. Each timestamp incorporates the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

In order to finalize a transaction, it is necessary to confirm that the relevant blockchain does not divide ("fork") after data is incorporated in the block and other blocks are built afterwards. Blocks are linked into a chain in a manner that they keep past information, and hence, in order to conclude an illegal transaction as a consensus in the Bitcoin blockchain, it is necessary to continue creating blocks faster than the authentic fork or re-create all past blocks. This process requires more than 50% larger percentage of the computing capacity of all computers participating in PoW. Since enormous computational resources are necessary, it is more economically rational to obtain profits

through proper mining, thus discouraging people from running illegal transactions. This mechanism has mostly solved what is known as "the Byzantine Generals' Problem" [17], which is associated with the agreement problem of consensus in the presence of uncertainties because of physical separation and use of means to send messages that might either not be delivered or be falsified.
In Bitcoin blockchain, a consensus on an authentic blockchain is obtained through PoW and mutual approval of the subsequent results.

Functions of the Bitcoin blockchain are typically classified into four categories: executions of applications, guarantee of the continuity of data, sharing of the blockchain data among nodes, and data communicating through the P2P network. These functions are achieved through the use of one or more constructing technologies in Bitcoin system (hash and digital signature, PoW, and P2P).(" Survey on Blockchain Technologies and Related Services, FY2015 Report, Nomura Research Institute, 2016).
The execution of applications, and so of various processing procedures, is enabled using a dedicated script. The guarantee of the continuity of data, provided by both hash and digital signature and PoW, prevent duplicate payments and ensure traceability of data warranting transparency in transactions. Difficult falsification is enabled by the sharing of the blockchain data among nodes as well, which reduces server costs for the development and operations and enables the development and operation of a stable system, usually referred to as "zero downtime system". This kind of system and the stability in maintaining the ecosystem against attacks by malicious users, without a central authority are permitted by the spread data communication throughout the P2P network.

However, Bitcoin blockchain increasing use has revealed various hidden problems for any of such achievements. Therefore, there exist 13 problems that can be grouped into 3 main families:

1. Problems arising from specifications and implementation of the system, which is further divided into three subcategories:
   1a. problems arising from the implementation of a script,

17 Byzantine Generals' Problem is an example of "Byzantine failures", considered the most general and most difficult class of failures among the failure modes. "A Byzantine fault is any fault presenting different symptoms to different observers. A Byzantine failure is the loss of a system service due to a Byzantine fault in systems that require consensus." From Wikipedia on Byzantine fault tolerance.

1b. problems arising from finality, which is defined as the process for transaction approval and authentication,

1c. problems arising from the P2P system;

2. Problems arising from gaps with actual business practices, related to the difficulty for Bitcoin blockchain to record transactions whose details may need correction afterwards and to the confidentiality of some information;

3. Mathematical and information science-related problems of the Bitcoin blockchain, since Bitcoin blockchain is subject to an information theory proof and the impossible simultaneous satisfaction in such a distributed system of the CAP Theorem. [18]

Detailed problems are illustrated in the table below with the relative belonging family.

1a	Script specifications lack Turing completeness
1b	Execution of the script requires a trigger (transaction, etc.)
	It takes time to finalize a transaction and there is a risk of rework by forking
	Timestamps affixed to transactions are neither accurate nor guaranteed
1c	Ballooning blockchain eat up capacity of nodes
	The amount of transactions processed per unit time is small
	Overall optimization of transaction processing in consideration of gaps in machine power levels is not conducted
	A fork in the blockchain may be possible in the event of a physical attack or failure cutting off the P2P network
	Only some organizations equipped with powerful machines can conduct mining as the computational power required increases and excessive power is consumed
	The system allows participation of anyone without a mechanism to exclude specific nodes and there is a risk for use in illegal transactions
2	Traders and transaction details are disclosed and privacy may not be completely protected
	It is difficult to correct transaction details afterward
	Transaction fees are difficult to predict due to fluctuation in token prices

The CAP theorem is about distributed systems consisting of multiple nodes that handle common data. It demonstrates that distributed systems can completely satisfy only two properties out of the following three: consistency, availability, and partition-tolerance. According to this theorem, the Bitcoin blockchain is unable to satisfy the consistency.

Summing up, we can say that there exist three levels of blockchain. The first level concerns the storing of digital records as blockchain allows unprecedented control of information through secure, auditable, and immutable records either of transactions or in general of any digital representation of physical assets. The second level has to do with exchanging of digital assets since users can issue new assets and transfer their ownership in real time without intermediaries (e.g. banks, stock exchanges, or payment processors). The third level involves the execution of smart contracts, which are self-governing contracts simplifying and automating lengthy and inefficient business processes.

2.1.4 History & Data

The history of Bitcoin is described through a timeline, highlighting the most important moments for the system.

- *August 15, 2008*: Bitcoin.org domain was registered at a site which allows users to anonymously register domain names.
- *October 31, 2008*: Satoshi Nakamoto publishes his "white paper" that describes the Bitcoin currency and explains the solution to double-spending problem in a decentralized system.
- *January 3, 2009*: Block 0 (aka the genesis block) is mined, establishing the blockchain.
- January 12, 2009: The first Bitcoin transaction takes place between Nakamoto and a cryptographic activist, Hal Finney.
- *October 5, 2009*: New Liberty Standard establishes the exchange rate of Bitcoin, using an equation including the cost of electricity to run a computer generating Bitcoins. The exchange rate is US$1= 1,309.03 BTC.
- *February 6, 2010:* The Bitcoin Market is established as a Bitcoin currency exchange.
- *May 22, 2010*: The first, real-world transactions involving Bitcoins takes place in Florida. US$1=400 BTC.
- *July 17, 2010*: The MtGox Bitcoin currency exchange market is established by Jed McCaleb.
- *September 18, 2010*: Bitcoin Pooled Mining, operated by slush, mines its first block.
- *October 2010*: The Financial Action Task Force, an inter-governmental group which works for the development and promotion of policies to prevent money laundering and funding of terrorists, publishes the first warning.

- *October 7, 2010*: The Bitcoin exchange rate, stalled at US$0.06/BTC for several months, begins to climb.
- *November 6, 2010*: Market cap, calculated by multiplying the number of Bitcoin in circulation by the last trade on MtGox, exceeds US$1 million. The exchange rate reaches US$1= 2 BTC.
- *2011:* Silk Road, a Bitcoin marketplace, opens an illicit business for drug deals.
- *January 28, 2011*: 25% of total Bitcoins is generated. (5.25 million Bitcoins on total of almost 21 million).
- *February 9, 2011:* Bitcoin reaches parity with US dollar. US$1/BTC.
- *End March – Beginning of April 2011*: First markets for the exchange of Bitcoin with the major national currencies open (GBP, Brazilian Reals, EUR, Zloty and others).
- *June 8, 2011*: Bitcoin reaches all-time high with the price on MtGox reaching the value of US$31.91 and the market capitalization of around US$206 million.
- *June 12, 2011*: An incident occurred to MtGox Bitcoin exchange rate that decreased to US$10, this is known as "the Great Bubble of 2011".
- *June 19, 2011*: MtGox suffers a significant breach of security.
- *August 23, 2011*: The first peer-to-peer decentralized pool, P2Pool, mines its first block.
- *February – May 2012*: Two Bitcoin exchanges are shut down after being hacked.
- *December 6, 2012*: The first Bitcoin exchange to be licensed as a European bank is Bitcoin Central, which operates within the European regulatory framework.
- *April 2013:* The MtGox exchange rate surpasses US$100.
- *April 10, 2013*: Bitcoin bubble expands the exchange rate up to US$266.
- *August 6, 2013*: Bitcoin is ruled as currency by a Texan judge
- *August 20, 2013*: Bitcoin is ruled as private money in Germany. It is recognized as "unit of account" and its use is allowed in commercial and private sales.
- *October 2, 2013*: FBI shuts down Silk Road. The closure impacted the Bitcoin price decreasing it from US$139 first to US$109.71, and then to US$128.
- *November 17 and 19, 2013*: Bitcoin price hits US$503.10 on MtGox, then it goes to US$1242. At this moment Bitcoin transaction volume surpasses Western Union Company.
- *December 5 and 17, 2013*: China's central banks bans Bitcoin transactions, causing a price drop to below US$1000. Furthermore, Bitcoin crashes to US$500 after it is banned from accepting deposits in yuan.
- *February 2014:* MtGox first suspended withdrawals citing technical issues, but then it filed for bankruptcy in Japan. Price fell following the shutdown of MtGox before recovering to the $600–$700 range
- *September 2014*: TeraExchange, LLC, received approval from the U.S. Commodity Futures Trading Commission "CFTC" to begin listing an over-the-counter swap product based on the price of a bitcoin. This approval represents first time a U.S. regulatory agency approved a bitcoin financial product.
- *August 2015*: It is estimated that more than 160,000 merchants accept bitcoin payments.
- *March 2016*: The Cabinet of Japan recognized virtual currencies like Bitcoins having a function similar to real money.

Figure 11
Source: https://blockchain.info/en/stats

- *January – June 2017*: 1 bitcoin surpassed the spot price of an ounce of gold for the first time and broke many all-time highs – May 1= US$1,402.03, May 20= US$2,000. Exchange trading volumes continue to increase (regularly processed transactions increase by 640% in a few months).
- *August 1, 2017*: Bitcoin split into two derivative digital currencies (BTC and Bitcoin Cash – BCH)
- *August 5, 2017*: Bitcoin price passed US$3000 for the first time
- *August 14, 2017*: The price of bitcoin was recorded at US$4,400
- *September 12, 2017*: After the last Chinese bans, JPMorgan chief executive Jamie Dimon issued a sharp condemnation of bitcoin, declaring it a "fraud". This causes an initial sharp decline in bitcoin price to US$3500, followed by a recovery in the following weeks.

