Department of Economics and Finance

Course of Macroeconomic Analysis

A DECENTRALIZED MONETARY POLICY: AN ANALYSIS OF BITCOIN IN A CASH-IN-ADVANCE MODEL

SUPERVISOR
Prof. Reichlin Pietro

CANDIDATE
Ianiro Annalaura
646671

CO-SUPERVISOR
Prof. Nisticò Salvatore

ACADEMIC YEAR 2013/2014

A Decentralized Monetary Policy: an Analysis of Bitcoin in a Cash-In-Advance Model

Acknowledgements

I would like to express my sincerest gratitude towards my LUISS supervisor, Prof. Pietro Reichlin, for its help and support throughout this work.

Then, I would like to thank my two Bitcoin comrades, Antonio and Davide: our project together has been the greatest motivation.

I want to thank my family, all of it. In particular my ant Anna, my uncle Damiano, and my cousins Nicodemo and Luigi, for they became my Rome parents and brothers. And last, but not least, my parents and sister, for without them I would not be where I am today.

Thank you for believing in me.

Contents

Introduction

In the last year and a half, Bitcoin, and crypto-currencies more in general, have invaded the scenes of financial markets, soon becoming one of the most discussed and controversial issue society is dealing with. Bitcoin, the crypto-currency created by the mysterious Satoshi Nakamoto in 2009, has given birth to an innovative phenomenon, still rich of unexplored potential. These decentralized currencies may represent the alternative, the answer to the numerous unresolved problems brought about by the last financial crisis. It is too early to confirm whether or not this is true: crypto-currencies are still in their infancy, and, apart from Bitcoin, only few of them are worth of attention. The information on them is dispersive and often confusing, constituting a serious limit to their understanding and diffusion among the general public, which often react with diffidence and doubts to the many issues raised by crypto-currencies. For this reason, this work aims, to the extent of its author's limited capacities, to shed some light on the subject, in particular on Bitcoin, trying to explain its functioning and implications, especially under a monetary policy perspective. Before doing so, it is necessary to define money. This has always been a difficult task for economists, who, therefore, instead of defining money for what it is, looked at its essential function: money is a medium of exchange, a unit of account and a store of value. This functional definition makes it clear why in the course of history money has taken various forms: from cattle, the first exchange medium after pure barter, to shells, to the first examples of metal coins. Precious metal coins, which have also an intrinsic value, ruled for many centuries, until the first banknotes were issued. In the beginning, these banknotes were not linked to the value of some commodity, leading in many cases to an abuse in their emission and usage. In 1816 however, England began using gold as a back-up commodity for paper money. This marked the beginning of the so-called Gold Standard. Despite the two World Wars and the Great Depression having shown the weaknesses of such system, the Gold Standard continued to live on. The Bretton Woods International Monetary Agreement kept it, even though without direct convertibility for all currencies: only dollars could be exchanged for real gold. This situation became soon unsustainable and thus it was abandoned. With the end of the convertibility of banknotes into gold or other

commodities, it has begun the epoch of *fiat* money. *Fiat* money has no intrinsic value, but its worth is guaranteed by the government or the central bank, which issues it: it is the law that guarantees and allows its usage. The introduction of the Internet and the World Wide Web, though, and its incredible diffusion, has changed the rules and expanded the landscape of money varieties. In particular, virtual currencies have emerged. They are basically private money, but with a digital nature: they have no physical entity, they are born, stored and used on computers and other electronically devices (smartphones, tablets, etc.), therefore they can be expected to gain always more importance as more advanced technologies are constantly developed. For some years the only type of virtual money has been the one used in side MMORPGs. These are web browser-based games in which many players interact with each other online. This type of games involves the creation of a virtual world, usually a fantasy or sci-fi one, in which every player build her own avatar and takes part into a story. Then, other web realities, like Facebook and Amazon, issued their own digital currencies, which could be used to purchase online content. In the last years, however, a new type of virtual currencies has emerged, the crypto-currencies. Crypto-currencies are virtual currencies that exploit cryptography to function. Crypto-currencies protocols heavily rely on cryptographic techniques throughout all the stages of the transaction. They can be used to purchase anything, as long as the parties involved in the transaction accept that particular crypto-currency. The first crypto-currency ever created is Bitcoin. In the intention of its creator, Satoshi Nakamoto, Bitcoin should be a mathematical answer to the need of performing anonymous, safe, immediate online payments (Nakamoto 2008). Even if in a still contained way, the phenomenon of virtual currencies, their interactions with real economies and implications, are being studied by academics, mainly under a microeconomic point of view. The macroeconomic analysis, instead, is just at the beginning, with some studies posing questions about the role of traditional money and central banks, now that virtual currencies, and crypto-currencies in particular, are on the scenes. The relevance of digital currencies for the monetary system is starting to be acknowledged even by central banks. In 2012, the ECB published a review on what they call virtual currency schemes, bringing up, as examples, the Bitcoin case and the Linden Dollars case. They try to set a rigorous approach to study this phenomenon, highlighting the risks that virtual currency schemes (how a particular virtual currency interacts within the community which it belongs to and, eventually, the real world, thanks to its specific retail

