LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Economia e Finanza Cattedra: Money and Banking

Bitcoin:

An "Alternative" Currency or an

Investment Opportunity?

RELATORE

Prof. Paolo Paesani

CANDIDATO

Sara Mariani

Matr. 167501

ANNO ACCADEMICO

2013/2014

Index

Chapter 2: Case Study: Bitcoin

Introduction

Since the development of Internet, from its early stages, it was clear to everyone that some kind of pacific and silent revolution was going to happen to change many things in our lives. The creation of a net of interconnected nodes, first just some hundreds, now billions, opened the doors to a huge variety of opportunities that were previously only science-fiction. The benefits offered by Internet range from the readily available to everyone knowledge and information to the possibility of communicating with people on the other side of the world as fast and cheaply as if they were at the next door. This new "online world" gave fertile ground to many people's creativity to develop infinitely many new ways to facilitate our lives on every possible field. For instance, in the field of the economy new frontiers were opened to international trade, internet banking, up to online shopping.

Exactly in this florescent environment, among the many other innovations, new forms of payment have developed. Starting from electronic money, where real money is *"stored on an electronic device"*[1], as well as credit cards and debit cards, can be used to make online payments transferring money digitally stored. Even though e-money and credit cards are indeed two different things as credit cards are legal contracts, a consumer loan, where interest rate is paid, they share a similar use as a means of online payment.

Building from the base-concept created by the first digital forms of real money, created with the aim of facilitating transactions in a more and more global environment, on the same wave length we find virtual currencies. Despite the substantial differences between e-money and virtual currencies, which will be deeply analyzed at the beginning of chapter 1, the leading element assimilating them is not only the digital, instead of physical, content of such money, but, from a more conceptual point of view, the common aim of speeding up

[1] Directive 2000/46/EC of the European Parliament and of the Council

transaction in a world where time is more and more important and where the web has permeated our everyday life without any possibility of going back.

Despite cash is still far from disappearing, world payments statistics report that thanks to many factors, above all the development of Internet with all its consequences as already mentioned, online and non-cash transactions are increasingly growing at a steady rate all over the world[2]. Even though this analysis is still about real money and the use of credit and debit cards, it proves people increasing willingness to simplify and improve payment methods in order to match the huge supply of online goods and services. Therefore, virtual currencies place them self in a context of an increasing need of being as close as possible to such fascinating world of opportunities which is the web.

Virtual currencies promise is an easy and available to everyone alternative to traditional money system. Different types of them exist, with singular and common features, uses and goals. Generally speaking, what they have in common is highlighted in their name: those currencies are "virtual" thus they wish to target the online world and be something different from traditional real currency, and in some cases to overcome traditional money's system.

The aim of this thesis is an in-depth analysis of virtual currencies, with all their different expressions and uses, considering their potential together with the related shortcomings, and a focus on the Bitcoin case will be in particular inspected, investigating the reasons of its success and evaluating eventual future scenarios.

The thesis is structured in two chapters. Chapter 1 deals with virtual currencies in general, explaining the points in common and the distinctions with electronic money and

[2] Capgemini and Royal Bank of Scotland, 2013, "World Payment Report, 2013"

with traditional currencies. The different forms of virtual currencies are further analyzed singularly together with the extension of the phenomenon, even though, due to the continuously changing environment, it is rather difficult to find exact data to quantify it and compare the market for virtual currencies with the already well-established traditional one. It follows a description of advantages and disadvantages of virtual currencies always taking into account the comparison with traditional one. Then, legal issues related to virtual currencies are examined from the point of view of regulatory actions that might be taken to avoid an improper use of those currencies both to elude tax payments and to get involved in illegal activities. Finally, a deeper analysis of those illicit activities is considered and the reasons why virtual currencies particularly attract criminals are explained.

Chapter 2 deepens the analysis of virtual currencies focusing on the case of the crypto-currency Bitcoin, created at the end of 2008 by a developer under the pseudonym Satoshi Nakamoto. The fundamental elements of the functioning of this particular virtual currency are described in details, with a special attention to the mining activity, namely the way in which Nakamoto solves the problem of double spending without the need of a central authority together with the problem of the incentives to act honestly. Furthermore, a brief history of the salient events related to Bitcoin, useful to understand its evolution across the last six years, is presented. Following the pattern of the first chapter, positives and negatives of Bitcoin are evaluated, including the reasons for its success among all the vast number of virtual currencies but also its “dark side” especially feared by governmental authorities. Finally, a quantitative analysis of price fluctuations and volatility is interpreted and studied also through some summary statistics evaluated by means of the program STATA, and some final considerations on possible scenarios of future evolution are drawn from the previous analysis.

Chapter 1
VIRTUAL CURRENCIES

1.1 Digital Money: Virtual Currencies vs Electronic Money

Confusion is often made between what is called "virtual currency" and electronic money, therefore a clear distinction should be made between the two both in terms of definition and use. Before this, however, a brief excursus on the types of money and their characteristics will be useful in order to understand what follows. The most remarkable types of money to consider are commodity money, fiat currency, managed money, scriptural money, and electronic money. Keynes (1930) defines *commodity money* as "actual units of a particular freely-obtainable, non-monopolized commodity which happens to have been chosen for the familiar purposes of money". On the other hand, *fiat currency* is characterized by being "created and issued by the State" as a representative of value even though not having an intrinsic value as for commodity money. Scriptural money is defined as "deposit balances held on an account at a credit institution or a central bank"[3] and can be converted in fiat money at any time. According to Directive 2000/46/EC of the European Parliament and of the Council[4], "*electronic money shall mean monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipts of funds of an amount not less in value than the monetary value issued; (iii) accepted as a means of payment by undertakings other than the issuer".*

Virtual currencies and electronic money are easily confused as both are considered "digital money", meaning that their content is not physical, as for instance coins and

[3] ECB, 26 April 2006, "Opinion of the European Central Bank on a Proposal for a Directive on Payment Services in the Internal Market, ECB/2006/21

[4] Directive 2000/46/EC available at: http://www.columbia.edu/~mr2651/ecommerce3/2nd/statutes/ElectronicMoneyDirective.pdf

banknotes, but as in the definition, it is "stored electronically". However, despite this similarity, there are important distinctions to point out. The most crucial one regards the unit of account which differs in the two types. On the one hand, electronic money is backed by traditional currencies, with a legal tender status, thus the unit of account is still euro, US dollar, pound or others. On the other hand, virtual currencies are not legal tender and are not backed by traditional currencies, but an exchange rate is needed to convert for instance Linden Dollars[5] into traditional US dollars. Given this main difference, it is clear that while electronic money must be accepted by everyone, as it is legal tender, virtual currency is often accepted only within a specific virtual community or platforms. More generally, despite the format in which it is stored, virtual currencies differ from electronic money as it does with traditional currencies as it can be observed from the table below. Specifically, while virtual currencies are issued by a private company, which can arbitrarily decide how to manage the supply of money, electronic money is subject to a legally established institution, which has to follow specified rules dictating about money supply and is also entitled to supervision over prudential requirements. Finally, while electronic money has mainly operational risk, which is linked to inadequacy or failure of "internal processes, people and systems, or from external events (including legal risk)", as defined by Basel II[6] regulation, virtual currencies are subject to a broader range of risks including not only operational risk, credit risk and liquidity risk, but also the risk of frauds and an uncertainty which derives mainly from the related lack of regulation.

[5] Linden Dollar is one of the many types of virtual currencies. Specifically, it is the currency used in the 3D virtual world "Second Life", which was created in 2003 and gained a great success in the first decade of XXI century.

[6] European Commission, "Basel II: Revised International Capital Framework"

Table 1.1. Electronic Money vs Virtual Currency: a Comparison

	Electronic money schemes	Virtual currency schemes
Money format	Digital	Digital
Unit of account	Traditional currency (euro, US dollars, pounds, etc.) with legal tender status	Invented currency (Linden Dollars, Bitcoins, etc.) without legal tender status
Acceptance	By undertakings other than the issuer	Usually within a specific virtual community
Legal status	Regulated	Unregulated
Issuer	Legally established electronic money institution	Non-financial private company
Supply of money	Fixed	Not fixed (depends on issuer's decisions)
Possibility of redeeming funds	Guaranteed (and at par value)	Not guaranteed
Supervision	Yes	No
Type(s) of risk	Mainly operational	Legal, credit, liquidity and operational

Source : ECB, October 2012, Virtual Currency Schemes, p.16

1.2 Virtual Currencies: General Characterization

Virtual currencies originated, as a natural consequence, after the creation and establishment of the internet in the 1980s, when the excitement for this new fashion exploded and flourished, and they are increasingly proliferating under many different and new forms. Virtual currencies differ from traditional ones in that they are not backed by a central bank which is a trusted party guaranteeing for the actual value of money represented by coins, banknotes, checks, and so on. Basically, a central authority that lies in between the two exchanging parties is not necessary for the transaction to be accomplished. Moreover, advantages in using virtual currencies compared to traditional ones concern their easier and faster use, as the intermediary between two users is bypassed.

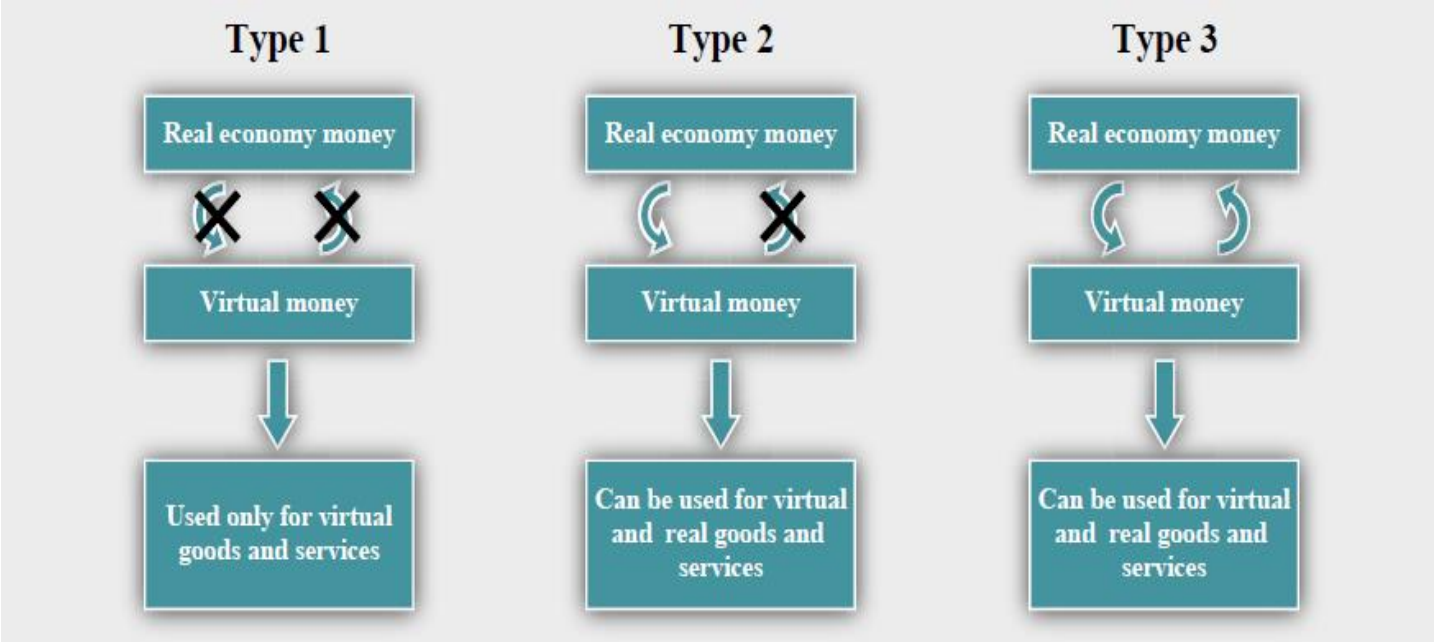
Virtual currencies have evolved mostly in the last decades, however their original roots might be dated back to 1887 in Coca-Cola's marketing strategy, with the first-ever coupon (J. McKee, Redefining Virtual Currency, 2013). Such coupons may not seem to belong to the category encompassing virtual currencies, however, they can be viewed as such because, even though they are not "digital", they anticipate them in that they "substitute" real currency within a certain community. After Coca-Cola's success, many other forms of virtual currencies have developed, such as retail loyalty points, air miles, credit card rewards, which have been a strong incentive to users' brand loyalty. In addition, virtual currencies have recently taken the form of online tokens, especially used in online games, peer-to-peer currencies, among which the well-known Bitcoin, and mobile payments (J. McKee, 2013).

J. McKee (2013) further classifies virtual currencies into two broad categories: "mature" and "up-and-coming" virtual currencies. Physical coupons, air miles, and loyalty points belong to the first type, due to their significant market penetration and high volume, but slower growth. On the other hand, mobile coupons, digital coins and tokens are identified as "up-and-coming" for their higher growth, but still low volume.

However, a more complete, reliable and detailed classification is to be found in the ECB report (2012) on "Virtual Currencies Schemes". First of all, a virtual currency is defined as *"a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"* (ECB, Virtual Currency Schemes, 2012). Further, ECB's classification of virtual currencies relies on their increasing relationships with real money and real economy and distinguishes three types as it can be observed in the figure below (see Figure 1.1). "Closed virtual currency schemes" have little or no link to the real economy: they may be purchased through

a subscription or earned during the game, and used only online, and cannot be converted into real money. "Virtual currency schemes with unidirectional flow" have as can be inferred from the name a unilateral relation with real economy, meaning that the virtual currency can be purchased using real money at a predetermined exchange rate, but cannot be exchanged back to traditional currency. Finally, "virtual currency schemes with bidirectional flow" are the most critical and interesting at the same time as they can be bought and sold on an exchange market as any other traditional currency (ECB, 2012). This last type is the most critical, thus the most deeply analyzed, due to its strong relationship with the real economy, causing fear in central banks and other authorities that an increase in the volume of such virtual currencies may compromise and pose at risk the real economy.

