AALBORG UNIVERSITY

C O P E N H A G E N

Semester: Spring 2014

Aalborg University Copenhagen

A.C. Meyers Vænge 15

2450 København SV

Title: Distributed Virtual Currencies – The Bitcoin Case

Project Period: February 2014-June 2014

Semester Theme: Design and Markets

Supervisor(s): Iwona Maria Windekilde

Project group no.: 1-2.2

Members: Md. Kamrul Islam

Vasiliki Ntarzanou

Miguel Portela
Fernandes de Almeida Pereira

Copies: 2

Pages: 90

Finished: 27/5/2014

Abstract:

The peer-to-peer virtual currencies market is one of the most exciting markets of our time, driven by an ocean of innovation which is changing its shape every day. In this ocean there is Bitcoin, which is a superlative of what a community together can do. Every day new features and services are added to Bitcoin and there are hundreds of people making sure that the Bitcoin network and its ecosystem is always updated and with improving quality.

In this project Bitcoin is being studied in detail and the authors will introduce a new tool that will be used to analyze many of the different aspects related to Bitcoin. This framework will be called BitPIN Framework and will include several theoretical frameworks that are crucial to the understanding of the ecosystem of Bitcoin, in an attempt to find out the reasons for the development and growth of virtual currencies the last few years as well as what the near future holds for them.

Table of Contents

1 Introduction

The exploding growth in the number of internet users since its creation a few decades ago, as well as the technological advancements, have led to a universal platform for online trading, gaming, social networking and information exchange. And as in all social structures created by humans, in the last few years, we have also witnessed the creation of virtual communities of people with common interests that need to interact with each other (online gaming communities, Facebook etc.) within the web. Within these communities, there was a need for exchange of goods (usually virtual) and services and thus they created digital currencies to serve this purpose, creating a new type of money, which is not regulated by governments or financial institutions.

Immediately this becomes a center of discussion about the extent to which this type of currency has or can have positive or negative effects on the economy. The European Central Bank or ECB (Anon 2012), in an attempt to clarify and define what virtual currencies are, provides the following definition: "a virtual currency is 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".

One possible classification of virtual currencies is to divide them in three types based on how they interact with currencies in the real economy(Anon 2012). The first one can be described as a closed scheme, which is typically used in online games, where players after paying a subscription for the game, earn virtual money as the game progresses and according to how well they perform. This type of virtual currency cannot be traded with real currencies and it's only used for the purposes of enabling the exchange of virtual goods in a specific virtual community.

The second type is a scheme that uses a unidirectional flow with the real economy. In this scheme the virtual currency can be bought using real money but it cannot be exchanged back to real money afterwards. It is mainly used for the purchase of virtual goods and services as for example Facebook Credits (FB), Facebook's virtual currency.

The third scheme provides a bidirectional flow. In this case, virtual money is exchanged as any other currency in the real world and can be used to buy both virtual and real goods and services, as is the case of the virtual currency Bitcoin.

The rate at which virtual currencies are exchanged is based on the demand and supply for the specific currency. There is no central control from a financial institution over these currencies and they are not regulated or undergo supervision like electronic money issuers, for example, are (ECB, 2012).
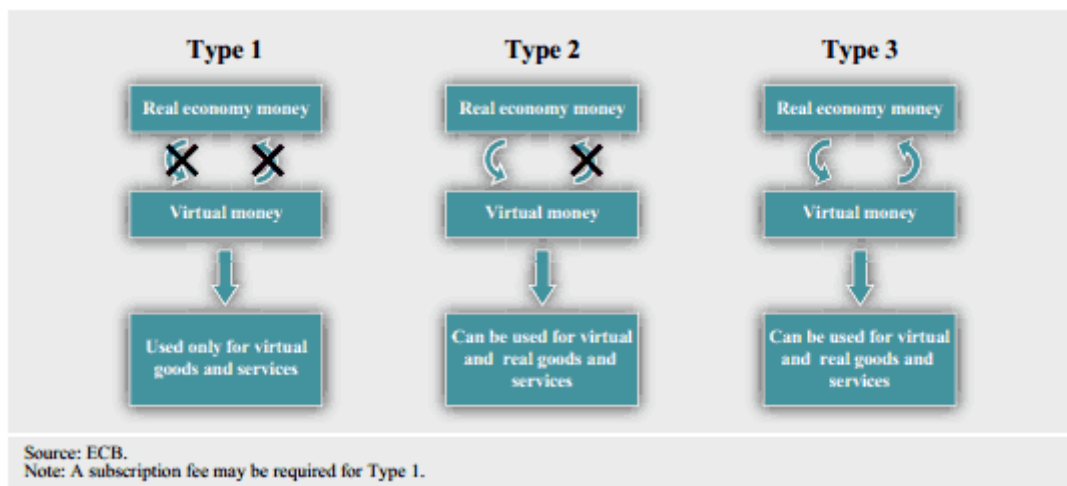
Figure 1: Types of virtual currency schemes (ECB, 2012)

All these characteristics of virtual currencies have of course raised discussion about their safety and reliability as well as the risks that their use might engage. On the other hand virtual currencies can also be seen as a promoter of innovation and an enabler of an alternative type of payment in the digital world.

Especially in the third type of virtual currencies we can even see competition between these currencies and real currencies. Bitcoin is one of the cases that this applies to, as a virtual currency that is gaining popularity and attempts to bypass the traditional financial system, where central banks regulate the money supply and currencies are regulated.

Another way to differentiate between the different types of virtual currencies is technology-wise. Here there are two categories; the type which uses a client-server model and the type that uses a distributed peer-to-peer model for the currency.

The Bitcoin case:

Bitcoin was created in 2009 by Satoshi Nakamoto(Sompolinsky, Y. et al. 2013) using a peer-to-peer scheme with no central control over the money flow by a financial institution and today it is one of the most exemplary cases of virtual currencies (ECB, 2012). It can be used for the purchase of goods and services of all types, just like any real currency, like the euro or the US dollar. The demand and the supply of Bitcoin are the only factors that influence the exchange rate. There are many online exchange platforms for it and users are responsible for performing public transactions with no intermediaries. Bitcoin users have their own digital wallet (free software) on their computer or mobile device and transactions are anonymous and performed from computer to computer. In addition, there are no or very low transaction costs charged. Transactions are registered and stored after they are first validated by the Bitcoin network and this task is performed by "miners".

Miners are computers in the Bitcoin network with significant computing power that perform complex mathematical computations and obtain Bitcoins after they solve the mathematical problems, thus creating new Bitcoins that go into circulation in the Bitcoin network. Bitcoin is designed in such a way that the complexity of the computations to be done by miners increases as more Bitcoins are mined and this happens until they reach a maximum of 21 million.

The discussions around Bitcoin include illegal activities in the Bitcoin network (for example money laundering), caused by the feature of anonymous transactions. In addition, there have been many cases where malware was used to steal digital wallets from their owners as well as many other hacking activities that compromise the integrity of the system. Such security as well as legality issues have yet to be faced by the Bitcoin community today.

1.1 Motivation

These are very exciting times in the virtual world. Internet usage is increasing every month and so do the Quality of Service and the bandwidth. This growth is general both in the developed world and in the developing countries as presented in figure 2 below [1].
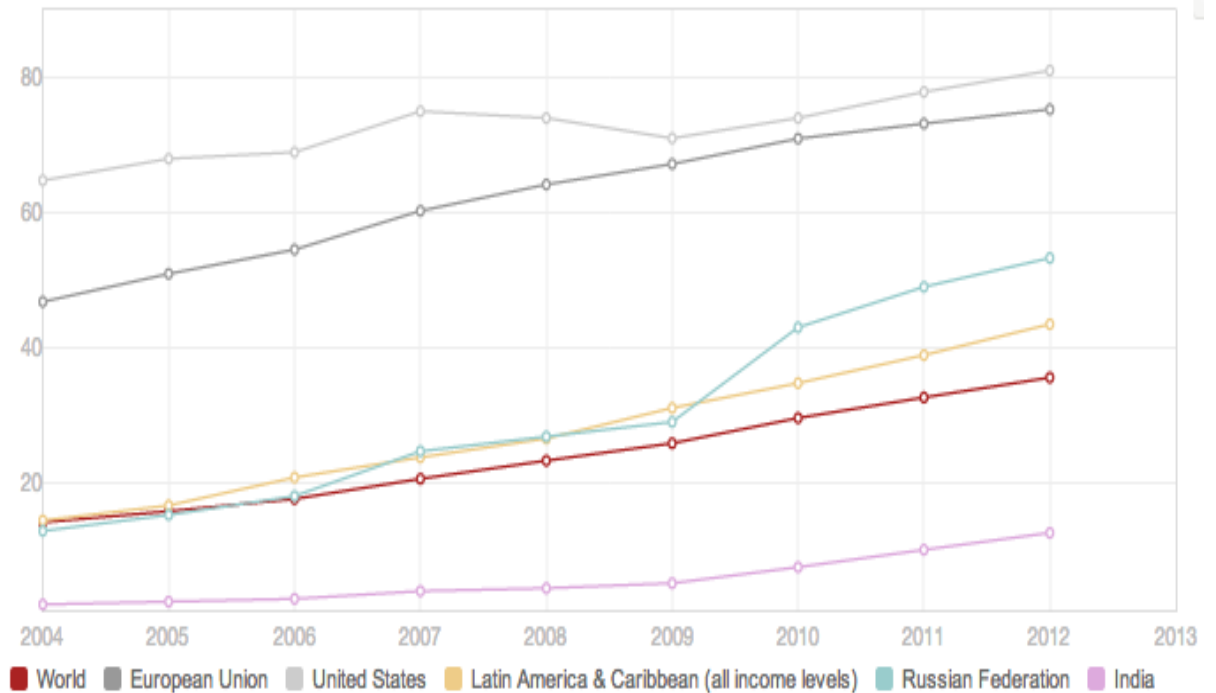
Figure 2: Internet users per 100 people. Source: data.worldbank.org [2].

All this growth has led to innovation in the way that online payments are done on the Internet. Crypto currencies are using the various open source algorithms and technologies, like peer to peer algorithms.

Bitcoin is the most prominent crypto currency nowadays and it's valuation in the last few years made it come from the shadows to the mass market. The fact that this currency respects the very basic supply and demand system makes it have very fast and wide variations in contrast with regulated currencies(figure 3 below).

The case of Bitcoin is a very interesting one, both from a technological but also from an economical point of view. The fact that a technology like Bitcoin has managed to disrupt the financial and banking systems of the whole world makes it an appealing case study. In addition, research on this case is a good combination both from an engineering point of view but also from the learning perspective in the business track of our study program.

Another reason that we chose this case study, is that some of the authors of this project have been using Bitcoin and have been extremely interested in this subject.
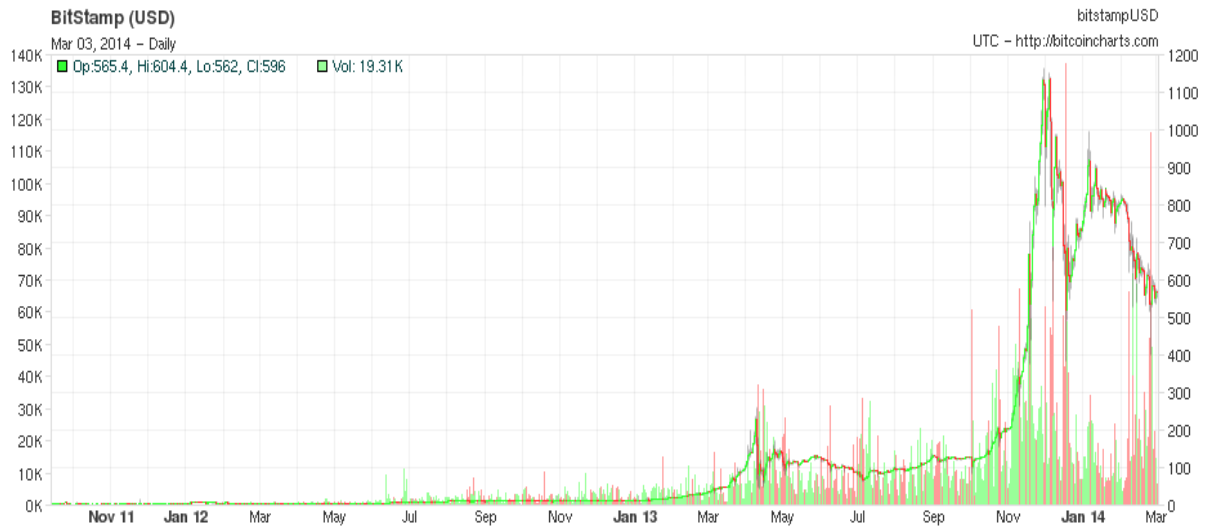
Figure 3: BitStamp in USD. Source: Bitcoincharts.com[3].

1.2 Problem Definition

- What are the main reasons for the monetized peer-to-peer virtual currencies' growing popularity?
  - What are the reasons behind Bitcoin's supremacy to other peer-to-peer currencies (economic and technological perspective)?
- What are the possible future trends regarding peer-to-peer virtual currencies?
  - What are most important regulatory trends related to virtual currencies?
  - Is a standard being formed (Bitcoin), or is there a growing spread of virtual currencies being used?

1.3 Methodology

In this chapter we present the tools we used in this project and the way we used them to complete this project and answer to the questions posed in subchapter 1.2. In the following figure (figure 4) we indicate the process of how we conducted our project work using those tools as well as how they interrelate with each other.
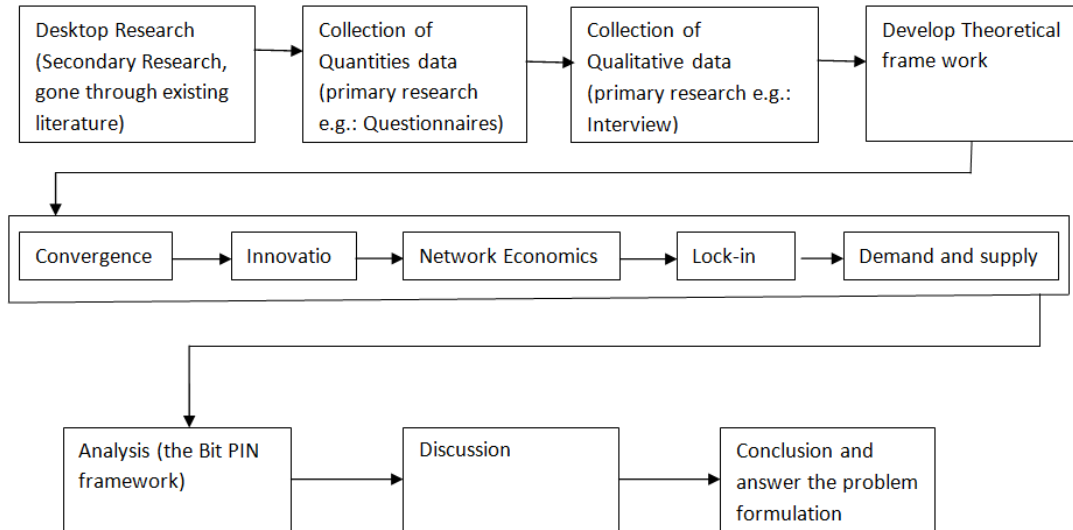
Figure 4: Methodology Diagram

In this project we conducted both primary and secondary research. Initially we started by doing desktop research (secondary research) in order to accumulate information and knowledge about the subject of virtual currencies as well as our case study, Bitcoin.

The next step was primary research. We distributed a questionnaire survey about Bitcoin (quantitative research) and we conducted an interview with a company producing and selling ATMs for Bitcoins.

In the meantime, we described several theoretical frameworks found in the literature (secondary research) in order to use and combine them in the last chapter and conclude about the questions of our project.

The methods used in order to answer the questions in the problem definition of this project are:

- Desktop research: Includes a literature review providing information from the material already available on the subject and giving a deeper understanding of virtual currencies as well as the technology relative to it.

- Qualitative research: Includes an interview conducted with an ATM company producing ATMs providing Bitcoins. In this way we are able to understand how virtual currencies like Bitcoin create opportunities for innovation in the market.

- Quantitative research: Includes the distribution of a questionnaire about Bitcoin. The results from this survey were used and analysed in order to see to what extent people and especially in the younger age groups, like students, are familiar with Bitcoin or even used it and get an idea about its levels of popularity and people's concerns and compare to the information provided by the literature.

- Convergence: The theory of Convergence is used to analyse and explain how in an era of major technological advancements, different technologies are brought together creating innovative products and services targeting the financial and payment markets.

- Innovation: The theory of Innovation is used to analyse how the creation of virtual currencies and especially Bitcoin, whether disruptive or not, become drivers for innovation from a technological and financial point of view. Bitcoin creates this way, new opportunities and challenges for all stakeholders making them directly or indirectly involved in this innovative product.

- Network Economics: The theory of Network Economics and more specifically the concept of the "network effect" play an important role in this project as the success of virtual currencies like Bitcoin is based purely on the demand for it. But in order for this demand to exist, there needs to be a large number of users and the larger this number becomes the more value the currency acquires. Consequently, more and more people will want to use it.

- Lock-in: The growing popularity of Bitcoin and the fact that its value and market share is by far the largest compared to other digital currencies, makes it a potential creator of "lock-in" effect in this market and so this theory needs to be included in this project [4].

- Demand & Supply: One of the most basic theories that needs to be used in order to analyse virtual currency and our case study, Bitcoin, is Demand and Supply. This theory helps explain the volatility that virtual currencies present and look into how they function in the market.

1.4 Delimitations

Crypto currencies create challenges that are very interesting from the point of view of macro economy, for example the impact on banking industry, the tax

repercussions from having crypto currencies and generally speaking, the impact of this currency in international trade. Nevertheless, our background and the time constraints that we have for this project don't allow us to give a meaningful analysis and discussion on these topics. So we will limit the scope of this project to microeconomics, lock in effect, supply and demand, standardization and the technologies evolved to communicate and to give security and privacy to the users.

There are many technologies associated to virtual currencies. This project is limited to distributed peer-to-peer virtual currencies, as Bitcoin, our case study belongs to that category. There are also many interesting virtual currencies that could be the subject of the case study but just as we explained before, in motivation, Bitcoin was an important aspect in our choice of this topic and as such we will limit the scope of this project to Bitcoin. But it is possible that in punctual locations, parallels will be drawn to other currencies, some of them virtual possibly, for comparison and argument reasons.

Finally, another delimitation for this project is related to the questionnaire distributed in order to get some quantitative data about its popularity and user concerns. The replies to this questionnaire were limited to 80 and they come mainly from the University's student community. Thus, the sample taken might not be representative enough, but it provides an indication of Bitcoin's popularity, especially among younger age groups.

2   State of the Art

2.1   Background

Nowadays Bitcoin is the most prominent and valued virtual currency in the sense that it can be exchanged in both ways with traditional money [4]. But besides being the most famous, it is far from being the first one.

The first attempts to create electronic money were made by Digicash with the brand name e-cash, DigiCash was conceived in 1982 by David Chaum. In his article "BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS" of the department of computer science in the University of California he describes these early challenges of electronic money as the following:

"Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of Criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns."(Chaum, D., 1982)

The problems he wanted to solve were lack of proof of payment, theft of payments, media, and black payments for bribes, tax evasion, and black markets.