payment system) could pose to the monetary system in terms of price stability, financial stability, payments system stability, lack of regulation, reputation (ECB 2012). Before looking at Bitcoin as a virtual currency scheme, its characteristics and functioning mechanism should be explained. Bitcoin is an electronic payment system, allowing transaction between two individuals directly. In fact, the Bitcoin system is decentralized, meaning that there is no central bank or authority, which controls it and guarantees its stability. All the transactions, instead, are based on a peer-to-peer network, whose integrity is kept by the nodes belonging to it. Bitcoin is defined as a crypto-currency, since cryptography is heavily used to enable every transaction. When we talk about Bitcoin transactions, we cannot consider them as traditional coin transactions: they represent entries in a global digital ledger. Therefore, suppose a party wants to transfer some Bitcoin to another, it has to specify the amount of coins involved in the transaction and apply a digital signature to the operation, so that her digital identity is tied to the transaction. It is important to highlight that identities in the Bitcoin network are not real, physical identities; they are numbers that act as a pseudonym for the real person behind the transaction, thus ensuring a high level of privacy. Once the transactions details are specified, they are broadcasted to the entire system. It is this public disclosure to all the nodes that guarantees the goodness of the operation to the recipient party. However, the latter still faces a problem: how can it be sure that the received Bitcoin have not already been spent? This phenomenon, known as double spending, is, in fact, one of the main problems afflicting electronic transactions. The main novelty of the Bitcoin system lies exactly in the way it deals with double spending. There are some nodes in the network, known as miners, whose task is essential to the survival and maintenance of the network itself: they collect all the transactions occurred within a certain time period in what is called a transaction block. In doing so, they give a sort of authenticity certificate to every transactions, allowing all the nodes to acknowledge each block as valid. This proof of work mechanism is the heart of the decentralized nature of the Bitcoin system and it is what controls the money supply, since miners are rewarded with brand new Bitcoin for each block they create, plus some optional fee users may decide to pay them with as a further incentive to their activity. Finally, money supply is limited: in 2140 the total amount of Bitcoin is reaching 21 million, with no further emissions. Far from being the perfect currency, Bitcoin indeed shows some concrete limitations, raising concerns both among its users and its critics. The major worries are the ones about

protocol security, mainly involving forgery, and the possibility of thefts, both at a network and hardware level, and the ones about ethical and ideological issues about Bitcoin usage, which should not be underestimated since one of the most important drivers leading to Bitcoin success is the ideology behind it.

The actual incentive compatibility of the mining system is one of the major concerns, but there are strong arguments to support it. The MtGox's case, instead, is exemplary to discuss security issues. MtGox was one of the major Bitcoin exchange platforms, counting thousands of users. In February 2014, it declared bankruptcy because of a bug, which led to a massive theft of Bitcoin from its accounts. However, MtGox's failure must not be considered as a failure of the Bitcoin protocol itself. The bug in question, the transaction malleability bug, has been known since 2011, and can be rendered harmless with software, which accurately reports balances and transactions. Indeed, other Bitcoin exchanges can perfectly manage it. Another case rising concerns about this crypto-currency is Silk Road's case. Silk Road was an online market for illegal products, especially drugs. It was indeed defined as the "E-bay for drugs". It resorted to Bitcoin as its only mean of payment, because of the anonymity of transactions and for years authorities had no idea how to close it. On October 2, 2013 the FBI managed to shut down the illegal website and arrest Ulbrich, Silk Road's founder, in a joint operation with the IRS Criminal Investigation Division, the ICE Homeland Security Investigation, and the Drug Enforcement Administration. However, on November 6, 2013 a new website, Silk Road 2.0 opened for business, aiming to be a direct successor to the previous project. As of today, this site is still operating. Silk Road, unfortunately, isn't the only example of this kind of illegal online markets, which can stay on business thanks to Bitcoin or other crypto-currencies. It seems like this trend is only going to increase, if governments and authorities do not take the right precautions and countermeasures. However, banning Bitcoin or virtual currencies more in general is not the right step in that direction. Instead, a reasonable starting point is trying to better understand the implications and potentialities behind digital currencies, and to conceive a way to integrate them in our realities, for example setting clear rules about taxation and other legal issues concerning them. At this point, after discussing the major characteristic and implications, Bitcoin can be analysed in the framework of virtual currency schemes. In particular, its effect on price stability, financial stability, payment system stability can be assessed. As of today, Bitcoin is not a threat to price stability. The size of the

phenomenon is still contained; however its relevance is growing day by day, therefore the impact of Bitcoin on these aspects discussed above can change completely in the future. For this reason, monetary authorities needs to be ready to deal with such an occurrence, monitoring the development of the crypto-currency, in order to continue to absolve their tasks to the best of their abilities. The same conclusion can be drawn for financial stability. However, Bitcoin weight in financial markets is growing and there are aspects of the crypto-currency, which could indeed become a menace, if they are not dealt in the proper way. For example, there is still no credit system related to Bitcoin, but if loans and debts in Bitcoin start to surface, then the interconnection of the crypto-currency with the financial system will become more complex and risky, especially as far as stability is concerned. Lastly, Bitcoin is still an unstable payment system, in which users bear themselves all the risks related to the transactions. If the number of people resorting to Bitcoin for retail transactions were to increase, then central banks should adopt some measures to protect the traditional payment system from the instability brought forth by the virtual one. As of today, Bitcoin, as a payment system, cannot be considered an actual threat, but this doesn't imply that it could become so in the near future. The main problem of Bitcoin as a virtual currency scheme, therefore as a new player in the monetary and financial scene, is its lack of regulation. Governments and authorities are having many problems when dealing with Bitcoin mainly because they don't know how to define it and its relationship with real currencies. Still, time is stringent: Bitcoin, and crypto-currencies more in general, have become a widespread reality, which cannot be ignored any longer. Governments and authorities need to lay out some clear guidelines to allow a more aware and responsible usage of virtual currencies. The main aim of this work, though, is that to try to introduce Bitcoin inside a neo-classical economy framework, a Ramsey Plan with money, specifically the cash-in-advance model. The CIA model and its results are well known to economics-literate readers, who are also aware of the difficulties of introducing money in a Ramsey Plan economy. Bitcoin is a currency completely different from traditional ones. Apart from its digital nature, which may be the first aspect making the difference, there are several characteristics that set Bitcoin apart from traditional money. In particular, Bitcoin is decentralised, without a central authority controlling it. Its growth rate is scheduled by an algorithm, setting a roof for its total supply. Simply these observations make it clear how complicated an attempt at modelling Bitcoin can be, especially inside a traditional neo-classical