Figure 1.1. Types of virtual currencies: ECB classification



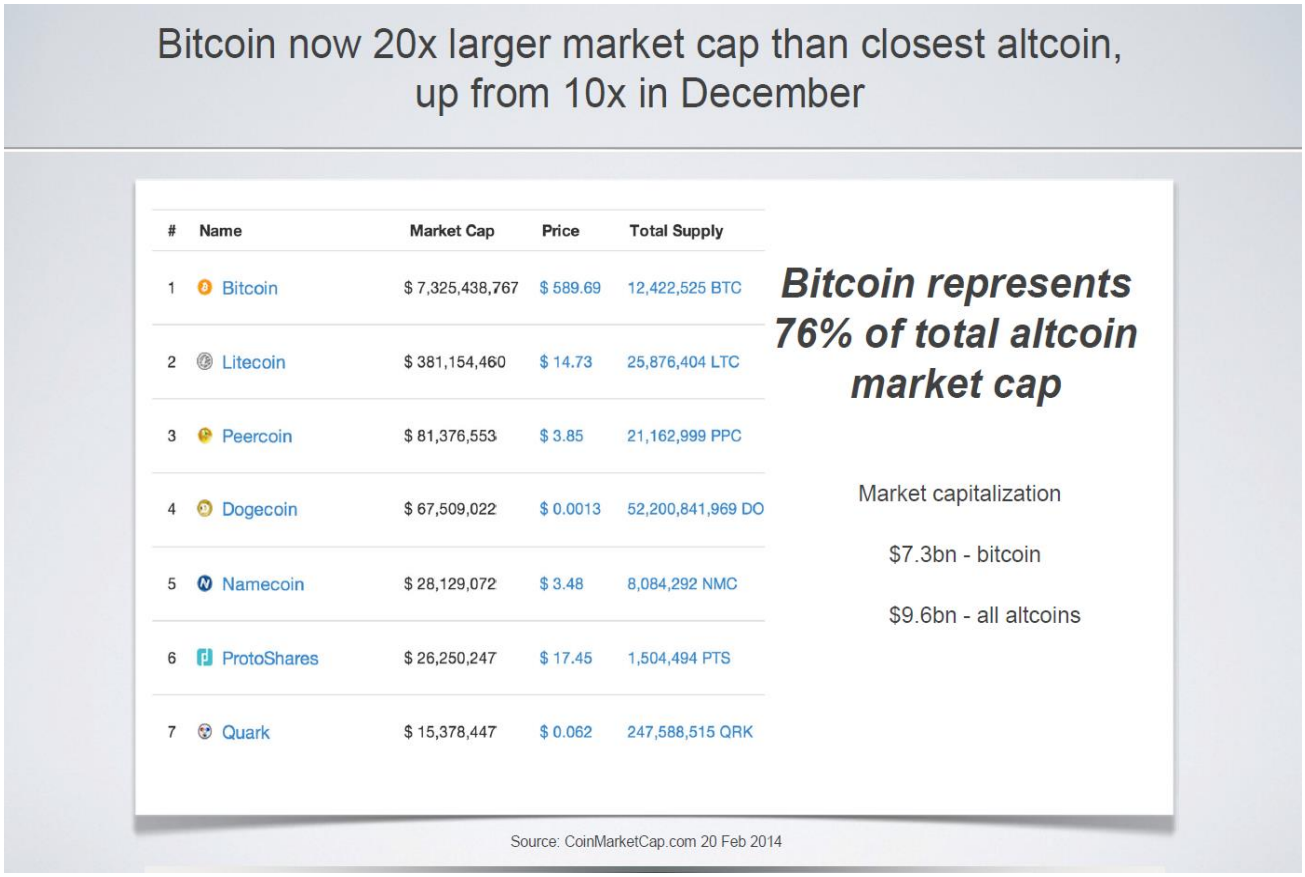
Source: ECB, Virtual Currencies Schemes, 2012

1.3 Market Size

Despite the rapid growth and continuous evolution over the last decades of virtual currencies, and the unstoppable creation of new ones, their market size is still relatively small if compared to the volume related to traditional currencies, which have, on their side, a time advantage. Moreover, trying to calculate an exact value of virtual currencies market share is fairly impossible due to the proliferation of always new digital currencies competing among each other. Overall, Bitcoin is considered to be the best-known and to own the largest share among its competitors.

As it is shown in the table below, Bitcoin represents the 76% of total *altcoin* market capitalization with about $7.3 billion over a total of $9.6 billion. Among the virtual currencies falling under the definition of altcoin appear Litecoin, Peercoin, Dogecoin and others with less remarkable market capitalization. Moreover, the price is also the highest among all the others, very far from $17.45 of the second highest with its $589.69 per bitcoin.

Figure 1.2. Virtual Currencies



Source: CoinDesk

Moreover, according to data from the FED[7], there are currently $7 billion bitcoin in circulation, which compared to $1,200 billion USD in circulation is quite a striking data taking into account that bitcoin was created in 2009. Further, to give an idea of the weight of virtual currencies we can take bitcoin as a proxy for the whole market, given that it represent quite a significant portion of it. In addition, an interesting data to observe is the number of transactions in both bitcoin and USD which is, respectively, 40 transactions per minute against 200,000 using Visa and even more notably is their average size, respectively, $2,000

[7] 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

against $80. This last data proves that as virtual currencies do not impose transaction limits, the average size tends to be far higher compared to these in real currencies using for instance a credit or debit card.

1.4 Virtual Currencies Other Than Bitcoin

Despite Bitcoin is probably the most well-known virtual currency broadly acquainted all over the world, many other types exist, such as Second Life's Linden Dollars, Gold, Silver and Copper coins used in the three dimensional online game World of Warcraft, and an infinite list of crypto-currencies developed after Bitcoin's large success.

1.4.1 Second Life and Linden Dollars

In 2003 Linden Lab, a company developing digital entertainment spaces, created its most famous product: Second Life, a 3D virtual world where users can create the so called "avatars", namely the characters that act in their place in this parallel world[8]. People can be whoever they want and do everything they like, and probably be and do through those avatars whatever they cannot be in their real life. Second Life shares some characteristics with online games, such as the interaction with other players in a three dimensional environment, but it also differs from them as no objectives or goals are set[9]. What it is interesting about Second Life is that, being a virtual copy of real world, it has its own economy, thus, with its own currency, which is the Linden Dollar (or L$). Second Life's economy is very similar to real world economy in that it is determined by demand and supply, where Linden Lab company plays the role of a central bank issuing money and

[8] On Second Life: http://lindenlab.com
[9] On Second Life http://www.cds.hawaii.edu/employable/downloads/tools/SLconnect.pdf

adjusting supply arbitrarily, although, on the contrary of real world economy, producers have no limited capacity *"therefore the supply curve is horizontal which implies that changes in demand only affect transactions but not the price level"* (Ernstbeger, 2009). Linden Dollar is defined by Linden Lab itself as follows: *"Second Life "currency" is a limited license right available for purchase or free distribution at Linden Lab's discretion, and it is not redeemable for monetary value from Linden Lab"*(Terms of Service, subsection 1.4). Linden Dollar belongs, therefore, to the second type of virtual currency according to the ECB's definition in that there is a unidirectional flow connecting real and virtual money: people can buy Linden Dollars with US Dollars (or other real currencies) on the LindeX, Linden Dollars' exchange market, but cannot give back Linden Dollars for real money. Moreover, Linden Dollars are acquired when paying for a "Premium account" and can be gained during the game in a huge variety of ways ranging from having a paid job in the virtual world to playing some games such as "Gold Hunt", "Fish Hunt", "Dragons and Princesses" and even getting them from "Money trees"[10]. Other ways of gaining in-game Linden Dollars are investing them within the virtual world, building and creating things and selling them or becoming land owners and for instance renting it. Creativity is one of the main factors that helps making money inside Second Life, as it is mainly a game thus often it is not necessary to find a boring job inside the virtual life as well.

Despite the great success of this virtual world, as it was predictable, after nine years the initial enthusiasm, together with users, has decreased until the phenomenon slowly disappeared[11].

[10] On how to earn Linden Dollars: http://wiki.secondlife.com/wiki/How_to_Earn_Linden_Dollars_in_Second_Life

[11] Second Life: http://nwn.blogs.com/nwn/2011/12/2012-linden-lab-pivots-from-second-life.html

1.4.2 MMORPG and World of Warcraft

Other kinds of virtual economies exist in relation to the so called MMORPG, namely Massively Multiplayer Online Role-Playing Games. In these online games people, either by purchasing them or acquiring achieving some in-game goals, gain a virtual currency whose use makes sense only within the game itself. One of the most famous MMORPG is World of Warcraft, a 3D multiplayer role-playing online game created in 2004 and that, together with its in-game virtual currency, gained large popularity among video-gamers with more than 12 million of monthly subscribers as of 2010[12]. World of Warcraft's money is some amounts of Gold, Silver and Copper, which can be spent during the game to pay for some items and obtained by "looting dead mobs, completing quests, selling items to vendor NPCs, via trade or mail from other player characters or by selling an item at the Auction House"[13]. At the beginning a player starts with no money and he "creates" it during game activities at an increasing rate, at the same time players "destroy" money from their server when the spend it, thus the amount of money on a server depends only on the game, however, a Gold cap exists at 999,999 Gold coins 99 Silver coins and 99 Copper coins. Anyway, money created and destroyed within the game essentially stays there, although some people sells and buy Gold coins outside the game such market is restricted and it does not affect in any way the real economy.

[12] On World of Warcraft: http://www.wowwiki.com/World_of_Warcraft
[13] On World of Warcraft's money: http://www.wowwiki.com/Money

1.4.3 Altcoin: Alternatives to Bitcoin

After Bitcoin's success, a huge number of alternative crypto-currencies of different kinds have been created, in the attempt of "nibbling" Bitcoin's large market share in the field of virtual currencies. Three broad categories of these so called "Altcoins"[14], meaning alternative coins, exist. Firstly, those using the same hashing algorithm as Bitcoin, SHA-256, such as Namecoin (NMC), Peercoin (PPC), Devcoin (DVC), Terracoin (TRC), Ixcoin (IXC), just to mention some of them, and many others. Then, other crypto-currencies using the same scrypt algorithm as Bitcoin exist: Litecoin (LTC), Novacoin (NVC), Feathercoin (FTC), Worldcoin (WDC), Megacoin (MΣC), Goldcoin (GLD), and so on. Those first two categories represent crypto-currency which mostly tried to "copy" Bitcoin and that for instance, can be mined using the same machines as Bitcoin, especially those belonging to the first type, while the second type are in some way easier to mine, thus they do not require the latest technologies, such as FPGA[15] and ASIC, but can still be mined through GPU cards[16]. On the other hand, some other crypto-currencies, among which Primecoin (XPM), Quark (QRK), Securecoin (SRC), Yacoin (YAC), have tried to bring some innovative features in the market and can still be mined using CPU devices.

However, all these alternative crypto-currencies together are not able to overcome Bitcoin's reputation and do not offer many marketplaces where they are accepted, therefore, until one of those virtual currencies comes up with some more-innovative technology, they are going to be relegated in a small corner, in Bitcoin's shadow.

[14] On Altcoins: http://altcoins.com/
[15] Field Programmable Gate Array
[16] For more details on mining see Chapter 2, paragraph 2.1.2

1.5 Advantages and Disadvantages

Despite the differences among the various types and uses of virtual currencies, ranging from massively multiplayer online role-playing game (MMORPG), social networks, virtual worlds, to Bitcoin, whose use has more connections to the real economy, Hernandez-Verme et al. (2013) have identified some general advantages and disadvantages typical of an "ideal" virtual currency. The main positives illustrated include characteristics which distinguish them from and make them preferable to traditional currencies, such as the greater privacy and anonymity, the possibility to "buy goods online without the need of using a credit card or disclosing private information", the increased speed of the transaction (Hernandez-Verme et al., 2013). Moreover, good reputation of the issuer, safety, divisibility and ubiquity are considered as requisites for an ideal virtual currency in order to spread out and be accepted. At the same time, Hernandez-Verme et al. (2013) highlight the eventual drawbacks which might be embedded and might arise from the use of virtual currencies, even if some of them are not exclusively related to them but are intrinsic problems of traditional ones as well, and in particular often typical of cash. Among them, it is worth mentioning, and will be more deeply analyzed later on, their link to the financing of illegal activities such as money laundering or drug dealings; the volatility in the valuation which, in some cases, fluctuates independently form any other currency; the vulnerability to system failures and to inflation crises. In addition, a characteristic which might be considered both from a positive and negative point of view is the decentralized frame which particularly distinguishes them from traditional currency issued by a centralized authority, specifically the central bank.