For this David Chaum proposed a currency that had the following characteristics:

- "Inability of third parties to determine payee, time or amount of payments made by an individual."
- "Ability of individuals to provide proof of payment, or to determine the identity of the payee under exceptional circumstances."
- "Ability to stop use of payments media reported stolen." (Chaum, D., 1982)

Later in 1990 David Chaum founded Digicash and created the e-cash, his technique selling this e-cash to banks only one implemented USA a few others around the world and the DigiCash went bankrupt in 1998. But the legacy of the blind signatures would later prevail…

Since 1990 a lot has changed. The definition of virtual currencies is a very wide one and it includes from air miles and coupons to Bitcoins and game-based currencies. The market for virtual currencies used within apps or currencies used to

obtain content or other goods is growing faster than the rest and it is expected to increase in value by $1.2 billion from 2012 to 2017 and reach $3.2 billion, as it is shown in figure 5.
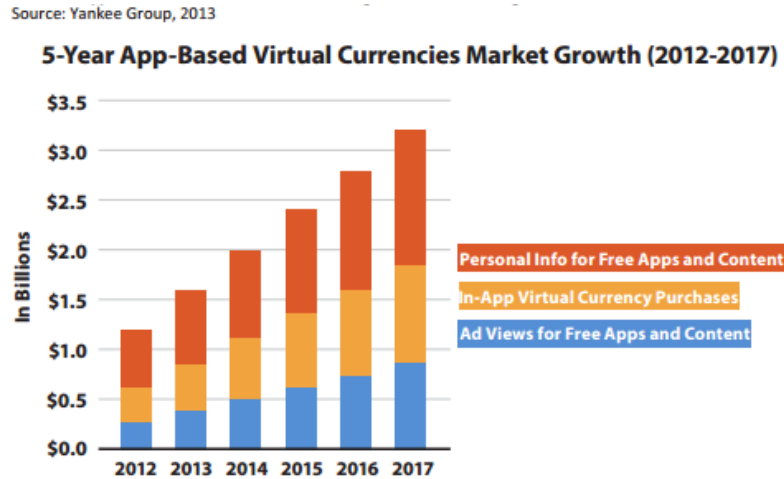
Figure 5: App-Based virtual currencies are among the fastest growing (McKee, J., 2013)

The first Bitcoin appearance as proof of concept was published back in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi work in the project until late 2010 and left without revealing much about himself. On other hand the community has since then grown exponentially with many developers working on Bitcoin [5].

The Bitcoin growth in the last years was very fast, not only in its value but also in the transactions per day. This is one of the most important indicators of its market importance and it can be seen in the chart below.
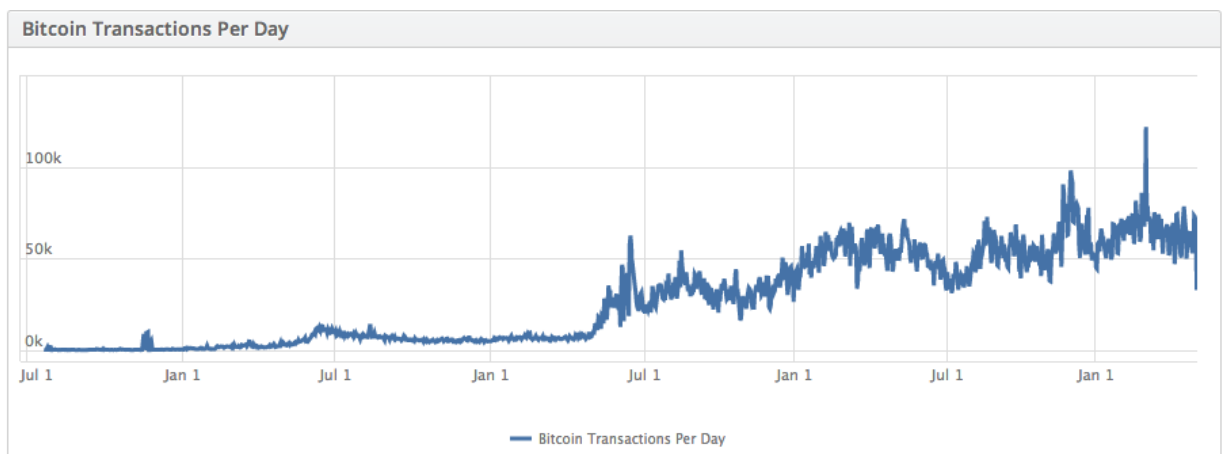
Figure 6: Bitcoin transactions per day. Source: coinbase.com[6]

But the revolution started by Bitcoin didn't stop here. New currencies are being created at a very fast pace, by a vast variety of different people, associations and even

companies. Today there are already more almost 300 peer-to-peer currencies being traded and this is a number that will be very fast obsolete, as can be seen in the webpage coinmarketcap.com that lists all the currencies values in a 24H actualization period [7].

Bitcoin's popularity has increased against the real economy(Rogojanu, A., 2014). The currency is accepted in different countries or business entities as means of payment. For example wordpress.com, reddit, mega accept payments in Bitcoin. Due to the wide popularity and advantages of the cyberspace, Cyprus and Canada introduced ATMs which can exchange virtual currencies into real currencies (Rogojanu, 2014). Moreover, in Cyprus, there is the first university that accepts Bitcoin as payment for tuition fees, and its representative stating that the strategy is to convert the alternative currency in to euro zone [8]. During the recent banking crisis in Cyprus, Bitcoin demand has surged due to people fearing the failure of their country's banking system. Investors start to transfer their wealth holding to Bitcoin as a safe. That lead to an increase in Bitcoin demand and its price went high [9] (Wan, P.N., 2013).

2.2   Categories of virtual currencies

The European Central Bank or ECB (2012: 13) in its paper about virtual currencies, provides the following definition: "a virtual currency is 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". They are currencies that can be obtained either in exchange for "real" money or by performing other types of activities (for example, mining in the case of Bitcoin). Since there is no standard classification for virtual currencies, and for the purpose of this project, the categorization following is based on the paper by ECB (2012: 13-16). This classification divides virtual currencies in three major categories based on how they interact with real currencies, using online currency exchange platforms and providing the ability to their users to buy goods and services in the real world.

Closed virtual currency scheme:

This type of currency is almost not at all connected to real currencies and transactions in the real world and is typically being used for online games. So in the

case of closed currencies online game players can earn this type of money throughout the game and according to how well they perform. The reason they are called "closed" is because they cannot be used for the purchase of goods and services in the real world, but only for the purpose of the specific online virtual community. Lately there have been initiatives, for example Currency Connect [10], that allow the exchange of closed type virtual currencies, as long as the virtual communities that have partnered with this exchange platform. Still there is no link to any real economy.

Especially in the world of online games, f.ex. RPG games (role-playing games) virtual money play an important role. They can be used to enhance the characters, buy special equipment and items that help throughout the game or even in order to progress in the game. Examples of such currencies used in game platforms are Zenny in Breath of Fire and Gold in World of Warcraft.

Figure 7: Zenny virtual currency (Source: capcom.wikia.com) [11] and World of Warcraft Gold (Source: www.wowgolds.com.au) [12]

Virtual Currencies with unidirectional flow:

This type of virtual currency can be bought using real money but it cannot be exchanged back to real money afterwards. It is mainly used for the purchase of virtual and in some cases, real goods and services.

In this category belonged Facebook's virtual currency, called Facebook Credits (FB). It was first introduced in 2009 as an attempt to provide additional revenue to the developers and Facebook itself, through the games developed for the platform. Users could use their credit card to buy Facebook credits in exchange for US dollars (initially) with 1 FB=USD 0.10, and use them to buy items, mainly for the gaming apps on the website. The payment can be done in many local currencies, for example US dollars, British pounds etc [13].

Figure 8: Facebook Credits (Source: worldpress.com) [14]

Another unusual type of exchange medium that could fall into this category is the bonus points (air miles) that airline companies offer their customers as a reward when they buy a ticket. The air miles then can be used to either buy another flight or to upgrade the passenger to first class. This way airline companies provide incentive to flyers to travel with them again and it's a strategy that has been proven very successful so far, since they have existed in many years (they were introduced in 1981 by American Airlines originally) [15]. Consequently they constitute a type of virtual currency that can be used for the purchase of real goods.

Virtual currencies with a bidirectional flow:

In this type of virtual currency, money is exchanged as any other currency in the real world and can be used to buy both virtual and real goods and services. The currency can be used any other real type of currency. Bitcoin, LiteCoin, Dogecoin, Peercoin, BlackCoin and many more virtual currencies belong to this category, with Bitcoin owning more than half of the market share and with a significantly higher value than the rest. All these currencies, despite their use just as any other real currency, they are not regulated by banks or other financial authorities and their value is based only on the supply and the demand.

Security concerns have also been raised especially after the latest developments with Bitcoin, when the biggest exchange platform for Bitcoins, MtGox, shut down, after several digital wallets were stolen, resulting in millions of dollars of

loss. Other concerns raised are about Bitcoin being involved in illegal transactions and money laundering [16].

Figure 9: Source: www.digitaltrends.com

Another interesting example, that is slightly different than the ones mentioned above is the case of Linden Dollars (L$), a virtual currency that was created and is being used in the virtual world of Second Life were users can create their own character and operate in the virtual world's virtual economy where the can buy goods and services, just like in any other real economy. In order to acquire Linden Dollars, people can use a credit card and then they can exchange it back to US dollars if they want. The user can also earn Linden Dollars by creating and selling virtual goods, or even by getting a virtual job [17].

2.3 Regulatory issues

Electronic transactions with credit and debit cards are becoming more and more popular, reaching $6 trillion worth of transactions worldwide, every year. Most vendors around the world accept electronic payment with a surcharge of 2-5% of the sale. Businesses that accept to get paid in Bitcoins could charge fees that can be down to 1% of the sale, without using credit card companies like Visa and Mastercard as intermediaries for the electronic transaction. In such an industry Bitcoin shows major potential, although this is not so apparent yet, as Bitcoin and its weaknesses hinder its adoption on national levels. One of its major weaknesses is its legitimacy (Alcron T. e al., 2013)

When we mention legitimacy, when we talk about currencies, we normally refer to transactions being conducted between parties, according to national laws and while the government is aware and interested in helping conducting such business.

Bitcoin's link to illegal transactions regarding black markets and money laundering is making governments hesitant towards its adoption or legitimization. The U.S. government for example, does not recognize Bitcoin as a real currency but merely as a virtual currency. In the U.S. there is no clear decision about Bitcoin from the government and so the possibility that in the future Bitcoin can be declared illegal by the U.S. government is worrying for businesses operating with Bitcoin and raises risk factors when it comes to investing in such businesses. (Alcorn T. et al., 2013)

Consequently, where there is lack of legislation, it is unclear whether Bitcoin transactions are legal and innovation is hindered. Legal regulation by national governments is necessary to clarify the situation. (Alcorn T. et al., 2013).

The following section presents the regulatory decisions made by several governments regarding Bitcoin, as today more and more countries take a clear stance as to what Bitcoin is in their district.

2.3.1 Germany:

One of the first countries where Bitcoin has gained popularity, forming a significant Bitcoin community, and the government has taken an official stance regarding this virtual currency, is Germany. The German Federal Financial Supervisory Authority (BaFin) released a statement on Bitcoin in the beginning of 2014 evaluating Bitcoin and stressing on the risks for its users [18].

In this statement it is clarified that Bitcoins are not a currency or e-money according to the definition by the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz). It recognizes the use of Bitcoin as a substitute for real currencies and as such processes like mining and purchasing are not subject to authorization requirements (licensing). However the exchange of Bitcoins in a market where a special fee is paid is a type of trading that is subject to licensing requirement, according to the German Banking Act (Kreditwesengesetz). This means that trading with Bitcoins is a process subject to regulations.

Anyone offering Principal Broking Services in Germany needs license from BaFin. This is also the case for buying and selling Bitcoins on behalf of others, making Bitcoin trading platforms falling into this category.

Bitcoin trading platforms are also subject to regulations regarding Multilateral Trading Systems in Germany. Such systems serve as a platform for selling and buying between third parties. Bitcoin trading platforms can also relate to this and thus can be subject to regulation according to German law.

Looking at the business models can define whether a financial activity is subject to regulations or not and this is what is being defined in this statement.

The second part of the statement states the risks for Bitcoin users. Just like real money, e-money or any sort of valuable object, Bitcoins can be stolen (through a cyber-attack for instance) and not recovered. In addition BaFin warns users of a rise in transaction costs as expenses will rise in order to increase computing power for generating Bitcoins as the process becomes more and more complex. Finally, they warn about the quickly fluctuating prices of Bitcoin, giving the opportunity to speculators to speculate and earn from the losses that simple users could be subject to.

Bitcoin is defined by BaFin as a risky investment to make and warns its users of the possible risks. Nevertheless, the fact is that they are trying to regulate it and that means that Bitcoin is growing in popularity in Germany.

2.3.2 Scandinavia:

In Scandinavia, governments have also started to pay attention to the Bitcoin case.

In Denmark, the National Bank and the Financial Services Authority (Finanstilsynet) have stressed that virtual currencies are not to be considered currencies but more like valuable items, like gold, silver etc. with no support from the authorities but trading it is nonetheless legal [19]. Since Bitcoin is not subject to regulations it cannot be considered as a currency but no steps towards taxing it have been taken yet in Denmark, as the Danish Tax Board does not recognize it as real money and therefore it does not generate taxable gains [20].

Norway on the other hand, although they also concluded that Bitcoin is not to be regarded as a currency, they decided on placing profits from Bitcoin under the wealth tax, with a 25% sales tax imposed on businesses [21]. And although tax revenue from Bitcoins is not a major one, it is an important step towards its regulation.

In Sweden, the Swedish Tax Agency classified Bitcoin as an asset and as such put taxes on it [22].

2.3.3 China:

In late 2013, People's Bank of China declared that Bitcoin is not a currency and banned Bitcoin transactions for financial institutions, which resulted in Bitcoin losing 20% of its value at the time. The public is free to transact with Bitcoins at their own risk. Although Bitcoin is not a threat to China's financial system, the regulatory authorities are worried that its growing popularity could create an unstable situation [23].

2.3.4 USA:

The U.S. is expected to take regulatory actions regarding Bitcoin later this year, especially after the failure of MtGox in Japan. Regulators in the U.S. are looking into what position Bitcoin should have in the markets and move towards some type of regulation [24]. The US Treasury considers Bitcoin transactions legal and businesses that are involved in the exchange of Bitcoins are considered money service businesses according to the Bank Secrecy Act. More specific regulations are to be taken by each state separately [25].

2.3.5 Iceland

In Iceland the Central Bank declared buying Bitcoin as an action of taking money out of the country and so such a transaction is illegal according to the rules imposed after the banking crisis in 2008 about capital controls and so trade of goods in and out of the country cannot be done in exchange for Bitcoins [26].

2.4 The Bitcoin Ecosystem

In order to study Bitcoin itself, it is necessary to take a look at its "ecosystem". The term ecosystem stems from biology but in the business world it is defined as:

"An economic community supported by a foundation of interacting organizations and individuals—the organisms of the business world. The economic community produces goods and services of value to customers, who are themselves members of the ecosystem. The member organisms also include suppliers, lead

producers, competitors, and other stakeholders. Over time, they coevolve their capabilities and roles, and tend to align themselves with the directions set by one or more central companies." (Moore, T., 1996).

Of course Bitcoin is not a business itself but we can describe its surrounding entities as part of its environment. In this environment, companies form symbiotic relationships. In this type of relationships, when one part is thriving then the others can also benefit from it. This means that each part can also be affected in a negative way if another one has problems. In the Bitcoin Ecosystem there are "entities" that are part of it and interact with each other, such as the merchants, the mining pools, the exchanges, and the user's remote wallets (Böhme, R., 2013).

All these entities interact with each other in various ways. For example, an exchange's activity might affect the value of Bitcoin and in return, the merchants' business. For instance, if the value of Bitcoin rises, then the merchants can make more profit.

2.5 The Bitcoin Algorithm

Bitcoin algorithm has no central server and is base in a peer to peer system. This means that the processing power from Bitcoin is divided by all the nodes of the network. The algorithm of Bitcoin relies on digital signatures to prove the ownership and public history of transactions to prevent double usage. The transactions history is also shared in the peer to peer network, where nodes have to agree about the history. (Nakamoto, S., 2008).

Like the picture below shows, the users from Bitcoin have two different keys, one public and one private. They can be used in many devices like phones, by using a web wallet or PCs by using local wallets or even a physical wallet. These keys are used to both digital sign in and secure the transactions. All the transitions are stored in a public Ledger and the ledger is processed by the Bitcoin network (Nakamoto, S., 2008).
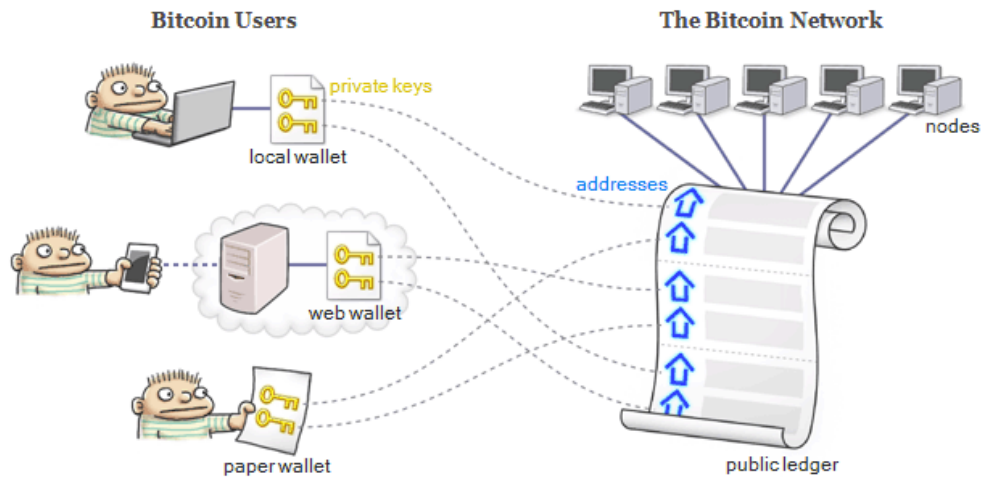
Figure 10: Bitcoin Network. Source: preshing.com [27]

The Bitcoin Network is made of all users that have active wallets in their local PC. They store all the information from all the transactions ever done in Bitcoin. And by mining they help the network information get processed (Nakamoto, S., 2008).

What miners do is to help process block chains (which will be explained in more detail in the security subchapter). By doing so, the miners are rewarded with Bitcoins for their work. In the early years, these coins were abundant but the amount of them being rewarded is decreasing through the years to ensure that in the future there will still be attractive for miners. Small fees are being charged to the people that do transactions and then feed these Bitcoins back to the miners when they process (mine) a special block chain. The block chains with Bitcoins are similar to a lottery ticket but very common (Nakamoto, S., 2008).

2.6 Privacy

The privacy aspect is one of the key aspects that attracts users to Bitcoin and for the most part all the attempts and search done, is to show that it is reliable. But the users sometimes make actions that can allow their privacy to be exposed (Reid, F. et al., 2012).

There were several tests made regarding Bitcoin and other software, surrounding this virtual currency safety and privacy. One of them is the case of TCP/IP Layer Information by Dan Kaminsky that will be discussed below. Still, many of the cases of disclosure are voluntary.

2.6.1   Voluntary Disclosures

One of the major sources of identifying information is the voluntary disclosure of public-keys by users, when posting to the Bitcoin forums. These keys are very easily indexed by search engines.

In the paper "An Analysis of Anonymity in the Bitcoin System" Fergal Reid and Martin Harrigan (Reid, F. et al., 2012) said "We identified many high-degree vertices with external information using a search engine alone. We scraped the Bitcoin Forums where users frequently attach a public-key to their signatures". This is a problem because these users lose the privacy that they got by using Bitcoin (Reid, F. et al., 2012).

2.6.2   TCP/IP Layer Information

TCP/IP Layer Information was another way identified that the privacy of Bitcoin can be compromised. Security researcher Dan Kaminsky did tests and analysis to the Bitcoin system, trying to identify problems in the TCP/IP layer. With this analysis, he discovered that unless the users use anonymizing proxy technology, such as TOR, it is possible to map the IP addresses of the Bitcoin Public-keys(Reid, F. et al., 2012). Although this is true and it is indeed a problem, Bitcoin users can use TOR, a network of virtual tunnels that allows privacy, security and anonymity on the internet [28].