Current situation data:

The market summary for September 27, 2017 is the following:

Market Price = US$4,188.32 Trade Volume = $302,484,409.35 or 72,220.94000000 BTC

2.2 MONETARY ANALYSIS ON BITCOIN – Bitcoin as a currency

Human beings have used several monetary instruments throughout history. Bitcoin in principle satisfies the technical properties of money as it is durable, divisible, fungible, easy to transport, and impossible (or at least very difficult) to counterfeit, hence it could serve as money.

However, there are other functions usually assigned to money which must be investigated in order to debate on the money status of Bitcoin. They are three: medium of exchange, so money that can

be exchanged for goods and services; store of value, so money that can be used to transfer purchasing power across time; and unit of account, so money unit whose terms goods and services can be quoted in. On the one hand, some critics on Bitcoin argue that the cryptocurrency does not fulfill these traditional functions of money. On the other, Bitcoin supporters reply that an asset does not have to satisfy them to be considered valuable. ("Understanding Bitcoin", Franco, 2014, ch.3)

The recognition of Bitcoin as a proper currency is easier for economists of the Austrian School, whose method is entrenched on the analysis of the motivations and subsequent actions of individuals. For what concerns Bitcoin acceptance as money, they believe that money emerges from the competition among several mediums of exchange and it is not declared as legal tender by governments, as for mainstream economists. So, Bitcoin could represent a real currency if it displays attributes which give it a competitive advantage on the existing alternatives.

Another belief from the Austrian School which is in agreement with Bitcoin currency system regards the fixed money supply, which in Bitcoin is fixed at almost 21 billion. They advocate it because they believe that deflation when it is caused by technological progress and not by a decrease in monetary supply is not harmful for economic growth. Fixed supply is a protective tool against inflation, which for these economists is merely an increase in money supply that mainly leads to economic instability.

The only Austrian theory not completely supporting Bitcoin is about the creation of money introduced in Mises' regression theorem. It states that the value of a currency stems from the fact that users assume its value will be kept with the passing of the time. As the value today is given to a currency based on the expectation that it could be used tomorrow, the value yesterday is what backs the value today. The problem for Bitcoin starts as soon as we go back in time where, at some point, the currency must have been pegged to some commodity having value: fiat money value today is rooted in commodity money; nevertheless, for Bitcoin there is no attached commodity from which extract the initial value.

Until now, a consensus among economists seems emerging: "Bitcoin is a good medium of exchange, a risky store of value, and a poor unit of account".[19] (Dourado, 2014)

19: Dourado, E. (2014) Here's How Cryptocurrencies Could Replace the US Dollar, elidourado.com/blog/bitcoin-dollar/

2.2.1 Bitcoin as a medium of exchange

There seems to be consensus on Bitcoin serving as a medium of exchange as it is already accepted by a very large number of businesses. We can see a steady increase in the number of transactions, which is still low compared to other payment methods. At the moment, Bitcoin is living between two stages of its development, it is expanding itself as a payment method but it is still growing and attracting the critical mass. At this point, benefits to new users would exceed the cost of adopting the new technology. While dealing with technological advances as digital currencies, we encounter what Varian defined as "network effect", since total benefits to all users increase quadratically with the number of users as there are more opportunities to transact and effectively using the system.

Critics argue two problems related to Bitcoin functioning as a medium of exchange. First, as there are several internet heavyweights desiring to enter into the digital payment infrastructure, Bitcoin would have to compete as an open source project with companies having great financial muscle. Thus, this would lead to a standards war, as Varian would have said. Second, Bitcoin might not be able to compete with emerging entrants due to the large costs associated with the mining sector. All the advantage Bitcoin has on its lower transaction fees would vanish over time because it should be used to cover the block reward decrease as the number of issuable bitcoins declines over time. If compensation to miners declined over time, the network could stabilize at lower compensation levels to miners so as not to lose one of its advantages.

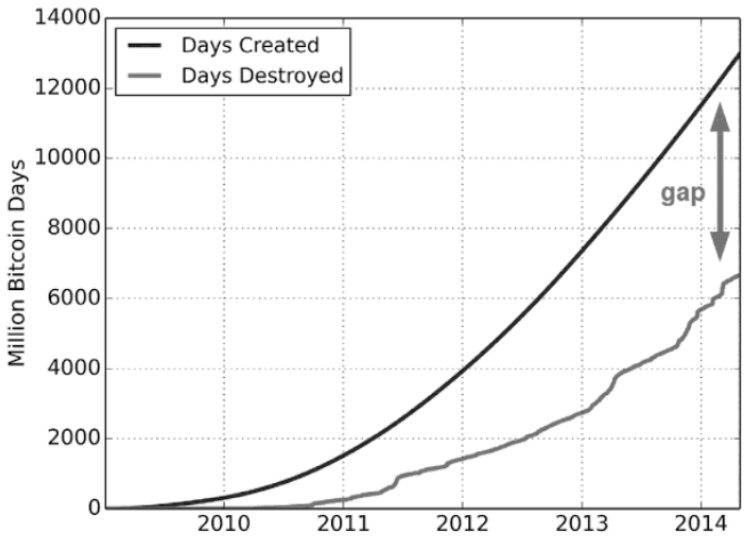
Together with current lower transaction fees compared to credit cards, Bitcoin has several pros. Firstly, Merchants using Bitcoin are protected from charge-back fraud, which is a customer looking for a withdrawal of the payment after the good has been delivered. On the other hand, as Bitcoin payments are almost irreversible customers are subject to fraud risk, that might be solved imitating charge-backs using escrow transactions. [20] Then, Bitcoin transfers are almost instantaneous compared to bank transfers, and have the advantage of enabling the transfer of any digital asset aside from currency. Bitcoin system does not collect base fees, unlike credit cards. For this reason, micropayments, that could allow content providers to charge for smaller slices of content, could be enabled. Bitcoin is more similar to cash than to other payments systems because it is a push

20: Escrow is a legal concept in which a financial instrument or an asset is held by a third party on behalf of two other parties that are in the process of completing a transaction. The funds or assets are held by the escrow agent until it receives the appropriate instructions or until predetermined contractual obligations have been fulfilled. Money, securities, funds, and other assets can all be held in escrow.

payment system, where users proactively generate transactions without the need for an intermediary authorizing and "pulling" the payment with the revealing of sensitive information. Push payment systems could reduce frauds and undesired purchases since users completely control the purchasing process.
The existence of Bitcoin as a new payment system independent from the traditional ones offers more resilience to the economy in case of a crisis because it could be a parallel payment system, coexisting as a gateway between local and global existing payment systems.

The cons about Bitcoin as a medium of exchange are numerous as well. "Cutting the middlemen" would not be absolute as many users would decide to use intermediaries either for convenience or for the technical barrier due to the technological difficulty of the system, leading to no significant decrease in costs. Existing fiat currencies are more liquid compared to Bitcoin for at least two reasons: they have three times larger volume of foreign exchange markets turnover, and they have larger network externalities impeding competition from alternative currencies. Additionally, Bitcoin transactions do not offer a credit option as credit cards do, where it is built by default. As Bitcoin is classified by the IRS ruling as a capital asset, this kind of regulations and other kinds aiming to protect consumers could increase either reporting or compliance costs, hindering the use of the cryptocurrency as a medium of exchange. An inconvenient linked to transactions is the fact that confirmation takes several minutes and the change from an unconfirmed transaction is locked and unusable until the clearing occurs. Scalability pressures as its use becomes generalized might be faced by Bitcoin as well. Most of all, competing established companies, governments and institution may adopt the same technology, leaving all cryptocurrencies behind.

Figure 12. source: Understanding Bitcoin. Franco. 2014



2.2.2 Bitcoin as a store of value

Volatility is the main criticism to Bitcoin as a stable store of value and the principal reason why until now it has been viewed more as a risky asset. Some factors explain Bitcoin's volatility and they are the following: regulatory uncertainty, low market capitalization and low liquidity compared to other currencies, limited

market access and narrow adoption. There is a tension between the use of the token as a store of value and as an investment. Hoarding might be the explanation for the low turnover of Bitcoin. Hoarding indicates the mechanism behind an investment in which a large portion of the bitcoins in circulation are kept by individuals assuming that their value would increase over time. Hoarding is evident in three behaviors. First of all, the majority of bitcoins are kept in inactive accounts. Furthermore, ownership is highly concentrated mostly in the hands of early adopters. Third, the difference between the coin-days created and coin-days destroyed is increasing and thus more bitcoins are created and rather accumulated than spent in transactions, as figure 12 shows. (Data on cumulative coin-days destroyed are available on blockchain.info until 2014).
The functions of store of value and medium of exchange are complementary, thus, Bitcoin needs to balance the two uses for the system to grow: if there is too much hoarding, bitcoins would be perceived difficult to get and lose their attractiveness as a medium of exchange. If a stationary state is reached, there would be less incentive for hoarding, and thus for speculators to hold the currency. Thereafter, as the value becomes stable, there could be more demand to use bitcoin as a store of value.

There are some advantages for Bitcoin to be used as a store of value. It avoids confiscation, disproportionate taxation and capital control, which is not the case for fiat currencies as they can be confiscated either physically or through an order to the holding financial intermediary. Bitcoin has no storage costs, once the initial set-up is complete. The tokens are easy to transport because private keys can be carried in any storage media or uploaded to the cloud. Scarcity is fixed by an algorithm; thus, no central authority can debase the currency at will, but only a unanimous vote by all participating nodes. The deflationary nature of bitcoin is not perceived as harmful by Bitcoin supporters as it would be technological progress to produce deflation. Two additional pros to focus on are: the use of cryptographic security, in principle sounder than traditional security methods; and the provision of automatic record keeping for all transactions in the blockchain.

The drawbacks are several. First of all, the status of Bitcoin as a store of value is challenged by its volatility: there is no central authority ensuring the stability of its value, thus the price is subject to self-fulfilling dynamics, where even news could create a confidence crisis. Bitcoin, unlike commodities as gold, does not have a marginal cost of production (if we do not look at the electricity costs) with which stabilize its price. This leads to more acute down-trends on the price. As Bitcoin is an open source code, it can be easily and, most of all, legally replicated, it gives the chance to other competing technologies to be created and to substitute time after time Bitcoin.