Further aspects of digital currencies are identified by N. A. Plassaras (2013), who largely argues in favor of their superiority compared to paper-based fiat ones. First of all, he

recognizes the substantial saving in transaction cost that would derive from using only digital currencies, which includes not only "production, transportation, and handling of physical currency" costs but also a cost-savings in terms of time, efficiency, and coordination. On the other hand , an obstacle to their ease of use lies in the necessity of a constant internet connection every time a payment has to be made, which nowadays is not a big deal with the widespread use of smartphones. Then, he praises, probably in a too idealistic and emphatic way, the supremacy of digital over traditional currencies on the three primary functions of money: medium of exchange, unit of account and standard of value, and store of value. As far as the medium of exchange function, Plassaras contends that digital currencies almost completely eliminating transaction costs, also considering currency exchange fees, can be considered a "universal" currency lying above those of the single countries. Virtual currencies also act as a unit of account as, in his opinion, bitcoin for instance may be viewed, as in the case of gold, as a scarce resource, which is considered intrinsically valuable due to the effort users have to put in generating new units. The store of value feature, then, depends mainly on the amount of reliability and stability perceived by user, which is most clearly observable when a currency is backed by a government. In this regards, the ECB (October 2012) clarifies its point of view as follows:

> *"In essence, virtual currencies act as a medium of exchange and as a unit of account within a particular virtual community. The question arises as to whether they also fulfil the store of value function in terms of being reliable and safe, or whether they pose a risk not only for their users but also the wider economy"*[17].

[17] ECB, October 2012, p.11

In fact, as also Plassaras (2013) recognizes, the shadow of uncertainty surrounding virtual currencies and the lack of regulation, which exposes them even more critically to risks such as credit risk, liquidity risk, and operational risk, are still remarkable obstacles to a full and widespread acceptance. Moreover, a feature, which is determinant to the success of virtual currencies lies in network externalities, perfectly described by Metcalfe's Law, which states that "aggregate network value is proportional to the square of network size"(Swan, 2002). For a network to actually work, it needs to be adopted by both sides of users, for instance merchants and customers, and the more one side uses it the more the other side wants to benefit from it. Therefore, at this stage virtual currencies, despite they are known and used by many people, haven't built yet a considerable network from which everyone can benefit, as the amount of transactions in virtual currencies represents only a small portion of the total amount of transactions that take place around the world.

1.6 Virtual Currencies' Potential

Virtual currencies do not involve only risks and a dark side, but represent a great potential for businesses where to invest and to take advantage of. It is a growing market and companies are increasingly understanding the importance of starting to be familiar with it. For instance, in 2011 American Express has acquired *Sometrics*, a company dealing with the establishment of virtual currency commerce in video games, investing $30 million for it (Button, 2011). This acquisition may be useful to integrate virtual currencies within traditional payment options, and make them more accepted by merchants as they are in this case backed by a colossal company widely trusted. American Express has already

demonstrated its openness to innovations and has proved to make interesting deal in this field with for instance Facebook and even Zynga[18]. In many cases, virtual currency is a profitable business as people often use real money to purchase virtual one, and this might be a profitable opportunity for companies; for instance, videogame players purchase their online tokens using real money or though subscription fees.

In addition to the market for video-games, another ground for a potential development of virtual currencies was found by a report of the World Bank[19] (April 2012). Though some statistical observations, they found out that 50% of adults in the world do not own a bank account and that in 35% of the cases this is due to barriers such as "high costs, physical distance, and lack of proper documentation", might suggest that potentially virtual currencies are more accessible to those people as they require just an internet connection and little more. This could be an astonishing benefit and improvement in the world financial system as it would connect more and more people across the countries, allowing those who, for several different reasons, do not have access to standard financial institutions. Of course, up to now this still remains only a potential, still to be exploited and analyzed deeply in its advantages and drawbacks.

Moreover, despite the potential benefits, most of the people still look skeptically at virtual currencies, pointing out the various risks concerning the lack of regulation, which may give incentives for illegal activities, frauds, and money laundering, and reputational risks.

[18] On American Express and Virtual Currencies, http://techcrunch.com/2011/09/20/american-express-buys-virtual-currency-monetization-platform-sometrics-for-30m/

[19] Asli Demirguc-Kunt and Leora Klapper, (April 2012) http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2012/04/19/000158349_20120419083611/Rendered/PDF/WPS6025.pdf

1.7 Legal Issues

Since the latest diffusion and use of virtual currencies the main authorities from many different countries in the world have begun questioning their state of "freedom" and deregulation and various commissions have gathered to discuss this hot topic.

For instance, on November 18th, 2013, the U.S. Senate Committee on Homeland Security and Governmental Affairs have met to discuss the "Potential Risks, Threats and Promises of Virtual Currencies" and try to find a perfect balance between the costs and benefits of regulation. They argue that regulating virtual currencies need not be, as it may appears to their supporters, something negative or restrictive but it would, above all, enhance the reputation of the companies using virtual currencies in their businesses and allow them to show their "transparency and integrity within the bounds of the law"[20]. In fact, the committee though understanding and accepting the innovation brought about by those currencies and the benefits that may come along, also views them as a potential instrument to be used by illegal actors. As previously noted, also the U.S. Senate Committee highlights some of the reasons why virtual currencies are particularly vulnerable to be exploited for illegal actions such as money laundering or terrorist financing:

- they guarantee some degree of anonymity
- they are easy to use and accessible throughout the world by only means of an internet connection
- they have low fees and transaction costs
- they do not have transaction limits
- they are generally secure

[20] Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network, United States Department of the Treasury Before the United States Senate Committee on Homeland Security and Government Affairs (November 2013)

- transactions are irrevocable
- if it is a decentralized one, it has no authority controlling regularly for suspicious activity.

The committee report, then, mentions how FinCEN[21] (Financial Crimes Enforcement Network) has managed to include virtual currencies in their rules on "money transmission services" considering them as "other value that substitutes for currency" as in most of the cases they have an equivalent value in real currency through which they can be converted. FinCEN is reported to have been efficiently following the enforcement of regulations and monitoring illegal activities with a close eye on virtual currencies, as in the case of e-Gold, Liberty Reserve and Silk Road.

The Department of Justice adds to the discussion and points out that one of the major challenges in dealing with virtual currencies, and trying to fight the related illegal activities, lies in the internationality intrinsic in their main essence, which in turns limits the actions of authorities when illegal activities take place over different countries with different authorities and legal rules. This obstacles are even further stressed by the characteristic decentralization of virtual currency schemes, in that very few information is collected about users, as no document or any kind of identification is required to be filled in, as instead in the case of creating a bank account, thus persecuting illegal actors is quite a tough task. Moreover, as long as those currencies are still developing and continuously changing and evolving, it will be always a problem for authorities to keep up with them and find over and over new ways to discover the related criminal activities.

[21] Financial Crimes Enforcement Network is one of the US Treasury's primary agencies, created in 1990, which control and enforce policies to prevent and detect money laundering. (http://www.treasury.gov/about/history/Pages/fincen.aspx)

Besides US, where FinCEN has provided some guidance for virtual currency users who will be subject to legal obligations[22], the approach to regulation of virtual currencies in various countries is quite fragmented and no unique characterization exists.

According to a survey[23] (January 2014) encompassing forty countries, the pattern and the attitude towards virtual currencies and bitcoin as the main example is not uniform. The only aspect everybody agrees on is that they cannot be considered as a real currency nor they are legal tender. Furthermore, most countries, such as Australia, Canada, Germany, The Netherlands, and United Kingdom, are compact in saying that a form of tax should apply to transactions and capital gains deriving from exchanges in virtual currencies; more specifically UK applies a value added tax of 10-20% on bitcoin sales. Many countries are strongly sure of what virtual currencies are *not*, for instance Denmark, France and The Netherlands do not consider them as financial instruments, not electronic money and neither means of payment. On the other hand, Brazilian regulation makes virtual currencies fall within laws on "payment arrangements" and treat them accordingly, while Chinese authorities have identified them as a "special virtual commodity". In this regards, China is the only country which is using a strong regulation, and actually banning the use of bitcoin from banks and any payment institutions, in addition to a strict control over internet websites providing bitcoin services.

On a totally different road lies Denmark which, together with Belgium and The Netherlands, has established that, due to its limited scope and relationship to real economy, virtual currencies do not represent a big issue and, therefore, need not to be regulated. Whereas, countries slightly more skeptical are Australia, Canada and the European Union,

[22] Guidance FIN 2013-G001. Issued March 18, 2013

[23] The Law Library of Congress, Global Legal Research Center, 2014 January, "Regulation of Bitcoin in Selected Jurisdictions"

which despite not considering it currently a huge risk for real economy, think that the situation should be still monitored to avoid losing control of it.

In this context Germany assumes a position different from other countries, in that at the end of 2013, the German Federal Financial Supervisory Authority has established that, specifically, bitcoin falls into the category of units of account for their being "legally binding financial instruments", to be treated as foreign currencies instruments. Therefore, when used in exchanges they assume the function of "private means of payment"; on the other hand, everything else concerning bitcoin, such as the "mining" activity, should not be subject to bank supervising.

1.7.1 Tax Concerns

Besides all criminal activities that might be carried on using virtual currencies, another legally-related issue concerns their classification for tax purposes. In fact, many people, and businesses as well, do not recognize that income coming from gains in exchanging real money for virtual currencies and vice versa should be declared in order to have it taxed. The reason for this misinformation lies in that governments had not clarified how each virtual currency has to be classified and considered. Therefore, after some years of "confusion" , just a couple of months ago, on the 25th of March 2014 the Internal Revenue Service has come up with the notice 14-21 which eventually clarifies the treatment of virtual currencies for tax purposes. Their decision is not straightforwardly coming from previous decisions about virtual currencies as, for instance, while Judge Mazzan in the case of the SEC against Shavers stated that bitcoin has to be treated as an investment contract, thus a security, the now official IRS' notice establishes virtual currencies as non-currency property

under a federal taxation purpose. An important remark about the notice issued by the IRS is that it specifically encompasses only the so called "convertible virtual currencies", namely those with the strongest link to real money. The Internal Revenue Service lies the basis of the notice in stating that virtual currency that "has an equivalent value in real currency or that acts as a substitute for real currency", namely convertible currency, is just a digital representation of money and can be used for the same purposes, such as paying for goods and services or holding an investment.

The main topics covered by the notice are the following:

- Convertible virtual currency is to be treated as property when determining one's tax liability;
- Taxpayers must compute gross income from transactions by taking into account the fair price of the currency on the transaction day, as it can be found on a market exchange, and converting it to US dollars;
- Gains or losses in exchanges involving virtual currencies are taxed on the basis of whether an ordinary gain or a capital gain is realized (a capital gain occurs when virtual currency is a capital asset in the hands of the taxpayer);
- The activity of "mining" practiced by bitcoin users is taxed as well, and the fair value of the virtual currency should be included in the gross income;
- For other concerns, payments using virtual currencies follow the same rules accounting for payments made in property.

Moreover, the notice is retroactive, as it declares that taxpayers will be subject to penalties if they do not comply with the above rules even for transactions occurred before the notice.

This decision has raised many concerns regarding its fairness, especially for the taxation on miners' gains. In particular, William Lewis, a Californian lawyer, has expressed his disagreement, in an interview by Reuters[24], stating that this new situation is going to harm bitcoin miners. In fact, he believes that taxation should occur only when and event is realized and not when new units are produced and illustrates it with a simple example: "mining Bitcoins is like baking bread, and the baker is taxed when he sells the bread (the realization event), not when the bread is baked"[25].

Moreover, taxing transactions with payments using virtual currencies has implications that might undermine their success, as one of the main benefit typical of virtual currencies over traditional ones was the absence, or low amount, of transaction costs and fees, which now have to be paid in the form of taxes also by virtual currency users. The effects of this new regulation, which by now cannot be observed yet, might, thus, take the form of a decrease in the transaction volumes due to the increase in the costs attached to each transaction and to gains deriving from them.

1.8 Risks

Among the various criticisms on the adoption of virtual currencies, one of the greatest issues concerns the various risk that are associated with their use. First of all, with the necessary differences among the different types of virtual currency, they are subject, perhaps to a highest degree, to the same risks of traditional financial assets, namely liquidity risk, exchange rate risk, and risks associated to price volatility. As for the first, it is clear that

[24]Bitcoin and Taxes: http://www.reuters.com/article/2014/03/25/us-bitcoin-irs-idUSBREA2O1LR20140325
[25] Bitcoin and Taxes: http://www.glbperspective.com/tax-law/why-the-irs-is-wrong-on-the-taxation-of-bitcoin-mining/

the market for virtual currencies is, despite its high growth, still quite restricted in terms of both transaction volumes and users, therefore, should some of these currencies fail, or experience a sudden drop in price, it would be more difficult to exchange them back to real currency. Furthermore, as in traditional currencies, for instance those not widely used and well-known or those circulating in unstable countries, price volatility makes a currency appreciating or depreciating against other ones, say US dollars or Euro. This uncertainty, of course, represents a risk also for virtual currencies, and to an even higher degree in that they are often, like in the case of Bitcoin, not tied to any traditional currency, thus they fluctuate on their own in an unpredictable way.

As far as more specific risks are concerned, what worries central banks and governmental authorities above all is that criminals, attracted by the anonymity granted by these digital currencies, will use them for illegal purposes such as drug dealing, money laundering, trafficking of child pornography, or financial terrorism.

This fear is then awakened every time a new scandal comes up on all international newspapers reviving the discussion about the need of more regulation in the field and, more importantly, undermines the reputation of all the remaining users and businesses that adopt them with honest purposes.

1.8.1 Money Laundering

The issue of money laundering in virtual currencies has been recently treated by KPMG in a 2013 document titled "Virtually Unregulated"[26], where the problem is described and more regulation is advocated in order to face it. As intuitively one can imagine, the main cause explaining why criminal might prefer virtual over traditional currency is, as already said, its characteristic of anonymity which is further exacerbated by their international character which makes even more difficult tracing such illicit actors back and by the irrevocability of transactions. In fact, while banks have various systems to keep track of transactions and to check their integrity, this cannot occur for virtual currencies as no central authority exist to perform such task. A recent example of money launder case within the virtual currency context is that of Liberty Reserve SA, with $6 billion involved, which have been investigated by FinCEN and finally prosecuted in May 2013.

As reported by *Bloomberg*[27], after the collapse of Mt. Gox, a Japanese exchange operator, in December 2013, further measures have been taken by China's central bank to cover the possible risks of virtual currencies, including money laundering and frauds.