framework. Nevertheless, this effort could be a starting point for future analysis, in the event Bitcoin or crypto-currencies more in general shall increase their weight in our economy. Among the assumptions, one is particular important: the active fee and the liquidity incentive. Each agent may choose to pay an active fee, f_t^a, to reward the miners for their effort and encourage them to confirm her transaction faster. However, once no more new Bitcoin will be issued, fees will become mandatory, as they will be the only reward for miners' activity. $\psi(f_t^a)$ is a liquidity incentive, in order to encourage the payment of the active fee. It is such that it "punish" those users, who pay an active fee lower than its equilibrium value, by reducing the value of their Bitcoin holdings. The closer the fee is to its equilibrium value, the more encouraged miner will be to validate sooner that transaction, thus giving it more purchasing power than to a transaction with a lower fee. The active fee may be higher than its equilibrium value, as well, but the marginal increase in the liquidity incentive would be irrelevant. This fee can also be seen as the price Bitcoin users are willing to pay to promote the crypto-currency and to make it an alternative to traditional money. Basically, the more they believe in Bitcoin potential as a currency, the higher active fee they will pay, since they want miner to keep playing their role as best as they can, guaranteeing the whole system functioning. If, however, once the fee is higher than the equilibrium fee, the liquidity advantage is compensated by the loss of competitiveness with real money in terms of inflation gap. One of the main results of this model is that, as long as Bitcoin's emission goes on, consumption is not the same as the consumption of a Ramsey Model without money in it. The amount of Bitcoin emitted each period influences it. In the steady state, instead, consumption goes back to its Ramsey Plan formulation. Moreover, because of the liquidity incentive, Bitcoin inflation and traditional money inflation are both equal to zero. Bitcoin can stop money inflation. The presence of Bitcoin in the economy can affect traditional money demand and therefore monetary policy. There can be competition between traditional currency and crypto-currency. This competition, if appropriately studied and understood, can actually bring benefits for the users: they are "in control" of Bitcoin and thus they have an instrument to react to monetary policy decisions.

Chapter 1

Giving a definition of money has never been an easy task, especially because of the different forms money has been taking throughout history. Economists, therefore, would rather characterize money not for what it is, but for the functions it carries out. These functions are three:

1. Medium of exchange: money is used to trade goods and pay for obligations, as a much more convenient alternative to barter;
2. Unit of account: money is the *numeraire* for the measurement of values and prices;
3. Store of value: money can be saved and maintain its value in order to be used in the figure.

These characteristics are fundamental for money to be considered such, however, they do not demand a specific form or vessel: anything possessing these characteristics is money. Thus, as it was mentioned before, during the course of time money has changed its form many times.

1.1 History of Money

[1]The first trading transactions were held through barter, exchanging goods and/or services for mutual benefit. This practice dates back to the dawn of human history and it's still used in some primitive communities. Barter, however, as Kiyotaki and Wright[2] argue, implies the so called "coincidence of wants" (Kiyotaki and Wright 1989), thus giving birth to the necessity of finding an alternative way to exchange goods and services. The first and oldest form of money was cattle (not only cows, but also sheep, camels and other livestock), dating back to 9000 - 6000 BC. Later on, with

[1] The following chapter is based on the information found on: http://www.theibns.org; http://www.pbs.org; http://www.minneapolisfed.org; http://en.wikipedia.org.
[2] Nobuhiro Kiyotaki and Randall Wright pioneered the use of search theory in monetary economics. Search - theoretic models of monetary exchange, contrary to the previous reduced form models, are based on detailed descriptions of the frictions that make money essential.

the agricultural revolution, grains and other similar products were introduced as medium of exchange. Around 1200 BC, in China the first usage of cowrie shells as money was registered. These were shells of a mollusc widely spread in the shallow waters of Pacific and Indian Oceans. This type of money has been used by many societies, even up until the mid 20th century in some part of Africa. The first type of metal coin, in bronze and copper, were firstly manufactured in China, around 1000 BC., as an imitation of cowrie money. Metal tool money (knives, spade monies) was also firstly used in China. The Lydians were the first in the Western world to use coins, around 500 BC. They produced them out of lumps of silver, giving them the now traditional round shape. Greeks quickly adopted this technique, refining it, and so did the Persians, the Macedonians and lastly the Romans. Unlike Chinese coins, these were made out from precious metals, thus having an intrinsic value. Still, the Chinese Empire was far more advanced than any other, in fact, around 118 BC, it introduced leather money (pieces of white deerskin with colourful borders), the first documented type of banknotes, and around 800 AD., the first paper banknotes. Their usage, however, came to a stop in 1455, after the excessive emission of paper banknotes caused inflation and depreciation. In Europe, instead, metal coins ruled undisturbed for many centuries, until Sweden issued its first banknotes in 1661. Accompanied by numerous criticisms, to encourage their diffusion, these banknotes were guaranteed by the government, which would have redeemed them in specie. In the end, they were a huge success, being much easier and safer to carry around. On the wake of Sweden's success, many European governments adopted banknotes of their own; however, some of them were not as cautious in the guarantees system as the Swedish were: realizing that not all the banknotes in circulation were likely to be redeemed, they began issuing more banknotes than the gold and silver reserves in their treasuries. Furthermore, since printing banknotes was much more convenient, governments, banks and issuers began printing money whenever the need arose. This led to a strong depreciation of banknotes, to the point that some of them became worthless. One of the main problem was that, at the time, even if there were anti-counterfeiting laws, in many countries there weren't rules about who could issue money: almost anyone with access to a printer could begin printing paper banknotes. The only limit was public acceptance of such currencies, which, when lacking, made the banknotes meaningless. Banknotes continued to be used in Europe after their first introduction, but their worth had never been tied directly some back-up commodity,