Evidence on this is the rise and proliferation of many cryptocurrencies from 2011 on, but Bitcoin still holds the first mover advantage as its network is much larger and known than alternative cryptocurrencies. If investors think that holding Bitcoin might be a good protection against inflation, they are wrong since gains for the appreciation of Bitcoin would be taxable. Even though it could constitute a partial hedge against an inflationary increase in the money supply of the attached fiat currencies. Bitcoins have no intrinsic value supporting them as they have no physical backing to any commodity. The intrinsic value supporters argue Bitcoin to have may lay in the proof-of-work computational power performed by miners. Bitcoin users do not enjoy any deposit insurance as bank deposits. Last but not least, Bitcoin does not have the legal tender status and furthermore governments and central authorities could ban its use at any time. The enforcement method of such ban is not clear at the moment due to the distributed nature of the cryptocurrency.

2.2.3 Bitcoin as a unit of account

The unit of account function of Bitcoin is generally not considered good, because of its high volatility. Though many products and services could be purchased using bitcoins, merchants do not have incentive to directly quote their prices in bitcoin since the price of bitcoin is not stable and they would incur in what are known as “menu costs”. They apply to an economic term that describes the cost a firm incurs in order to constantly adjust prices in their stores.

Some economists debate on the fact that these three traditional functions attached to money are unbundling due to the introduction of new technologies which are disruptively changing the financial and economic system as a whole. If this is the case, it would not matter so much that Bitcoin poorly serves the unit of account function, provided that it fulfills the other functions.

2.3 FINANCIAL ANALYSIS ON BITCOIN RETURNS

So far, we have analyzed the characteristics and the diffusion of many cryptocurrencies and the ecosystem behind their functioning. We have concentrated our research to Bitcoin since it is the cryptocurrency which has captured much attention either in the financial sector or in the media, and upon which news and reports are growing their concerns for an upcoming bubble. The evidence for such an event for some people, as Jamie Dimon from JPMorgan or Ron Insana from CNBC, is crystal clear from the behavior of the exchange rate, while for others it remains just a hypothesis. Indeed, Insana wrote about the fact that most disruptive developments as Bitcoin do eventually turn into speculative bubbles and, according to him, the driver of such an increase in price is investor enthusiasm.

That said, we enter into a more applicative research divided into two paths: the first seeks to highlight the relationships linking the USD/BTC exchange rate to one of the key indicators used from the macroeconomic and financial perspective, such as the perception about the market sentiment, VIX; and the second is labelled to the estimation of an autoregressive model to describe the phenomenon and try to forecast the future.

2.3.1 Indicator analysis

We have decided to take weekly data on prices from the end of November 2013 until mid-September 2017. In this period of time we wanted to capture the effects of several events. From April 2013 bubble, we have seen a steady increase in the price up to US$900 in January 2014, then a lower peak in March 2014 due to MtGox bankruptcy. From then on, there have been continuous fluctuations whose trend has been increasing in the price, challenged only by bad news from financial experts or most importantly by bans from governmental authorities such as the Chinese central bank.

Although prices are the terms in which sales and purchases occur in the market, we have chosen to look at the returns from Bitcoin, since what is interesting is not the price on its own but the variation in the price across time. Moreover, if we want to measure risk, we would use the standard deviation of the returns, and thus the distribution of returns is needed for an analysis of this kind. Furthermore, prices probability distribution is not stable over time, while returns display distributions which have the tendency to maintain some characteristics in the long run. This could be a useful tool to enable easier forecasts.

The table below shows some summary statistics on the returns obtained in Excel and the graph plots the returns over time. The number of observations is 198.

Table 2: Summary Statistics on BTC/USD cross, source: personal examination

Mean	0,016264646
Volatility	0,11115752
Median	0,0093
Mode	0,0026
Skewness	1,503725524
Kurtosis	8,335401891
Exc.of Kurtosis	5,335401891

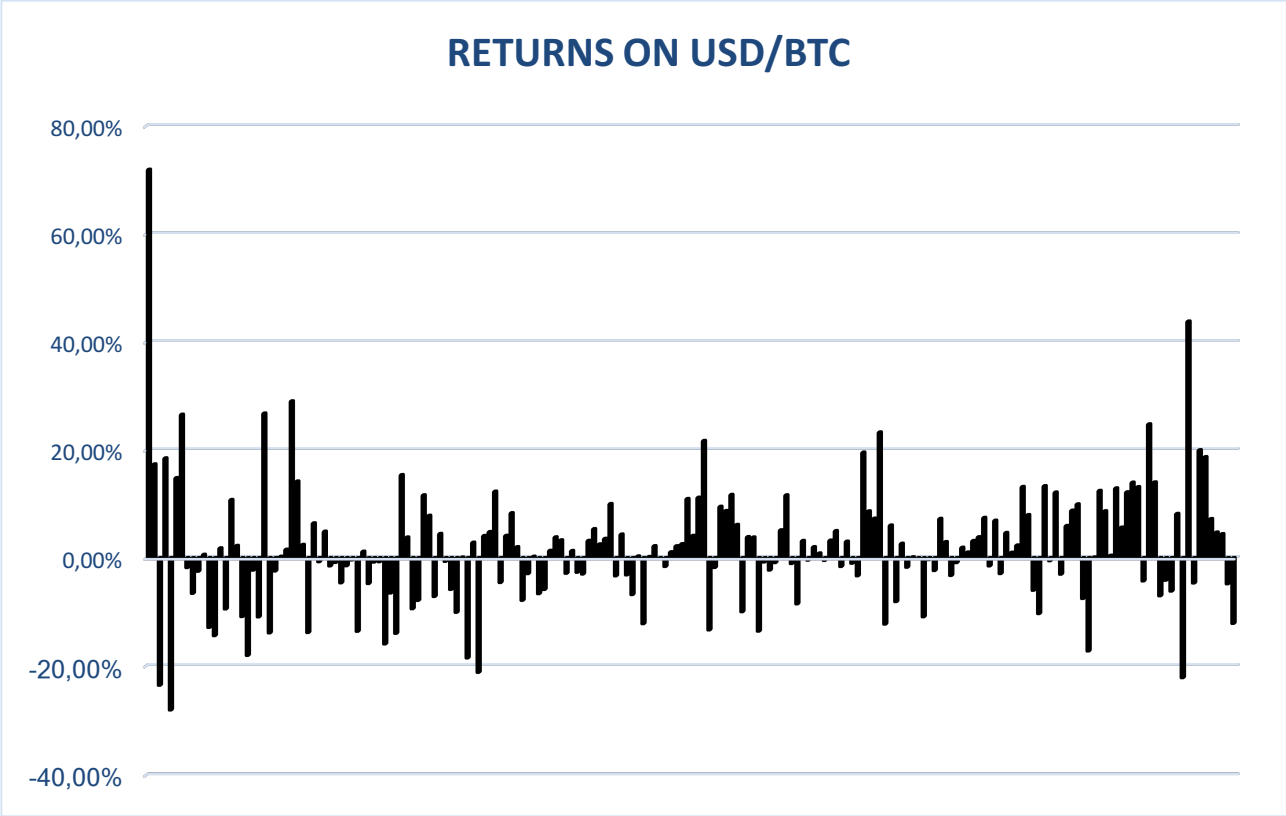
The results we got in our summary statistics clearly show that our sample is not normally distributed. Actually, the strong excess of kurtosis (5,33) hints relevant departures from the Gaussian distribution, together with the positive skewness of the data-set. Indeed, the kurtosis coefficient of our sample is larger than the one associated with a normal distribution, which is

around 3. This signals that the probability of attaining an extreme value in the future is higher, since the kurtosis is a measure of the likelihood that an event occurring is extreme in relation to a given distribution. Considering that we are examining historical returns, the higher the kurtosis coefficient is above the normal one, the more likely that returns in the future will be extreme either large or small. Kurtosis is usually referred to as the "volatility of the volatility". Skewness is a measure for the extent of asymmetry from the normal distribution. If the data is positively skewed, mean and median will be greater than mode, and in majority of the cases, mean will be greater than median in this way: **Mean ≥ Median > Mode**, and that is the case for our sample. The cross exhibits occasional large upmoves, and not equally large drops.

In finance understanding the way in which data is skewed helps the investor in the estimation on whether a given future data point will be more or less than the mean. Assets with positively-skewed returns are usually perceived as good investments.

The graph clearly shows the intrinsic volatility of the USD/BTC cross. More details on volatility will be revealed in the autoregressive model, where we look at the volatility clustering of the returns.