1.8.2 Drug Dealing

As for money laundering, virtual currencies and the so called "deep web" are the ideal environment to hide other illegal activities such as drug dealing. The reasons why

[26] On money laundering, KPMG, http://www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG-Countering-Money-Laundering.pdf

[27] On Bitcoin and money laundering, http://www.bloomberg.com/news/2014-03-13/singapore-to-regulate-bitcoin-operators-for-money-laundering.html

virtual currencies are seen as the perfect way to leave unlawful traffics unpunished are the anonymous and untraceable actions, and irreversible transactions.

However, on the contrary, last year have been witness of many cases in which such illegal activities were successfully discovered and punished by US authorities, namely FinCEN, the SEC, and the Department of Justice. For instance, the "Silk Road"[28] case has been on every newspaper with several updates from the end of 2013 till the first months of 2014, discussing Mr. Ulbricht's arrest recognized as the owner and main actor involved in a series of crimes, from narcotics trafficking to money laundering and even hiring of contract killers[29].

At the beginning of 2014, another case involving illegal drug trafficking and a Dutch young man ended up on newspapers for having been discovered and the BitInstant CEO and co-founder arrested. However, as noted in an article on *Bloomberg-Businessweek*[30] by Drake Bennet, all such cases are not new at all, neither they are exclusively operated in the context of virtual currencies, but similar illicit transfers of considerable sums of money to Mexican cartels were made by HSBC bank. This time, however, the bank was clearly "too big to fail" and a criminal indictment would have posed at risk financial stability, together with thousands of jobs, therefore nothing happened to bankers.

[28] More on this in Chapter 2
[29] On Silk Road, http://business.financialpost.com/2013/10/03/fbis-shutdown-of-illicit-drug-website-silk-road-will-reveal-bitcoins-resilience/
[30] On Bitcoin and drug dealing: http://www.businessweek.com/articles/2014-02-07/bitcoin-enables-a-fraction-of-the-drug-dealing-banks-facilitated

1.8.3 Ponzi Schemes

Virtual currencies, for their intrinsic innovative and decentralized character are particularly vulnerable to various kinds of frauds. A remarkably famous one is the so called *Ponzi Scheme*, which "is an investment scam that involves the payment of purported returns to existing investors from funds contributed by new investors" (SEC, Office of Investor Education and Advocacy). The scheme is made to "grab" new money promising high returns with low risks to new investors and use such money to favor and give private benefits to the organizers (SEC)[31]. They manage to catch potential investor under the pretext of new investment innovative technologies which are able to produce the promised high return almost without risk. For this reason virtual currencies are more attractive for fraudsters who count on the related less regulatory oversight and greater privacy and anonymity of the transactions.

The SEC, in its "investor alert", gives some tips to recognize the pattern of action of Ponzi schemes and avoid to fall in their trap. First of all, they warn people of who promise them high returns with low risk, as this is very unlikely to be true; moreover, outstanding returns regardless of market condition are implausible as well, in that investments tends to fluctuate over time. Further, investors should be skeptical of unregistered investments and unlicensed sellers as they might not be completely trustworthy or they might have something to hide, or when no minimum qualification is required to investor, as nobody gives something for nothing.

For instance, in July 2013 the well-known and most representative example of virtual currency, namely bitcoin, was involved in a Ponzi scheme fraud, where a Texas man, Shavers, and his company, the Bitcoin Savings and Trust (BTCST), promised their investors

[31] On Ponzi schemes: http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf

a weekly interest up to 7% "based on BTCST's bitcoin's market arbitrage activity, which supposedly included selling to individuals who wished to buy bitcoin "off the radar" in quick fashion or large quantities" as The Wall Street Journal's Market Watch reports[32]. Shavers managed to raise about 700,000 Bitcoin between 2011 and 2012 for an amount of $4.5 million which corresponds to $60 million at July 2013 price. Such amount was used to pay the fraudsters' personal expenses rather than pay back the newest investors. However, besides the uproar caused by the fraud involving bitcoin, what is important to notice concerning this case is the legal implication brought about by the judge's decision. Virtual currencies, and thus more notably bitcoin, were born with an intrinsic nature of being unregulated as a pivotal characteristic, also used to draw a line of division between them and traditional money; however, after their success and increasingly permeation legal authorities have begun to question such deregulation and tried to constraint them within existing laws read in the new light of the virtual context. Here it comes Judge Mazzan's decision to treat bitcoin as an investment contract, thus as a security, claiming that "since acquiring bitcoin involved an investment of money, it should be treated as a currency or a form of money and thus be subject to regulations" as Kirby Garlitos writes in his article (Bitcoin Ponzi Scheme Judge Rules Virtual Currency Regulated by SEC, August 2013)[33]. The importance of the judge's decision is not only restricted to the specific case of Shaver's fraud, but will likely have implication on the next cases involving bitcoin and virtual currencies more in general.

[32] Kollmeyer, B., 2013, July 24, Bitconned: SEC sounds the alarm over virtual currency fraud, The Wall Street Journal, Market Watch

[33] CalvinAyre.com, Gambling News

2. CHAPTER 2
CASE STUDY: BITCOIN

2.1 Bitcoin: How it Works

The basics of Bitcoin and its functioning are described in a clear but essential way in a white paper written by Bitcoin's developer and designer, hidden behind the pseudonym Satoshi Nakamoto, and published in October 2008. Nakamoto[34] focuses on the pivotal aspects of Bitcoin's innovation and on the key technical notions regarding transactions and their verification. First of all, he points out simply what Bitcoin is meant to be, namely a *"purely peer-to-peer version of electronic cash"* that *"allows online payments to be sent directly from one party to another without going through a financial institution"* (Nakamoto, 2008). In fact, one of the main principle around Bitcoin is the lack of a central authority issuing a monetary base and acting as an intermediary, a *"trusted third party"*, which leads to a decrease in transaction costs and an increase in the speed of the transaction. In Bitcoin payment system the integrity of each transaction, instead of being checked by a central bank or by a company is validated by users themselves through the so called "Proof-of-Work". In this regards, Nakamoto also scrupulously conceives a system to avoid the eventual problems that he anticipates might arise from a crypto-currency like Bitcoin. For this purpose, a timestamp server is needed to avoid the double-spending problem, namely to ascertain that the data, thus a particular Bitcoin unit, had not been already spent at the time a transaction occurred. In order to accomplish this verification, each single coin is designed as a *"chain of digital signatures"*, keeping track of all old and newest transactions so as to build up a full chain of ownership. Moreover, for the integrity of the transactions to be

[34] Nakamoto, S., 2008, October, Bitcoin: A Peer-to-Peer Electronic Cash System

verified, all transactions are required to be publicly available, so that users are able to agree on a single history of the block chain. In order to achieve this goal, therefore, Bitcoin’s developer established a mechanism such that a particular category of users called “miners” solve, through appropriate powerful computer-machines, more and more difficult computations to *“find a value that when hashed, the hash begins with a number of zero bits”* (Nakamoto, 2008). The Proof-of-Work procedure has also another important characteristic, namely a majority representation of users, that have to “approve” the work by attaching a new transaction to the longest fork of the block chain, representing the greatest effort.

In addition, Nakamoto points out in his paper that such system has intrinsic security advantages, in that the reward from mining and eventual fees give incentives to users to be honest, as it is very unlikely that an “attacker” is able to be faster and “assemble more CPU-power than all the other honest nodes”. Therefore, given also the fact that difficulty increases exponentially, a user will always prefer to be honest and try to gain the reward from mining.

The first thing that one needs to do to start using Bitcoin, is to open a Bitcoin "wallet": just like cash, coins need to be stored in a virtual wallet as no bank account exists that keeps them for you; for this reason it is good use to keep your wallet safe and protect it against theft. The parallelism with a "normal" wallet storing cash still holds when thinking about losing it or having it stolen: all money is lost and there is no way to claim it back. Thus, the first step is to create a wallet on some trusted sites, for instance bitcon.org, and secure it through safe complex passwords and by making backups regularly. A wallet is an easy to use software where it is possible to store Bitcoin or make transactions, send and receive coins. Transacting in Bitcoin is meant to be simple and fast, and accessible to everybody. Each user owns both a public and a private key, which need to be remembered

otherwise they are lost, and cannot be recovered. In addition, each user has an address, an ID where to send and receive payments. However, people usually prefer to create a new address for every transaction, with the aim of being more protected in terms of privacy and anonymity. On the contrary of what most people think, and what many newspapers write every time a new scandal comes out, every single transaction is not anonymous, but publicly available on the internet in order to allow miners to verify their validity.

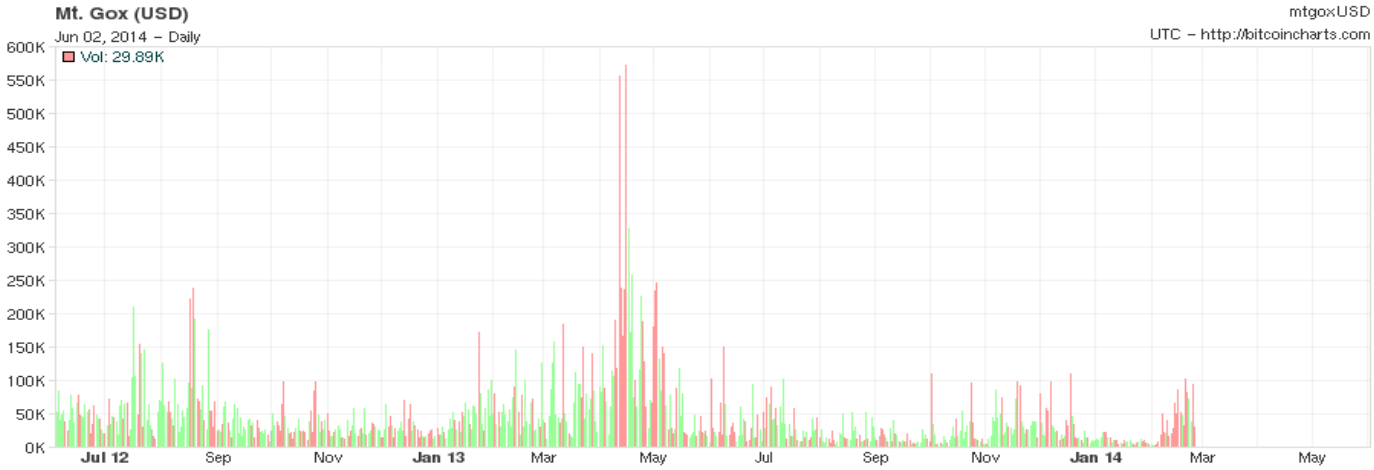
Afterwards, once a bitcoin wallet is created, two ways to get Bitcoin (and to make money with them) exist: acquire them on some exchange platform and trade them, or become a Bitcoin "miner", namely invest in powerful rigs that makes complex computation in order to validate transaction, gaining a reward which is currently 25BTC.

2.1.1 Bitcoin Trade Exchanges

Bitcoin started trading in a more remarkable way since the spring of 2010, with a surprising pace, though always subject to the impact of related events, on online exchange platforms such as Mt. Gox, Bitstamp, BTC China, BitfinexUSD, BtceUSD, BtcnCNY, and many others which proliferated with the increasing success of Bitcoin.

Until the first half of 2013, the biggest exchange platform, by volume, trading Bitcoin was the Japanese company Mt. Gox ("Mount Gox"), founded in 2010 as the first Bitcoin exchange, with a peak of over 550,000 BTC on 16th April 2013 (see Figure 1). However, as it can also be inferred by the chart, Mt. Gox got into troubles at the beginning of 2014 till its shutdown in March, when the company filed for bankruptcy protection in the US.

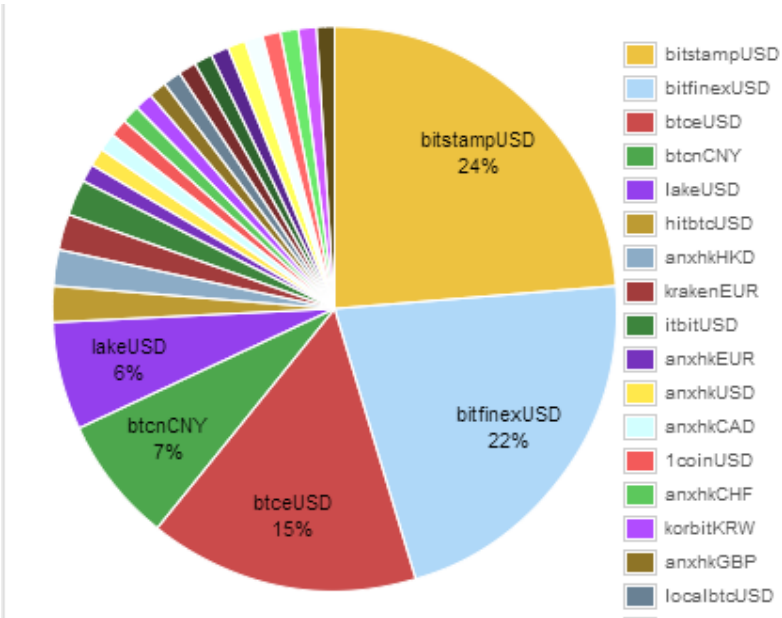
Figure 2.1. Mt. Gox Trading Volume (daily)



Source: Bitcoin Charts[35]

At the moment, according to data of the last 30 days, the four largest Bitcoin exchange markets are Bitstamp, BitfinexUSD, BtceUSD, BtcnCNY with a market share of, respectively, 24%, 22%, 15 %, 7%, making up about 68% of total Bitcoin trading volume as it can be seen from the pie below (Figure 2).