like gold. Gold was officially made the standard of value in England in 1816. At this time, guidelines were made to allow for a non-inflationary production of standard banknotes, which represented a certain amount of gold. In the United States, the Gold Standard Act was officially enacted in 1900, which helped lead to the establishment of a central bank (Federal Reserve Act, 1913). After the First World War and the following Great Depression, the Gold Standard system began to collapse. The value of the gold reserves fell down and so did the banknotes value. Moreover, some economists argue that the Gold Standard exacerbated the magnitude of the depression: many central banks, in order to maintain a certain exchange rate between their banknotes and the gold reserves, couldn't expand the money supply to support an economic recovery (Eichengreen 1992). The Great Depression was one of the main causes that led to the Second World War. In 1944, the Bretton Woods International Monetary Agreement was stipulated. Thanks to it, the Gold standard was kept, even though without direct convertibility, instead many currencies fixed their values to the dollar. However, this convention put the dollar under an excessive stress and in 1971 the U.S. president Nixon announced the end of the convertibility between the dollar and gold reserves[3]. With the end of the convertibility of banknotes into gold or other commodities, it has begun the epoch of *fiat* money. *Fiat* money has no intrinsic value, but its worth is guaranteed by the government or the central bank, which issues it: it is the law that guarantees and allows its usage. People are willing to accept fiat money in exchange for the goods and services they sell only because they are confident it will be honoured when they buy goods and services. Every central bank is responsible for its own currency value, which is handled through accurate and specific monetary policies and instruments. The introduction of the Internet and the World Wide Web, though, and its incredible diffusion, has changed the rules and expanded the landscape of money varieties.

[3] This event is known as the Nixon Shocks and was due to the beginning of a period of stagflation.

1.2 Virtual Currencies

It can be easily said that the Internet Revolution has been the most relevant breakthrough of the 20th century. Indeed, it has affected every aspect of our lives, changing the way we perceive society, economy, politics, through a full-scale penetration into our reality. Since it was first implemented in the '50s for military purposes, the Internet has reached its fame thanks to the creation of the World Wide Web[4] in 1984, and since then the number of internet users has grown exponentially, with particular emphasis after the year 2000. From that year to June 2012, the number of Internet users increased by 566.4%, amounting to 34.3% of the global population[5]. Under an economic point of view, one of the main impacts of the Internet revolution is the one on the payment system. In fact, a relevant number of transactions is completed online. This has deemed necessary for banks to update their payment systems, offering methods to allow online payments and guarantee their safety. Furthermore, there has been a development of companies, which act as a medium to facilitate and speed the online transaction process, like PayPal, always relying on bank accounts, though. Such an evolution in the traditional payment system is not that surprising: it is logical for the bank system to follow the trends and needs of its clients and enhance new ways to meet those necessities within their control sphere. What can be considered truly revolutionary in this contest is the birth of the so-called virtual currencies. A virtual currency is a form of private money, and private money is not something new, there having already been some examples in the past. More in general, we could even consider all currencies to be virtual, in the sense that they have no intrinsic value on their own. Every currency is a proxy for a value, but, as mentioned before, traditional ones are backed up by a central bank (McKee 2013). The type of virtual currencies, which this work aims to analyse, is the one without a central bank behind. This category enumerates in its ranks airline miles points, grocery coupon, online games tokens, cryptocurrencies; their number is impressive; however, I personally believe that among these the most interesting ones are the digital currencies[6]. Their peculiarity is, indeed, their digital nature: they have no

[4] The Internet and the World Wide Web are two terms often used interchangeably, however they are two different things. The WWW is just one of the services that operates through the Internet, like e-mails.
[5] Source: http://www.internetworldstats.com/stats.htm
[6] From now own the terms virtual currencies and digital currencies will be used interchangeably.

physical entity, they are born, stored and used on computers and other electronically devices (smartphones, tablets, etc.), therefore they can be expected to gain always more importance as more advanced technologies are constantly developed. It all began during the dot.com bubble, when there was an unfolding of IT related businesses. Flooz.com was an online company, launched in 1999 by iVillage co-founder Robert Levitan that promoted the first example of virtual currency. Flooz.com sold online currency that could be used instead of credit cards in agreed upon online stores. Despite the relevant amount of collected investments, the company failed and closed up in 2001. After this example, for some years the only type of virtual money has been the one used in side MMORPGs[7]. These are web browser-based games in which many players interact with each other online. This type of games involves the creation of a virtual world, usually a fantasy or sci-fi one, in which every player build her own avatar and takes part into a story. Being parallel realities, the worlds in these games have their own currency, which can be used exclusively inside the game to purchase in-games objects or contents. This virtual currency can be acquired in different ways: either by playing, as a retribution or reward for completing a certain activity or task, or by purchase, meaning that players exchange real currencies for the in-game one. Exemplary is the case of Second Life[8]: Linden Dollars (L$), Second Life's currency, can be bought through Linden Lab's currency brokerage, LindeX Currency Exchange, or other third party currency exchanges. They can even be converted back into real money, exhibiting a rather stable exchange rate with the dollar (as of 12/02/2013 L$236=$1) (ECB 2012). One of the main impacts of the diffusion and the growth of the Internet has manifested in the birth of social networks, boosting a huge number of related businesses. Obviously, the phenomenon of virtual currencies involved these realities, too. In 2009, Facebook launched its own virtual money: Facebook credits. Facebook credits could be purchased via real currency and spent on Facebook apps and games. However, in 2012, Facebook credits were dismissed and since then Facebook payments are handled in real currencies. Another example is Zynga's RewardVille, Zynga's virtual in-game currency and reward system. This program was launched in 2011 and allows Zynga's games players to gain Zcoins and Zpoints to spend within the games for virtual goods or gifts. Also Amazon created its own virtual currency. Since May

[7] Massively multiplayer online role-playing game.
[8] The game developed by Linden Lab in 2003 rather than a MMORPG is a simulation of our real world, with a very complex economic and social structure.