Figure 13, source: personal examination



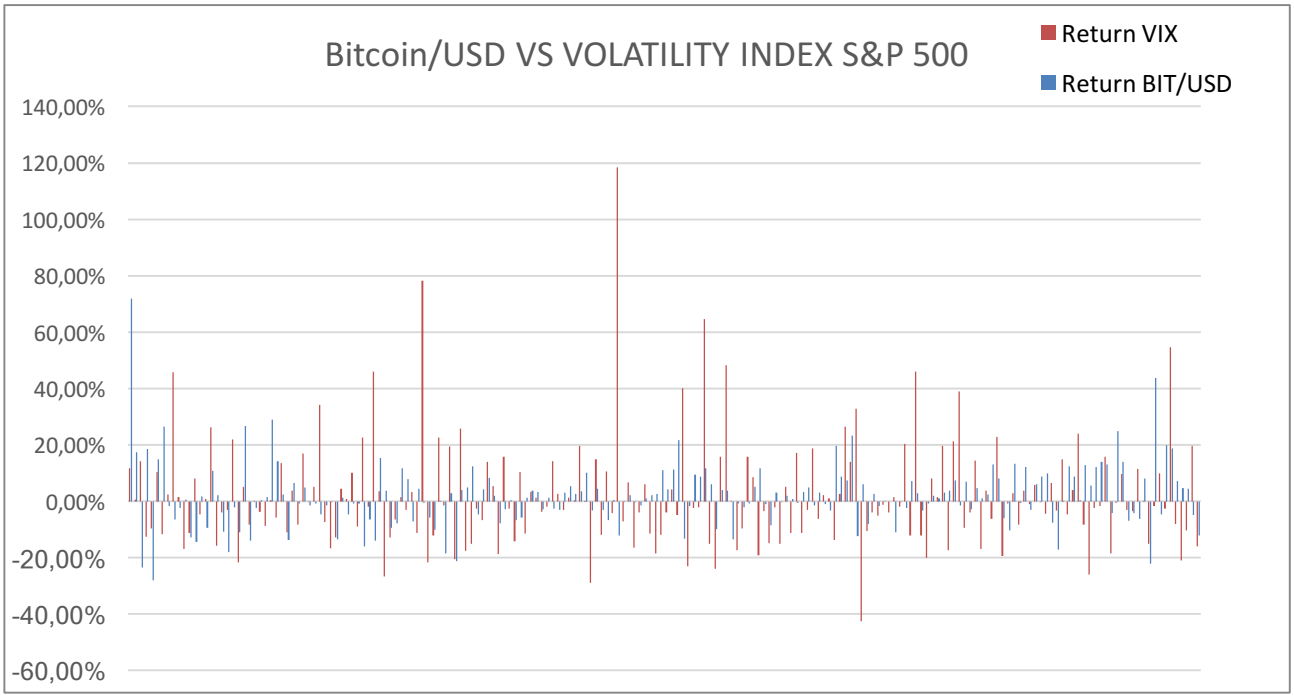
Thereafter, we have chosen to look for a correlation between the VIX, the volatility index S&P 500, and the returns from USD/BTC cross. The VIX, CBOE Volatility Index, is a contrarian sentiment indicator which is used to determine when there is too much optimism or fear in the market. Once the sentiment touches one of the two extremes, the market reverses its course. The indicator is based on data collected by the Chicago Board Options Exchange (CBOE). CBOE each day computes a figure for a "synthetic option", which is based on prices paid for calls and puts, written on the underlyings listed on the S&P 500 option series. A synthetic option with respect to a standard option minimizes some of the problems that affect traders as volatility risk or time decay; they are generally used when making exploratory trades or when establishing trading positions.

We decided to look for such a correlation because we wanted to investigate whether there exists a relation, positive or negative, between the index and the returns from Bitcoin or not. This would allow us to determine the behavior of the returns in respect of the perceived sentiment in the market: if the optimism or fear in the market is high, we would like to try to forecast whether the returns would follow the same direction as the market or not. Our purpose is to see in relation to the sentiment in the market which is the market behavior towards Bitcoin. If, for example, there is an increase in the volatility index, so an increase in the risk perception and the market is nervous, people usually shift to safe-haven assets, such as gold. Due to its high volatility, we expected that the correlation between the VIX and its returns would have been negative, as Bitcoin ups and downs are very common and intense. We took data from the same time interval as before, therefore weekly data from the last week of November 2013 to the first week of September 2017, for a total amount of observations of 198 for each series.

However, as we can see from the graph below, the correlation displayed by the two series is weak since the coefficient is equal to 0.017 and we know that its value ranges from -1, where there is a strong inverse correlation, to +1, where the strong correlation is positive. To assess if the correlation coefficient is statistically significant, we performed a test. Our H_0 is that the coefficient is equal to zero, and the alternative hypothesis H_1 is that it is different from zero.

We calculated the t value using the following formula: $t = r \cdot \sqrt{\frac{n-2}{1-r^2}}$, where n is the number of observations, r is the coefficient, and n-2 represents the degrees of freedom. Once we computed t statistics, which is equal to 0.238, we compared it to the critical value on the t distribution table with an alpha of 5%. We cannot reject H_0 as the value on the table is larger than our t, so the coefficient r is not statistically significant. This implies that the correlation is weakly positive and the estimation is not reliable.

Figure 14: personal examination



Thus, we can conclude that BTC/USD returns move randomly compared to the sentiment trend on the market, and therefore Bitcoin cannot be considered as a safe-haven asset. This could have been in some sense intuitive since a safe-haven asset usually gives investors a relative security in times of turbulence as it is generally viewed as a "store of value", while Bitcoin does not possess this function.

2.3.2 The autoregressive model on Bitcoin returns

The model we have estimated belongs to the univariate regressive models, which are a class of specifications where the attempt is to model and make predictions about financial variables only using information contained in their own past values and possibly current and past values of an error term. There exists a contrasting practice, referred to as structural models, whose nature is multivariate and whose attempt is to explain changes in a variable by reference to movements in the current or past values of the variables which are called "explanatory". While structural models have theoretical grounds but it is hard to determine the right explanatory variables to be used, time-series models are usually a-theoretical and attempt to capture empirically relevant features of the observed data which may result from various different but unspecified structural models. [21]

Time-series models are grouped into 3 categories, which represent different stochastic processes and depend linearly on past data points, and they are: the moving average models (MA), the integrated (I), and the autoregressive (AR). These three categories can be combined in autoregressive moving average (ARMA) and autoregressive integrated moving average (ARIMA) models.

Among those models, we went for the autoregressive (AR) since it can be estimated through ordinary least squares (OLS) method. This is true as the model needs the orthogonality condition and heteroskedasticity, conditions provided by the method. Furthermore, these conditions make the causality link between the variables unidirectional: the explanatory variables cause the dependent variable and not vice versa. In autoregressive models this is even more straightforward because of the "consecutio temporum": past events in any case cannot be influenced by future events. Unidirectional causality is provided by the exogeneity of the explanatory variables, circumstance linked to the stochastic nature of the regressors. The rationale of the model we estimated is the following: using the historical data, we investigate whether the process in its evolution displays some level of dependence (to be more precise has persistence) and thus, it presents so stable characteristics over time to estimate a robust model.

An autoregressive model of order p, denoted as AR(p), takes the form of:

$$y_t = \mu + \varphi_1 y_{t-1} + \varphi_2 y_{t-2} + \cdots + \varphi_p y_{t-p} + u_t \, .$$

The current value of a variable y (y_t) depends only upon the values the variable took in previous periods plus an error term (u_t), which is a white noise disturbance term. [22]

We decided to run an autoregressive model of order 3, using three lagged values of the returns as explanatory variables for the current return. Before running the AR, we have to test for the autocorrelation of the series. We are trying to detect some form of "memory" in the process which could justify the estimation of a single time-series model for more lagged values, specifically an autoregressive one potentially useful to predict future values of the BTC/USD cross. In order to perform the analysis, we used a data set which is different from the one used to show the relationship between the BTC/USD returns and the VIX; here data are collected on a daily basis in the time interval going from September 16, 2013 to September 17, 2017, for a total amount of 1442 observations. This change was for the purpose of getting a more reliable estimate of the parameters of the model.

21: Brooks, Introductory Econometrics for Finance, 3rd edition, 2014, page 251 and ff.

The estimated autocorrelation coefficients are summarized in Table 3.

Table 3, source: personal examination

Autocorrelation (1lag)	-5,86%
Autocorrelation (2lag)	-1,59%
Autocorrelation (3lag)	1,57%

Once we have estimated the first three autocorrelations, we estimate an AR(3) model through OLS method. Since the order of the model is 3, as the number of lagged values used as regressors, we run the regression from the 4th value in order to try to capture in a more effective way underlying patterns of the process, so the used observations become 1439. The linear regression can be expressed as follows:

$$\text{AR(3): } Y_t = \mu + \varphi_1 Y_{t-1} + \varphi_2 Y_{t-2} + \varphi_3 Y_{t-3} + \varepsilon_t \, .$$

As we stated the model, before the actual estimation we have to check for volatility clustering together with conditional heteroskedasticity and for the stationarity of the model.

We have to look at the behavior of the returns over the entire series and particularly, we take the square of the returns as an approximation for the volatility. Our purpose is to check the property either graphically or through an analysis of the data.
By plotting the returns over time (look at Figure 13, pg. 49), there is a clear evidence of the volatility clustering: large changes tend to be followed by large changes and vice versa. This leads to the alternation of flat days in the market where volatility is low and more turbulent ones, both showing a strong persistence over time. A cluster appears when there is persistency of the series over time, and such a persistence is attested by positive autocorrelation coefficients. In particular, we plotted the square of the returns over time and lagged the values four times to get a more accurate measure for the volatility clustering. Then, we calculated the autocorrelation coefficients and we tested their statistical significance either individually or jointly through a procedure called "Test Ljung Box". The single tests using the confidence intervals, with a 5% α , as a way to test the hypotheses that the results are statistically significant give the outcome shown in Table 4.

22: Brooks, Introductory Econometrics for Finance, 3rd edition, 2014, pages 259-260

LAGS	τ(AUTOCORR)	Confidence interval for α=5%	
1lag	0,314556397	-0,051614704	0,051614704
2lag	0,128527084	-0,051614704	0,051614704
3lag	0,170549309	-0,051614704	0,051614704
4lag	0,056271879	-0,051614704	0,051614704

Table 4: source: personal examination

The single autocorrelations tests, where our hypothesis H_0 is that the coefficient is equal to zero and the alternative H_1 is that it is different from zero, have to be interpreted as the correlation of the square of the returns at time t with the lagged values of one period, two, three or four periods separately. As they all lie outside the confidence interval, they can be considered statistically significant.