Figure 2.2. Bitcoin exchange market share, by volume

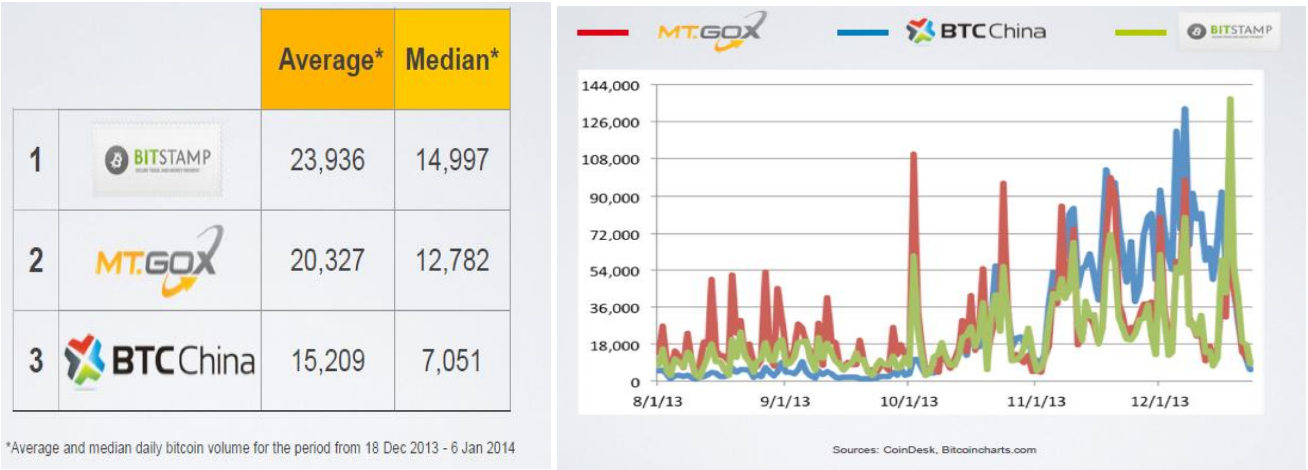


Source: Bitcoin Charts[36]

[35] http://bitcoincharts.com/charts/mtgoxUSD#rg730zm1g10zm2g25zv

Bitstamp is currently the largest Bitcoin exchange, founded in 2011 as a "European alternative" to Mt. Gox, but gaining more success by the end of 2013 and "dethroning" the previous leading exchanges Mt. Gox and BTC China (Coin Desk, 2014).

Figure 2.3 & 2.4. Bitcoin leading exchange markets at the end of 2013



		Average*	Median*
1	BITSTAMP	23,936	14,997
2	MT.GOX	20,327	12,782
3	BTC China	15,209	7,051

*Average and median daily bitcoin volume for the period from 18 Dec 2013 - 6 Jan 2014

Source: Coin Desk 26 February 2014 – State of Bitcoin 2014

Bitstamp presents itself to clients as a trustworthy company, which decided to self regulate employing some basic policy in order to ascertain the identity of customers and attempt to make therefore a selfselection of the most honest ones. Currently, Bitstamp's situation is perfectly summed up by the chart below (Figure 5), which shows a market capitalization of about $8 billion and a total of almost 13 million BCT traded. Moreover, a leading exchange market, as Bitstamp is doing, also performs the role of developing Bitcoin as an investment instrument, as it can be shown by its appreciation against the USD, reaching a peak on the 4th of December 2013 with 1,132.01 USD/BTC and is revealed by a current daily volume of over 23 thousand BTC for a price of almost $631.

[36] http://bitcoincharts.com/charts/volumepie/

Figure 2.5. Bitstamp market data

Source: www.bitstamp.net

The next current largest exchange is Bitfinex, which has features similar to Bitstamp, except that it allows margin trading, meaning that you can "borrow funds from peer liquidity providers to trade bitcoin"[37]. Bitfinex current daily volume is more than 27 thousands BTC and shows on its webpage an "sentiment index", which tells that the market for BTC-USD currently feels "very bullish", meaning that investors believe in a price appreciation, thus they have a positive attitude towards the investment. The Bitcoin Sentiment Index (BSI) is based on actual user transactions and not on voting on a poll[38]; moreover, it is considered by some people not much as a prediction tool but simply as the ratio of long on short positions of users.

The third market exchange, with 15% of all Bitcoin trading volume, is BTC-E, which, compared to Bitstamp policy and that adopted by Mt. Gox before its shutdown, preferred to make anonymity its main feature. In addition, similarly to Bitfinex, which trades also Litecoin, BTC-E does not trade only bitcoin but other crypto-currencies as well.

[37] On Bitfinex: https://www.bitfinex.com/pages/howitworks
[38] On Bitcoin Sentiment Index: https://bitcointalk.org/index.php?topic=129326.0 and http://www.reddit.com/r/BitcoinMarkets/comments/281kiw/is_the_bitfinex_sentiment_index_a_good_indicator/

2.1.2 Bitcoin Mining

Mining is an activity performed by some Bitcoin users, who carry out a fundamental role in the whole Bitcoin system, namely what keeps it trustworthy by other users. Mining activity, however, is not an easy task and it requires powerful computers and the employment of a great deal of electricity power. As previously mentioned, each Bitcoin is designed so that it contains all its transaction history, forming the so called "block chain". Therefore, miners' goal is to be the fastest to add a new block to the chain and confirming, in this way, the last transaction occurred. Such an hard work was designed by Nakamoto to be rewarded with newly minted coins every time a miner manages to add a new block to the chain, providing at the same time an incentive for users to be honest miners and a solution to the creation of monetary base without the need of a central authority issuing new coins arbitrarily. As far as incentives and money supply are concerned, the reward from mining initially accounted for 50 BTC but was set to half every 210,000 blocks, thus about every four years, and now it equals 25 BTC (Taylor, 2013). The halving of the reward is useful to control money supply, which is going to reach a limit maximum at 21 million BTC, calculated to happen around 2040[39]. In addition to the "block reward", miners can get also the transaction fees related to the transaction they are verifying. However, such fees are at the moment quite low as they are not compulsory but considered as tips, accounting for about a quarter of a bitcoin per block (Taylor, 2013). Nevertheless, it can be predicted that, as with time the "block reward" will lower halving every four years, transaction fees will increase as transaction volume is going to increase, and they will make up the greatest part of a miner's incentive. Moreover, profitability depends on exchange rate USD/BTC

[39] Taken from: http://historyofbitcoin.org/

fluctuations as well, which is a factor that cannot be forgotten as it determines the main part of the monetary incentive.

Furthermore, all such a system, in order to work, needs to stay stable against dishonest nodes' attacks. According to J. A. Kroll et al. (2013), it is important to verify whether the Bitcoin protocol represents a stable equilibrium where users pursue the "right" incentives. They argue that, to avoid failure of the system, Bitcoin needs three forms of *"consensus"*: firstly, *"on the rules to determine the validity of the transaction"*, thus that everybody agree on the criteria to verify transactions, namely mining, secondly on the state of the transaction, meaning that there must be a common view of the block chain, and, last but not least, that Bitcoin's value in user's eyes does not fall remarkably (J. A. Kroll et al., 2013). These three conditions are interconnected and influence each other so that an equilibrium is stable only if all of them hold, thus they conclude that *"if the Bitcoin price falls substantially, so too does the incentive to mine"* which could bring about a *"death spiral"* leading to a further decrease in price and a consequent failure of the system because of a sudden loss of the three "consensus" (J. A. Kroll et al., 2013). This study, examines Bitcoin's security and describes the eventual consequences of an attack to the mining system. According to Nakamoto (2008), the mining system should provide incentives to behave honestly rather than put some effort in trying to attacking the system, however, a malign player might have different driving forces which are external to the Bitcoin ecosystem, such as agents wishing to weaken the system, being it a governmental institution or an opponent's community. In this regards, J. A. Kroll et al. (2013) argued that, should a cartel of miners set up, holding more than 50% of Bitcoin's network, and change the rules of the game, obliging everyone else to follow those rules, these would not necessarily be followed. On the contrary, if other player don't want to accept the new system they would

just move out and make all the network go down, nullifying in this way the cartel's effort to control the system.

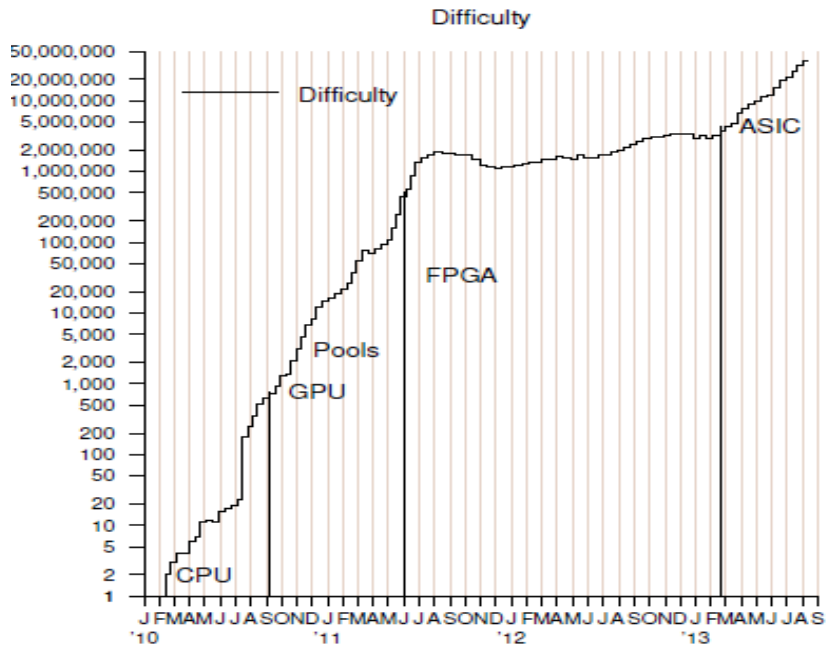
Moreover, other kinds of attack might occur with the aim of undermining the system. Although, the decentralization of Bitcoin network plays a role in evading attacks to a central authority, as should a single user's account be hacked this would not have a big impact on the whole community, the development of mining pools or exchange platforms has started to represent a vulnerable heel (R. Grinberg, 2012). This vulnerability was proven several times to be true, when, for instance, Mt. Gox, at the time the greatest Bitcoin exchange, was hacked on 15th June 2011[40]. In that situation, an hacker managed to steal Mt. Gox's database with all users' passwords and codes and using those keys he transferred a huge amount of coins to his account. 500,000 were the Bitcoin either sold or stolen from 478 different accounts, with the result of a sharp decrease in price from $17.50/BTC to just as little as $0.01 per Bitcoin. The total worth of the loss was estimated to be around $8.75 million at the market value before the hack. This massive breach is just one of the most famous attempt to put the system down, which was afterwards restored with Mt. Gox subsequent increase in its security protection, and which has shown that, despite the encryption system is able to protect the broader scope of the network and the incentive-based idea of mining, it is far harder to find a way that totally avoid the risk of theft of passwords and private keys, both from a single user or from a trading market exchange.

In addition to the economic-based point of view of the mining activity, where a reward-incentive model was analyzed and tested against several possibilities of failure, there is also a more technical perspective which will be now briefly explained.

[40] On Mt. Gox hack: http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm

Miner's job is to validate transactions by adding each new one to the block chain and this process occurs at a fixed rate which is currently around every ten minutes, guaranteeing therefore the constant creation of new coins. Explaining how all this process is performed would require a deeper informatics knowledge, nevertheless, we ca say that in order to keep the process at a constant rate, miners *"must find a nonce value that makes a double SHA-256 hash of the block's header be less than (65535<< 208)/difficulty"* (Taylor, 2013). As difficulties increases every 2016 blocks, according to the "network hashrate", this means that the "nonce value" is every time more difficult to find and it will require more and more complex computations. Mining difficulty is affected by two main factors: the rising exchange rate between USD (or any real currency) and BTC and the continuous innovations in technologies to mine Bitcoin. Given these two factors, growing mining capacity makes difficulty adjust upward as we can observe from the graph below (Figure 6).

Figure 2.6. Mining Difficulty



Source: Taylor, 2013, "Bitcoin and The Age of Bespoke Silicon"

From the above graph, it can not only be seen how steeply mining difficulty has increased over time, especially until mid-2011, but also which are the main phases of innovation characterizing such process. In the beginning, in fact, computations were very easy as the block chain was made of just a few transactions, thus, a "normal" computer was able to perform them. However, as difficulty increased, more powerful computers were needed, thus the so called "second generation mining" is characterized by the shift from computer power based on CPU to that based on GPU[41]. GPU's capabilities are well-known among 3D gamers, as it is a fundamental characteristics for the definition of the image, which requires harder and, most importantly, faster computations to be displayed clearly[42]. Therefore, when mining difficulty increased and computations began to be more complex, a more powerful computer was required in order to keep pace in the "mining competition", where only the faster miner gets the reward. However, soon GPU became inadequate and a user alone was not able to gather enough power to succeed in mining, hence users began to create "mining pools" where several individual contributed some share of power into a "pool" and then the rewards from mining were to be divided among all the users in a proportional way. After some months, GPU's limitations were solved by a new technological improvement, namely FPGA[43] (Field-Programmable Gate Arrays), an open source implementation, which came out in June 2011, characterizing the "third generation mining". This new technology performed quite well for over a year, despite its inefficiency as far as its cost per Gh/s was regarded, and was then substituted by a new product line developed by Butterfly Labs at the end of 2012. Such ASIC generation, currently the last one, is predicted to last more than the preceding one, also due to the time needed to amortize

[41] Where CPU stays for Central Processing Unit and GPU for Graphics Processing Unit
[42] On computer power: http://blogs.nvidia.com/blog/2009/12/16/whats-the-difference-between-a-cpu-and-a-gpu/
[43] FPGA is "an integrated circuit designed to be configured by a customer or designer aftermanufacturing" (Wikipedia).

the investment in the ASICMINER "rig", to be added to the enormous amount of energy costs coming from its constant use.