2.7   Security

Bitcoin protocol has a strong security track [29]. Bitcoin security is well defined —a Hash function algorithm is used to transmit the block chain over the peer-to-peer nods. However, Bitcoin uses pseudonyms in the network to transmit the block chain so that the user can be anonymous (Decker, C. et al., 2013). But while the block chain is transmitted around the network, it will take 10 minutes to verify by the nods (miners) in the network so that dishonest users cannot double spend (two different users signing over the same coin) their coin (Nakamoto, S., 2008). Below is the Bitcoin secure transaction model:
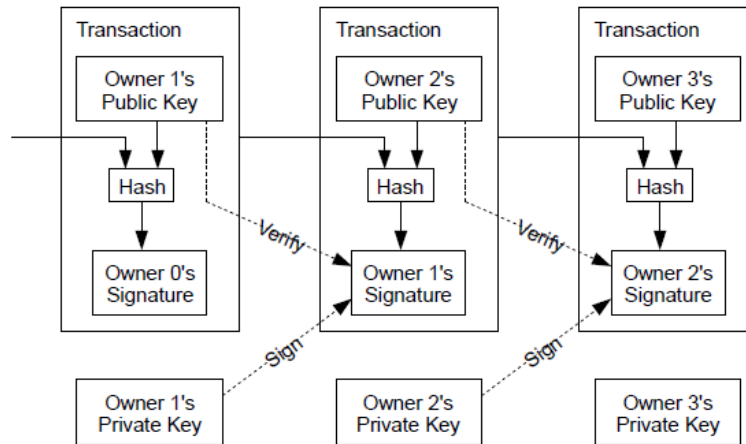
Figure 11:Peer to Peer secure Transaction Model (Nakamoto, S.,2008)

Every user has two keys for their nods one private key and one public, which can also be referred to as signature key. While one owner transfers his Bitcoin to the next owner, they broadcast it using the owner's private key and a pseudonym including the owner's previous transaction history and the next owner's public key plus some transaction fees, typically 0.0005 BTC or lower(Taylor, M.B., 2013). These hash function contains all the transition information (from beginning to current time) of a particular coin, which makes the coin secure because no dishonest or hacker nods could replicate the coin.

The security of Bitcoin relies on the distributed consensus achieved by the mining process (Kroll et al., n.d.). This means that a cartel of miners is not possible because of the Bitcoin distributed peer-to-peer network. That is because a single miner or coordinated group of miners cannot hold more than 50% of the network's mining (puzzle solving) computing capacity(Kroll et al. n.d.). For the same reason double spending is also prevented.

Bitcoin can suffer a type of attack called 51% attack. Although it is very hard for such an attack to take place, in theory it is possible. If someone hold 51% of the active nodes could disrupt the entire network (King, S. et al., 2012).

Bitcoin can be stored digitally in the user's mobile, computer wallet or third party service provider server. There is a security risk in the user level, because Bitcoins can be stolen from third party Bitcoin service providers and from individual Bitcoin wallets(FBI, 2012). For example, one way to steal Bitcoins is by sending malware to the Bitcoin user computer or service provider server and transferring the coins from one account to another. Another very important aspect for the end user is the private

key, also called signature key. If a user loses or forgets their private key, the account is useless and all the coins they have are lost. It is the same as losing one's wallet in real life. Private Key retrieval from the system is impossible.

Bitcoin transactions face the same risks as today's online banking transactions (hacking, fraud etc.) and virtual wallet theft is the same as someone having their physical wallet being stolen. The difference lies in the fact that governments have not recognized Bitcoin as a currency and since there is no regulation by financial institutions, it cannot be backed by the government. This is what creates an unsafe feeling in those who consider investing in Bitcoin and hinders Bitcoin's extended use.

3 Theoretical frameworks

In this chapter of the project several significantly relevant frameworks will be introduced.

These frameworks will be used later in the analysis part of the project report. The first theoretical framework is convergence theory that deals with the standardization process. This theory will be succeeded by Innovation Theory. After this Network Economics and lock-in will be described and the value created by having more users and merchants. Then the chapter will be finalized with the Demand and Supply theory.

3.1 Convergence

3.1.1 Definition

Like the word convergence says this framework is about coming together. And it's done by studying the field from two perspectives - industry and technology. In 1997 convergence was defined as a merger of two or more industries producing substitute or complementary products (Greenstein, S., 1997), also in the same year and this time by the European Commission in their green paper, convergence was defined as the ability of different platforms to carry essentially similar kind of services and the process of coming together, one example can be consumer devices such as the telephone, television and personal computer (European Commission, 1997).

3.1.2 Historic Perspective

The first time that the term convergence was used, was in 1963 by Rosenberg (Rosenberg, N., 1963). The term was used in order to find a more precise description of the implementation of specialized machine tools in the US industry. In his article he is referring to it as a trend concerned with manufacturing a broad variety of products by using a similar type of machinery and technology. The result of this process was that process industries that were previously separated became very closely related on a technological basis.

The second important landmark, this one especially in ICT field, was the already referred green paper from European Commission in 1997. In this paper the convergence wasn't only about industry or even only about technology, it was also about services and platforms. The global nature of communications platforms at that time, in particular, the Internet, were providing a key which would in time open the door to the further integration of the world economy like it happen (European Commission, 1997).

3.1.3   Types of Convergence

Industry convergence is normally defined as the converging of two or more separate and distinct industries like explained before. But the basic push towards industry convergence occurs normally due to technological convergence. Nevertheless there is a possibility for other factors involved like customer demands, regulation and the industry structure needs, etc. (Greenstein, S., 1997)

Technological Convergence is very common in the present days and is shown by a vast array of different types of technologies performing substitute tasks. The examples are countless. One simple example can be the usage of smartphones to listen to music, see movies and navigate in the internet (European Commission, 1997).

Service Convergence is present in several aspects of today. One of the most common examples was the digitalization of the telecom market. This process allowed one shift in the way telecommunications were done. From the one-service via one-network concept the new concept of multiple services via multiple networks (Han, S.P, et al., 2004).

3.1.4   Drivers of convergence

Most of the academic theory around convergence has been centered on drivers, typologies and consequences of convergence. So after discussing the typologies and its consequences, it is important to also discuss the drivers.

The two factors driving the market convergence can be examined industry- and technology-wise, with these two aspects closely related with each other. But the main driver pushing for convergence has always been technological change and

innovation. This driver includes the appearance of integrative technological platforms (Gambardella, A. et al., 1998), such as the Internet (Lei, D.T., 2000; Wirtz, B. W. 2001).

3.2 Innovation

Joseph Alois Schumpeter was the first who started working on what is innovation. In his economic model directed to innovation, he defines the process of innovation as a Trilogy: "Invention - Innovation - Diffusion" (Mahdjoubi, D., 1991). Schumpeter theory can also be used in R&D – production – marketing and only in innovation.

What is Innovation?

Innovation theory can be defined in many ways but some bright people have defined it as:

- "The ability to deliver new value to a customer" (Jose Campos)
- "Change that creates a new dimension of performance" (Peter Drucker)

So innovation is when something new or improved is created to address and meet new requirements or existing market needs. In addition, innovation doesn't come only in one form. In fact there is many ways innovation can be defined:

- Sustaining vs Disruptive
  - o Sustaining –innovation that improves product performance (Clayton, C.M., 1997)
  - o Disruptive – innovation that brings an entirely different value proposition to the market and cause existing products' performance worse (Clayton, C.M., 1997)
- Incremental vs Radical
  - o Incremental – Innovation that improves the cost or the features of already existing products or services (Leifer, R. et al., 2000)
  - o Radical – Innovation that creates a completely new product, with new customers, creating new business models, changing the economics of a business (Leifer, R. et al., 2000)

What can be concluded from these cases, is that the choice when creating a new product or service, is between building upon an existing product or service in the market, by making it better, or developing something entirely new. Sometimes this means to create an entire new category of product that can substitute the old one or even make it obsolete. In some cases the product is ahead of time and it fails.

3.2.1 Diffusion of innovation

Diffusion of Innovation theory was created to understand how new ideas both scientific and corporate are diffused to the public. Everett Rogers first created Diffusion of Innovation Theory in his book in 1962. The categories that he created back then where: innovators, early adopters, early majority, late majority, and laggards (Rogers, E.M., 1962)

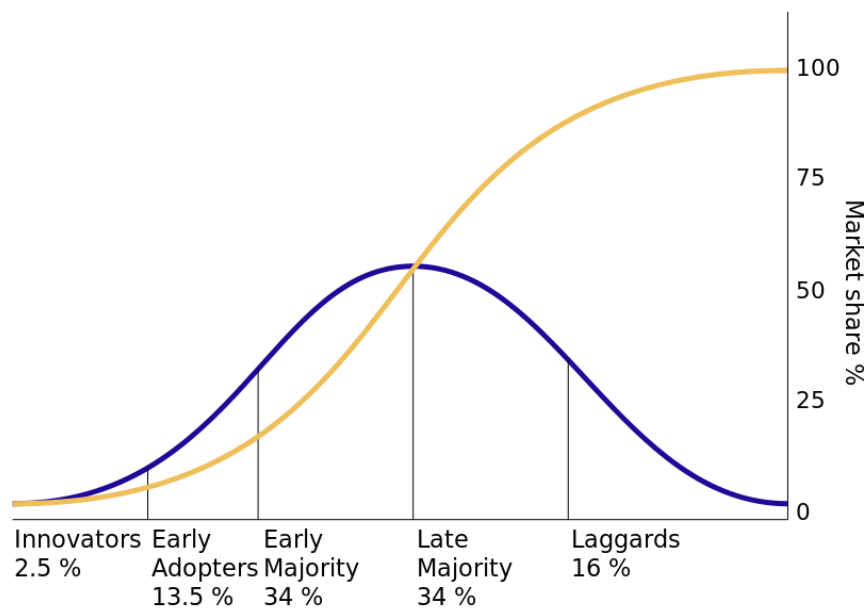Figure 12: Diffusion of Innovation. Source: (Rogers, E. M., 1962)

- Innovators: People with a strong interest in technology and who like to experiment with new technologies
- Early adopters: People with deep technical knowledge who might use a new technology for professional and academic purposes
- Early majority: People who consist big part of the mainstream who are comfortable with technology

- Late majority: People who consist the second part of the mainstream but are not so comfortable with technology
- Laggards: People who are more conservative towards a technology.

The speed of diffusion is also an important factor, and there are several aspects that can help or constrain the growth of a technology. Nowadays the consumption of new products spreads faster than before due to the many ways to communicate, better knowledge about technologies, etc.
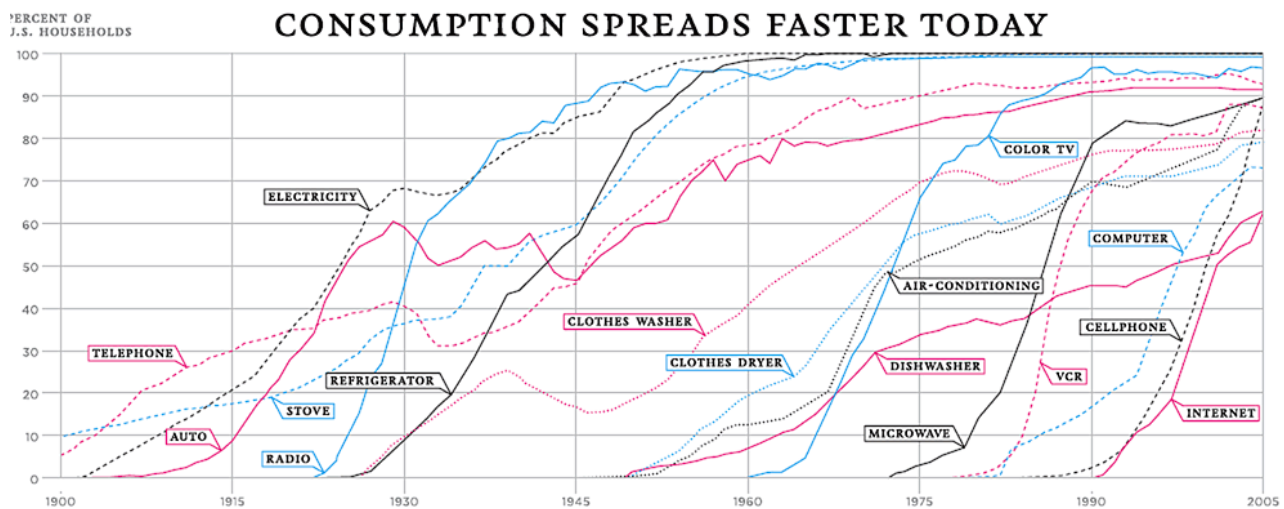
Figure 13: diffusion of technologies. Source: andrewgelman.com [30]

Everett Rogers explains this diffusion with five factors that he believes influence each individual's decision to adopt or reject a new technology (Rogers, 1962):

- **Relative advantage -** What the new generation brings as new.
- **Compatibility** - Compatibility with the individual's life.
- **Complexity or simplicity** - If the users see a technology as simple to use or difficult to use
- **Trialability** - How easy an innovation can be tested. If a user tests the new product and likes it, then the more easily they will adopt it.
- **Observability** - User can understand the extent of the innovation.

The theory of Innovation is central in this project, it will help analyze everything new that Bitcoin has brought to the markets, both from a technological and a financial perspective and explain how that affects Bitcoin's growth.

3.3 Network Economics

Network economics is a theory that studies the effect of a growing network, in a business. In a network there are *externalities*, that is when an individual is affected by the actions of other individuals. When the individual is affected in a positive way and receives benefits from it, then it is called a positive externality. When they are affected in a negative way, then it is called a negative externality (Easley, D., et al., 2010).

In networks we may have network effects. This means, that the increase of the size of the network will also mean an increase in the utility that a user receives by using a certain product or service (Shapiro, C. et al., 1999). And this effect will get stronger as other consumers join in the usage of product or service. This means that the network effect today has the complete opposite meaning than in neo classical economics.

Network effects can be either direct or indirect. A direct network effect is when for example the utility for a user of a telephone increases as the total number of telephone users increases. The indirect network effects come from complementary products or services. For example a DVD player becomes more valuable to its owner when the variety of DVDs that can be played increases. And the more the users, the more variety there will be (Clements, M.T., 2004).

Networks are composed of links and nodes; the links connect the nodes to each other. In most cases nodes are complementary to each other. Networks can be classified in two ways. The first one is about the way they are linked. That can be **physically** (Telephone) or **virtually** (social networks). And the second is about the direction of connections. If IT is a **two-way** communication like the Internet or **one-way** communication like an ATM network (Zang, L., 2009).

One other important aspect about network economics is the feedback. The negative one can be hazardous for the future of a company and the positive one has very good effects on it. In addition, according to Shapiro and Varian, "positive feedback is a more potent force in the network economy than ever before" (Shapiro, C., et al. 1999). In general, feedback could directly impact on the market share and popularity of certain business sectors. In other words, positive feedback makes a company get stronger than it is and negative feedback makes companies get weaker than they are (Shapiro, C., et al. 1999).
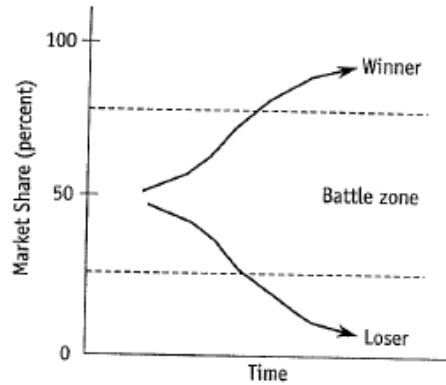
Normally positive feedback follows a predictable pattern with the correlation adaption of new technology, which is represented in the S shaped curve bellow.
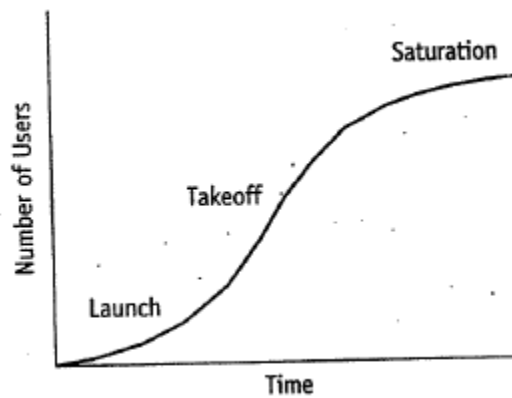
Figure 15: Adoption of new technology (Shapiro, C., 1999)

It has three phases such as:

- Launch
- Takeoff
- Saturation

In the first phase during the launch the angle of the curve is flat, then with the positive feedback there is a steep rise during takeoff and saturation is reached and the curve starts to level of. Another aspect that influences the angle of the growth is the Demand side and supply side economic aspect, which also impacts network economics, and will be discussed, further below in the next chapter.

This theory is extremely relevant in this project, because the value of a virtual currency that isn't based in any institution or any commodity is only based on the strength of the network and the demand generated from it.

3.4 Lock-in Effect

In markets subjected to network effects, like the ICT industry, a phenomenon called "lock-in effect" is also present. This describes a situation where on standard or technology is adopted by everyone in the market. As the utility from the use of a specific technology increases for a user when more and more people use it (network effects), we often see that the adoption of this technology is so widespread that it ends up dominating the market. As a result every participant in the market is "locked-in" to the specific technology even if it might not be the best one or the cheapest one (Draisbach, T. et al., 2013).

Figure 16: The QWERTY keyboard lock-in (Source: wikipedia.org) [31]

The QWERTY keyboard is one of the most well-known examples of a lock-in effect. When the type-writer was invented, in order to reduce the type-bar clashes, there was a rearrangement of the alphabetical order of the letters on the keyboard which resulted to what we know today as the QWERTY standard. There were three main factors that lead to the dominance of this keyboard from the days of the type-writers until today. First, when this keyboard came out, typists were professionals whose ability to perform faster on a type writer contributed to the adoption of one keyboard. Second the wider adoption lead to a cost decrease (scale economies) for the QWERTY keyboards and finally switching to a different keyboard arrangement would be a costly investment (David, P.A., 1985).

This theory is necessary for exploring the possibility of a lock-in effect being created with Bitcoin.

3.5 Demand & Supply

3.5.1 Demand

"The *law of demand* says that if we hold all other factors constant (*ceteris paribus*), a decrease in the price of a good will cause consumers to increase their consumption of that good."(Fox M. et al., 2012)
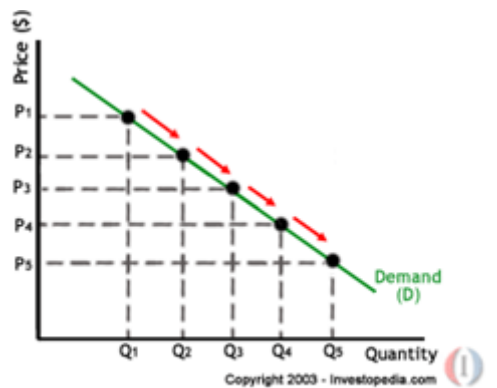
Figure 17: Demand curve. Sources: www.investopedia.com [32]

There are also different factors determining the demand for a good. Those factors can shift the demand curve from left to right and vice versa. Moving the curve to the right means increase in demand, while moving the curve to the left means decrease in demand. (Fox M. et al., 2012) The factors determining demand are:

- Income: An increase in a person's income means increase for the demand of normal goods (the most common goods) and a decrease for the demand of inferior goods (for example bus tickets, secondhand clothing etc.) A decrease of someone's income leads to the opposite results for these two categories of goods.

- Tastes: A consumer's taste might change from time to time. If their tastes switch to the favour of a good then it increases its demand, while if tastes switch a consumer from one product to another then the demand for the first one is decreased.