It is possible to test the joint hypothesis that all the autocorrelation coefficients, which can be identified as τ_k, are simultaneously equal to zero using a variant of the Q-statistic developed by Box and Pierce (1970), that is called the Ljung-Box (1978) statistics. This choice is due to the better small sample properties that this test has. Here it is the formula: [23]

$$Q^* = T(T+2)\sum_{k=1}^{m}\frac{\hat{t}_k^2}{T-k} \sim \chi_m^2$$

Where the symbols are as follows:

- T is the number of observations (= 1442 in our case);
- τ_k are the correlation coefficients, where k is the lagged value taken into account;
- m is the total number of lagged values (= 4 in our case).

Our H_0, which is in this case that all the coefficients are equal to zero, cannot be rejected since the t-statistics we got is far above the χ^2 critical value at α = 5%. This test is unidirectional because the χ^2 distribution is positively skewed and it assumes only positive values of the coefficients. Results of this test are shown in Table 5.

23: Brooks, Introductory Econometrics for Finance, 3rd edition, 2014, page 254

Table 5: source: personal examination

Test Ljung-Box		LAG	τ	τ^2
H_0: $\tau_1=\tau_2=\tau_3=\tau_4=0$		1	0,314556397	0,098945727
		2	0,128527084	0,016519211
Statistical test	213,5381216	3	0,170549309	0,029087067
Critical χ^2	7,814727903	4	0,056271879	0,003166524

Where 213,5381216 > 7,814727903.

Both tests give the same result: the square of the returns display a serial correlation, in this case of positive sign, and thus, periods of high volatility are more likely followed by periods of high volatility and the contrary holds for low volatility periods. The autocorrelation coefficients are statistically significant; therefore, estimations can be considered as reliable. The existence of a strong structure of serial correlation with respect to second moment implies returns are not IID random variables, because there exists some dependence among them. If the random variables are not independent and identically distributed, they do not have the same density with the same expected value and variance. Since returns are not IID random variables, variance follows a stochastic process in which future levels are positively correlated with past ones; this enforces the purpose of our autoregressive analysis.

In addition, once the volatility clustering has been detected in the series, this proves the existence of conditional heteroskedasticity, that implies a time-varying conditional variance. In fact, a conditional heteroskedastic time series shows high volatility periods spaced out by flat sessions in the market, which is a representation of the volatility clustering itself.

When variances and covariances are time-varying we speak about conditional heteroskedasticity, for which we have to remember and understand three simple facts. First of all, the fact that the conditional variance may change in heteroskedastic fashion, does not necessarily mean the series is non-stationary; even though the variance may go through high and low periods, the unconditional variance may exist and be actually constant. Second, conditional heteroskedasticity implies that the unconditional, long-run distribution of asset returns will be non-normal. Third, although many models show conditional heteroskedasticity, in the end we care for their forecasting performance.

For reason number one, we have investigated the stationarity of the model; we aim at detecting no stationarity in order to estimate the AR(3) model. The first step was the assessment on whether the data series is stationary: a stationary series can be defined as one with a constant mean, constant variance and constant autocovariances for each given lag. An examination of whether a series can

be viewed as stationary or not is essential for many reasons. First, the stationarity or otherwise of a series can strongly influence its behavior and properties, as for example for what concerns the effect of a "shock" to the series. For a stationary series, "shocks" to the system will gradually die away; while for non-stationary data the persistence of shocks will always be infinite and the effects will stay almost the same as t goes to infinite. Then, the use of non-stationary data can lead to spurious regressions, where the R^2 of the regression on two variables may end up being high even if they are unrelated. If standard regression techniques are applied to non-stationary data, the end result could be a regression that 'looks' good under standard measures (i.e. significant coefficient estimates and a high R^2), but which is really valueless. Finally, if the variables employed in a regression model are not stationary, then it can be proved that the standard assumptions for asymptotic analysis will not be valid.[24]

The method we used to assess the stationarity of the model is the following. we test for a unit root according to the augmented Dickey and Fuller procedure so, we try to figure out whether the process is a random walk, thus not forecastable. A unit root test investigates on whether a time-series variable is non-stationary and possesses a unit root. The null hypothesis is generally defined as the presence of a unit root and the alternative hypothesis is either stationarity, trend stationarity or explosive root depending on the test used. A unit root is a characteristic of some stochastic processes that can cause problems in statistical inference involving time series models.[25] We perform the regression by using as explanatory variables for the difference of return on BTC/USD cross on a daily basis the same difference lagged twice and the return lagged on one period. The following regression is employed:

$$\Delta Y_t = \mu + \psi Y_{t-1} + \beta_1 \Delta Y_{t-1} + \beta_2 \Delta Y_{t-2} + \varepsilon_t$$

The relevant hypotheses are:

- H_0: $\psi = 0$, the series contains a unit root
- H1: $\psi < 0$, the series is stationary

We compute the test statistic on the coefficient of the first lagged returns to be compared to the critical value at 5% significance level allowing for the intercept in the following way:

$$test\ statistic = \frac{\widehat{\psi}}{\widehat{SE}(\widehat{\psi})} = -40{,}02725018 < -2{,}86 \text{ (Critical value for ADF test)}$$

24: Brooks, Introductory Econometrics for Finance, 3rd edition, 2014, pages 353-355
25: Wikipedia on "unit root test"

We have to keep in mind that the test statistics follows a non-standard distribution. The estimated statistic falls into the rejection region as the t-stat is more negative than the critical value, therefore the series is stationary.

As the time series is stationary, we can directly estimate an AR(p) model on it without performing transformations in order to induce stationarity. The fact the series is stationary means it has constant and finite moments (mean and variance) and constant autocovariance structure. In addition, we care for stationary as stationary series are mean-reverting: this makes it easier to predict the dynamics of the series over time, as we do expect the series itself to evolve crossing its unconditional mean. Indeed, the variance being finite, the range of fluctuations of the process around its long-term mean is given and constant, therefore, the larger the departures from the mean, the higher the probability the series will reverse coming back to the unconditional mean.

Ultimately, we estimate our AR(3) model that is represented by the following equation:

$$AR(3): Y_t = 0{,}0035 - 0{,}0595Y_{t-1} - 0{,}0185Y_{t-2} + 0{,}0137Y_{t-3} + \varepsilon_t$$

Table 6 depicts the regression output with the regression statistics, the analysis of the variance (aka ANOVA) and the estimation of the coefficients.

Regression statistics						
Multiple R	0,06321309					
R square	0,003995895					
Adjusted R square	0,001913656					
Standard Error	0,043636349					
Observations	1439					
ANOVA						
	df	*SS*	*MS*	*F*	*Significance F*	
Regression	3	0,0109623	0,0036541	1,919037952	0,124557162	
Residual	1435	2,73242789	0,00190413			
Total	1438	2,74339019				
	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	0,003497796	0,00116094	3,01291001	0,002632868	0,001220482	0,005775109
Variable X1	-0,059506595	0,02639792	-2,25421572	0,024332909	-0,111289235	-0,007723956
Variable X 2	-0,018543423	0,02644055	-0,70132516	0,483213828	-0,070409694	0,033322848
Variable X 3	0,013744886	0,02649096	0,51885184	0,603944063	-0,038220281	0,065710052

Run the regression, the considerations are as follows. First, we do not have to focus on R^2 either because it conveys the fit of the regression with respect to past values, and our goal is to try to forecast the future values, or because we are in a time-series model. In time-series model R^2 is valueless as it is an indicator of goodness of the fit of the model with respect to past data. Second, the F-test hints the overall significance of the model; this means that it exists a linear relationship

between the dependent variable and at least one of its lagged values, which are used as regressors. In this way, as the obtained F (1,92) is greater than the significance F (0,13), we reject H_0 for which each coefficient of the explanatory variable is equal to zero; this allows for the hypothesis of a linear model. In the end, we have to interpret the coefficients: both the intercept and the lag-1 value are statistically significant at 5% level; the same does not apply to lag-2 and lag-3 values.

The appropriateness of an estimated model has to be carefully evaluated according to different criteria, such as: the stationarity of the model and the comparison between empirical properties (i.e. mean and variance of the series) and theoretical ones (i.e. mean and variance of the fitted values).

This being said, when it comes to choose a model, there is an explicit trade-off between its performance and its complexity.

Looking at the output of the regression, we found out that the last two coefficients are not statistically significant (their estimates are not sufficiently reliable); for this reason, we estimate again the model with just one lagged value of Y_t. The model would be then:

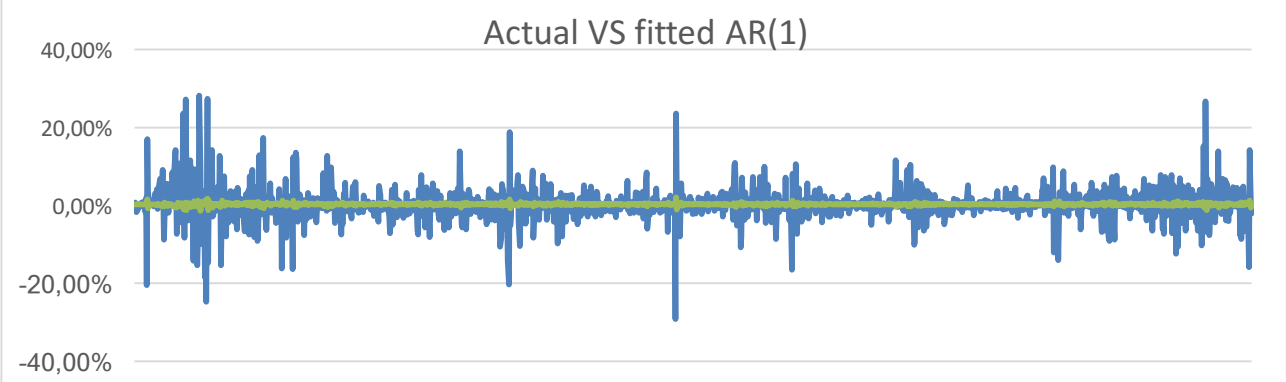
$$AR(1): Y_t = \mu + \varphi_1 Y_{t-1} + \varepsilon_t \text{ , or}$$

$$AR(1): Y_t = 0{,}00348 - 0{,}058625 Y_{t-1} + \varepsilon_t.$$

Now we have to think about the performance of the model. First of all, we have to stress the fact that the model is not stationary; indeed, for an AR(1) to be stationary it takes an estimated coefficient lower than 1 in absolute value.[26] This is a very negative drawback as a non-stationary model would show autocorrelation coefficients non-declining as lags increase (i.e. previous lagged values have a non-declining impact on Yt, that is counter-intuitive as the longer the lag, the lower the effect on Y_t we do expect). Second, to assess how reliable the forecasts of a model are we should compare empirical and theoretical properties, but a non-stationary model would have time-varying moments (computed on the fitted values), therefore it is useless as its robustness cannot be checked.