2.2 Timeline of Bitcoin-Related Main Events

- **August 18, 2008.** Bitcoin.org is registered
- **October 2008.** Nakamoto publishes a white paper describing bitcoin currency and his solution to double spending problem


Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Figure 2.7. Nakamoto's white paper

- **January 3, 2009.** The first block (Block 0), called the "Genesis Block" is mined.
- **January 12, 2009.** The first Bitcoin transaction between Satoshi and a developer and cryptographic activist.
- **October 5, 2009.** First exchange rate established between USD and Bitcoin. 1USD = 1,309.03BTC
- **May 22, 2010.** The first real word transaction paid in bitcoin: the so called "most expensive pizza". Lazslo Hanyecz pays 10,000 BTC for a pizza, worth $25 with the exchange rate at that time.
- **July 17, 2010.** Mt. Gox currency exchange market is established.
- **July 18, 2010.** ArtForz establishes an OpenGL GPU hash farm and generates his first Bitcoin block.
- **September 18, 2010.** First mining pool (Slush's Pool) mines his first block.
- **October 7, 2010.** Bitcoin's exchange rate starts to increase from a stationary USD0.06/BTC
- **November 6, 2010.** Market capitalization is above $1 million (USD 0.50/BTC).
- **December 9, 2010.** Mining difficulty increases over 10,000

- **2011.** The illegal market Silk Road accepting payments in Bitcoin opens his business.
- **January 28, 2011.** Generation of block 10,500 for a total of 5.25 million Bitcoin in circulation (25% of the predicted total limit of 21 million).
- **February 9, 2011.** Parity with USD: $1/BTC at Mt. Gox.
- **April 30, 2011.** Mining difficulty rises above 100,000
- **June 8, 2011.** Bitcoin exchange rate on Mt. Gox is at USD 31.91/BTC
- **June 12, 2011.** The largest Bitcoin bubble: in four days price drops to USD10/BTC.
- **June 13, 2011.** First largest theft: 25,000 BTC stolen by a user's wallet.
- **June 14, 2011.** WikiLeaks starts accepting Bitcoin
- **June 19, 2011.** Mt. Gox database with user names, addresses and passwords gets hacked. The site shuts down for seven days. Price falls to USD 0.01/BTC.
- **September 6, 2011.** First physical Bitcoins are minted by Mike Caldwell.

Figure 2.8. First physical Bitcoin
Source: http://historyofbitcoin.org/

- **March 2012.** Website hosting company Linode is hacked and 46,000 BTC are stolen.
- **May 9, 2012.** FBI shows interest in Bitcoin and published a report on illegal drug and weapons traffics facilitated by this payment system.
- **May 11, 2012.** Bitcoinica exchange is subject to an hack resulting in a loss of 18,000 Bitcoin
- **September 3, 2012.** Bitfloor is hacked for a loss of 24,000 Bitcoin.

- **September 24, 2012.** Security and Exchange Commission starts investigation on Bitcoin Savings and Trust for running Ponzi Scheme.
- **September 27, 2012.** Bitcoin Foundation is formed.
- **November 28, 2012.** Mining reward is halved for the first time at block 210,000 from 50 to 25 BTC.
- **February 22, 2013.** Bitcoin price goes back to USD 30/BTC for the first time since 2011.
- **March 8, 2013.** BitInstant, a brokerage firm, is hacked and suffers a loss of $12,000 in Bitcoin.
- **March 18, 2013.** FinCEN[44] defines its position on virtual currencies.
- **March 28, 2013.** Market capitalization reaches $1 billion
- **April 2013.** The value of Bitcoin is over USD 100/BTC.
- **April 10, 2013.** Bitcoin bubble: price grows at USD 266/BTC.

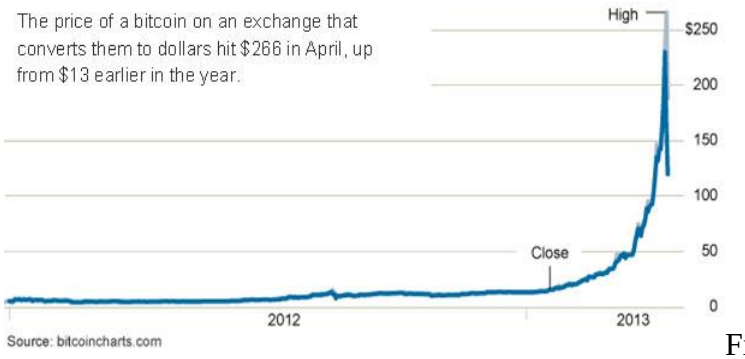


Figure 2.9. Bitcoin bubble

Source: http://historyofbitcoin.org/

- **April 20, 2013.** Bitcoin Central is hacked and price fall down to around $80.
- **May 2013.** Online gaming company ESEA is caught for using customers' computer power to mine Bitcoin.
- **May 2, 2013.** First Bitcoin ATM, in San Diego.

[44] Financial Crimes Enforcement Networkof the United States Department of Treasury

- **May 14, 2013.** The United States Department of Homeland Security seizes funds from Mt. Gox subsidiary because it "failed to register as *money transmitting business* in accordance with 18 US Code 1960".
- **August 6, 2013.** Judge Mazzant (Texas court) rules that "Bitcoin is a currency or a form of money, and investors wishing to invest in Bitcoin Savings & Trust provided and investment of money" regarding a misappropriation of funds by BTCST's founder, Trendon Shavers.
- **August 20, 2013.** Bitcoin is ruled as a form of private money by the German Federal Minister of Finance and it is exempted from taxed only if held for more than one year.
- **October 2, 2013.** Silk Road online marketplace is shut down by FBI for illegal activities.
- **November 17, 2013.** Bitcoin price doubles and reaches USD 503.10/BTC.
- **November 19, 2013.** Bitcoin price peaks above $1,000 ($1,242/BTC) after the US Senate discusses about virtual currencies after Silk Road shut down.
- **December 5, 2013.** China Central Bank bans transactions in Bitcoin for financial institutions. Price drops by more than 20%.
- **January 26, 2014.** BitInstant CEO is arrested for money laundering connected to Silk Road.
- **January 31, 2014.** BTC China, the biggest Chinese Bitcoin exchange market reopens despite Bank of China's ban.
- **February 7, 2014.** Apple bans Bitcoin and removes the wallet app from its Apple store.
- **February 28, 2014.** Mt. Gox, once the largest Bitcoin exchange market, files for bankruptcy in Japan due to a hack which caused a loss of almost half a billion dollars.

- **March 25, 2014.** The Danish commission for taxed established that virtual currencies are not "real" money so they will not be subject to taxation.
- **June 13, 2014.** US government announces it will auction 29,656.5 Bitcoin among those seized from Silk Road, accounting for a value of around $18 million.

The above timeline of Bitcoin-related main facts[45] is meant to highlight some important characteristics regarding Bitcoin. First of all, it shows its vulnerability, especially considering large exchange markets where a great amount of data is stored and attracts hackers. All the largest trading platforms or companies dealing Bitcoin seem to have suffered from theft or hacks at least once, representing a big challenge for all such entities despite the many different security measures undertaken. Moreover, it is easy to see how such hacks immediately affect Bitcoin price showing its great volatility and sensibility to each kind of Bitcoin-related even. Huge drops in price verified each time a big theft or loss have occurred, demonstrating how much Bitcoin more than any other currency, virtual or not, it is linked to people's trust in it. Nevertheless, what is noticeable is that Bitcoin users do not take long to recover their trust as the "before-the-theft" price is usually restored in a few days, and sometimes even hours. This might mean that people keep on believing in the value of such virtual currency, although they know that they could lose their money at any time. Bitcoin's history also shows us the recent growing interest of governmental authorities in virtual currencies and their attempts to enforce laws to regulate Bitcoin and avoid its use by illicit players for their drugs traffics and to launder money, attracted by the shadow of anonymity surrounding the identity of Bitcoin users. In fact, at the beginning Bitcoin was considered a phenomenon only related to "techies" and people interested in cryptography but after a while authorities realized the growing popularity of such virtual currency and started seeing it as a threat and an instrument for criminals. Therefore, since 2012 US

[45] Bitcoin timeline mostly taken from the site http://historyofbitcoin.org/

authorities in particular, began to keep an eye on Bitcoin and its relationship with illegal activities. In this regards, it is important to notice that, despite the broadly-known anonymity which attracts people with something to hide, in many cases the FinCEN, together with other US governmental authorities, has managed to find out several cases of money laundering and drugs dealing traffics such as the illegal marketplace Silk Road and Shavers’ Bitcoin Savings & Trust and shut those activities down.

2.3 Bitcoin Success Compared to Other Crypto-currencies

Bitcoin belongs to the family of Crypto-currencies, "a type of digital currency that is based on cryptography [...]: public, private keys, signing, SSL, DES, etc." (The Bitcoin Pioneer Book). Crypto-currencies can be considered as fiat currencies, in that their value is not intrinsic, but it depends on the value people assign to them, thus the value that comes from adjustments of demand and supply. An interesting characteristic of crypto-currencies is decentralization, being an attempt of creating the "currency of the people", not restricted by regulation and free from central authority's control. However, decentralization has its negatives when we consider it from the point of view of legal authorities working to enforce rules which aim at protecting citizens against dishonest users involved in illegal activities. Crypto-currencies, in fact, makes it harder to track dirty money transfers and, in the case of Bitcoin, it is impossible to reverse transactions or to freeze accounts.

Among the many different types of digital coins, crypto-currencies, and e-cash that have recently proliferated like mushrooms under so many different forms, a natural question that comes to mind is which are the characteristics that have determined Bitcoin’s great success compared to its similar. A research by Barber et al. (2012) in the attempt to answer such dilemma has found nine main characteristics that make Bitcoin outstand over all the

other digital currencies. They argue, first of all, that while all the other e-cash schemes are always based on a centralized entity, being it a company or a bank, entitled to issue and control the currency, Bitcoin's greatest innovation relies on a "distributed architecture" and on an incentive-based structure which ensure honesty among the nodes of the network. As Barber et al. (2012) point out, the spirit of Bitcoin's decentralized structure may be assimilated to the one animating the inventors of internet, which, as Bitcoin, is not subject to any governmental entity. This idea of decentralized and distributed structure, together with the "mining" process and all its details, makes monetary supply predictably increasing at a fixed rate, up to a fixed level, following a logarithmic algorithm, differing from all other virtual (and real) currencies where a central authority is in some way freer to decide on the issuance of new money.

Another advantage of Bitcoin in comparison with other forms of e-cash concerns divisibility, in that Bitcoin can be "divided and recombined to create essentially any denomination possible" (Barber et al., 2012). Moreover, Bitcoin's "open-source nature" makes it very flexible and versatile, qualities that makes it appreciated by many users. A linked characteristics to Bitcoin open- source flexibility is that the community is always active to supply new implementations, so that Bitcoin can be managed not only through a computer but also by a mobile application. Furthermore, Bitcoin system differs from other ones for its very low transaction fees, which is especially noticeable for small payments, as in other systems fees might make up the greatest part of the payment. Finally, for some users an important characteristic, which is typical of Bitcoin and no other currency is transaction irreversibility, thanks to which business in some countries are protected against frauds made through credit-cards.

2.4 Bitcoin's "Dark Side"

As already discussed in chapter 1, virtual currencies, and Bitcoin above all, have a bad reputation for a widespread belief of facilitating criminality and illegal activities. Bitcoin's decentralized nature and advocated anonymity at the same time attracts criminals and worries governmental authorities and policy makers. Criminals have seen in the use of Bitcoin for online payments the same appealing factors they see in cash payments: anonymity and impossibility of traceability. However, on the contrary of cash which indeed leaves no track, as it will be explained in the next section, with some effort Bitcoin's ownership might be tracked as all transactions are public and available to everybody. Moreover, as pointed out by Brito et al. (2013, p. 10) *"cash has historically been the vehicle of choice for drugs traffickers and money launderers, but policymakers would never seriously consider banning cash"*.

2.4.1 Silk Road

A well-known case in which Bitcoin was the only currency accepted in an illegal marketplace is Silk Road marketplace, which was hidden through the anonymizing network TOR (The Onion Router), and where illegal goods such as drugs, fire arms, fake passports and child pornographic content could be sold or bought, and even hackers and assassins could be hired. After two and a half years of illegal activities, on the 2nd October 2013, Silk Road was shut down and Ross William Ulbricht the man behind all this illicit activities and drug traffics was accused of money laundering and narcotics trafficking activities and

arrested[46]. It was estimated a total revenue since Silk Road creation of over $1.2 billion revenue with its activities.

Two days ago, several months after Silk Road shutdown, the US government announced that it will sell through an auction a fraction of Bitcoin seized from Silk Road, roughly $18 million[47], accounting for 29,656.5 Bitcoin, with 144,342 other Bitcoin still in the hands of US government. This auction represents only 0.25% of total Bitcoin in circulation, but some believe that this move has the aim of bringing down Bitcoin price, which is actually what occurred after the news, resulting in a 2% decrease in price[48].

On the other hand, Gavin Andresen, chief scientist at Bitcoin Foundation, believes that if the Department of Justice wanted to undermine Bitcoin's economy it could have just destroyed them instead of selling them, thus this might mean that they consider Bitcoin as something valuable. In addition, the choice of selling Silk Road's Bitcoin through an auction instead of on an exchange market has been widely discussed and may be considered a way to identify user buying them, which couldn't have been possible otherwise.