- Prices of related goods: A good might have complementary (used together whit this good) or substitute (used instead of this good) goods. An increase in

the price of a complementary good means a decrease in its demand and since the two goods are used together, the demand of the first good is going to decrease as well. A decrease in the price of a complementary good means and increase in the demand of both goods. With substitute products, if the price of one of them increases then its demand decreases and so the substitute's demand increases.

- Expectations: If a consumer expects the price of a good to fall at some point in the future, then they will decrease its demand today in order to buy it when the price is lower. Or if a consumer's income is expected to be increased then their demand for a good might increase as well.

- Number of buyers: More buyers mean more demand for a good, while less buyers mean less.

(Fox M. et al., 2012)

3.5.2 Supply

"The *law of supply* says that if we hold all other factors constant (*ceteris paribus*), an increase in the price of a good will cause suppliers to increase their production of that good." (Fox M. et al., 2012)
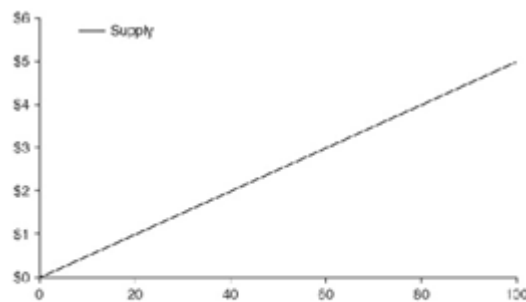

Figure 18: Supply curves. Sources: (Fox M. et al., 2012)

Next are the factors that affect the supply of a good and either shift it to the right when they increase the supply or to the left when they decrease it:

- Input prices: When the price of a good needed for the production of another good changes, then it also affects the supply of the latter. If, for example, the price of such a good increases, then the cost of producing the final good also increases moving the supply curve to the left.

- Production technology: The use of a new technology for the improvement of the production of a good, can lead to the increase of supply.

- Prices of related goods and services: The supplier of a good might change the supply of a good if they have more profit from another good they produce. For example, if the price of one of the goods produced from a supplier increases, then the supplier might increase the supply of the more profitable good and decrease the supply of another one less profitable.

- Expectations: Suppliers, just like consumers have expectations about the prices of a good. If the price of a good is expected to increase at some point in the future, the supplier will decrease the supply today and increase it when the price is higher.

- Number of producers: The more producers produce a good, the bigger the supply for it will be.

(Fox M. et al., 2012)

3.5.3 Supply and Demand

The supply and the demand of a good determine its price in a market. Putting the demand and supply curves together in a graph shows the point of equilibrium where the quantity demanded by the consumers equals the quantity supplied by the producers.
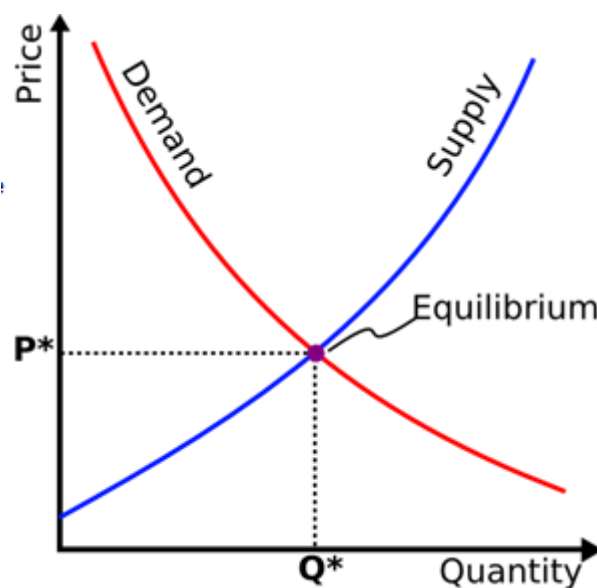
Figure 19: Supply and Demand curves and point of equilibrium. Source: worldpress.com [33]

There are four basic laws of supply and demand (Braeutigam R., 2010):

- An increase in demand while the supply remains the same means shortage for the good and a higher equilibrium price.
- A decrease in demand while the supply remains the same means surplus for the good and a lower equilibrium price.
- An increase in supply while demand remains the same means surplus for the good and a lower equilibrium price.
- A decrease in supply while demand remains the same means shortage for the good and a higher equilibrium price.

Demand and supply play an important role for our case study, Bitcoin, as they are basically the reason for its value's volatile behavior. Bitcoin is not an asset with value unless there is demand for it. Consequently the demand and supply theory needs to be thoroughly examined to define to what extent it is applied to Bitcoin, which are the factors that affect Bitcoin's demand and supply and what the role of Bitcoin alternatives and substitutes is.

4 Analysis

In this chapter, the project focuses on the case of Bitcoin as well as the data collected from the interview, the survey conducted and other sources from our desktop research. The analysis will be done both by applying the theories presented in chapter 3 to the case of Bitcoin and by analysing the data extracted from the qualitative and quantitative research. In order to do that, an analytical framework has been developed and is going to be presented in chapter 4.1 that combines the different elements studied regarding Bitcoin.

Analysing Bitcoin as well as the parts that comprise its ecosystem and the factors that affect it, provide a good overview of the growing trend for the development of virtual currencies as well as their position in today's economy. This way it becomes easier to answer the questions posed in the beginning of this project and conduct a valid and more complete discussion and conclusion.
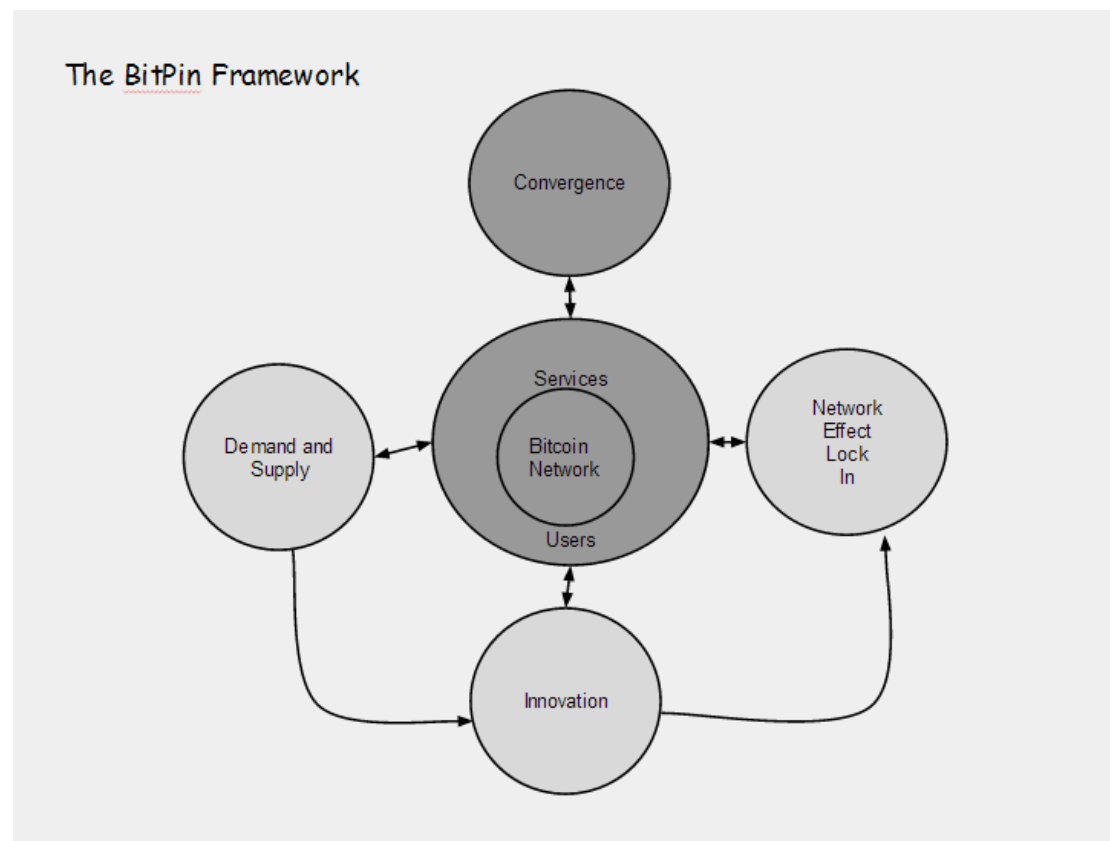
4.1 Analytical Framework

Figure 20: The BitPIN analytical framework

The way this analysis of Bitcoin is constructed in this chapter is presented in the analytical framework sketched in the figure above, which helped structure the analytical part of this project and explain the processes that take place. In this framework, called the BitPIN framework- a name which derives from the name of the currency (Bitcoin) and the authors' last names- there are five major parts which are going to be analysed and comprise the factors that form and define Bitcoin and its ecosystem.

In the centre of it all, there are the users and the services that keep the Bitcoin network "alive". Everything else in the analytical framework revolves around them and affects the Bitcoin network in various ways. First there is demand and supply, which predetermine Bitcoin's value and in the long run, its success. Innovation is another important aspect. The innovation stemming from Bitcoin is not only the virtual currency itself; it includes all the new services and products that were later created because of it. In addition, there are the network effects and possibly lock-in in the Bitcoin network, which are fuelled by the stream generated in the demand and supply that pass through innovation, also play a vital role for the prosperity and survival of Bitcoin. Finally, the role of convergence is discussed as a result of the processes taking place within the Bitcoin ecosystem.

Before closing the chapter, there will be a subchapter that brings all of the above together in order to form a complete framework and provide an analytical overview of the chapter to summarize the important parts and facilitate the discussion in chapter 5.

4.1.1 The Bitcoin Network-Services and Users

At the heart of Bitcoin lies its network, with its users and the services surrounding it. The theory behind this network was explained in chapter 2. Without them Bitcoin would not exist, as it is no national currency and its survival is based on its user base. In order for the user base to grow, it is necessary to facilitate transactions as much as possible so that people can find Bitcoin easier to use and have better access to it. Ease of use is important for the network, and consequently demand, to grow. The simplicity of Bitcoin will be further analysed in the Roger's five factors in chapter 4.1.3.3.

In order for the Bitcoin network to function, there is need for services, mainly software, that support the platform in various ways. The first and most important

piece of software that facilitates Bitcoin transactions is the virtual wallet. The Bitcoin wallet is responsible for managing a number of addresses in a seamless way for the user. The user is able to see their balance and make transactions with other wallet by transferring Bitcoins from their wallet to another address. The user is allowed to have more than one address themselves (Goldfeder, S., et al., 2014).

Besides the wallet software there is the need for the completion of the transaction and its validation from the miners. Bitcoin transactions are irreversible (once validated by the network cannot be changed, even in the case of fraud), automated (no human action required) and anonymous (Bitcoin addresses don't need to be linked to a physical person) (Goldfeder, S., et al., 2014). This means that security is important when transacting with Bitcoin and services like BitPay were created. BitPay provides secure payment services, similar to PayPal for traditional currencies. Businesses and people conducting payments with BitPay decide what percentage of the money they receive stays in Bitcoin and what is converted to real currencies and deposited in their bank account [34].

Another type of product that was created to provide Bitcoin related services is Bitcoin ATMs. There are different variations of this product, but most ATMs allow the purchase of Bitcoins with cash, like Lamassu's ATM [35]. Some others can also be used the other way around, which means users can sell Bitcoins and receive cash, like Robocoin's ATM [36].

Those are some of the services and products provided today and many more are around the corner as Bitcoin has fuelled innovation as will be later described in 4.1.3. Of course none of that would have reason for existence if it wasn't for the users in the Bitcoin network that need reliable services to transact with Bitcoins.

Until today, there are no official or large-scale statistics as to who the Bitcoin users are, how and how often they use Bitcoin or what holds the rest of the world back from using it. Bitcoin has come a long way since its creation but it's still growing and attracting more people to its network. The services and products that are being developed to help the diffusion process are still at an initial stage but as the network grows so will they.

For the purpose of this project, it was interesting to see to what extent people know and/or use Bitcoin in order to get an idea of its popularity and so there was a survey conducted, whose results are going to be presented and analysed in this chapter. Of course the sample is too small in order for the results to be 100%

statistically correct and the conclusions from it are limited, as explained in 1.4. The sample is almost exclusively members of Aalborg University's student community and the questions are general questions about Bitcoin. The intention was to find Bitcoin users and interview them but unfortunately that was not an option, since the few regular users (monthly or yearly) that answered the survey weren't available.

From the survey conducted it was obvious that the biggest part of the participants had previous knowledge of Bitcoin (85%). This is an impressive number although it is expected that this number in the general public would be lower.

Do you know what Bitcoin is?

YES
NO
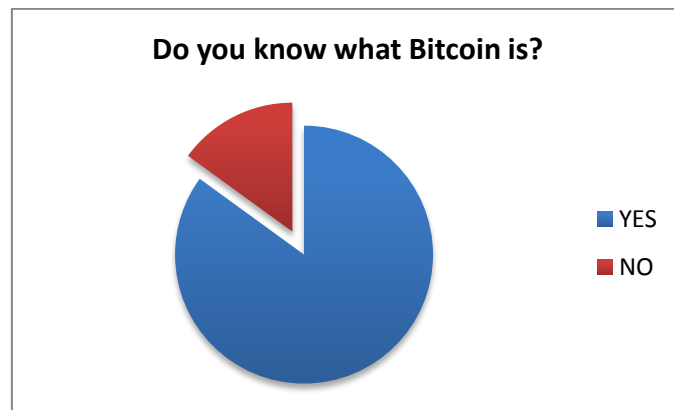
Which brings us to the next observation which also brought some interesting results. Although the participants are members of the University community and it would be expected to know about Bitcoin through their academic environment the next chart shows that in fact the biggest part of it knows Bitcoin through the different media, such as TV, newspapers etc. (64.7%).

How do you know Bitcoin?

From School or University

From Family or Friends

From media (TV, Newspaper, Online, Social media)
Other
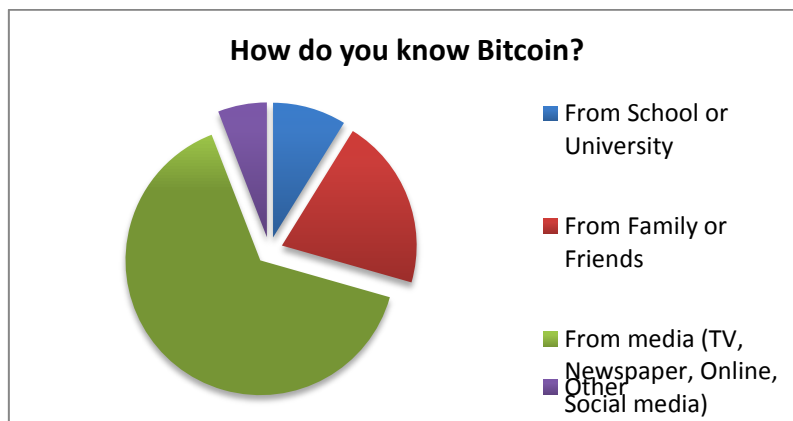
In fact the percentage of people who know Bitcoin through school or university is only 8.8%, while social environment, like family and friends come second with 20.6%.

The rest of the answers to our questions reflect that although most people knew Bitcoin, very few had used it even once and there were very few regular users.

More specifically 91% answered that they never use Bitcoin in any sort of transactions. That was a very interesting result and the next question attempted to find out why that might be, by asking one of the basic questions that reflects the argument that Bitcoin is not safe.
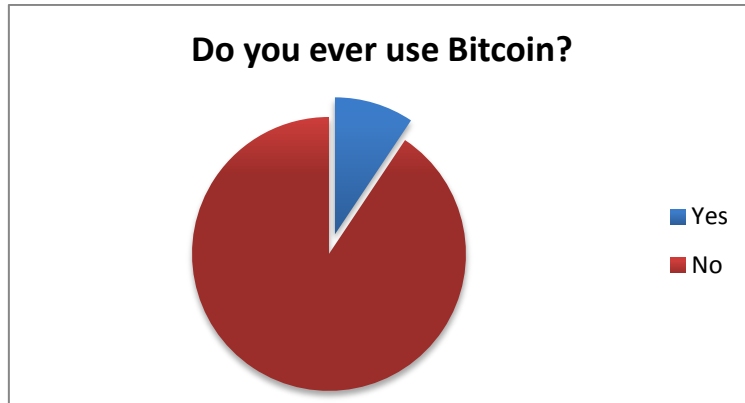
To the question about security concerns regarding Bitcoin, 56% answered that they are concerned about how safe it is to use Bitcoin. This doesn't justify entirely the big percentage that doesn't use Bitcoin, so although security is an important factor that might affect people's decision on whether to use Bitcoin or not, it is probably not the only one.
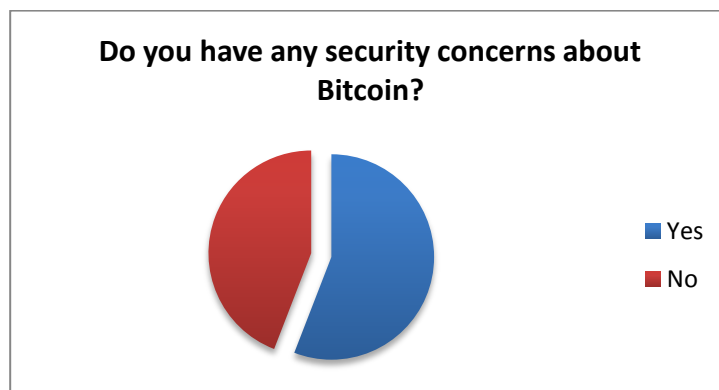
When asked about what sort of concerns those are, most people mentioned security concerns (hacking of their digital wallets, fraud etc.), while others were concerned about the value of Bitcoin and its volatile price mechanism, as well as Bitcoin's legality, since the lack of regulation leaves Bitcoin in a legally grey area.

In conclusion, this survey is not able to show who the Bitcoin users are, but it explains to a certain extent how people feel about Bitcoin today. And even though a lot of people know it, not so many have tried to use it and almost all of them are concerned about Bitcoin's instability, security or legality. This means that people still see Bitcoin as a risky investment and so they are wary when it comes to using it.

A more extended survey about Bitcoin would provide many more valuable results, but this one is a first step to understanding Bitcoin's popularity among people.

4.1.2 Demand & Supply in the Bitcoin Network

Each digital currency has its own rule which defines how coins are produced. Normally new coins are created, in order to increase the supply, which are given as rewards to those who, in one way or another, serve the digital currency platform. Supply for digital currencies is affected by two parameters. First, the more the transactions there are, the more work there is to be done by the people that provide services to the digital platform and so the more rewards, in the form of coins, they will get, increasing the supply. Second, according to the rules that each currency abides by, there is a specific amount of coins awarded to those in the network who perform the validation of the transactions (Evans, D.S., 2014).