2013, in US and in UK is possible to use Amazon Coins to purchase apps, in-apps items and games from the store. In the last years, however, a new type of virtual currencies has emerged, the crypto-currencies. Crypto-currencies are virtual currencies that exploit cryptography to function. Crypto-currencies protocols heavily rely on cryptographic techniques throughout all the stages of the transaction. They can be used to purchase anything, as long as the parties involved in the transaction accept that particular cryptocurrency. The first cryptocurrency ever created is Bitcoin. In the intention of its creator, Satoshi Nakamoto, Bitcoin should be a mathematical answer to the need of performing anonymous, safe, immediate online payments (Nakamoto 2008). On its wake many other cryptocurrencies have been developed, their appeal growing always more: Ripple, Litecoin, Peercoin, Namecoin, Dogecoin, Primecoin, Mastercoin, are the most diffused, but the list is much longer. These virtual currencies are also known as peer-to-peer currencies, with the entirety of the network managing them, rather than a single entity. Crypto-currencies like Bitcoin are immensely fascinating, presenting implications that will be further addressed later on in this elaborate. In general virtual currencies hold an enormous potential and may represent a first step into the evolution of the monetary system, as we know it now.

1.3 Literature Review

At this point, many could be asking: why should digital currencies be studied? Is it only for one's personal curiosity or interest? Because of a simple intellectual exercise? Obviously these are not the reasons behind this work. The issue of virtual currencies is truly worth the attention and the time spent on analysing it, and the literature available on this subject, although rather new and not so vast, is concrete proof of the academic and practical worthiness of digital currencies. Indeed, the points of view, which this study can be conducted from, are several. The first one involves digital currencies in online games. The pioneer in this type of research is Edward Castronova, who in 2002 laid the basis for a first economic analysis of the

famous MMORPG EverQuest[9] in his paper "On Virtual Economies". He developed an economic theory of the demand for gaming time, since "Willingness to pay, to sacrifice time and effort, is the ultimate arbiter of significance when it comes to assessments of economic value. As avatar games consume more human time, the assets within them will very likely grow in value; understanding how these assets are produced and traded will ultimately require a unique theory of the demand for avatar gaming" (Castronova 2002). In 2004, Hiroshi Yamaguchi analysed a common practice in MMORPGs, the so-called eBaying, in the paper " An Analysis of Virtual Currencies in Online Games". EBaying consists in players buying in-game objects with real money. He analysed the value of virtual assets in the real and virtual markets, revealing that the game design itself is an incentive to eBaying (Yamaguchi 2004). Moreover he argued that virtual currencies are currencies (they perform the three functions of money inside the virtual world they belong to) and that if we consider virtual worlds as objects of economic analysis, since their activities take a considerable amount of human time (Castronova 2002), then the distinction between real currencies and virtual ones looses very meaning (Yamaguchi 2004). However, he distinguished between virtual currencies and meaningful virtual currencies, the latter being virtual currencies that can be exchanged for real money: "Both a building in Monopoly and an item in EverQuest are imaginary goods. However, it is quite different that many EverQuest players are willing to purchase the in-game items by using the real currency; in contrast, no one would buy an imaginary building in Monopoly by paying real money…The existence of exchange rate is the condition for an in-game money to become a " meaningful" currency" (Yamaguchi 2004). Yamaguchi's main conclusion is that meaningful virtual currencies should be considered as a "global LETS[10]". Following along this kind of approach to the study of virtual economies, there is a 2005 paper, by Vili Lehdonvirta, " Virtual Economics: Applying Economics to the Study of Game Worlds". According to him, "Economic analysis of virtual worlds may produce results that are both academically interesting as well as useful for the developer. There are differences between virtual economies and real economies, so that assumptions that are valid in one are not necessary valid in another. Nevertheless, there are also similarities. If not all the theory, at least the rigorous analytical approach and the modelling techniques can no doubt be imported

[9] EverQuest is a 3D fantasy MMORPG released on March 1999. It was developed by Sony's 989 Studios, Verant Interactive and published by Sony Online Entertainment.
[10] Local Exchange Trading System.

from earthly economics to the virtual environment. Microeconomic analysis is perhaps the most advanced area of virtual economics, while macroeconomic models are in their infancy. It is interesting to note than it virtual economics, a macroeconomic model need not be an idealized abstraction of the actual economy, but the very rules after which the game is programmed" (Lehdonvirta 2005). The success which virtual worlds such as Second Life, Entropia Universe, Cyworld have been met with has led to the proliferation of real worlds businesses establishing virtual counterparts to operate in the virtual universe. Project Entropia Dollars can be even exchanged into real currency through specific ATMs, and some banks, operating only inside virtual worlds, were born (Bray and Konsynski 2008). In their paper " Virtual Worlds, Virtual Economies, Virtual Institutions", Bray and Konsynski argue that "Virtual avatars are building the future — complete with virtual businesses, economies, and institutions — online today". It is evident how important an economic analysis of these digital realities and their digital currencies is. As far as the use of digital currencies in the real world is concerned, the first aspect to analyse is the micropayments system. Micropayments are all those transactions of low imports and are the principal way in which virtual currencies are used, for example, Amazon Coins buying apps. However, the diffusion of virtual currencies is expected to increase (McKee 2013), affecting the monetary system in a more prominent way. Hernandez-Verme and Benavides, in their 2013 paper "Virtual Currencies, Micropayments and the Payments System: A Challenge to Fiat Money and Monetary Policy" try to analyse virtual currencies and their possible inclusion in standard Economic Theory, especially in Monetary Dynamic General Equilibrium models. Regarding the role of monetary policy, they state: "Electronification and the use of alternative means of payment has been growingly at tremendous speed over the years changing the incentives and costs structure underlying particular institutional arrangements in payment systems. Thus, the ratio of central bank money to total value of payments has decreased considerably. This development gives rise to concerns about the future role of money and the central bank. Although we are still far from living in a cashless society, the role of monetary policy is in the verge of changing dramatically, especially because of two elements: a) the falling use of cash as a form of payment and b) the changes of regulation" (Hernandez-Verme and Benavides 2013). The relevance of digital currencies for the monetary system is acknowledged even by central banks. In 2012, the ECB published a review on what they call virtual

currency schemes[11], bringing up, as examples, the Bitcoin case and the Linden Dollars case. They try to set a rigorous approach to study this phenomenon, highlighting the risks that virtual currency schemes could pose to the monetary system in terms of price stability, financial stability, payments system stability, lack of regulation, reputation (ECB 2012).