2.4.2 Anonymity

Anonymity in Bitcoin transactions is widely discussed when talking about criminal's incentives to use Bitcoin as a payment for their illegal traffics to avoid being traced and caught. However, without an in-depth analysis of this crypto-currency, people are often mislead on this topic. The kind of privacy praised in Bitcoin network regards the

[46] On Silk Road: http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/
[47] On Silk Road: http://www.cbc.ca/news/business/silk-road-bitcoins-worth-18m-us-to-be-auctioned-off-1.2674402
[48] On Silk Road: http://www.wired.com/2014/06/silkroad-bitcoin-auction/

information about single users, which is usually collected by banks when one wants to open a bank account and which is not required for instance when people create a Bitcoin wallet. However, all transactions ever occurred in Bitcoin network is registered on the block chain, which is in turn publicly available to everyone. Of course, on the block chain there is not written name and surname of users involved in a certain transaction, but every Bitcoin address, or public key, appears and could be linked to the computer's IP where the transaction has been made. Nevertheless, it is possible, as many people do, to create several different accounts, or one for each transaction, in order to improve anonymity and make it harder to link the different accounts to a single person. Moreover, most of illegal activities are performed in the so called "Deep Web" through the anonymizing software TOR (The Onion Router). Anyway, as proven by the Silk Road case, the illegal marketplace has been discovered and the transactions traced, therefore this shows that it is really possible, with a deep and careful analysis to overcome anonymity and discover criminals in Bitcoin network as well as authority can do it in the real world.

Moreover, an experiment by Androulaki et al. (2012), have shown through an experiment that it is possible to find out identities of 40% of Bitcoin users by means of a "behavior-based clustering technique".

2.5 Quantitative Analysis

As previously mentioned, Bitcoin price is very characteristic as for its decentralized nature it is not tied to any other currency's movements. Every change in price is, in fact, only determined by factors related to the Bitcoin environment as well as by demand and supply. For this reason, as it took some time for Bitcoin to become widespread known, after already several months from its creation, its price was less than one cent (1USD= 1,309.03 BTC[49]) and remained below parity (so one Bitcoin was worth less than one US Dollar) until February 2011. Therefore the following analysis, performed with the help of the program STATA, will be centered mainly on prices since 2011, based on an exchange rate on Bitstamp exchange market[50].

Figure 2.10. Closing prices (13th September 2011- 12th June 2014)

[49] http://historyofbitcoin.org/

[50] Data on prices taken from: http://www.quandl.com/BITCOIN/BITSTAMPUSD-Bitcoin-Markets-bitstampUSD?utm_source=quandl&utm_medium=graph

From the above graph, we can see that between March and May 2013 price has started increasing, going above US$ 200, and then shortly has fallen down below US$ 100. The cause of such bubble was attributed to a DDoS (Distributed Denial of Service) at the exchange market Mt. Gox, which led to a widespread panic among Bitcoin owners that then begun to sell their Bitcoin altogether causing the sharp decrease in price (Skinner, 15th April 2013)[51]. Anyway, just a couple of days later, price was restored above US$ 100, and remained quite stable around that price for several months, until October. During the month of November, due to the shut-down of the famous illegal marketplace, Silk Road, Bitcoin price, probably driven by people's greater trust in the soundness of the currency, sharply increased enormously to an unprecedented peak above US$ 1,000. As for April's bubble, this one was predictably going to burst as well, falling back down to around US$ 500, to increase again up to US$ 900 in January 2014, and down again till a lower peak in March, and then up and down again. The last semester was characterized in fact by a continuous increase and decrease in a wide range going from US$ 400 to around US$ 1,000.

Even though given these continuous fluctuations average prices are not so relevant to analyze Bitcoin prices, some summary statistics might be useful to consider a more precise measure of volatility, which can be well represented by prices' variance or standard deviation, and to see more precisely the range in which they have fluctuated in determined periods of time.

Table 2.1 Summary Statistics: Closing Prices (13th September 2011-12th June 2014)

Variable	Obs	Mean	Std. Dev.	Min	Max
close	986	173.7668	263.2974	2.24	1132.01

percentiles:	10%	25%	50%	75%	90%
	4.85	6.4	20.48	141.9	637.24

[51] On Bitcoin bubble: http://thefinanser.co.uk/fsclub/2013/04/the-real-cause-of-the-bitcoin-bubble.html

From the above table, the most interesting data is the range of prices, which is very wide as it includes all prices ever since September 2011, when they were still very low as the minimum is slightly more than US$ 2. On the other hand, the maximum is represented by the already mentioned peak occurred on the 4th of December 2013. In addition, as the range of prices is very wide, volatility considered over such time period is measured by a very high standard deviation (263.3).

Instead, it will be more interesting to consider the whole period divided in three separate smaller periods. For instance, the first period might be chosen from the beginning until march 2013, thus considering the first 18 months.

Table 2.2 Summary Statistics Closing Prices (13th September 2011-12th March 2013)

Variable	Obs	Mean	Std. Dev.	Min	Max
close	529	9.59034	7.38219	2.24	48.25

As we can see from the table above, this time the standard deviation is way lower and thus the mean is a more representative tool to analyze. Prices have been quite low over the period and have ranged between a minimum of US$ 2.24 up to a maximum of US$ 48.25, hence the lower fluctuations are identified with a lower standard deviation.

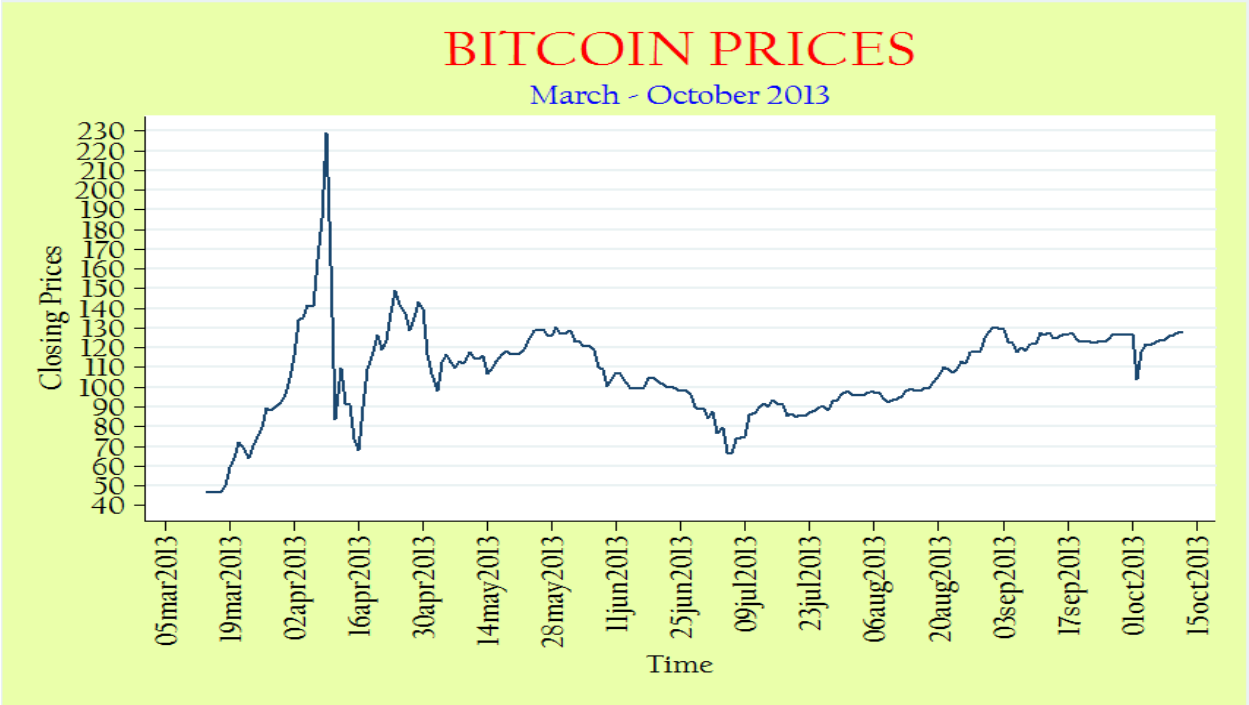
Next, we will focus on the following seven months from 13th of March to 12th October, when, as we can also see from the previously shown graph (Figure 2.10), price stabilized around US$ 100 with an initial peak above US$ 200.

Table 2.3 Summary Statistics Closing Prices (13th March 2013-12th October 2013)

Variable	Obs	Mean	Std. Dev.	Min	Max
close	213	107.7927	23.37379	46.74	229

The above table confirms the analysis of the graph as the mean is US$ 107.79, and the volatility, despite higher than the previous period, is still quite low considering the peak at US$ 229 and a wider range of prices.

Figure 2.11 Closing Prices (13th March 2013-12th October 2013)



Finally, the last period since 13th October 2013 until today, 12th June 2014, was characterized by more fluctuations in price. This, in fact, is clearly shown by the measure of volatility represented by the standard deviation, which is, for that period, 212.58. As observed from the table below (Table 2.4), closing prices ranged from US$ 132.82 to US$ 1,132.02 without stabilizing for longer periods, therefore, the mean price US$ 589.52 cannot be considered a reliable estimate for Bitcoin prices of the last 8 months. Anyway, as noted in Figure 2.12, the first months of 2014 where somehow more stable, even though not completely flat.

Table 2.4 Summary Statistics Closing Prices (13th October 2013-12th June 2014)

Variable	Obs	Mean	Std. Dev.	Min	Max
close	243	589.5225	212.5797	132.82	1132.01

Figure 2.12 Closing Prices (13th October 2013-12th June 2014)

2.6 Structural Problems

Bitcoin system, of course, is not perfect. Among the many types of problems concerning Bitcoin, there are first of all, the so called "structural problems", namely those problems which are intrinsic and derive directly from how the currency is defined. In fact, the monetary base with a fixed cap at 21 million BTC has some negatives as well: it condemn the currency to a predictable "deflationary spiral"[52]. What is considered Bitcoin's

[52] "Economic occurrence where inflation rate is negative and continuing to decrease. […] When this occurs the supply of money usually decreases, leading to a stronger currency…". (http://www.investorwords.com/7598/deflationary_spiral.html)

strength can be seen as a weakness as well. The lack of a central authority which has the power to adjust the supply of money accordingly with the state of the economy, gives Bitcoin a more rigid and predictable path. According to D. Kervick (2013) when the production of Bitcoin will stop, assuming the economy keeps on growing, two scenarios may occur: "either *(i)* prices in bitcoin remain stable as the rate of bitcoin transactions increase, or *(ii)* the rate of transactions stays roughly the same, but bitcoin prices fall as the finite quantity of bitcoin is spread over more and more transactions"[53]. This last case is what would happen in a deflationary spiral and is thought to be the most likely scenario. Two problems are considered to come along with deflation: first of all, if price keeps on increasing people see it more valuable to keep it as an investment rather than spending which would become a problem if everybody does so, secondly, "deflation makes debt more onerous" because they are usually fixed at nominal value (Kervick, 2013). In addition, if people stop spending their Bitcoin, the system might become unattractive, leading to a drop in its value and reputation (Barber, 2013).

However, many critics to this theory have been developed and some people believe that this deflationary spiral is not going to occur. Among the Bitcoin enthusiasts, one of the counter-arguments to the possibility of a deflationary spiral relies on the fact that, price is expected to fall only due to lower production costs, which would make businesses more profitable, not less[54]. Moreover, Pacia (2013) believes that "prices do not always spiral upwards only to crash down to zero" and that people will not cut all their spending to zero as they will still need to buy things. Another critic against the deflationary spiral argues that since people already know that a deflationary spiral might occur and make people hoard more money instead of spending it, as they know what a deflationary spiral would bring

[53] On Bitcoin deflation: http://neweconomicperspectives.org/2013/04/talking-bitcoin.html
[54] On Bitcoin deflation: http://chrispacia.wordpress.com/2013/10/22/bitcoin-and-the-deflationary-spiral/

about, they are likely to act in an opposite way to avoid such occurrence. In addition, the current volatility in Bitcoin price tells us that the currency is not stable yet, but it is likely to be so by the time Bitcoin production stops, therefore, without volatility and upward expectations price might not reach the predicted maximum levels[55]. Finally, some others believe in intermediate outcome as people will keep using dollars for most of consumption thus the eventual case of a deflationary spiral would affect only bitcoin economy, not the whole economy.

2.7 Currency or Investment?

At this point of the analysis a question comes natural: which is Bitcoin's most likely future scenario? Will it become so widespread and broadly accepted to be a serious alternative to real currencies? Will it stay like it is now, with its high volatility and little stability? Will it be generally considered more as an alternative virtual currency or just a risky, considering current volatility, investment as many other? Will some other virtual currency come out to be better than Bitcoin and substitute it, leaving it in the shadow of our memories? Future is of course a dark box and answering with certainty all these question marks it is nearly impossible. We cannot tell for sure what it is going to happen to this promising virtual currency, but we can only make some forecasts and predictions from a personal point of view.

Resuming briefly all the discussion about Bitcoin, this is a virtual currency, also falling in the narrower definition of crypto-currency, based on a peer-to-peer network, developed at the end of 2008 by a person or group of people under the pseudonym of Satoshi Nakamoto. This virtual currency was originally born to overcome some of the

[55] On Bitcoin deflation: http://www.panture.com/why-bitcoin-is-not-heading-towards-a-deflationary-spiral/

problems related to traditional real currencies, such as the need of financial intermediaries, slowing down transactions and requiring probably too high fees, in order to solve the problem of double spending. The primary scope was, thus, to create a competitive alternative capable of threatening and maybe revolutionizing the current system subject to the power of banks. Moreover, in the first enthusiastic spirit it was perceived as "everybody's currency" without any country or continental limit, a currency able to travel the world without any frontier, just with a click and an internet connection.