Here it is a graph (Figure 15) where actual (blue line) and expected (green line) values of the returns are plotted: the scarce reliability of the model is furthermore evident in the graph.

Figure 15, Source: personal examination



26: Brooks, Introductory Econometrics for Finance, 3rd edition, 2014, pages 260-261

2.3.3 A structural model for Bitcoin

Once we have estimated an autoregressive model, we have tried to estimate a structural model, based on explanatory variables other than the past values of the dependent variable. The explanatory variables we chose are the returns of other currencies' exchange rates and in particular, the EUR/USD and the JPY/USD crosses.

Before we estimate the model, we have previously investigated the specific statistics and properties of the two series separately, to see if they are similar to BTC/USD behavior. This choice was made for the purpose of studying Bitcoin again as a currency, since the currencies we have chosen are two of the most important currencies in the world and have a long history backing them. We looked at the summary statistics and at the stationarity of the series for the comparison.

For what concerns the exchange rates, first of all we looked at the summary statistics of the series already considering the correlations with their lagged values, so that we could compare it to BTC/USD results. Table 7 shows the summary statistics of the three crosses based on daily data from September 16,2013 to September 17,2017. We have to pay attention to the amount of observations we have for each series since every exchange rate has a particular schedule for trading (e.g. EUR/USD is not traded on Saturdays and Sundays, while JPY/USD is not only on Sundays and BTC/USD is almost traded everyday with some exceptions for regulatory reasons). Therefore, for BTC/USD we have 1442 observations, for EUR/USD 1045, and for JPY/USD 1248.

Table 7, source: personal examination

BTC/USD		EUR/USD		JPY/USD	
Mean	0,33%	Mean	-0,01%	Mean	-0,01%
Volatility	4,36%	Volatility	0,55%	Volatility	0,69%
Median	0,17%	Median	-0,01%	Median	0,00%
Skewness	0,316834225	Skewness	0,198029275	Skewness	0,08929885
Kurtosis	9,368462902	Kurtosis	2,648437896	Kurtosis	2,210313212
Excess Kurtosis	6,368462902	Excess kurtosis	-0,351562104	Excess kurtosis	-0,789686788
Autocorr (1lag)	-5,86%	Autocorr (1 lag)	-3,30%	Autocorr (1 lag)	-18,33%
Autocorr (2lag)	-1,59%	Autocorr (2 lag)	0,80%	Autocorr (2 lag)	2,01%
Autocorr (3lag)	1,57%	Autocorr (3 lag)	-2,83%	Autocorr (3 lag)	-2,21%

Already at first glance we can see that the traditional currencies' exchange rates returns are more similar to each other than compared to Bitcoin. Bitcoin's mean is higher that Euro and Yen means

which are the same. The two national currencies display completely different volatilities with respect to Bitcoin's one is far above the other two levels, which are very close one to the other. The only similarity stands in the skewness as they are all positively skewed but at different degrees: Yen's skewness is the nearest one to the normal distribution value, which is zero, followed by the one of the Euro and then by Bitcoin. The kurtoses are extremely dissimilar: Bitcoin's kurtosis is the highest and the excess of kurtosis makes its distribution leptokurtic, as it has flatter tails; while the other two, especially the Euro, exhibit values which are closer to the normal distribution value (=3) and are said to be platykurtic. When we look at the autocorrelations with each lagged value we can distinguish two paths of return evolution: for traditional currencies the sign of each correlation coefficient changes from time to time, it is negative for the first and the third lag and positive for the second one; while for Bitcoin the change in the sign of the correlation coefficients takes longer, as they are negative for the first two lags and then positive for the third way. This may be an evidence of the volatility clustering we investigated in the previous section.

The second step requires the test to see whether the singular series display the properties we investigated for BTC/USD cross, therefore volatility clustering and conditional heteroskedasticity, and whether they are stationary. For both of them we went through the same procedures as before. For what concerns the Euro, we tested the correlation coefficients of the square of the returns, whose structure allows for a linear dependence. They are all positive and statistically significant both through the individual test and through the Ljung-Box test; the outcome is that there is volatility clustering and therefore conditional heteroskedasticity, and returns are not IID random variables, as for Bitcoin. We tested for the stationarity of the series but we did not get the same result as in the case of Bitcoin: our series is not stationary as the t statistic lies inside the interval which do not refuse the H_0 hypothesis, that states that the series contains a unit root. A table with the results is shown in the appendix at the end of the paper (Table A).
For what concerns the Japanese Yen, the autocorrelation coefficients are all positive and statistically significant as both tests stated so; therefore, we have volatility clustering, conditional heteroskedasticity and returns which are not IID random variables. The stationarity test procedure has given positive results for our purpose: the series is stationary because the t statistic is smaller than the critical value at 5% significance level. Results are plotted in the appendix at the end of the paper (Table B).

After all these tests, we run a multivariate model of the form:

$$Y_t = \alpha + \beta_1 X_{1t} + \beta_2 X_{2t} + \varepsilon_t$$

Table 8, source: personal examination

Correlation	
BTC/USD and EUR/USD	1,04%
BTC/USD and JPY/USD	1,64%
EUR/USD and JPY/USD	34,5%

where the symbols are as follows:

- Y_t stands for BTC/USD return
- X_{1t} stands for EUR/USD return
- X_{2t} stands for JPY/USD return.

We have adapted the samples since the number of observations were different for each of the series, so as to obtain a consistent number of observations, which is equal to 1027 for the same time period used in the previous paragraphs. This is due to the fact that trading of each currency does not occur sometimes in the same days

Before the actual estimation of the model, we looked at the correlations (Table 8) between the explanatory variables and the dependent variable which are very low, whereas the correlation between the two explanatory variables is much higher. The correlations we are interested in are the lowest and this does not bode well for our estimation. We run the regression and this is the outcome, presented in Table 9.

Table 9, source: personal examination

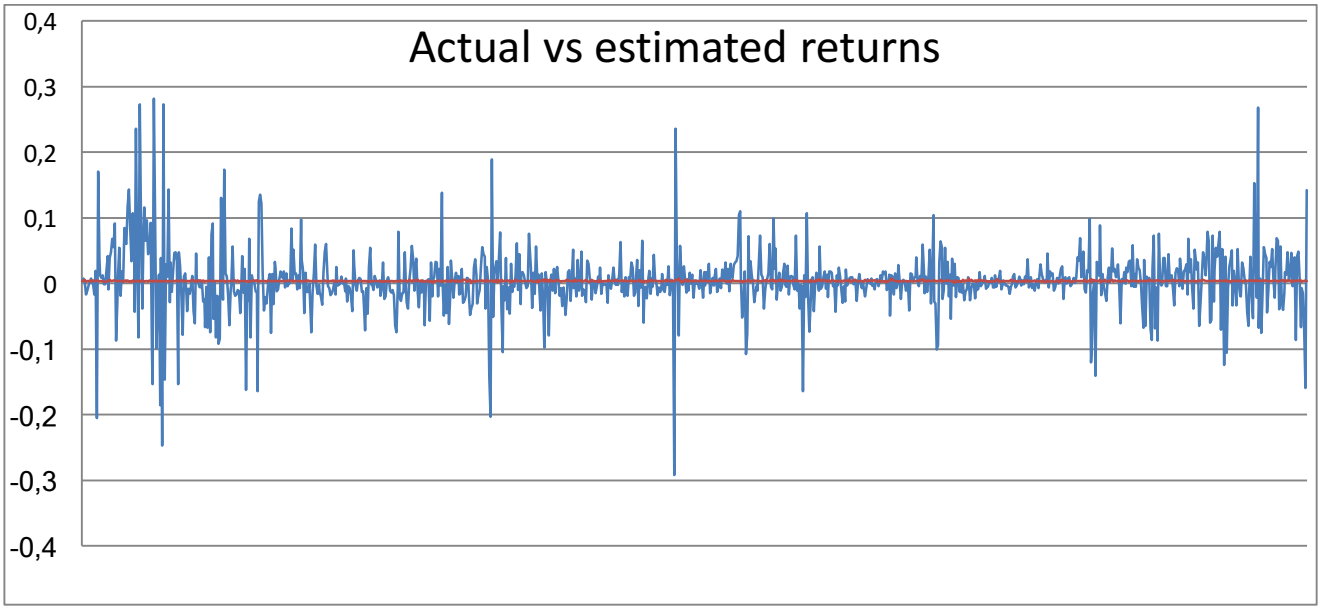
Regression statistics						
Multiple R	0,017135495					
R square	0,000293625					
Adjusted R square	-0,001658926					
Standard Error	0,047099869					
Observations	1027					
ANOVA						
	df	*SS*	*MS*	*F*	*Significance F*	
Regression	2	0,000667206	0,000333603	0,150380258	0,860399745	
Residual	1024	2,271639183	0,002218398			
Total	1026	2,272306389				
	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	0,004014651	0,001469934	2,731177275	0,006419292	0,001130223	0,006899078
Variable X1	0,046482857	0,285917556	0,162574337	0,87088567	-0,514568402	0,607534116
Variable X 2	0,094367882	0,216645418	0,43558679	0,663228357	-0,330751815	0,51948758

When we look at the regression we care for two issues: the evaluation of the significance of the entire model and of the statistical preciseness of the estimations we obtained.