1.4 Virtual Currency Schemes

In order to further proceed with the object of this analysis, it is necessary to adopt a more rigorous approach to virtual currencies, in particular to their classification. Virtual currencies are numerous, and their typologies are vast and different, therefore it may be useful to set some more general guidelines that can help find the way inside this labyrinth. The ECB, in a 2012 report called "Virtual Currency Schemes" offers an effective solution to this predicament. It talks about digital currencies in terms of schemes, choosing a specific point of view from which its classification can begin. I believe the ECB's work to be rather enlightening, thus I want to borrow its methodological approach. First of all, a definition of virtual currency scheme is in order. A virtual currency scheme is how a particular virtual currency interacts within the community which it belongs to and, eventually, the real world, thanks to its specific retail payment system (ECB 2012). Given this definition, in order to classify these schemes, it's important to focus on one aspect, in particular how virtual currencies interact with the real money and the real economy. In this way, three different types of virtual currency schemes can be identified:

1. *Closed virtual currency schemes*: in this type of schemes, the link between the digital currency and the real economy is basically inexistent. Online games currencies usually belong to this scheme. The players pay a subscription fee, when required, and obtain the virtual currency by performing task inside the game. The earned currency can be only used inside the game community to buy virtual objects.

[11] For the definition, see the following paragraph.

2. *Virtual currency schemes with unidirectional flow*: the virtual currency can be bought using real money at a certain exchange rate, however it cannot be exchanged back into real currency. The digital currency allows its owner to by virtual good and services, offered by specific communities that accept the currency. In some of these schemes it is even possible to buy real goods with the virtual currency. An example of this scheme is Facebook credits.
3. *Virtual currency schemes with bidirectional flow*: the virtual currency can be easily exchanged with the real ones and vice-versa. As far as the usage of the virtual currency in the real world is concerned, it is similar to the usage of any other real currency, allowing the purchase of both digital and real goods and services. Bitcoin and the other cryptocurrencies belong to this scheme.

(ECB 2012)

Virtual currency schemes must not be confused with electronic money, a digital equivalent of cash, stored on an electronic device or remotely at a server (E-Money Directive 2009/110/EC). The main difference between the two lies in the fact that, as far as e-money is concerned, the link between the digital currency and the traditional ones has a legal basis, with a demand and supply still controlled by the central bank; moreover the unit of account is the same. Virtual currencies, instead, are connected to real money through an exchange rate, thus being exposed to its fluctuations, which are amplified by a money supply in the hands of a non-financial institution or even decentralized. It comes from this, that e-money and virtual currency schemes face different types of risks, which in the case of the latter are more pronounced, especially because of the lack of regulation on the matter. It was mentioned before that virtual currency schemes are a form of retail payment system. They indeed show all the characteristics a retail payment system should have: a payment instrument; payment instructions for processing and clearing; debit and credit's settlement inside the user's account (ECB 2012). In addition to this, retail payment systems of virtual currencies present their own feature:

1. Transactions are held outside the traditional banking channels, they are simple transfers of claims among agents on the virtual currency issuer (three-party scheme).
2. Payments are usually numerous, each one of low amount.

3. Payments are settled on a continuous gross basis throughout the day.

The reasons to implement a virtual currency scheme are several, and may vary according to the specific digital currency taken into account. As it was said before, this work aims to analyse the cryptocurrencies, in particular Bitcoin, and their impact on a traditional monetary economy environment. Therefore, the next chapter will look at Bitcoin and its implications as a virtual currency scheme.

Chapter 2

Since the invention of the Internet and the World Wide Web our society has become more and more "digitalized". In the last 30 years we have been witnesses to a massive shift of our lifestyle from real connections to digital ones, articulated by an unparalleled growth and development in IT technologies. Obviously, the changes in our customs have affected also the economy and business activity, giving birth to a relevant number of businesses, operating mainly and even exclusively on the web. In this perspective, the development of virtual currencies appears as the natural step to be taken along this road. As it was said in the previous chapter, there are several examples of virtual currencies, some of which more successful than others; however, in the last months one virtual currency in particular has been under the spotlights, attracting the attention of medias, investors and institutions alike: Bitcoin. Bitcoin is, as in the definition given by its inventor, Satoshi Nakamoto[12], "A purely peer-to-peer version of electronic cash…allow(ing) online payments to be sent directly from one party to another without going through a financial institution" (Nakamoto 2008). Bitcoin is a mathematic answer to the malfunctioning and problems embedded in our centralized monetary system. It is an ambitious project, with roots inside the cypherpunk movement[13], which offers an alternative that may appear utopian to some, but must not be underestimated for two simple reasons:

1. The phenomenon is still in its infancy; nevertheless it has caught the world's attention. Never mind if good or bad, this publicity is a strong premise for a further expansion.
2. Apart from the economic efficiency this system may present and its effective feasibility in the long run, its ideological component is real and has opened the path for future similar projects.

[12] Satoshi Nakamoto's figure is shrouded in mystery. After releasing the Bitcoin protocol in 2008 and the Bitcoin software in 2009, he disappeared in 2010 without leaving any trace behind. Nobody knows who he actually is, many think the name is just a pseudonym hiding not simply one person, but several, the main reason being the complexity of the Bitcoin algorithm. In February 2014, Newsweek's Leah McGrath Goodman claimed to have tracked down the real Satoshi Nakamoto. Dorian S. Nakamoto has since denied he knows anything about Bitcoin, eventually hiring a lawyer and releasing an official statement to that effect.

[13] Activist movement, which advocates the use of cryptography on the Internet as a tool for social and political change.