Of course, in order to become an plausible good alternative to the already well-established traditional currencies, say Dollars or Euro, it needs some further steps other than a well-designed and structured system aimed at solving the double spending problem, together with the constant creation of monetary base, without a central authority, increasing speed and security of transactions and all the other characteristics already mentioned that make it an innovative virtual currency. Those fundamental steps include making Bitcoin a stable, reliable and widely known and accepted currency. Currently Bitcoin is broadly known among many people and used by quite a substantial number of them. However, we are still rather far from stability because of the many and unpredictable fluctuations previously analyzed in the quantitative section. Indeed, as long as volatility stays so high we cannot expect people to trust it completely, both from the point of view of merchants, who would incur in great risks if they started accepting them widely and from the point of view of users who, at the moment, are more inclined to keep them as an investment, waiting for price increases to make profits, rather than spending them. Moreover, we can look at reliability both from the stability point of view, reinforcing the previous argument about stability and volatility, as if price keeps on fluctuating so much, it would be quite risky to rely on it as the only currency to use, and from the point of view of hacks. As a matter of

fact, hacks to Bitcoin accounts, especially those held on exchange markets, are not so rare, and despite each hack, theft or loss is not going to harm or undermine the system as a whole, it is for sure nothing really good from the point of view of individual users who lose quite huge amounts of money. Therefore, it is easy to understand that those characteristics are strongly linked to each other as unless Bitcoin’s volatility decreases leading to a more stable currency, we cannot expect people to accept it and trust it as traditional currencies. So, if volatility keeps the same current levels I believe Bitcoin could never be able to threaten traditional currencies and become widespread enough to fulfil the initial dream of a universal currency. In fact, as Bitcoin keeps appreciating people are more tempted to save rather than spending them, meaning that they expect to make gains from price increases and, thus, that they consider it more an investment than a currency.

Should instead Bitcoin become, with time, more stable and reliable and accepted throughout the world, or a large share of it, there might be the basis for a serious alternative to the current traditional system of real currencies, and it would be particularly popular for payments with are either very small or very large. In fact, in the first case, under the current system, transaction fees would make the largest part of the payment and in the second case, users are likely to be subject to constraint on an upper cap on the maximum amount allowed for each transaction.

3. Conclusions

At the end of these two chapter's analysis of virtual currencies and, more specifically, Bitcoin we can briefly sum up the main concepts and draw some last considerations. As we have seen, virtual currencies are going in the same direction of many other current technological innovation, trying to simplify more and more every step of our daily life, heading towards, in this field, faster and easier online means of payment. The direction might be the same as electronic money, but the path is totally different, and despite some drawbacks, virtual currencies are trying to take a quicker way, being more free, for instance, from a regulatory point of view and even cheaper when transaction fees are considered.

However, from the above analysis it is clear that the only virtual currency which might currently be able to revolutionize the payment system is the crypto-currency created in 2008 by Satohi Nakamoto, Bitcoin. Bitcoin has several advantages on traditional currencies, first of all, the low costs, in that transaction fees are considered a tip given to the miner who validate that transaction. Moreover, the decentralized structure of the network give his users many advantages, among which the lack of financial intermediaries, with a well-designed solution that solves the double spending problem, and the derived greater privacy, as nobody will ask you to give your personal details and credential to open a Bitcoin wallet or to make transactions. This method of course opens the doors to people who currently are not able to make use of the banking system, for instance due to distance problems or lack of physical infrastructures, as might be the case in African states or other poor countries, although some other limitations should be taken into account. Indeed, the majority of people actually owns a smartphone, or an internet connection, and this is the only thing needed to make payments through Bitcoin. Therefore, Bitcoin has an advantage

in terms of ease of use and accessibility to everyone, which is not necessary a bank's characteristic.

Moreover, Bitcoin is able to overcome some other limits currently belonging to the traditional system, in that it allows both small payments which would otherwise be too onerous because of the too high transaction fees, and in the opposite direction, it makes possible the transfer of high sums without any transaction constraint made by banks. Thus, the target of users is rather broad, ranging from poor countries' inhabitants where infrastructures lack, to people willing to make either micropayments or transfer huge amounts freely and cheaply.

Currently, a wide range of people, both from the consumer and from the merchant's side, have understood the benefits of Bitcoin transactions and with volumes around 20,000 BTC per day. With the increasingly known advantages of this crypto-currency, also more and more merchants are willing to accept them as a payment, being able to save huge amount of money on credit card fees, which might make, especially small shops or enterprises, run out of business. The names of companies accepting Bitcoin include not only those unknown companies looking for some popularity, or those who had problems with traditional currency, but also famous brands such as Victoria's Secret, Subway, Amazon, Expedia.com, Bloomberg.com, and many others from different industries and countries[56].

However, no system is perfect and Bitcoin has suffered a bad reputation because of several scandals of frauds, hacks, illegal drug traffics and criminality, but as already pointed out such criminal activities do not occur only within Bitcoin's ecosystem, and cash has the same features appreciated by criminals, although nobody has never thought of prohibiting it. In this regards, many advocate the need for more regulation to avoid Bitcoin's improper uses

[56] http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html

and to improve its reliability and stability, but more regulation would mean depriving it from its most important features, which are those allowing the speed of transactions and the low transaction costs. More regulation would make Bitcoin closer to the current payment system from which it wished to move away and subtract from it all its characteristic appeal. Moreover, it has been proven that even without any strict regulation, authorities have always managed to find out criminals and make justice, therefore these past scandals might act as a deterrent for other delinquents wishing to circumvent the law by making illegal traffics paying in Bitcoin.

In addition, another possible threat to Bitcoin future acceptance is the widely discussed volatility which prevents price stability and, to some extent, it reliability as a currency. Therefore, what it is hoped for a prosperous future of such innovative crypto-currency is, above all, related to price stability enhancing both people and authorities' trust.

4. Bibliography

- 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
- 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
- Barber, S., Boyen, X., Shi, E., Uzun, E., 2012, "Bitter to Better - How to Make Bitcoin a Better Currency", Palo Alto Research Center
- Bennet, D., 2014, February 13, "Bitcoin Enables Drug Dealing, Just as Major Banks Do", Bloomberg Businessweek, available at: http://www.businessweek.com/articles/2014-02-07/bitcoin-enables-a-fraction-of-the-drug-dealing-banks-facilitated
- Brito, J., Castillo, A., 2013, August 19, "Bitcoin: a Primer for Policymakers", Policy: A Journal of Public Policy and Ideas Vol. 29 No. 4, Mercatus Center
- Button, K., 2011, Virtual Currencies, Real Potential, American Banker
- Chokun, J., 2014, "Who Accepts Bitcoin as a Payment? List of Companies, Stores, Shops", available at: www.bitcoinvalues.net
- CoinDesk, 2014, February 26, "State of Bitcoin 2014"

- Dorit, R., Adì, S., YEAR, "Quantitative Analysis of the Full Transaction Graph", Department of Computer Science and Applied Mathematics, The Weizemann Institute of Science, Israel
- 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
- ECB, 2012 October, Virtual Currency Schemes
- Ernstberger, P., 2009, January 23, "Linden Dollar and Monetary Policy", University of Bayreuth, Working Paper "Forschungsstelle f¸r Bankrecht und Bankpolitik", available at http://www.bankrecht.uni-bayreuth.de/pdf/lindendollar.pdf
- Garlitos, K., 2013, August 8, Bitcoin Ponzi Scheme Judge Rules Virtual Currency Regulated by SEC, CalvinAyre.com
- Greenberg, A., 2013, October 2, "End of the Silk Road: FBI Says It's Busted the Web's Biggest Anonymous Drug Black Market", available at: www.forbes.com
- Greenberg, A., 2014, June 12, "The Feds are Auctioning a Small Fortune in Silk Road Bitcoins", available at: www.wired.com
- 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

- Harris, A., 2014, April 24, "Dutch Man to Plead Guilty to Dealing Drugs for Bitcoin", Bloomberg, available at: http://www.bloomberg.com/news/2014-04-24/dutch-man-dealt-drugs-for-bitcoins-on-internet-u-s-charges-1-.html
- 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?"
- IRS, International Tax Alert, 2014, March 28, "IRS Issues Guidance on Taxation of "convertible" Virtual Currencies such as Bitcoin", EY Global Tax Alert, available at: http://www.ey.com/GL/en/Services/Tax/International-Tax/Tax-alert-library#date
- IRS Notice 2014-21
- IRS, Tax Insights from Washington National Tax Service, 2014, March 28, "IRS Issues Long-awaited Guidance on Treatment of Virtual Currency", available at: www.pwc.com
- Keynes, J., M., 1930, "A Treatise on Money", Macmillan Publishers, London
- Kervick, D., 2013, April 24, "Bitcoin's Deflationary Weirdness", New Economic Perspectives, available at: http://neweconomicperspectives.org/2013/04/talking-bitcoin.html
- 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/
- KPMG, 2013, "Virtually Unregulated", Countering Virtual Currency Money Laundering in the 21st Century, available at:

http://www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG-Countering-Money-Laundering.pdf

- Krewell, K., 2009, December 16, "What's the Difference Between a CPU and a GPU?", NVIDIA Blog, available at: http://blogs.nvidia.com/blog/2009/12/16/whats-the-difference-between-a-cpu-and-a-gpu/
- Kroll, J., A., Davey, I., C., Felton, E., W., 2013, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", Princeton University
- Lee, A., 2014, January 19 , "A Beginners Guide to Margin Trading on Bitfinex: Why You Shouldn't be Trading on Exchanges" , available at: http://alunacrypto.blogspot.it/2014/01/beginners-guide-margin-trading-bitfinex-exchange.html
- Lewis, W., D., 2014, March 27, "Why the IRS is Wrong on the Taxation of Bitcoin Mining", The Global Law & Business Perspective, available at: http://www.glbperspective.com/tax-law/why-the-irs-is-wrong-on-the-taxation-of-bitcoin-mining/
- McKee, J, 2013 May, Redefining Virtual Currency, Yankee group
- 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
- Nakamoto, S., 2008, October, "Bitcoin: A Peer-to-Peer Electronic Cash System"
- Pacia, C., 2013, October, "Bitcoin and the Deflationary Spiral", available at: http://chrispacia.wordpress.com/2013/10/22/bitcoin-and-the-deflationary-spiral/

- Pagliery, J., 2013, October 2, "FBI Shuts Down Online Drug Market Silk Road", available at: http://money.cnn.com/2013/10/02/technology/silk-road-shut-down/
- Panture, 2014, June 9, "Why Bitcoin is not Heading Towards a Deflationary Spiral", available at: http://www.panture.com/why-bitcoin-is-not-heading-towards-a-deflationary-spiral/
- Plassaras, N. A., 2013, "Regulating Digital Currencies: Bringing Bitcoin Within the Reach of IMF", Preliminary Draft
- SEC, Ponzi Schemes Using Virtual Currencies, SEC, Office of Investor and Advocacy (https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf)
- 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
- The Bitcoin Pioneer Book, Unpublished secret book, only for Bitcoin Robot member eyes, available at: http://www.bitcoin-evolution.com/wp-content/files/bitcoin_pioneer.pdf
- The Law Library of Congress, Global Legal Research Center, 2014 January, "Regulation of Bitcoin in Selected Jurisdictions"
- U.S. Senate Committee on Homeland Security and Governmental Affairs, 2013, November, "Beyond the Silk Road: Potential Risks, Threats and Promises of Virtual Currencies", Homeland Security Digital Library

- United States District Court, Eastern District of Texas Sherman Division, 2013, June 8th , Case 4:13-CV-416, Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust
- Vallikappen, S., 2014, March 14, "Singapore to Regulate Bitcoin Operators for Laundering Risk", Bloomberg, available at: http://www.bloomberg.com/news/2014-03-13/singapore-to-regulate-bitcoin-operators-for-money-laundering.html
- Viswanatha, A., 2013, November 18, "U.S. Officials: Virtual Currencies Vulnerable to Money Laundering", Reuters, available at: http://www.reuters.com/article/2013/11/18/us-senate-virtualcurrency-idUSBRE9AH0P120131118
- Wilhite, T., "Difference Bteween E-Money and Credit Cards", available at: http://www.ehow.com/about_6676381_difference-between-e_money-credit-cards.html

5. Sitography

- Altcoins: http://altcoins.com/
- Bitcoin charts, http://bitcoincharts.com/charts/mtgoxUSD#rg730zm1g10zm2g25zv
- Bitcoin Sentiment Index, https://bitcointalk.org/index.php?topic=129326.0
- Bitcoin Sentiment Index, http://www.reddit.com/r/BitcoinMarkets/comments/281kiw/is_the_bitfinex_sentiment_index_a_good_indicator/
- Bitfinex, www.bitfinex.com
- Bitstamp, https://www.bitstamp.net/
- Financial Crimes Enforcement Network, http://www.treasury.gov/about/history/Pages/fincen.aspx
- History of Bitcoin, http://historyofbitcoin.org/
- Linden Lab, http://lindenlab.com/about
- Linden Lab, http://lindenlab.com/products/second-life
- Planet Bitcoin, Complete List of Bitcoin Exchanges, http://planetbtc.com/complete-list-of-bitcoin-exchanges/
- Second Life: http://wiki.secondlife.com/wiki/How_to_Earn_Linden_Dollars_in_Second_Life
- Sometrics acquisition by American Express, http://techcrunch.com/2011/09/20/american-express-buys-virtual-currency-monetization-platform-sometrics-for-30m/
- World of Warcraft: http://www.wowwiki.com/World_of_Warcraft
- On World of Warcraft's money: http://www.wowwiki.com/Money