For some of these currencies the rules impose an upper limit to the supply of coins. Bitcoin belongs to a type of currency that defines this limit to 21 million coins, while the rate of supply of Bitcoins is defined by an algorithm. After all 21 million Bitcoins are in circulation, no more coins can be awarded to the miners. Nevertheless Bitcoin can be divided down to eight decimal places [37]. Other currencies choose a different path. For example, Dogecoin is one of the currencies which doesn't define a limit for the number of coins in circulation but increases the limit at a steady rate. The rules for the supply of coins for each digital currency is predefined from the start and cannot be changed later on by anyone (Evans, D.S., 2014).
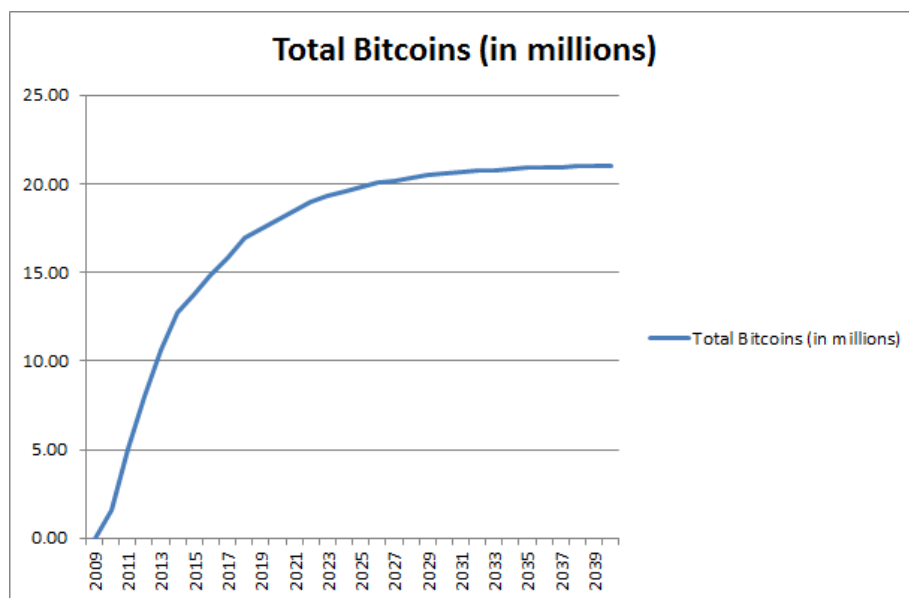

Figure 21: Bitcoin's supply curve [38]

Since Bitcoin is not a regulated "currency" what defines its value is mainly the expectations regarding demand and supply, which are one of the main determinant factors according to the theory presented in the previous chapter. While demand is dependent on the demand for coins in order to transact in the market, supply is dependent on the stock of Bitcoins and on the circulation of new coins in the system until it reaches the barrier of 21 million. Demand could change for a number of reasons that might have to do with the Bitcoin platform itself, competitive currencies or conditions of different markets (for example, the financial crisis in Cyprus which caused an increase in the demand for Bitcoins [39])

This mechanism makes Bitcoin susceptible to fluctuations of its value and gives a degree of high volatility. This might affect a more extended adoption of Bitcoin since it causes instability to its value, which a lot of people will see as a risky investment (Evans, D.S., 2014).

Adjusting the supply of money is one of the main mechanisms national banks use in order to control an unstable national currency (Evans, D.S., 2014). With Bitcoin this is impossible, which means that if supply is not adjusted according to the demand for a currency, its value will remain unstable.

Expectations about a currency or an asset are always influenced by speculation (Feiger, G., 1976). Bitcoin is no exception to that. Since Bitcoin has no real value (as gold or other valuable assets) it is highly susceptible to speculation that could infer major changes to the value of the virtual currency.

The case of Cyprus:

To indicate the importance of expectations as the major factor that influences the demand for Bitcoin, the Cypriot banks' bailout in 2013 is an exceptional example that proves it.

In March 2013, the financial crisis led Cyprus' leaders to consider using part of its people's bank deposits in order to bail the Cypriot banks out. Facing the risk of a banking system failure, investors started showing mistrust to national banking systems. At the time, Bitcoin was a new currency that, only three years previously to that event, was worth 5 cents and $47 before the bailout discussion started [39].

Figure 22: Value of 1 BTC in $USD from 2010 to the Cyprus Banks bailout in 2013. Source: money.cnn.com [39]

Since the discussions for the EU and IMF bailout of the Cypriot banks began [40], in order to avoid the country's banking system default, there was a rise of 87% in the value of Bitcoin, reaching $88 right after the bailout, at the end of March 2013. At the same time the number of transactions also surged within the same period [39].In conclusion, at times of financial stress investors turned their trust from traditional banking systems to an alternative choice.

In the meantime, grabbing the opportunity from this event, an entrepreneur announced his hope to install the first Bitcoin ATM in Cyprus, to announce a couple of months later that he would withdraw from the project [41]. Nevertheless, this indicated the importance that Bitcoin acquired after the existing traditional monetary system failed to inspire trust in people.

Bitcoin Demand from the beginning till today:

Bitcoin is a new currency counting almost 5 years of life. Yet the fluctuations of its price over the years have been immense. One example that illustrates this better than charts and numbers themselves is the case of a programmer from Florida, named Laszlo Hanyecz, who back in 2010 had mined 10000 Bitcoins, which he exchanged for two pizzas [42]. The interesting fact is that in 2013, when Bitcoin's price spiked to $1200 those Bitcoins spent for two pizzas would be worth $12 million. Even today, after Bitcoin's price dropped significantly when the Chinese government banned financial institutions from transacting in Bitcoin [23] and after the closedown of

Tokyo based exchange MtGox, the Bitcoins used to buy these two pizzas would be worth $4,5 million.
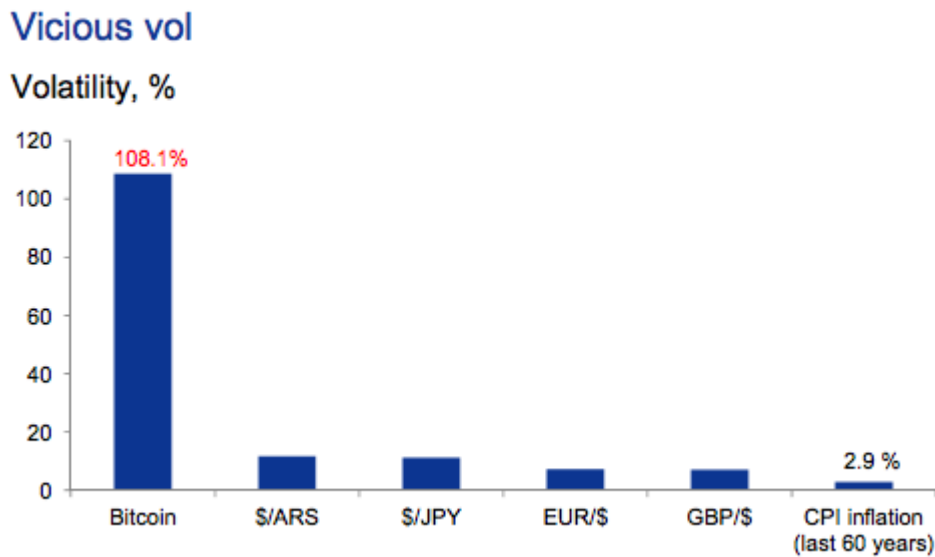
Figure 23: Bitcoin's volatility compared to other traditional currencies. Source: businessinsider.com [43]

Bitcoin might not be a traditional currency and for that reason it might be a volatile and risky investment, but its demand keeps growing and people are putting more trust in this new currency. The more the Bitcoin network grows and the more people use it, it gains more and more value, although that depends highly on the expectations for the future.

4.1.3   The need for Innovation in the Bitcoin Network

Innovation in our analytical framework is driven both by demand and supply and by the users and services. The more the Bitcoin network and infrastructure grows the more opportunities there are to newcomers bringing new Bitcoin-related services and profit from an expanding market. Not that they are the only aspects influencing the need for innovation but they are important nevertheless.

4.1.3.1 Types Of Innovation

Bitcoin brought something really new and disruptive to the currency market, and it wasn't as much in the technology, because peer-to-peer technology was already very common and successful in other applications, like file-sharing networks, Instant messaging systems, online chat networks, etc. In fact the disruptive part from Bitcoin is its decentralization and the fact that it isn't controlled by any entity making it

possible this way for the community to decide what to do with the future of Bitcoin. And the possibilities that come with an open community of contributors help with its development.

When compared with other virtual currencies, Bitcoin can also be considered as a sustaining development because it didn't bring something really different from other virtual currencies, like the already described linden dollars from second life. But still its decentralized and open nature were revolutionary.

In addition, the Bitcoin platform uses a chain of blocks in order to keep a public record of the Bitcoin transactions and so allow to assign the different addresses to the correspondent balance (Nakamoto, S., 2008). This was a new addition to the peer-to-peer technology.

In their webpage Bitcoin describes their innovation as "The Bitcoin protocol is not just about sending money from A to B. It has many features and opens many possibilities that the community is still exploring. Here are some of the technologies currently being researched and in some cases, turned into real products and services. The most interesting uses of Bitcoin are probably still to be discovered" [44].
Some of those technologies are:

- **Control against fraud** - Bitcoins are impossible to counterfeit and the system protects from common frauds like chargebacks or unwanted charges.
- **Global accessibility** - "Bitcoin allows any bank, business or individual to securely send and receive payments anywhere at any time, with or without a bank account." [44]
- **Cost efficiency** - Bitcoin transaction fees are much cheaper than any alternative and use cryptography, making it possible for secure payments to be conducted without slow and expensive middlemen.
- **Tips and donations** -Bitcoin is a good solution for tips and donations because sending a tip only requires one click and receiving donations can be done by displaying a QR code with the receiver address.
- **Crowdfunding** - One interesting implementation from Bitcoin is its application in crowdfunding. People can pledge money to a campaign and the Bitcoins will only be taken if the conditions of the campaign are fulfilled.

- **Micropayments –** Bitcoin can process payments as small as one dollar and soon even smaller, and is efficient enough to enable services that are paid per second, like a phone call or a radio paid for the exact usage in seconds.

- **Dispute mediation** - It's possible for a third party to accept or deny a transaction in case of disagreement between the parties.

- **Multi-signature accounts** - Bitcoin wallets allow multiple signatures. This would allow for example one company with several shareholders to have to sign to one payment be done and this way not allow one individual to use the assets alone.

- **Trust and integrity** - Bitcoin nature could help people trust the banks because it isn't allowed to do some of the actions of fraudulent banks are used to, like selective accounting transparency, digital contracts and irreversible transactions.

- **Resilience and decentralization** - Because of its high degree of decentralization, Bitcoin created a very resilient and redundant network. This network is able to handle millions of dollars in trades without requiring military protection.

- **Flexible transparency** - Although the identity from the users is private by default, the transactions are public and transparent. This allows the users to have flexible transparency rules.

- **Automated solutions** - Automated services suffer from the cost of the credit cards, Bitcoin could be used in a new type of machines like vending machines, coffee machines etc. cutting their operating costs.

The possibilities are only limited by the imagination of developers and the critic of the rest of the community.

4.1.3.2 Development

These innovations that Bitcoin brought to the table were initiated by Nakamoto, but they were improved by the community like mentioned before. At the moment this project is being written there are eight core Bitcoin developers and two hundred and one Bitcoin Core contributors [45].

Some of the developers have hundreds or commitments but most of them have one or two.

Bitcoin Core contributors

(Ordered by number of commits)

laanwj (1611)	Gavin Andresen (1015)	sipa (615)	Diapolo (447)	TheBlueMatt (212)
gmaxwell (133)	luke-jr (120)	jgarzik (87)	fanquake (40)	muggenhor (34)
cozz (31)	petertodd (30)	CodeShark (27)	jonasschnelli (22)	dooglus (20)
Michagogo (19)	rebroad (16)	xanatos (14)	super3 (14)	wtogami (12)
codler (10)	wizeman (10)	jordanlewis (8)	joshtriplett (8)	devrandom (8)
Nils Schneider (7)	freewil (7)	celil-kj (7)	roques (7)	mikehearn (7)
sje397 (7)	mgiuca (6)	Matoking (6)	vegard (6)	p2k (6)
forrestv (6)	jrmithdobbs (6)	runeksvendsen (6)	dertin (6)	JoelKatz (6)
r000n (5)	vinniefalco (5)	fcicq (5)	robbak (5)	mndrix (5)
alexanderkjeldaas (5)	brandondahler (4)	paraipan (4)	EricJ2190 (4)	jayschwa (4)
kdomanski (4)	paveljanik (4)	vsrinivas (4)	globalcitizen (4)	grimd34th (4)
mibe (4)	ldenman (3)	maraoz (3)	tholenst (3)	gubatron (3)
pstratem (3)	al42and (3)	colindean (2)	cbeams (2)	cdhowie (2)

Figure 24: Bitcoin contributors. Source: Bitcoin.org [45]

Being a developer for Bitcoin the community has to learn how Bitcoin works and all the material necessary is public in their development page [46].

The development process for new innovations uses five stages:

- First the developers work in their own branches until they think their improvement is ready. In this phase they share and test each other's patches.
- When they think it's ready they submit to Github and post a message in the development forum.
- If there is consensus that the new patch is safe, useful, well written, match coding style, then the new code is merged into the 'master' branch.
- Bitcoin is regularly tested passing for 4 phases "release candidate" and then the official, stable, released Bitcoin.
- After being accepted bug fixes are merged or backported into the current stable branch.

This process is only possible by the usage of github and sourceforge where all information related to Bitcoin is stored. This process is improving Bitcoin but people starting using Bitcoin is another thing and mailing lists and communities of developers can't go so far alone. So it is important to study the process of diffusion of innovation.

4.1.3.3 Diffusion

In terms of diffusion the Bitcoin number of users has been growing very fast and doesn't seem to be affected by the devaluation from the currency. This can be seen very easily in the image below.
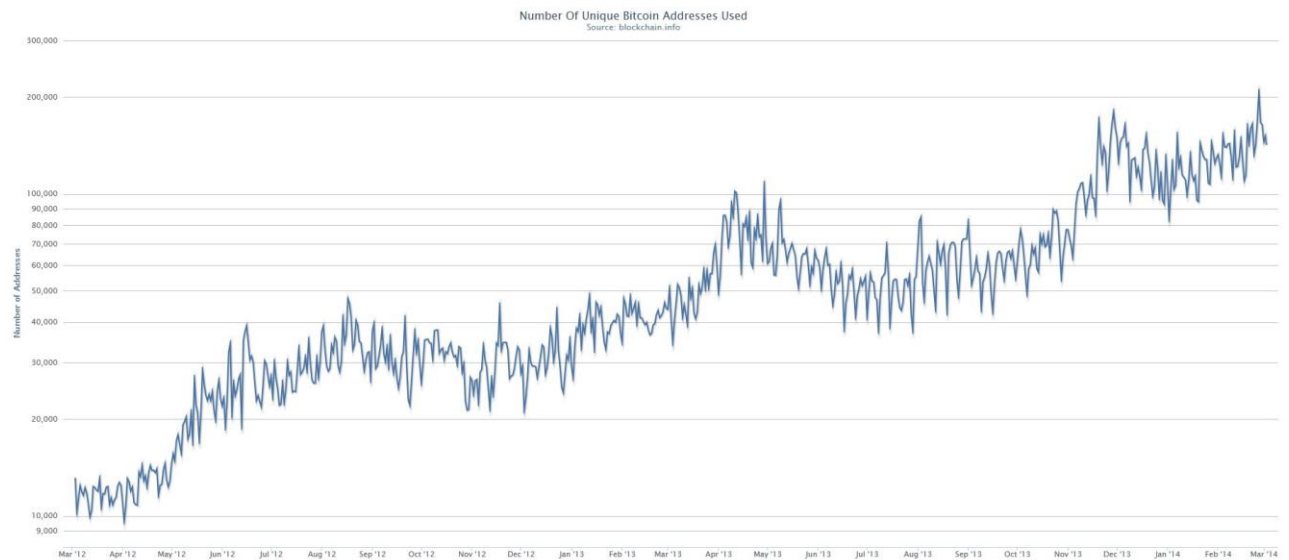
Figure 25: Number of unique Bitcoin addresses used. Source: cryptocoinsnews.com [47]

In 2011 there were roughly 10.000 people using Bitcoin daily. Nowadays there are around 200.000 people's unique addresses connected to it. This means that Bitcoin is diffusing very fast, but put in perspective next to the cell phone or the internet itself it isn't so fast.

So if this virtual currency is so disruptive and so innovative why isn't it being faster in its diffusion process and why aren't there more people using it?

At the moment, the number of Bitcoin wallets in use are about 1.6 million [48], a number which is very small compared to 2.9 billion internet users globally [49] and the 7.2 billion people on earth [50]. This means that according to Roger's model about the diffusion of innovation that was analyzed in the previous chapter, and these

numbers, Bitcoin is still not adopted by the early majority and it is only diffused in the group of innovators (figure below).

Figure 26: Bitcoin diffused in the group of innovators [51].
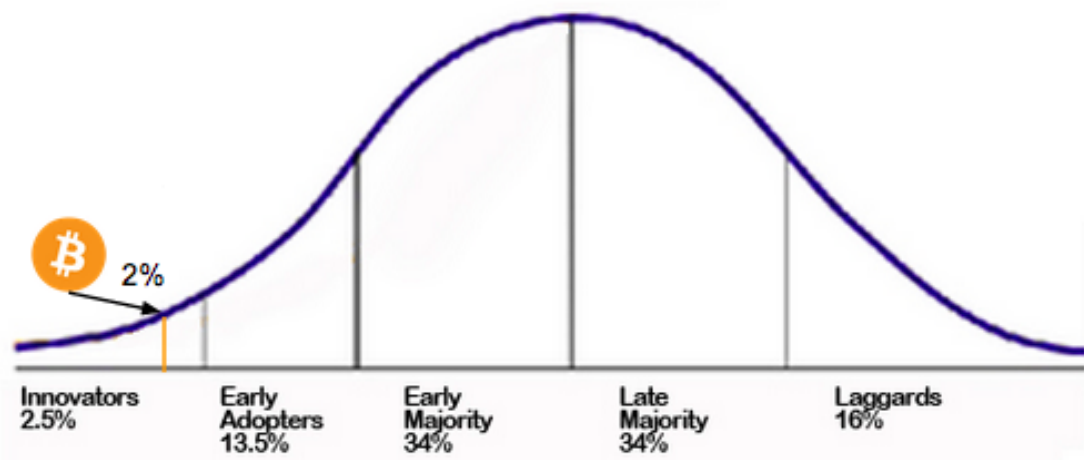
Well the answer to why aren't more people using Bitcoin isn't so easy. Our survey results taken from the academic community of our University, show that most of the people, at least in an academic environment, know about Bitcoin. In our study 85% of the people that answered our survey knew about Bitcoin, but from that 85% of people that knew about Bitcoin only 9% ever used it and only 1 or 2 % were using it frequently. Comparing to another survey conducted by GfK and reported by the Wall Street Journal, 76% of Americans are not familiar with Bitcoin [52]. The results are contradicting and so these numbers cannot provide a definite conclusion about who the Bitcoin users are.

To answer this question and to understand what is delaying the growth of Bitcoin, it is important to use Roger's five factors that influence each individual's decision to adopt or reject a new technology.

Relative advantage

In our survey the people that use Bitcoin say that it is good for investing, simple, fast, almost free and untraceable. In our interview with Cláudio Castro, the industrial designer that developed the hardware for the Lamassu ATM machine, told us that he had never used Bitcoin before but now he is using BitPay to receive payments from Lamassu and it is working even better than before, when he was being paid in bank transactions. In beginning he was a little concerned about using it but later on all went well. This relative advantage, of course is not always obvious to people that are not involved in business transactions (merchants etc.) or users of

online services. This is also connected to the other factor from the Roger's theory; the triability.

Trialability

"Degree to which an innovation may be experimented with on a limited basis"(Rogers, E.M., 2003).This means that it will be faster for an innovation to be adopted if users can try it out. A Bitcoin wallet is easy to acquire, transactions can be done for even a small amount of money, users can have many different wallets and buy, send or mine Bitcoins with processes similar to online banking (Byrne, A., 2014). This means that a trial phase for Bitcoin can be easily done, by people who are familiar with online services.

Other parts of the population though, that are not technologically literate or are reluctant to new technologies/services might find it hard to try it out. In addition, in order to try using Bitcoin, people need to actually invest an amount of money, which can be discouraging in the trialability phase.

In a survey done by coindesk.com with 200 answers of merchants, they answered 97% that they are satisfied with Bitcoin and they recommend it to their peers [53].This survey shows that trialability is one of the bottlenecks from the diffusion of Bitcoin and the word of mouth plays here an important role in the growth of the Bitcoin ecosystem.