The former requires the scrutiny of the R square, the number of observations and of F. R^2 is very low, which implies that the proportion of the variance, which represents the behavior of the BTC/USD returns, explained by the two chosen regressors is small. Thus, the scarce goodness of fit suggests that the model is inappropriate as estimated values are mostly different from the ones of the series. Besides, R square estimation is more precise as the number of observations increases: in this case the number of observations is high (1027), thus R^2 result is reliable. Furthermore, to complete the examination of the significance of the complete model we considered the F-test. The F-test is a multivariate test where the test statistic has an F-distribution under the null hypothesis; it

is frequently used when comparing statistical model fitted to a data set, in order to identify the model that best fits the population from which data are sampled. In our case, we cannot reject the null hypothesis since the F statistic is smaller than the critical value of the significance F (0,15<0,86). This implies that there is no regression effect: we cannot assume a linear relation between the dependent variable and none of the explanatory variables.

Once we have determined the inadequate significance and reliability of the model, we have evaluated the statistical preciseness of the obtained estimations. We considered the t-test on the coefficients. With a significance level of 5%, the only coefficient whose estimation is statistically significant and accurate is the one of the intercept; whereas for the other two coefficients the same cannot be stated. This means that they do not only have any effect on the model but also their estimation is not reliable. Probably if we run the same test for different samples, we would get completely different coefficients and results. Figure 16 show the expected values of the returns in red and the actual values in blue. Figure 16, source: personal examination



The use of such a model due to its poor performance is not recommended. The modest performance of the model could have been foreseeable already from the correlation coefficients which are very low. Additionally, this sustains our previous decision to choose a univariate model to make predictions about the returns. Perhaps, other variables would have been needed for the estimation of a model explaining the behavior of the returns of BTC/USD cross, but this choice has been prescribed by the purpose of our investigation in this chapter. We wanted to investigate the nature of Bitcoin either as a currency or as an investment, and we wanted to check the relationship, if there was any, between its returns and the returns of other currencies which have the most important role in the economy, together with the US dollar which has always been considered in this research as all exchange rates were based on it.

CHAPTER 3 CONCLUSION

At the end of our analysis on digital payment systems and virtual currencies, with a special attention for Bitcoin case, we can briefly sum up the main concepts and draw some final considerations. The digitalization brought by the FinTech revolution has strongly impacted the financial and economic systems, bringing them to a further level of efficiency and inclusion. Indeed, we have discovered that the integrated payment system, which is part of the innovation associated with the distributed ledger technologies and cryptocurrencies, possesses, at least in principle, four out of five criteria for an efficient payment system: it is technically efficient, accessible and non-discriminatory, priced efficiently, and internationally compatible. All these factors have contributed to a better functioning of the payment system thanks to the international operability of the system, which is able to reach people from all over the world in the shortest times ever. The most important invention which for sure is going to completely modify in the long run the entire infrastructure is the distributed ledger technology, whose main example stands in Bitcoin's Blockchain. Moreover, Blockchain does not only provide a procedure in payment systems for monetary uses, but also enables for non-monetary uses beyond the digital assets and currencies, which is projected to have a big impact on the future of the whole financial system. Smart contracts are the main outcome Blockchain has achieved and we are sure that we will be witnesses of future developments for what concerns decentralized applications.

The ecosystem of decentralized currencies has enlarged in the last decades and many entities which were not even conceivable some years ago, now can be part of our daily lives just in our hands, through the option to control and manage wallets by cellular phones. Bitcoin could be considered as a prototype of the kind of money that in the future will represent the custom of everyone, as Internet infrastructure is becoming more and more common in every part of the world. Indeed, the primary scope of Bitcoin's creator, Satoshi Nakamoto, was to create a competitive and more democratic alternative monetary system that could be capable of threating and modifying the current system and of establishing a real globalized world without frontiers. The utopist spirit that accompanied Bitcoin, at least at early stages, was that people who are living in a world where every angle is smoothing and everyone can establish relationships with anyone else without concerning about distance needed to get back the power of controlling a fundamental instrument as money. The first impulse given to the creation and development of instruments was actually the loss of trust on the supervising and "super partes" role of central authorities and in general of intermediaries in the financial system. Central banks evaluation of these new technologies is still very vague, although

increasing attention is posed to Bitcoin and other competing cryptocurrencies. Apart from the Chinese central bank, other supervisory institutions have only raised concerns and awareness about decentralized currencies and applications, which are starting to be studied and considered so as to be provided by the same central institutions they were trying to beat. Many central banks are planning to implement the distributed ledger technologies and some, as the Bank of England, are already developing their own cryptocurrency due to their advantages. Nevertheless, we cannot forget about the drawbacks, risks and potential disorders any problem could create in these kinds of systems. Fortunately, the impact of any problem in these systems is still very small as they are not commonly used, even though their usage is becoming more and more popular.
In order to become a plausible alternative to the already well-developed and established traditional payment systems, cryptocurrencies need some further steps that will help these innovative systems to become more stable, reliable and widely accepted.
Through our analysis of the cryptocurrencies world, we have obtained a more exhaustive picture of the industry as a whole and of the particular sectors, whose role is becoming increasingly important due to the fact that perhaps many jobs in the future will deal with such a reality. This shift of the professions towards a more digitalized and automatized world will have of course an immense impact on our lives, not only as workers and financial systems' participants, but also as a society, that will be utterly reshaped, causing new internal contrasts but may solving existing ones.

Bitcoin analysis was developed by following two different pathways. The monetary analysis has highlighted three major facts. Bitcoin is a good medium of exchange, a risky store of value, and a poor unit of account. Currently, it is well-known among people and used by an increasing number of them, as volume of transactions expressed in and Bitcoin in the last years has increased a lot. However, it is not stable at all because there are many and unpredictable fluctuations in the price and in general changes in its behavior. Volatility is still the most relevant concern about Bitcoin's function as a store of value and subsequently as a unit of account. As long as its behavior remains so erratic, and thus its volatility so high, we cannot expect a total trust by people on the system. The most terrific aspect of the system stands in the fact that financial authorities could ban them from one day to another, causing a drop of the economy as a whole, whose size is not foreseeable.
For this reason, most users tend to use it more as an investment due to its high returns. That is why we have chosen to estimate a model on the returns. We have tried two ways: the univariate and the multivariate one. The autoregressive model gave some positive results about the correlation between the returns and the lagged values, but of course since the currency is still so unstable, making predictions through our model is reckless at the moment. The structural model is neither

significant nor reliable as the explanatory variables we chose do not influence our dependent variable. This result supports our first choice to use a time-series model, which lead to a more significant result. However, the model should not be considered completely comprehensive as Bitcoin's returns behavior is very unpredictable. This may be due to its intrinsic instability, caused by the uncertain regulatory framework it would be submitted to and to its ambiguous legal status. Due to its high volatility and legal instability, Bitcoin cannot be considered as a currency in the traditional sense up to now; as an investment, it is surely not a safe-have asset and its behavior can be described by a random walk, as for many other kinds of investment. To conclude, the chances of an upcoming bubble cannot be excluded as much interest and unrest is stressing the financial environment around the cryptocurrency.

We think that if Bitcoin is still be used as a medium of exchange with more regularity and a sounder regulatory background, which may give security to users and to the system as a whole, and if Bitcoin's volatility is going to decrease over time due to the fixed supply, therefore leading to a stabilization of the price, Bitcoin could become a feasible alternative currency to the current traditional system of currencies. As it is now, Bitcoin's behavior is too different from traditional currencies' one to be considered as a 'real' currency; its continuous appreciation tempt people to save the token rather than spending them, as they expect to make gains from price increases, thus considering it more as an investment.

APPENDIX:

Note: All data for Bitcoin returns are taken from the exchange rate on Bitfinex.

Tables A and B for section 2.3.3

Table A, source: personal examination about the stationarity of EUR/USD exchange rate

Statistica della regressione	
R multiplo	0,044685062
R al quadrato	0,001996755
R al quadrato corretto	-0,000890429
Errore standard	0,00546741
Osservazioni	1041

ANALISI VARIANZA

	gdl	*SQ*	*MQ*	*F*	*Significatività F*
Regressione	3	6,20204E-05	2,06735E-05	0,69159249	0,557251019
Residuo	1037	0,030998603	2,98926E-05		
Totale	1040	0,031060623			

	Coefficienti	*Errore standard*	*Stat t*	*Valore di significatività*	*Inferiore 95%*	*Superiore 95%*
Intercetta	-0,000110753	0,000169541	-0,65325389	0,513737419	-0,00044343	0,000221929
Var X1	-0,057364999	0,054778163	-1,047223845	0,295240369	-0,16485368	0,050123684
Var X2	0,02331041	0,044533413	0,523436417	0,60078242	-0,06407547	0,110696288
Var X3	0,027932222	0,030990915	0,901303564	0,367636215	-0,03287983	0,088744275

Table B, source: personal examination about the stationarity of JPY/USD exchange rate

Statistica della regressione	
R multiplo	0,185206438
R al quadrato	0,034301425
R al quadrato	0,03196694
Errore standa	0,006774023
Osservazioni	1245

ANALISI VARIANZA

	gdl	*SQ*	*MQ*	*F*	*Significatività F*
Regressione	3	0,002022719	0,00067424	14,69335915	2,09158E-09
Residuo	1241	0,056946241	4,58874E-05		
Totale	1244	0,05896896			

	Coefficienti	*Errore standard*	*Stat t*	*Valore di significatività*	*Inferiore 95%*	*Superiore 95%*
Intercetta	-9,06187E-05	0,000192016	-0,471934031	0,637056843	-0,00046733	0,00028609
Variabile X 1	-0,225722531	0,0553285	-4,079679241	4,79747E-05	-0,334270264	-0,1171748
Variabile X 2	0,039472518	0,043996744	0,897169086	0,369802708	-0,046843699	0,12578874
Variabile X 3	0,021628097	0,028373961	0,762251606	0,446054697	-0,034038136	0,07729433