Leaving aside for now all the issues and implications this crypto-currency has, we shall look at how Bitcoin system works. The technical complexity is indeed an issue. I do not want to go too deep into the details of its mechanic, both because this is not the aim of this analysis and because cryptography is not one of my competences. However, I will try to explain as much as it is necessary for my purposes, since otherwise any attempt to any kind of analysis would be pointless and superficial.

2.1 Bitcoin Mechanics[14]

2.1.1 A Brief Summary

Bitcoin is an electronic payment system, allowing transaction between two individuals directly. In fact, the Bitcoin system is decentralized, meaning that there is no central bank or authority, which controls it and guarantees its stability. All the transactions, instead, are based on a peer-to-peer network[15], whose integrity is kept by the nodes belonging to it. Bitcoin is also defined as a crypto-currency, since cryptography is heavily used to enable every transaction. When we talk bout Bitcoin transactions, we cannot consider them as traditional coin transactions: they represent entries in a global digital ledger. Therefore, suppose a party wants to transfer some Bitcoin to another, it has to specify the amount of coins involved in the transaction and apply a digital signature to the operation, so that her digital identity is tied to the transaction. It is important to highlight that identities in the Bitcoin network are not real, physical identities; they are numbers that act as a pseudonym for the real person behind the transaction, thus ensuring a high level of privacy. Once the transactions details are specified, they are broadcasted to the entire system. It is this public disclosure to all the nodes that guarantees the goodness of the operation to the recipient party. However, the latter still faces a problem: how can it be sure that the received Bitcoin have not already been spent? This phenomenon, known as double spending, is, in fact, one of the main problems afflicting electronic transactions. The

[14] The following paragraph is based on Khan Academy Bitcoin tutorials, available at:https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it

[15] A peer-to-peer network is a type of decentralized and distributed network architecture in which individual nodes in the network, called peers, act as both the suppliers and consumers of the resources. The key behind its functioning is the cooperation among the peers.

main novelty of the Bitcoin system lies exactly in the way it deals with double spending. There are some nodes in the network, known as miners, whose task is essential to the survival and maintenance of the network itself: they collect all the transactions occurred within a certain time period in what is called a transaction block. In doing so, they give a sort of authenticity certificate to every transactions, allowing all the nodes to acknowledge each block as valid. This proof of work mechanism, which will be discussed in more details later on, is the heart of the decentralized nature of the Bitcoin system and it is what controls the money supply, since miners are rewarded with brand new Bitcoin for each block they create.

2.1.2 Cryptographic Hash Functions

In order to be able to explain the Bitcoin mechanism in an exhaustive way, some concepts needs to be clarified, even if just at an intuitive level. It is not possible to talk about Bitcoin transactions and crypto-currency more in general, if we do not define what a cryptographic hash function is. As its name may suggest, it is the building block of cryptography, and it can account, as one of its first applications, the digital signature system. In general, a hash function is a mathematical function that takes an input, of arbitrary length, and applies a mathematical transformation to it, in order to obtain a single output, the digest or the hash, of fixed size. The hash function is deterministic: for a given input the output will always be the same. A hash function can be defined as cryptographic, when it shows some properties, which make the function suitable for cryptographic purposes:

1. Computational efficiency: when using a cryptographic hash function, it should not take too much time to compute the output from any input.
2. Collision resistance: it must be hard to find two inputs, whose corresponding digests are identical. Given the fact that the input can have an arbitrary length while the output size is fixed, it is not mathematically possible to guarantee this property. Therefore, for the property to hold, it is required an astronomically long time to find such two inputs.

3. The function must give an output that hides any details concerning the input, even the most irrelevant ones. It must not be possible to infer something about the input from the output.
4. The output must be well distributed, in other words it must look random.

Therefore, a cryptographic hash function is a function that applies a mathematical transformation to an input, so that the output looks completely unrelated to it. Unfortunately, these properties cannot be mathematically guaranteed: a cryptographic hash function is trusted to have them, based on how long it has been used.

2.1.3 Digital Signatures

As it was mentioned above, cryptographic hash functions were firstly conceived with the digital signature mechanism in mind. A digital signature is a mathematical mechanism to combine a public sequence of number with a digital message. As a handwritten signature binds the identity of the person who signs a document to the document itself, a digital signature is way to obtain the exact same result when dealing with digital documents. Since it accomplishes such a task mathematically, a digital signature is harder to forge than a physical one. Supposing we have an agent, A, that wants to digitally sign a document. In order to do so, she has to generate two keys:

- A signing key, which is private, only agent A knows it.
- A verification key, which is public, instead, and is provided to the message receiver.

These two keys are mathematically related to each other; most importantly, only knowing the verification key, it should be nearly impossible to find the equivalent signing key. The digital signature process can be divided into two steps:

- Signing process:

Before proceeding with the actual signing, a cryptographic hash function will be applied to the arbitrary length message. Then the digest and the agent's signing key

will be combined, with a mathematical transformation, in order to obtain a shorter sequence of numbers, which will be the signed message. This signed message will be such that only the agent owning that specific signature key could have produced it.

- Verification process:

It requires three elements: the original message, the signed message and the verification key. It's a simple validation procedure. Basically the verification key is used to confirm whether the message was signed by the agent whom the key is referred to. This can be done without knowing the used signing key, thanks to the mathematical relationship between it and the verification key.

With this procedure an identity has been tied to a digital message: it's the mathematical analogue of a handwritten signature. Some things need to be noted, though. First of all, the signed message has, as one of its inputs, the hashed message, so the signature changes if the original message changes. Secondly, since a cryptographic hash function is used in the beginning to obtain a fixed size message, it is very important that the collision resistance property holds, otherwise we could end up with a same-signed message for two different original messages.