Compatibility

"Degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters" (Rogers, E.M, 2003). On the one side, Bitcoin is accompanied by services that try to make it resemble the current system. For example, the Bitcoin ATMs and services like BitPay (a service that resembles PayPal) are trying to facilitate the use of Bitcoin and make it acceptable by people. Also the potential adopters are mainly people that seek anonymity.

Nevertheless the "inconsistency" that Bitcoin presents to the traditional monetary system, which means the fact that it is not mediated, regulated or controlled by any financial institution as well as the lack of regulation, is another factor that hinders its diffusion as some people won't find it easy to trust.

Complexity or simplicity

"The degree to which an innovation is perceived as difficult to understand and use" (Rogers, E.M., 2003). The fact that Bitcoin originated from the online community and the internet, might be discouraging for some people to use it, either because they are not comfortable with online platforms and services or because they don't trust online services when it comes to transacting money. Transacting with Bitcoin today, is as simple as online banking, although as mentioned before there are parts of the population that either don't know how to use, or don't want to use such services, which hinders the diffusion of Bitcoin even more.

Nevertheless, in 2012 423.5 million people accessed online banking sites [54], which means that even among people that use such services Bitcoin is not yet diffused.

Observability

"Degree to which the results of an innovation are visible to others" (Rogers, E.M., 2003) Bitcoin is more and more discussed in the media and especially among the technical communities. Google returns 39 million results when one searches the word Bitcoin. Our survey results confirm that most people that knew about Bitcoin, learned about it from the different media (TV, newspapers etc.) rather than from the academic community. This means that Bitcoin is attracting attention but still the people that know about it are few, as discussed before At the same time, Bitcoin communities in cities around the world organize events, which they advertise through social networks etc. which also help people get to know about Bitcoin.

One important factor that is helping the diffusion of Bitcoin is the convergence of services and technologies and this convergence is being fueled mainly by innovation but also by the need to solve the problems and misconceptions of the Bitcoin network, like the period of time that one transaction takes to be processed or the problems with security in the end nodes.

4.1.4 The role of Network Effects and Lock-in in Bitcoin

Central Banks have well defined tools for controlling the monetary system around the world. On the contrary Bitcoin doesn't have such tools. It has a peer-to-peer distributed network in which a "virtual currency" is transmitted from one peer to another. However, Bitcoin benefits from network externalities that increase its

popularity and the utility that users receive from being part of this virtual network. These externalities get stronger from the innovative Bitcoin services such as BitPay, Lamassu ATMs and so on.

Since Bitcoin was created in January 3, 2009 nobody knew what it was and how it worked. At that point Bitcoin was growing slowly until the first time it was used by Laszlo Hanyecz, who paid 10.000 BTC for a pizza(Taylor, 2013). After that, the utility of Bitcoin was proven as a means of exchange.

Bitcoin's value, as discussed before, is highly dependent on demand and people's expectations about its value in the future. When demand for Bitcoin grows, thus its network of users grows, so does its value, which increases utility for its users.

Like shown in the innovation chapter the innovators were the first group to become aware of Bitcoin, and since there are only still now a days 1.6 million users [48] the diffusion is still at that point. In our survey done with people from the AAU Students community it showed that that 65% of people became aware of Bitcoin from places as newspaper, TV, social media. Also like explained before the first step to generate growth in the network is to people know about it.

After this initial period of Bitcoin being considered a novelty, the open source community joined in and several services started being created that facilitated Bitcoin transactions, like exchange platforms, virtual wallets, electronic payment services etc. All these complementary services brought more value to the network, thus strengthening the indirect network effects that stem from the growing usage of such complementary products and services and triggering even more innovation.

This open source community is comprised of developers. Each time a new one joins the community they bring new ideas and solutions to the problems that network has. Sometimes they present solutions with complementary services like explained before, but others times they improve the Bitcoin network itself with new code. When they work on a new version of Bitcoin, they generate direct network effect.

The active nodes also contribute with direct network effect, because they store the information related to transactions, which protects the network from losing the public ledger and from 51% attack what were presented in the security part, so since new wallets bring more security to the network it brings some positive direct network effect.

In our interview with Claudio Castro, the designer of the Lamassu ATM, when he is asked "Do you think that investing in Bitcoin is safe for a company?" his answer

was that besides the initial concerns, all worked well and the fact the he's paying much less fees allows for more profitability. This shows that even manufacturers, like Claudio's company, the network effect is present and is driving the diffusion of Bitcoin worldwide.

Another effect that is being generated by the Bitcoin network in this manufacturing business strategy works as a lock-in effect, because it gives them more profitability and since business seek profitability, it is hard for them to go back to less profitable methods.

But the network effect is not only creating lock-in for manufacturers and retailers. Also speculators and investors are benefiting from the volatility of Bitcoin and so they are also subject to lock-in effect, because if they stock up bigger quantities of Bitcoin than they can easily sell due to low market liquidity they are locked in. This is not a strong type of lock-in but it exists. There are also negative network effects. The more users that are active (that is users trading Bitcoins) in the network, there is an increase in the traffic and the space needed to the public ledger.

People's expectations about Bitcoin can also be the reason for the creation of Lock-in effect, because, since Bitcoin supply is limited, as more people join the network, they expect that the price of Bitcoin will go up and so they are reluctant to spend their coins.

All these theories about demand and supply, innovation, network effect and lock-in drive the need for more convergence. As such, in the next chapter convergence will be analyzed.

4.1.5   The role of Convergence in the Bitcoin Network

The convergence in Bitcoin started with the Bitcoin creation itself but is being fueled every day by all the stakeholders needs in the Bitcoin ecosystem. This convergence of services and technologies is very active and relevant. Services like BitPay and Lamassu ATM's are changing Bitcoin and solve some of the diffusion problems like Complexity, Compatibility and showing the relative advantage from using them in comparison with the traditional payment systems.

The convergence of the Bitcoin transaction and payment services, with those of their main competitor, the banks, is unlikely to happen anytime soon and this can also be seen by the reaction of the players in the Bitcoin industry when Zach Harvey,

co-founder of Lamassu, was asked why their ATM only accepts notes and not credit cards or debit, his answer was "I didn't want to have to deal with banks" [55].

The banking industry is interesting, but like mentioned in the delimitations, it won't be analyzed or discussed in this project. The rest of the chapter will talk about the new services that were created recently and the drivers that are pushing for convergence.

4.1.5.1 New Services

There are many important services that try to make the ecosystem of Bitcoin simpler and more meaningful. But because there are always some holes in any system, innovation is constant in order to solve the problems that appear with the growth of the Bitcoin network.

One the major constraints in the Bitcoin world was how to buy Bitcoins physically and companies like Robocoin, Coin Plug, Bit Access, Lamassu, etc. answered the call and created ATM machines for people to buy Bitcoins.

Lamassu

Lamassu, Inc. is a company that developed the first Bitcoin ATM machine from scratch and for this project the authors had the opportunity to interview the man behind "the design of the physical machine the hardware part". From this interview it is possible to get a picture of the competitive advantages from this machine compared to the competition. It is the most secure machine in the market in terms of robustness because it has a very strong vault, the price is very good compared to their competitor's. Lamassu machine cost 5500 dollars where their main competitor's, Robocoin, will cost 20,000 dollars [56].

Figure 27: The LamassuBitcoin ATM [35]

The only drawbacks from Lamassu ATM are that for now it works only one way. You can't sell Bitcoins in this ATM, you can only buy them and only in cash.

The movement generated by this company and others is helping the creation of new businesses, like Claudio Castro told us in his interview. The main clients for these machines are startups and at the point of our interview "170 machines had been shipped and 230 had been produced". These numbers, while small for the global market, show that there is a huge potential for this market.

The startups that are buying these machines are using them in a similar way that the vending machines companies do. They place them in Bars, Cafes and other places, make an agreement with the owner to pay or share profit and make money the same way Forex (Foreign exchange market) companies do. Putting a rate on top of the Bitcoin value. The other clients are bars and cafes that make money the same way but also allow the users to pay them in Bitcoin avoiding this way the transaction fees.

Also another indicator for the potential of this market is the return of investment that the buyers of these machines are having. Claudio also told us that "In some cases the clients would break even and making profit just in one year with the machines." It is expected that this market will keep on moving forward and Lamassu as a first mover and with high quality, can grab a good share of the ATM market.

But ATMs aren't the only innovative and revolutionary systems that are helping propel Bitcoin. The payment systems are also helping a lot. In our interview

Claudio told us how he went from being unfamiliar with Bitcoin, himself, he became very fast and easily a user of Bitcoin and BitPay.

To our question "Do you think that investing in Bitcoin is safe for a company?" Claudio's answer was "yes, now more and more. I was also concerned about using Bitcoin in beginning, I have a company and I can't pay my taxes in Bitcoin. I didn't know much about Bitcoin before but then I researched and read a lot about it and in the end it worked really well for me and my company. With services like BitPay every company can use it and it is even better because it has much less fees. All worked fine and now I like using Bitcoin."

BitPay

BitPay Inc is in their words "an electronic payment processing system for the Bitcoin currency. We enable online merchants to accept Bitcoins, as a form of payment, just as they accept payments from Visa, Mastercard, or PayPal." [57]

So BitPay is a service for merchants that has some very strong advantages. In the beginning they used a transaction fee of 0.99% in any transaction, which is less than most other payment systems charge, but now they changed this model to a monthly subscription for every merchant that starts from 30$ a month and without any transaction fees [58].

Also the major headaches for online merchants is the charge backs and the loss of information of clients and BitPay resolves both. First there are no charge backs. Only the merchant sends the money back if he wants to and BitPay doesn't need personal info from the clients to send the money, so an embarrassing problem is avoided [59].

Figure 28: The Bitcoin App [60]

BitPay also allows companies to pay to each other using their platform and at the both ends the deal is made in traditional currencies. They just use the platform to make the transfer cheaper [61].

All this convergence has some drivers that make it go faster and wider.

4.1.5.2 Drivers

The first driver of convergence in Bitcoin case was and is innovation and this driver is analyzed in chapter 4.1.3.

But there was another important driver for Bitcoin, and it was the lack of regulation. The way the currency was developed using peer to peer and decentralized makes it very difficult to regulate.

The first moves for regulating this market are being made right now and this will be further discussed in the discussion but the fact that there weren't any limitations to the creation of a virtual currency helped a lot with the conception of Bitcoin. But nowadays it might need some regulation to reduce people's insecurities about Bitcoin [62].

4.2 Analytical overview

The purpose of this subchapter is to summarize all of the above and at the same time connect them all together in a way that explains the interrelations that were presented in the analytical framework used in the beginning of 4.1.

In this framework, there is what seems to be a cycle that begins from the vital part of Bitcoin, which the network and the services and users around it. The growth of this network is fuelled by this cycle, which includes the demand and supply of Bitcoin, the innovation process and its diffusion, as well as the network effects and lock-in that it is subject to. The convergence of the different technologies and services that stem from this cycle is also included in this framework as an important result from the growth of Bitcoin and the innovations it brought along.

Bitcoin counts only a few years of life, which means that it is not yet in a mature phase and its diffusion process is difficult and at a very early stage. With a supply dictated by its algorithm, an upper limit that will be reached in a few years, and no governmental or authoritative control over it, Bitcoin's value presents a volatile behaviour.

Demand also affects its price and it causes fluctuations according to users' expectations and speculation in the market, with the example of Cyprus proving this. At the same time lack of regulation by local governments, creates uncertainty about its legality but at the same time becomes a driver for convergence. Demand can also be affected in a negative way, due to security concerns for instance, as explained in the previous chapters through our desktop research and survey results.

Despite the price fluctuations, Bitcoin's value has exploded since its creation, which attracts attention for investors that see it as an opportunity to bypass the current banking system, which the last few years has had problems in most countries in the world. This way demand is growing and more people use Bitcoin. This growing demand is an opportunity for new people with innovative ideas to create products and services that will facilitate Bitcoin transactions (e.g. Bitcoin ATMs, BitPay etc.). By making transactions simpler and Bitcoin more accessible to everyone, more people can join the network.

The innovative aspect of Bitcoin can be looked at from a technological and a financial point of view. Bitcoin itself brought some sustaining innovations to the peer-to-peer technology as far as virtual currencies are concerned but it was disruptive to

the financial system, as a substitute for traditional currencies that doesn't need any central authority to operate and it's the network itself that is the heart of the system. The innovative products and services that were created around Bitcoin, were not disruptive but mashed together services and products that complement Bitcoin's use as a currency.

The degree to which these innovations are diffused in the market depends on many factors. Bitcoin itself is still at a very initial stage of diffusion and subsequently the products and services around follow the same course.

Through demand and innovation, there is a growing network being created. A network which is subject to network effects, as the more people join it, the more value it has for its users. No currency, virtual or not, has any value unless people use it. And the bigger the number of people that use it, the more powerful it becomes. The American dollar for example has been for years the currency that world trade was being conducted in. Its importance was based on the fact that everybody wants to transact in American dollars. The same effect applies to virtual currencies like Bitcoin.

At the same time, when a currency or asset becomes powerful and has value it creates lock-in effect, as people will possibly become reluctant to spend it or sell it, if they expect it to grow in the coming years.

And on goes the cycle making Bitcoin and its network grow in value and importance, whether at a fast or slow pace. In all this process one can recognise how technologies and services are converge. Starting from Bitcoin itself, a technology is used as a form of currency that can substitute traditional currencies.

The traditional concept of an ATM was also changed with the creation of Bitcoin ATMs, which allow you to use real currencies to buy Bitcoins or take out real money in exchange for Bitcoins. The concept of a wallet was also turned into digital form that stores our virtual money and allows us to transact in it. The possibilities are endless, when it comes to what innovators can do, which means that convergence is present in every aspect of it.

Bitcoin is a relatively new virtual currency and as such it has a long way to go before it is well-known and widely accepted. The environment of uncertainty created around it has drawn governments' attention, which means that the regulatory issues about Bitcoin are an important aspect of it nowadays.

The future of Bitcoin and the trends to follow are going to be discussed in the next chapter where the analysis done previously will help us identify how Bitcoin can evolve in the years to come.

5   Discussion

In this chapter there will be a general discussion about virtual currencies, which will be based on the analysis made for our case study, Bitcoin. This discussion will attempt to look into the reasons for the creation of virtual currencies and their growing popularity, as well as compare the ones with the biggest market share. Next we will try to find out the future trends regarding virtual currencies and more specifically we're going to look into the peer-to-peer virtual currencies popularity.

In the chapter there will also be a discussion about the regulation trends that the Bitcoin currency faces and to finalize there will be a discussion on whether Bitcoin is turning to be a standard or the market is diverging from forming standards.

5.1   Peer-to-peer currencies popularity - Front runner discussion

The number of peer-to-peer currencies is growing very fast during the research and writing of this project. More than 50 currencies were added to coinmarketcap.com, a webpage that tries to track the current value for all the virtual currencies being traded. When this project was initiated they were around 240 and now a few months later there are 290 and it is very likely that this number will keep on growing [63].

The table that appears next was updated with the information collected on May 25th of 2014 at 11:30 AM UTC. The information shown in the table, especially the value of the currencies, as well as their position relative to each other, will be constantly changing. A bigger version of this table can be found in the appendix.

Table 1: Comparative table of the frontrunner virtual currencies

Peer to Peer Currencies	Year of Foundation	MarketCap	Price	Market Share	Mining	Open Source	Limited supply	Related to Bitcoin
Bitcoin	2009	$7,220,760,389.00	$563.52	91.44%	yes	yes	21 million	yes
LiteCoin	2011	$329,061,745.00	$11.48	4.17%	yes	yes	84 million	yes
DarkCoin	2014	$62,750,897.00	$14.51	0.79%	yes	yes	22 million	yes
PeerCoin	2012	$51,980,535.00	$2.43	0.66%	yes	yes	no	yes
Nxt	2013	$38,612,625.00	$0.0386	0.49%	no	yes	1 billion	no
DogeCoin	2013	$33,919,380.00	$0.0004	0.43%	yes	yes	no	yes
Ripple	2013	$28,510,076.00	$0.0036	0.36%	no	yes	100 billion	no
NameCoin	2011	$23,314,310.00	$2.63	0.30%	yes	yes	21 million	yes
MasterCoin	2013	$16,197,063.00	$28.76	0.21%	no	yes	619.478,6	yes
BlackCoin	2014	$11,019,329.00	$0.15	0.14%	yes	yes	no	yes

During the time this project was developed many currencies passed by the top 10 in terms of Market Cap. When the last information was collected, all the peer-to-peer currencies combined had a market cap of 7.9 billion dollars and Bitcoin would account for almost 92% of that. Although this is true the first two currencies (Bitcoin

and LiteCoin) have been the front runners since their creation and no currency yet was able to challenge them.

LiteCoin currency was created from a fork of Bitcoin. It is limited at 84 million coins exactly, which is 4 times the amount of Bitcoin. The reason it was created was to be faster and more efficient than Bitcoin. Its algorithm is capable of handling more transactions than Bitcoin because its blockchain is more frequent. LiteCoin was designed to be a complementary coin to the Bitcoin ecosystem.

The third coin in the list is Darkcoin, which was created at 18 March 2014 and is already third in market value. This project was focused in the security part, the main difference with Bitcoin being that the users can choose to make the transactions public or not and the last ones won't be stored in the public ledger, like in the Bitcoin case. Maximum number of coins is 22 million (Duffield, E., et al., 2014).

The next peer to peer currency is PeerCoin, focused in solving some of the flaws of Bitcoin, one of them being the 51% attack, where one large entity or a government holds 51% of the network being able to disrupt the network. This is because Peercoin moved the security from the network to the client side. In order to perform the same attack the entity would have to hold 51% of the coins, which is infinitely more expensive than in the Bitcoin case, because this type of attack would raise the prices massively and then disrupt the network and cost a lot to the attacker. Many currencies claim that Bitcoin takes too much processing power and because of that spends too much energy. One of the cases is PeerCoin. PeerCoin doesn't have a limit for the number of coins that will be generated. In the code it is defined that it can reach 2 billion coins but that can change and at the current rate of growth it will take hundreds of years to reach that (King, S. et al., 2012).

Next comes NXT and it is the only one that is 100% different from Bitcoin. NXT can't be mined. Instead they call it forging; this process is requires less computing power and there is no need to use special hardware to do it. Forging doesn't create new NXTs. Instead users receive a part of the transaction fee for helping the network with processing. All the 1 billion NXTs were generated in the genesis of the code and they were given to the stakeholders that invested Bitcoins in the beginning. This currency also allows for data to be sent, not only currency [64].

The sixth currency in the list is DogeCoin, which started as a joke but grew to become a serious currency. There is no limit to how many coins can be generated which puts DogeCoin in the same league as a normal inflationary currency. By the

end of 2014 there should be 100 billion DogeCoins out there. DogeCoin is also more effective than Bitcoin by spending less processing power for mining it or transferring it [65].

The Ripple has a public ledger, like Bitcoin, with all the activity in the network. It works similarly to the email protocol and makes it easier for different users to send money to each other. The maximum supply is 100 billion that were pre-created and are now being distributed. There is a bridge between Ripple and the Bitcoin ecosystem. But although it is compatible with Bitcoin it has its own code and it isn't a fork from Bitcoin [66].

The next currency in the table is NameCoin, which was the first fork from Bitcoin. Similarly it is also limited at 21 million coins and it allows users to do merge mining, which means they can mine both Bitcoins and NameCoins at the same time. Also it created the first decentralised domain system the .bit [67].

The ninth currency in the list is MasterCoin. The protocol of MasterCoin is using the Bitcoin protocol to enable features like smart contracts and user-defined currencies without disrupting Bitcoin. MasterCoin is developing the concept of smart property to users by enabling them to not only trade coins but also properties. MasterCoin has very similar features with Bitcoin. For example, in the internet the applications use TCP/IP to communicate with each other and build on top of it new functionalities [68].