BIBLIOGRAPHY

- Ammous, S., 2015, "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation, and International Development", The Journal of Private Enterprise 30(03), 19-50
- Andolfatto, D., 2014, March 31, "Bitcoin and Beyond: the Possibilities and Pitfalls of Virtual Currencies", Dialogue with the FED, Federal Reserve Bank of St. Louis
- Androulaki, E., et al., 2012, "Evaluating User Privacy in Bitcoin", IACR Cryptology ePrint Archive 596
- Aristotle, "Politics", translated by Benjamin Jowett, 1994-2009, Book 1, Part 1
- Asli Demirguc-Kunt and Leora Klapper, (April 2012) "Measuring Financial Inclusion: The Global Findex Database", Policy Research Working Paper No. 6025, The World Bank, Development Research Group, Finance and Private Sector Development Team, available at: http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2012/04/19/000158349_20120419083611/Rendered/PDF/WPS6025.pdf
- Boel, P., 2016, "Thinking about the future of money and potential implications for central banks". Sveriges Riksbank Economic Review 2016:1
- Bohme, et al, Spring 2015, "Bitcoin: Economics, Technology, and Governance", Journal of Economic Perspectives – Volume 29, Number 2, Pages 213-238
- Brainard, L., 2016, April 14, "The use of distributed ledger technologies in payment, clearing, and settlement", Speech by Ms Lael Brainard, Member of the Board of Governors of the Federal Reserve System, at the Institute of International Finance Blockchain Roundtable, Washington DC.
- Brooks, 2014, "Introductory Econometrics for Finance", 3rd edition, Cambridge University Press
- Camera, 2017, "A perspective on electronic alternatives to traditional currencies", Economic Science Institute, Chapman University and WWZ, University of Basel
- CCD, Computer Communications Division, Ministry of Internal Affairs and Communications, "Working Group on Ideal P2P Network, Network Neutrality Committee", (http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/network_churitsu/pdf/wg2_061129_1_si_1_2. Pdf
- Chohan, U., 2017, August 4, "Cryptocurrencies: A Brief Thematic Review", School of Business and Economics, University of New South Wales, Canberra, Discussion paper
- Chokun, J., 2014, "Who Accepts Bitcoin as a Payment? List of Companies, Stores, Shops", available at: www.bitcoinvalues.net
- CPMI, Committee on Payments and Market Infrastructures, 2015, November, "Digital currencies", Bank for International Settlement
- CPMI, Committee on Payments and Market Infrastructures, 2017, February, "Distributed ledger technology in payment, clearing and settlement – an analytical framework", Bank for International Settlement
- D'Alfonso, et al., 2016, October 17, "The Future of Cryptocurrency – an investors'comparison of Bitcoin and Ethereum", Ryerson University

- Deloitte LLP, 2016, "Blockchain Enigma. Paradox. Opportunity", The Creative Studio at Deloitte, London. J7969
- Dourado, E. (2014) Here's How Cryptocurrencies Could Replace the US Dollar, elidourado.com/blog/bitcoin-dollar/
- Drawbaugh, K., and Temple-West, P., 2014, March 25, "Bitcoins are property, not currency, IRS says Regarding Taxes", Reuters, available at: http://www.reuters.com/article/2014/03/25/us-bitcoin-irs- idUSBREA2O1LR20140325
- EBA, 2013, December 12, "Warning to consumers on virtual currencies", EBA/WRG/2013/01
- ECB, 2015, February, "Virtual currency schemes- a further analysis" , www.ecb.europa.eu
- Financial Action Task Force (FATF) Report, 2014, June, "Virtual Currencies – key definitions and potential AML/CFT Risks", www.fatf-gafi.org
- Franco, P.,2014, "Understanding Bitcoin. Cryptography, Engineering and Economics", Wiley
- Glaser F., et al., 2014, "Bitcoin - Asset or Currency? Revealing users' hidden intentions", complete research, Twenty Second European Conference on information systems, Tel Aviv
- Greenwood, J., 2013, October 3, "FBI's Shutdown of Illicit Drug Website Silk Road Will Reveal Bitcoin's Resilience", Financial Post, available at: http://business.financialpost.com/2013/10/03/fbis-shutdown-of-illicit-drug-website- silk-road-will-reveal-bitcoins-resilience/
- Grinberg, R., 2012, "Bitcoin. Today Techies, Tomorrow the World?", The Milken Institute Review
- Hayek, F., 1974, "Denationalization of Money – the Argument Refined, An Analysis of the Theory and Practice of Concurrent Currencies", Third edition, the Institute of Economic Affairs, 1990
- Hernandez- Verme, P. L., Valdes Benavides, R. A., 2013, June, "Virtual Currencies, Micropayments and the Payment Systems: a Challenge to Fiat Money and Monetary Policy?"
- Hileman G and Rauchs M., 2017, "Global Cryptocurrency Benchmarking Study", Cambridge Centre for Alternative Finance, University of Cambridge
- Keynes, J., M., 1930, "A Treatise on Money", Macmillan Publishers, London
- Kollmeyer, B., 2013, July 24, Bitconned: SEC sounds the alarm over virtual currency fraud, The Wall Street Journal, Market Watch , available at: http://blogs.marketwatch.com/thetell/2013/07/24/bitconned-sec-sounds-the-alarm- over-virtual-currency-fraud/
- Kroll, J., A., Davey, I., C., Felton, E., W., 2013, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", Princeton University
- Liikanen, E., 2015, June 4, "Enhancing reliability and efficiency of future payments – five criteria", Speech by Mr Erkki Liikanen, Governor of the Bank of Finland, at the European Central Bank/Bank of Finland Retail Payment Conference
- Mick, J., 2011, June 19, "Inside the Mega-Hack of Bitcoin: The Full Story", Daily Tech, available at http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm

- Mills, David, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kar- genian, Max Ellithorpe, Wendy Ng, and Maria Baird (2016). "Distributed ledger technology in payments, clearing, and settlement," Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2016.095
- Nakamoto, S., 2008, October, "Bitcoin: A Peer-to-Peer Electronic Cash System"
- Nakaso, H.,2016, November 18, "FinTech - its impacts on finance, economies and central banking", Remarks by Mr Hiroshi Nakaso, Deputy Governor of the Bank of Japan, at the University of Tokyo - Bank of Japan Joint Conference on "FinTech and the Future of Money", Tokyo.
- Niederjohn N., et al., 2015, "Is Bitcoin the Money of the Future?", Teaching about Money and the FED, Social Education 79(2), National Council for the Social Studies
- Nomura Research Institute, March 2016, "Survey on Blockchain Technologies and Related Services: FY2015 Report", survey contracted by Japan's Ministry of Economy, Trade and Industry
- Pacia, C., 2013, October, "Bitcoin and the Deflationary Spiral", available at: http://chrispacia.wordpress.com/2013/10/22/bitcoin-and-the-deflationary-spiral/
- Plassaras, N. A., 2013, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of IMF", Preliminary Draft
- PwC's Financial Service Institute, 2015, August, "Money is no object: Understanding the evolving cryptocurrency market", PwC, www.pwc.com/fsi
- SEC, Ponzi Schemes Using Virtual Currencies, SEC, Office of Investor and Advocacy (https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf)
- Segendorf, B., 2014, "What is Bitcoin?", Sveriges Riksbank Economic Review
- Skinner, C., 2013, April 15th, "The Real Cause of Bitcoin Bubble and Burst", Financial Services Club Blog, available at: http://thefinanser.co.uk/fsclub/2013/04/the-real-cause-of-the-bitcoin-bubble.html
- Swann, G. M. Peter, 2002. "The functional form of network effects," Information Economics and Policy, Elsevier, vol. 14(3), pages 417-429, September
- Taylor, M., B., 2013, September, "Bitcoin and The Age of Bespoke Silicon", University of California, San Diego
- Thiele, C., 2016, November 21, "Blockchain technology - opportunities and challenges", Keynote speech by Mr Carl-Ludwig Thiele, Member of the Executive Board of the Deutsche Bundesbank, at the 6th Central Banking Workshop 2016, Eltville
- Weber, B., 2014, December 22, "Bitcoin and the legitimacy crisis of money", Cambridge Journal of Economics 2014, 1 of 25 doi:10.1093/cje/beu067
- Wilhite, T., "Difference Bteween E-Money and Credit Cards", available at: http://www.ehow.com/about_6676381_difference-between-e_money-credit- cards.html
- Wilkins, C., 2014, November 13, "Money in a digital world", Remarks by Ms Carolyn Wilkins, Senior Deputy Governor of the Bank of Canada, at the Wilfrid Laurier University, Waterloo, Ontario,

- Wilkins, C., 2016, June 17, "Fintech and the financial ecosystem – evolution or revolution?", Remarks by Ms Carolyn Wilkins, Senior Deputy Governor of the Bank of Canada, at Payments Canada, Calgary, Alberta
- Williams, D., 2017, ""Cryptocurrency compendium: A Reference for Digital Currencies"
- Zuckoff, M., 2005, "Ponzi's Scheme: The True Story of a Financial Legend", Random House, New York

SITOGRAPHY

- Bitcoin charts, http://bitcoincharts.com/charts/mtgoxUSD#rg730zm1g10zm2g25zv
- Bitfinex, www.bitfinex.com
- History of Bitcoin, http://historyofbitcoin.org/
- Data on returns: http://investing.com/
- Payment system Definition: BusinessDictionary.com. WebFinance, Inc. http://www.businessdictionary.com/definition/payment-system.html .
- Wikipedia on Byzantine fault tolerance, https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
- Wikipedia on Escrow account, https://en.wikipedia.org/wiki/Escrow
- Wikipedia on Ponzi Scheme, https://en.wikipedia.org/wiki/Ponzi_scheme
- Wikipedia on Unit root test, https://en.wikipedia.org/wiki/Unit_root_test