The last currency in the list is BlackCoin, a currency more efficient than Bitcoin, which will have only 1% yearly inflation and doesn't have a limit for how many coins will be created. Its creation is very recent so many details can only be seen by an analysis of its code [69].

From the study of these currencies it is possible to see that Bitcoin is without a doubt the main currency. Not only because it's 90% plus market share but also because most of the other peer-to-peer currencies were created based on Bitcoin. Also it is very interesting that although some of these currencies were created to compete with Bitcoin many of them, like MasterCoin, NameCoin, LiteCoin, etc. were created to complement Bitcoin and give a new array of services to the Bitcoin ecosystem.

It is also possible to see that there aren't close source currencies on the top ten and almost all of the currencies were created as a platform that companies and users can contribute and innovate. Many tools are being created around these currencies,

tools that are attracting innovators, investors, speculators. These tools are allowing new possibilities and the future is wide open.

5.2 Future trends

The idea of virtual currencies goes back to the 1990s. Since then, a lot has changed in the way that transactions are done. As technology advanced and more and more people acquired internet access, transactions became easier and faster, electronic payments grew and the use of credit and debit cards became the easy way to buy, without the use of cash or the physical presence of someone in a store. Transactions were facilitated through services offered by companies such as Visa or Mastercard, which allowed safe and instant exchange of money between people's bank accounts.

This globalized electronic payment system, though, took away an important characteristic that only paper money offered before; the user's privacy. Every credit or debit card, every bank account, every electronic transaction is related to people's personal details and recorded by their bank. At the same time transaction fees are charged for online transactions, which is another difference from paying with cash.

In a world where privacy and anonymity are no more taken for granted, virtual currencies, such as Bitcoin, came to change that. Based on a peer-to-peer decentralized network, they allow anonymous transactions, which are validated by the network itself and not by a central authority, with very low transaction fees and a public record of transactions that prevents double spending.

At the moment there are almost 300 different virtual currencies that are either an improvement to Bitcoin or independent technologies. Nevertheless none of them have reached Bitcoin in value or market share. And despite all the drawbacks or even misconceptions about virtual currencies, they seem to keep growing, indicating that virtual currencies are here to stay. At least for the time being. And since virtual currencies are not just in-game currencies that are used to only buy virtual goods anymore, but have actually the potential to become a substitute for real currencies and overcome national borders, it is expected that governments will have to take an official stance in the near future, especially as their usage grows.

5.2.1 Virtual Currencies and regulation

The more popular virtual currencies become, the more they attract the attention of countries and their central banks. Bitcoin and all virtual currencies are becoming by becoming a means of transaction have turned into part of the financial and trading system but without being controlled by it. It is too early to say that this might be threatening to banks or other financial institutions, since their diffusion in the market is at a very early stage, but if their popularity keeps growing, companies facilitating transactions, like Visa, as well as banks, could lose a significant amount of money since currencies like Bitcoin bypass the need for their services.

Moreover, governments are also not profiting, while Bitcoin remains unregulated. Also, it is necessary for them to make an official decision about Bitcoin or virtual currencies in general since that will clarify the situation about Bitcoin's legality, so that businesses and people can decide whether they will invest in it or not.
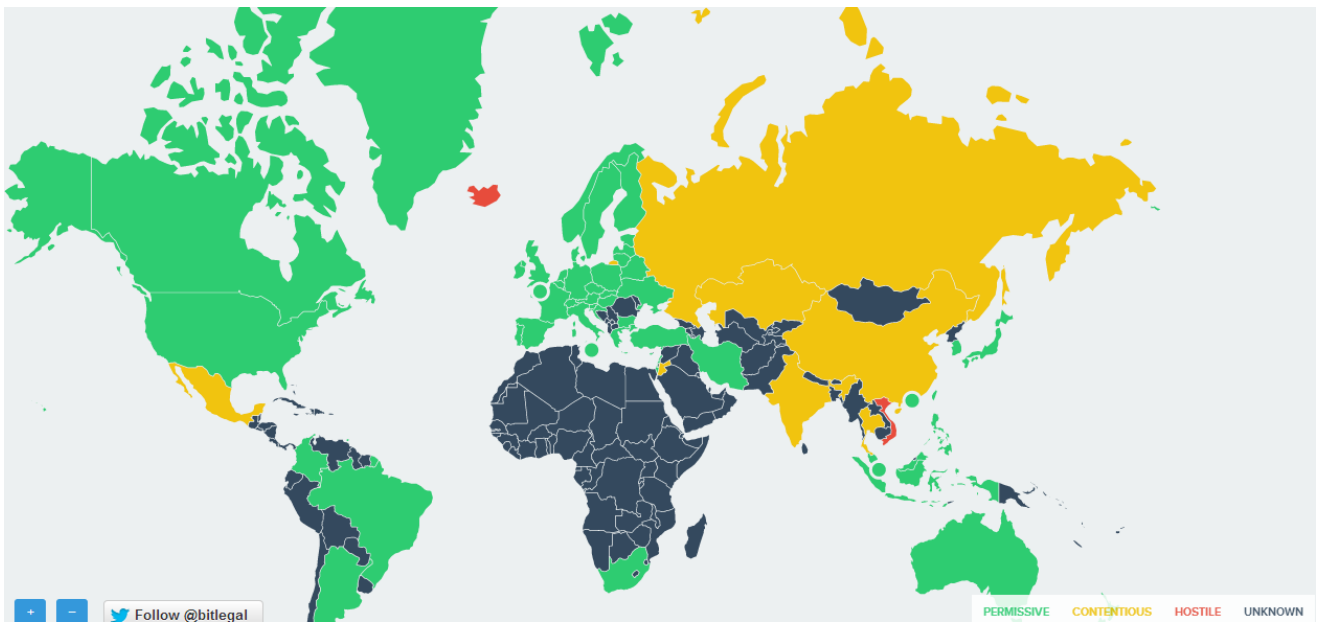

Figure 29: Regulation map for Bitcoin. Source: BitLegal.net [70]

So far, what seems to be the trend in terms of regulatory decisions is that most countries tend to allow Bitcoin's usage and exchange and some have also announced their intention to put taxes on it. Others, like China and Russia, want to put more strict regulations on it, although there are no official actions towards it yet. Finally very few, like Iceland and Vietnam, have a hostile stance against Bitcoin, banning it from financial transactions.

What seems to be the most possible scenario for the majority of countries, is that they will try to somehow integrate Bitcoin into the financial system, by calling it

an asset and possibly receive taxes on it. Depending of course on the national laws and financial systems, the exact legal framework that Bitcoin is going to be surrounded by, will be adjusted by each country separately and this might take time.

Nevertheless, regulatory decisions will affect Bitcoin to a great extent in the near future. Businesses that offer Bitcoin related services and products, not just in one country, will have to take seriously into consideration every decision that national governments make and adjust their products or services to them.

Finally, the regulations that apply to Bitcoin today or will apply in the future, are only restricted to this specific virtual currency. The cases of other virtual currencies will have to be examined thoroughly by governments, in order to become regulated, unless a complete legal framework about virtual currencies is created in each country.

5.3   Bitcoin: A Standard of virtual currencies?

Bitcoin counts only five years of life. And although it wasn't the first virtual currency created, since its creation, the number of virtual currencies has exploded, compared to the years prior to Bitcoin. Bitcoin can be called the most successful among the existing virtual currencies, both in terms of value and market share. At the moment its price is valued at $517,52, which is much more than the second in row, LiteCoin, with $11,05.
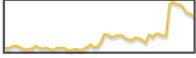
#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Market Cap Graph (7d)
1	Bitcoin	$ 6,628,556,816	$ 517.52	12,808,225 BTC	$ 30,880,677	-1.29 %	
2	Litecoin	$ 316,233,117	$ 11.05	28,623,804 LTC	$ 6,960,072	-3.76 %	
3	Darkcoin	$ 55,315,680	$ 12.80	4,320,135 DRK	$ 6,069,032	+2.76 %	
4	Peercoin	$ 48,249,347	$ 2.25	21,421,953 PPC	$ 513,949	-0.80 %	
5	Nxt	$ 36,144,942	$ 0.036145	999,997,096 NXT*	$ 125,019	-3.01 %	

Figure 30: Most valued virtual currencies 24/5/2014. Source: coimarketcap.com [63]

In addition, Bitcoin is the only virtual currency that is complemented by services such as Bitcoin ATMs and online payment platforms like BitPay and it is the

only one, which has attracted attention on government level and raised discussion for regulation.

Nevertheless, saying that Bitcoin is going to be the standard among other virtual currencies would be a hasty conclusion. It is true that Bitcoin has withstood many events that could have been the end of the currency; the shutdown of the exchange platform MtGox, China's decision to exclude it from transactions within financial institutions and many more. Its price went from $1200 to $400 and back up to $500, within weeks, but the Bitcoin community managed to keep the currency alive.

But whether Bitcoin will be the standard between virtual currencies and prevail or there will be a wide spread of virtual currencies in the future, is almost impossible to answer at the moment. The reasons for that vary.

First, Bitcoin's future will be to a great extent defined by what regulatory decisions will be made by the different governments. Some may recognize it as a currency, some others may reject it. Others might call it an asset and put taxes on it. Those decisions are important for the future of Bitcoin and the virtual currency market.

Second, Bitcoin, just like any other virtual currency, is not imposed by any national government, like national currencies are. This means that any negative effect on demand could lead Bitcoin to extinction. As demand is what makes Bitcoin valuable, any changes in people's expectations as well as speculation play a vital role to its survival in the future. Therefore it is difficult to say that Bitcoin will turn out to be the standard for virtual currencies, while all others will disappear.

Finally Bitcoin has roughly 90%, at the moment, of the virtual currencies market share in terms of value, and in a market that as no barriers of entrance and where all the rules from perfect competition can be applied, Bitcoin has the monopoly (if it was a company, since according to the Sherman Act (Sherman, 1890), companies that have more that 75% of the market share have the monopoly). But in the case of virtual currencies everything changes very fast, especially because there are no barriers of entrance.

Bitcoin's growth is important for its way to become a standard in the virtual currency market. But whether that will happen or not, is still too early to say and it depends on all the factors mentioned previously. The next few years will determine its future and prove whether the innovations it brought will change the scene to its favor.

6   Conclusion

In this chapter of the project all the analysis and discussion will come to a conclusion. The questions in the problem definition will be answered with the information gathered and discussed during the project.

It is also important to say that the ecosystem behind these currencies is very volatile and some of the conclusions can change with innovative or regulative steps taken from all the stakeholders, them being the developers of all the currencies, the governments and other institutions.

6.1   What are the main reasons for the monetized peer-to-peer virtual currencies' growing popularity?

Virtual currencies materialized new trend of innovative ideas that used technology and the Internet in order to satisfy users' need for online transactions of not just virtual but real products and services. With virtual currencies transactions can be done cross-border, without the implications of national governments and banks or intermediaries for online payments, like Visa and Mastercard. And so freedom of capital movement is enabled, although this can soon and easily change depending on each country's regulatory decisions.

But besides being able to transact without restrictions, another reason that virtual currencies have become appealing to people, and most importantly investors, is the low transactions fees they offer. So merchants, investors and even speculators can benefit from being able to bypass intermediaries and transact with the lowest cost possible.

Virtual currencies are also vulnerable to speculative moves, since their volatility offers a good opportunity for major profits for the speculators. This might also have negative effects on virtual currencies but speculation exists in a every financial system.

Another important aspect of our research that the users seem to care a lot about, is the privacy and security that these currencies give them. Virtual currencies offer anonymity and privacy features that are not available in online payment systems today. In the security section there were some problems in this area but for the most

part the Algorithm of Bitcoin has proven very resilient and so most of the new currencies use the code as their point of origin for their work.

Virtual currencies and especially Bitcoin have proven to be a way for investors to secure their money in times of financial stress, just like in the case of Cyprus which we studied in our analytical part, where the value of Bitcoin raised to double.

6.1.1 What are the reasons behind Bitcoin's supremacy to other peer-to-peer currencies (economic and technological perspective)?

There are many reasons for Bitcoin's relative success but when compared to the other virtual currencies Bitcoin has a very clear advantage, being the first comer in the peer-to-peer currencies market. The first mover advantage in the peer-to-peer virtual currency market can also be seen by the fact that Bitcoin is the first and has proven to be a reliable platform to other currencies and services to build upon and improve it.

The Cyprus case in 2013 helped validate Bitcoin as the frontrunner. At that point Bitcoin was seen as a profitable asset to invest the money that the banks were about to use for their needs. The first mover aspect played an important role because Bitcoin ecosystem had proven itself for four years its resilience and the investors saw the relative advantage to the other currencies that were less known and consequently less reliable, also the gold was that all time high and it also helped some investors to choose Bitcoin.

The rate of creation of new currencies is very high which is flooding the markets with innovative types of peer-to-peer coins, and takes time for new users to understand them all and make an educated decision. Bitcoin is a new currency itself and after its 5 years of existence it is still not widely adopted. This flood of new currencies that has been going on after Bitcoin is too premature yet and so it will take time before all these new currencies, or at least some of them, will start being used or invested in as much as Bitcoin.

6.2 What are the possible future trends regarding peer-to-peer virtual currencies?

The future of virtual currencies and the extent to which they will substitute for real currencies is still debatable, but some conclusions can be drawn from the

indications we have today. The volatility that virtual currencies appear to have makes it very hard to make predictions in the long run.

6.2.1 What are most important regulatory trends related to virtual currencies?

At the moment, the regulations existing in different parts of the world are only related to Bitcoin, since it is the most popular among virtual currencies. Governments all over the world are, in one way or another, trying to come up with regulatory acts, others more strict, others less, in order to clarify the situation about Bitcoin's legality and define whether Bitcoin is a currency or not.

The trends that seem to be appearing at the moment is that most countries have declared Bitcoin an asset and have announced that they will include it under tax law. None however, have recognized Bitcoin as a currency but they do recognize it as a substitute for real money. There are cases of countries whose stance against it is more hostile, banning it from transactions.

No matter what these regulations will be, it is certain that they will affect the future of Bitcoin and they will set the base for regulating all virtual currencies.

6.2.2 Is a standard being formed (Bitcoin), or is there a growing spread of virtual currencies being used?

In our last view over the market Bitcoin had more than 90% market share among all the peer-to-peer virtual currencies that exist. In itself it's a strong argument that Bitcoin is the standard right now but in the future it will be very hard to know if Bitcoin will sustain this place. Every week there are many newcomers and most of them don't have too much expression but there are others, like the case of DarkCoin, that is 2 months old and very similar to Bitcoin except it allows people to not publish their transaction in the public ledger giving this way much more privacy and making the currency much lighter in terms of harddrive space. The result was that in 2 months DarkCoin got to the third place in terms of marketshare and seems to keep on growing.

The volatility of those virtual currencies do not allow any definite conclusions about Bitcoin being the standard in the future but so far Bitcoin is the most important

player while it is complemented by many other services and products and has a strong community that supports it. Nevertheless, this can change in the future based on regulations, expectations about its value and many other factors, making it hard to predict the developments in this market.

7 References

Alcorn, T., Eagle, A., Sherbondy, E. (2013) *Legitimizing Bitcoin: Policy Recommendations*

Androulaki, E., Karame, G. O., Roeschlin, M., Sherer, T., Capkun, S.*Evaluating User Privacy in Bitcoin*

Braeutigam, R. (2010). *Microeconomics* (4th ed.).Wiley

Byrne, A., (2014), *Working Title: Diffusion of the Bitcoin Innovation*

Böhme, R., (2013), *Internet Protocol Adoption: Learning from Bitcoin*

Chaum, D.,(1982) *Blind Signatures for Untraceable Payments. In Crypto '82*,pp 199–203. Plenum, NY,

Clayton, C.M., (1997) *The innovator's dilemma. When new technologies cause great firms to fail*, pp 11

Clements, M. T., (2004), *Direct and Indirect Network Effects: Are They Equivalent?*

David, P.A.,(1985) *Clio and the Economics of QWERTY, The American Economic Review,pp. 332-337*

Decker, C. &Wattenhofer, R. (2013) *Information Propagation in the Bitcoin Network*

Draisbach, T., Widjaja, T., Buxmann, P.(2013) *Lock-ins in Network Effect Markets – Results of a Simulation Study*

Duffield, E., Hagan, K., (2014), *Darkcoin: Peer to Peer Crypto Currency with Anonymous Blockchain Transactions and an Improved Proof of Work System*

Easley, D., Kleinberg, J., (2010), *Networks, Crowds, and Markets: Reasoning about a Highly Connected World, Cambridge University Press*

ECB (2012) *Virtual Currency Schemes*

European Commission, (1997): 3-12 *Green paper on the convergence of the telecommunications, media and information technology sectors, and the implications for regulation.COM (97) 623.*

Eyal, I. &Sirer, E. G. (November 2013), *Majority is not Enough: Bitcoin Mining is Vulnerable*

Evans, D. S., 2014, *Economic Aspects of Bitcoin and other Decentralized Public-Ledger Currency Platforms*

FBI (24 April 2012) *Bitcoin Virtual Currency: Intelligence Unique Features PresentDistinct Challenges for Deterring Illicit Activity*

Feiger, G., (1976), *What is speculation, Introduction and summary, 677*

Fox, M., Dodge, E., (2012) *Economics demystified*

Gambardella, A. and Torrisi, S. (1998),*Does technological convergence imply conver- gence in markets? Evidence from the electronics industry, Research Policy,* 27, pp445– 463.

Goldfeder, S., Bonneau, J., Felten, E.W., Kroll, J.A., Narayanan, A., (2014), *Securing Bitcoin wallets via threshold signatures, pp.3*

Greenstein, S., andKhanna, T.(1997): *What does industry convergence mean. Competing in the age of digital convergence.*pp.201-226

Guo, J. &Xie, M. (2013) *Achieving Satisfied Virtual Exchange Rates through Multiple-Stage Virtual Money Supply*

Han, S.P., Ahn, J.H., Skudlark, A., (2004), *Convergence Phenomenon and New Service Development in the Telecommunications Industry, chapter 19*

Kim, W.C., Mauborgne, R. (2005). *Blue Ocean Strategy: How to Create Uncontested Market Space and Make the Competition Irrelevant.* Boston: Harvard Business School Press

King, S., Nadal, S., (2012), *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*

Kroll, J. A., Davey, I. C., Felten, E. W. *The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries*

Leifer, R., McDermott, C.M., O'Connor, G.C., Peters, L.S., Rice, M., Veryzer, R.W., (2000), *Radical Innovation. How mature companies can outrun upstarts*, Harvard Business School Press

Mahdjoubi, Darius (1991*), Schumpeterian Economics and the trilogy of 'Invention-Innovation-Diffusion'* First version: November 21, 1997, Last revision: January 24, 1999, Research paper, pp.1-3

McKee, J., (2013), *Redefining Virtual Currency,* Yankee Group, pp. 4-5

Moore, T., Christin, N.,(2013), *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, pp.6

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*

Ober, M., Katzenbeisser, S., Hamacher, K. (2013*) Structure and Anonymity of the Bitcoin Transaction Graph*

Reid, F., Harrigan, M., (2012), *An Analysis of Anonymity in the Bitcoin System*

Rogers, E. M. (1962). *Diffusion of Innovations.* Glencoe: Free Press. pp. 150.

Rogers, E.M., (2003). *Diffusion of Innovations 5ᵗʰ Edition*

Rogojanu, A. (2014). *The issue of competing currencies . Case study – Bitcoin*, *XXI*(1), 103–114.

Rosenberg, N., (1963): 414-443*Technological change in the machine tool industry, 1840-1910.The Journal of Economic History 23.4.*

Shapiro, C., Varian, H.R. (1999) *Information Rules. A Strategic Guide to the Network Economy*, Ch.7, page 175-183, Harvard Business School Press

Sherman Anti-Trust Act (1890)

Sompolinsky, Y. & Zohar, A. (2013),*AcceleratingBitcoin's Transaction Processing Fast Money Grows on Trees, Not Chains*

Taylor, M.B., (2013)*Bitcoin and The Age of Bespoke Silicon How Bitcoin Works : User Perspective BitcoinMining : Miner ' s Perspective.*

Wan, P. N. (2013). *Bitcoin : Currency or Commodity ?*

Weaver, B., (2007): 1-20, *Research proposal: Industry convergence-Driving forces, factors and consequences.*

Wirtz, B. W. (2001) *Reconfiguration of Value Chains in Converging Media and Communications Markets, Long Range Planning, 34:489-506.*

Zhang, L. (2009). P*ositive Feedback in Network Economic System, (Economides 1996), 5695–5699.*

7.1 Internet references

[1]http://data.worldbank.org/indicator/IT.NET.USER.P2?order=wbapi_data_value_2012+wbapi_data_value+wbapi_data_value-last&sort=desc

[2] http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W-EU-US-ZJ-RU-IN?display=graph

[3] http://Bitcoincharts.com/charts/bitstampUSD#rg2920ztgSzm1g10zm2g25zv

[4] http://www.forbes.com/sites/reuvencohen/2013/11/27/the-top-30-crypto-currency-market-capitalizations-in-one-place/

[5] https://Bitcoin.org/en/faq

[6] https://coinbase.com/charts

[7] https://coinmarketcap.com/all.html

[8] http://www.businessinsider.com/cyprus-university-Bitcoin-tuition-2013-11

[9] http://www.binaryoptionsleader.com/making-the-news/Bitcoin-passes-750-us-agencies-voice-approval/

[10] http://www.currencyconnect.com/

[11] http://capcom.wikia.com/wiki/Zenny

[12] http://www.wow.freemmorpgguides.com/wow-gold-guide/

[13] https://developers.facebook.com/blog/post/2012/06/19/introducing-subscriptions-and-local-currency-pricing/

[14] https://ronnie05.wordpress.com/tag/facebook-credits/

[15] http://www.frequentflier.com/programs/

[16] http://www.economist.com/blogs/freeexchange/2014/03/Bitcoin

[17] http://secondlife.com/shop/faq/

[18]http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_Bitcoins_en.html

[19] http://politiken.dk/oekonomi/dkoekonomi/ECE2162454/guld-soelv-eller-glasperler-danmark-forkaster-Bitcoin/

[20] http://bitlegal.net/nation/DK.php

[21] http://www.bloomberg.com/news/2013-12-12/Bitcoins-fail-real-money-test-in-scandinavia-s-wealthiest-nation.html

[22] http://bitlegal.net/nation/SE.php

[23] http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-Bitcoin-transactions.html

[24] http://www.reuters.com/article/2014/03/11/us-Bitcoin-regulation-idUSBREA2A1W020140311

[25] http://bitlegal.net/nation/US.php

[26] http://bitlegal.net/nation/IS.php

[27] http://preshing.com/20140127/what-is-a-Bitcoin-really/

[28] https://www.torproject.org/about/overview.html.en

[29] https://Bitcoin.org/en/faq#is-Bitcoin-secure

[30] http://andrewgelman.com/2012/04/08/technology-speedup-graph/

[31] http://en.wikipedia.org/wiki/File:QWERTY_keyboard.jpg

[32] http://www.investopedia.com/university/economics/economics3.asp

[33] http://developingcatan.wordpress.com/2010/10/21/manipulating-market-price/

[34] http://www.crunchbase.com/organization/BitPay

[35] https://lamassu.is/

[36] https://roboco.in/

[37] https://en.Bitcoin.it/wiki/FAQ

[38] http://compoundingmyinterests.com/compounding-the-blog/2013/11/11/the-rise-and-inevitable-fall-of-Bitcoin-1.html

[39] http://money.cnn.com/2013/03/28/investing/Bitcoin-cyprus/

[40] http://money.cnn.com/2013/03/16/news/economy/europe-cyprus-bailout/index.html?iid=EL

[41] http://dollarvigilante.com/blog/2013/5/2/my-official-withdrawal-from-the-Bitcoinatm-project.html

[42] http://www.forbes.com/sites/ericmack/2013/12/23/the-Bitcoin-pizza-purchase-thats-worth-7-million-today/

[43] http://www.businessinsider.com/goldman-completely-debunks-all-the-arguments-for-Bitcoin-2014-3

[44] https://Bitcoin.org/en/innovation

[45] https://Bitcoin.org/en/development

[46] https://en.Bitcoin.it/wiki/Development_process

[47] http://www.cryptocoinsnews.com/news/Bitcoin-technical/2014/03/03

[48] https://blockchain.info/el/charts/my-wallet-n-users

[49] http://www.internetlivestats.com/internet-users/

[50] http://www.worldometers.info/world-population/

[51] http://connect.burrellcolourimaging.com/wp-content/uploads/2010/11/600px-Diffusionofideas.jpg

[52] http://blogs.wsj.com/moneybeat/2014/02/05/most-people-still-dont-know-what-Bitcoin-is-and-dont-care-to-know/

[53] http://www.coindesk.com/survey-results-96-of-merchants-would-recommend-Bitcoin-peers/

[54] http://www.comscoredatamine.com/2012/06/1-in-4-internet-users-access-banking-sites-globally/

[55] http://www.euromoney.com/Article/3228013/Worlds-apart-banks-and-Bitcoin-convergence-unlikely-anytime-soon.html

[56] http://techcrunch.com/2013/08/28/robocoin-the-first-20000-Bitcoin-atm-now-available-for-pre-order/

[57] https://BitPay.com/faq

[58] https://www.goldsilverBitcoin.com/BitPay-worlds-first-zero-transaction-fee-payment-processing/

[59] http://siliconangle.com/blog/2013/01/23/BitPay-announces-10000-Bitcoin-transactions-with-zero-cases-of-payment-fraud/

[60] http://Bitcoinexaminer.org/BitPay-presents-its-three-new-all-inclusive-pricing-plans-with-zero-fees/

[61] https://www.goldsilverBitcoin.com/BitPay-worlds-first-zero-transaction-fee-payment-processing/

[62] http://www.coindesk.com/regulation-help-Bitcoin/

[63] http://coinmarketcap.com/

[64] http://www.NXT.org/

[65] http://dogecoin.com/

[66] https://ripple.com/

[67] http://namecoin.info/

[68] http://www.mastercoin.org/

[69] http://www.blackcoin.co/

[70] http://bitlegal.net/

8   Appendix

8.1   Timetable

Tasks/Weeks	week 3 Fev	Week 10 Fev	Week 17 Fev	Week 24 Fev	Week 3 Mar	Week 10 Mar	Week 17 Mar	Week 24 Mar	Week 31 Mar	Week 7 Apr	Week 14 Apr	Week 21 Apr	Week 28 Apr	Week 5 May	Week 12 May	Week 19 May	Week 26 May
Brainstorm					1st Seminar						Holidays			2sd Seminar			Project Delivery
Idea Choosing					1st Seminar						Holidays			2sd Seminar			Project Delivery
Propouse Topics					1st Seminar						Holidays			2sd Seminar			Project Delivery
Table of Contents					1st Seminar						Holidays			2sd Seminar			Project Delivery
Research					1st Seminar						Holidays			2sd Seminar			Project Delivery
Problem Formulation					1st Seminar						Holidays			2sd Seminar			Project Delivery
Introduction					1st Seminar						Holidays			2sd Seminar			Project Delivery
Delimitations					1st Seminar						Holidays			2sd Seminar			Project Delivery
Motivation					1st Seminar						Holidays			2sd Seminar			Project Delivery
State of the art					1st Seminar						Holidays			2sd Seminar			Project Delivery
Theoretical Frameworks					1st Seminar						Holidays			2sd Seminar			Project Delivery
Analysis					1st Seminar						Holidays			2sd Seminar			Project Delivery
Discussion					1st Seminar						Holidays			2sd Seminar			Project Delivery
Conclusion					1st Seminar						Holidays			2sd Seminar			Project Delivery
Surveys					1st Seminar						Holidays			2sd Seminar			Project Delivery
Review and Corrections					1st Seminar						Holidays			2sd Seminar			Project Delivery

8.2   Bitcoin Survey Results

Number of Answers: 80

Number of Emails Collected: 8 emails (2 fake)

Introduction:

"Hello everyone!

We are a group of three students from ICTE and this semester our group is working on a project with virtual currencies as the main topic, with one of the most popular of them, Bitcoin, as a case study. By the term virtual currencies we mean digital money used in the online world in exchange for goods or services, without any regulations applied by central authorities or banks. Bitcoin is at the moment one of the most popular virtual currencies and consists a very interesting case for this project. The following questionnaire aims to find out information about Bitcoin's use and popularity in our student community. Your participation in this survey will provide very valuable information for our research, so please take the time to answer the

questionnaire. Even if you don't know what Bitcoin is, it's still important that you provide this answer. And in case you're a Bitcoin fan and use it regularly we would be delighted to have a cup of coffee or tea with you and use a little of your time for a small interview!
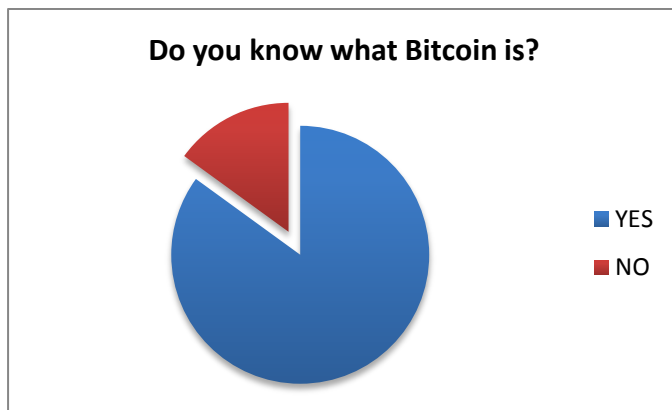
Thank you for your time, Kamrul, Vasiliki, Miguel."

1º Question.

"Do you know what Bitcoin is?"

Results

Yes: 68 (85%)

No: 12 (15%)

2º Question:

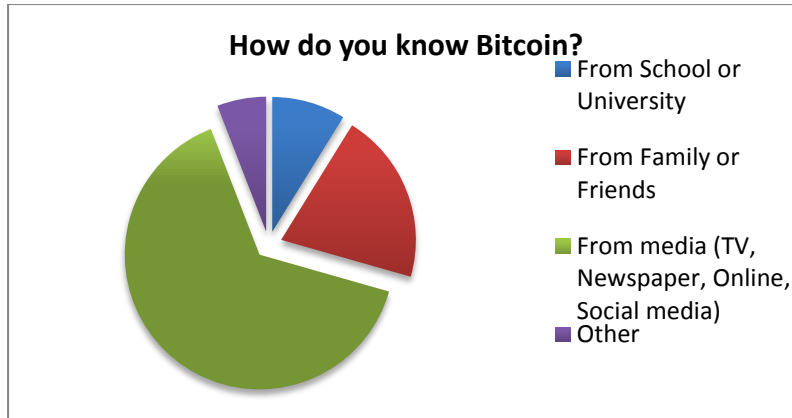*"How do you know Bitcoin?"*

Results

From School or University: 6 (8.8%)

From Family or Friends: 14 (20.6%)

From media (TV, Newspaper, Online, Social media): 44 (64.7%)

Other: 4 (5.9%)

Total: 68

3º Question
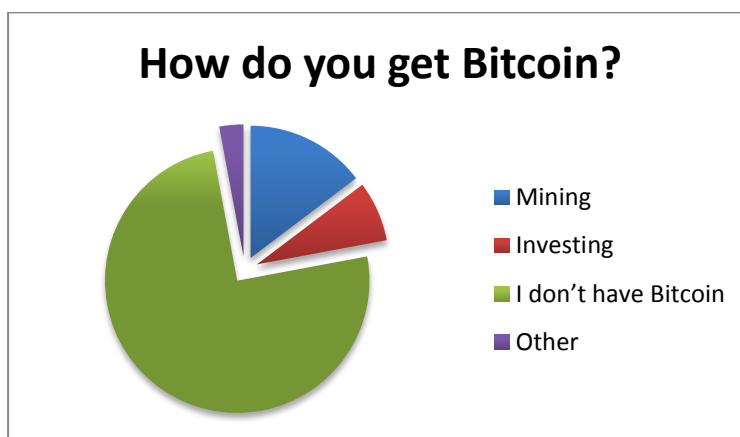
"How do you get Bitcoin?"

Results

Mining: 10 (15%)

Investing: 5 (7%)

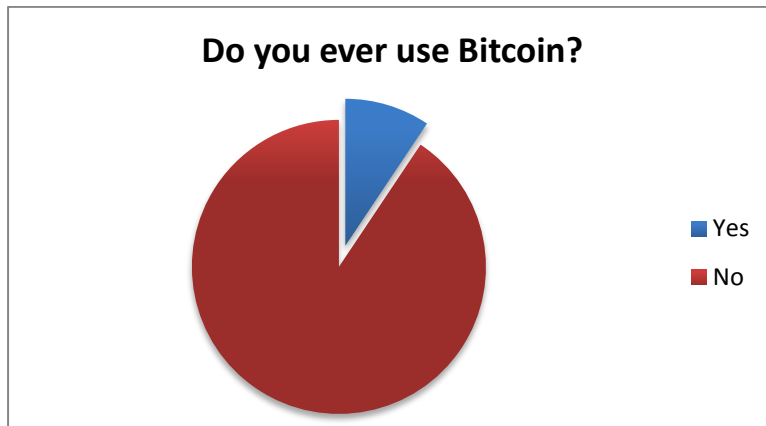I don't have Bitcoin: 51 (75%)

Other(Both): 2 (3%)

Total: 68

4º Question

"Do you ever use Bitcoin?"

<u>Results</u>

Yes: 6 (9%)   No: 58 (91%)

5º Question

"Where do you use Bitcoin and how often?"

<u>Results:</u>

Online stores:

      Daily : 0

      Weekly: 0

      Monthly: 2

      Yearly: 1

      Once: 0

      Never: 3

Physical stores:

      Daily : 0

      Weekly: 1

      Monthly: 0

Yearly: 0

Once: 0

Never: 5

Investment:

Daily : 0

Weekly: 0

Monthly: 1

Yearly: 0

Once: 2

Never: 3
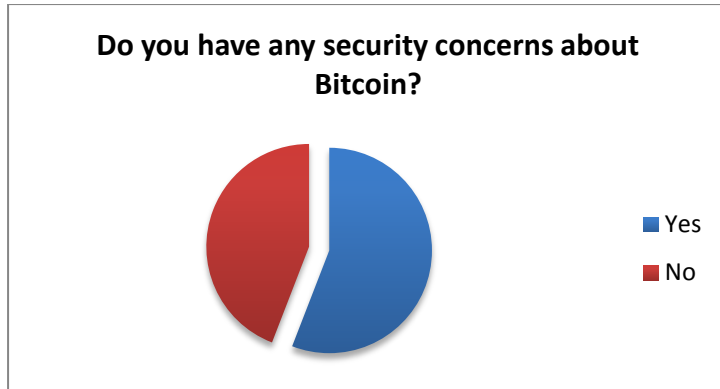
Total :6

No graphs made because of lack of data.

6º Question

"Do you have any security concerns about Bitcoin?"

Results

Yes: 38 (56%)

No: 30 (44%)

Do you have any security concerns about Bitcoin?

■ Yes
■ No

7º Question

"What sort of concern do you have?"

Most of concerns were.

- Security and Transitions.

- Hacking (very common)

- Fraud

- Bitcoin = Air

- No Guarantee of the value

- state tracking

- currency being entirely virtual

- money theft

- No regulation might be illegal.

- Destroy global finance

8º Question

"What are the reasons for using or not using Bitcoin?"

Results

I use because?

- to be sure

- new thing and wanted to learn about it

- safe

- good way to invest

- is required for a particular store

- Its fast, simple, Free from stupid banks

- it is untraceable

I Don't use because?

- I don't have any

- I don't need it

- Exchanges are currently to high for me

- Not interested in the market

- I like my currency

- Not interested in crypt currencies

- To unstable

- The value can go up and down very fast

- don't like to gamble

- no use for it yet

- not relevant for me

- don't really untherstand it

- I use dogecoin instead less unstable.

- security reasons

- it's a bubble

- Not enough information about it

- not popular

- I don't want to support it

- too niche

- associated with illegal activites

- Lack of time

- not wield accepted

- takes to long to mine

8.3 Interview

This interview was conducted with Claudio Castro, an industrial designer, who designed and overviews the production of the world's first Bitcoin ATM for the company LamassuBitcoin Ventures, who sells these machines worldwide.

1) What does Lamassu do?

- *"Lamassu is a company that sells Bitcoin ATMs all over the world. The machines that were made before where just ATMs converted to use Bitcoin. Lamassu was the first one to develop a product from the beginning for Bitcoin."*

2) What is your role in the creation of the ATM?

- *"I designed the physical machine (hardware-not the software) and I manage the production and quality control of the ATMs. Everything is produced in Portugal, in Famalicão and Trofa."*

3) What are advantages from of this machine compared to the other machines?

- *"The advantages of this machine are that it is the most secure machine in the market (robustness), its competitive price (only $5000), secure software. The good looking design is also one advantage as well as its simplicity. Competitive companies have produced machines like robocoin which have more features but are also a lot more expensive."*

4) How secure are these machines both physically and software-wise?

- "Physically we have made sure that they contain the most secure vault in the market, software-wise (I am not an expert on it) it's very secure and they keep upgrading the software in order to make it even more secure and avoid new security breaches"

5) How many machines have you sold so far?

- *"170 were shipped already from Portugal but Lamassu has sold around 230. This is the number of machines sold from September until now."*

6) Who are the clients buying these machines?

- *"Mainly startups that operate this machine and put them in locations for people to use it. Also some bars and shops."*

7) How long is needed for the return of the client's investment?

- *"I am not the best person to answer about this one but I know that the companies that bought them 1 year ago are having now some profit on it, so I would say one year. Lamassu itself is already making profit on them."*

8) Do you think that investing in Bitcoin is safe for a company?

- *"Yes, now more and more. I was also concerned about using Bitcoin in the beginning. I have a company and I can't pay my taxes in Bitcoin. I didn't know much about Bitcoin before but then I researched and read a lot about it and in the end it worked really well for me and my company. With services like*

BitPay every company can use it and is even better because it has much less fees. All worked fine and now I like to use it."

9) Do you see a bigger interest for Bitcoin-related services now than before?

- *"Yes Lamassu and BitPay and other companies offering Bitcoin services are creating something new. I don't know where this is going to but it seems very promising. We are living in an era where everything is digital and so I see this as the beginning of something new and interesting."*

8.4 Comparison Table.

Peer to Peer Currencies	Year of Foundation	MarketCap	Price	Market Share	Mining	Open Source	Limited supply	Related to Bitcoin
Bitcoin	2009	$7,220,760,389.00	$563.52	91.44%	yes	yes	21 million	yes
LiteCoin	2011	$329,061,745.00	$11.48	4.17%	yes	yes	84 million	yes
DarkCoin	2014	$62,750,897.00	$14.51	0.79%	yes	yes	22 million	yes
PeerCoin	2012	$51,980,535.00	$2.43	0.66%	yes	yes	no	yes
Nxt	2013	$38,612,625.00	$0.0386	0.49%	no	yes	1 billion	no
DogeCoin	2013	$33,919,380.00	$0.0004	0.43%	yes	yes	no	yes
Ripple	2013	$28,510,076.00	$0.0036	0.36%	no	yes	100 billion	no
NameCoin	2011	$23,314,310.00	$2.63	0.30%	yes	yes	21 million	yes
MasterCoin	2013	$16,197,063.00	$28.76	0.21%	no	yes	619.478,6	yes
BlackCoin	2014	$11,019,329.00	$0.15	0.14%	yes	yes	no	yes