2.1.4 Proof of Work Protocol

The last building block, needed in order to comprehend the Bitcoin mechanism, is the proof of work protocol. A proof of work protocol is a vehicle through which someone is able to prove that she has engaged in a considerable amount of computational effort. It basically consists in a puzzle, a mathematical problem, which needs to be solved. This problem, also called challenge, requires a huge effort in terms of computations, but once a solution is provided, it is straightforward to check the amount of work behind it. The challenge and its solution are bound together by some mathematical properties; usually, the main requirement is that combining together the challenge and the solution with a cryptographic hash function gives an output such that a certain number of its first bits will be zero. Since, as it was said before, the output of a cryptographic hash function looks random, coming up with a proof that

gives the required number of zero is not easy, it resembles the process of flipping a coin: the challenger will have to try for an amount of time which is proportional to the number of zero bits required (i.e., if the first 40 bits of the output must be zero, the average number of trials corresponds to 2^{40}, which is approximately one trillion trials). Therefore, the proof of work protocol can immediately assure that a relevant computational effort has been employed.

2.1.5 The Mechanism

After having briefly explained the key concepts behind the Bitcoin protocol, it is finally possible to start describing how it works.

Basically, every transaction from a node to another works with the digital signature mechanism described above. When installing the Bitcoin software on a computer, the user has access to its own digital wallet, where all of her Bitcoin will be stored[16]. This wallet has a verification key and a signing key. Obviously, the former is available to all the participants in the network and it's used by the recipient of the transaction to verify the authenticity of the transaction itself. The signing key, instead, is known only by the owner of the wallet and it's used to digitally sign the transaction. It is extremely important to keep this key secret: if someone finds it, she could access to the key owner's Bitcoin wallet.

The main feature of the Bitcoin protocol is the so-called transaction block chain. Every Bitcoin transaction, which is nothing but a sting of numbers, can be seen as an entry in a digital ledger, which is broadcasted to all the nodes belonging to the network. Some of these nodes, the miners, collect and order every transaction, thus creating a transaction block, which can be seen as a page in this digital ledger. New transaction blocks are constantly added to the previous ones, thus forming a chain,

[16] "A Bitcoin client installation currently takes more than 14 GB of disk space and requires several hours in order to download and index the current block chain. Therefore, users started relying on centralized services that host the main Bitcoin functionalities, called web wallets. A web wallet is an online wallet, hosted on a remote server and accessible through a website. It is instantly functional, does not occupy hard disk space, is accessible anywhere and is consequently more convenient than a local Bitcoin client" (Gervais, et al. 2013).

through a proof of work system. In the Bitcoin case, this system works as following. First of all, every miner in the network gathers all the transactions occurred within a certain time interval and begins to hash them in pairs, until they obtain a single digest. This digest is then combined with the previous transaction block through a cryptographic hash function. The output thus obtained is the challenge every miner tries to win, by finding a proof that, once combined with the challenge, gives a hash whose prefix contains a certain number of zero. When a solution to the challenge is found, it is broadcasted to the network; the block is immediately added to the chain and the miners start working on the next block. The winning node is rewarded with newly emitted Bitcoin[17] (in a fixed amount) and all of the transaction fees[18] related to that specific block. Obviously, as in every proof of work protocol, finding the proof is extremely difficult. In the Bitcoin system the complexity is calibrated to the computational power and six of the network, so that on average it takes 10 minutes to solve the challenge. It may happen that more than one miner finds a solution, in this case there is a fork in the transaction block chain. More specifically, supposing two solutions are found for the same block, they are both broadcasted, therefore some miners will work on one solution, some on the other. When a new solution is found on one of the two forks, the longest branch is the one that will be unanimously accepted, and its blocks will be added to the chain. In this way, any eventual tie is easily resolved, by choosing the chain that required the greatest amount of effort[19].

Money supply is the reward for miners' effort, but it is limited: once the number of Bitcoin in the system reaches 21 million, new Bitcoin creation is going to cease. At this point, miners, whose work is essential to the network functioning, are going to be rewarded with transaction fees only. The hope is that by the time Bitcoin generation is over, the number of nodes in the network will be huge; therefore transaction fees will have much more weight than they do now. The number of Bitcoin created every 10 minutes decreases over time. When the system started, each new block granted 50 new Bitcoin. Every 200,010 blocks the reward gets halved. Since on average it takes

[17] Each miner is allowed to insert a transaction for themselves in the first transaction block that will reward them with new Bitcoin if they find the proof. This type of transaction is called coin base transaction or generation transaction and it's basically how money supply is managed in the system.
[18] Transaction fees are optional (for now) and set by the payer of each transactions. They are an incentive for miners to do their job.
[19] With effort we mean the amount of CPU computational power and electricity devoted to solving the algorithm of the proof of work.

10 minutes to add one block, 200,010 blocks requires more or less four years[20]. Given this progression, the money supply is reaching its roof in year 2140. The proof of work complexity calibration occurs every 2016 blocks. The network estimates the time that was needed to add them: if it took significantly more than two weeks[21], than the challenge becomes simpler, on the other hand, if the work took significantly less than two weeks, then finding the proof is going to be much more complicated. In general, as the number of nodes increases, the proof of work will be solved faster, therefore its complexity is constantly increasing. As for now, it has been reached a point where normal CPUs are not enough anymore to solve the algorithm, thus specialized hardware is being built to be exclusively devoted to Bitcoin mining.

Having given, hopefully, a clear and exhaustive explanation of the Bitcoin protocol mechanism, it is now possible to move onto a more in-depth analysis of the phenomenon. In particular, one of the most interesting issues, which have been object of heated discussions, is the possibility of cheating the system, and other securities concerns. Exemplary is MtGox's case: the major Bitcoin exchange declared bankruptcy because of a bug, which led to a massive theft of bitcoins from its accounts. Therefore security is a key problem, worth specific consideration in this analysis. Moreover, thanks to the high level of privacy involved in Bitcoin transactions, this crypto-currency has been an ideal choice for illegal dealings, raising also ethical concerns about its use.

2.2 The Limits of Bitcoin

Far from being the perfect currency, Bitcoin indeed shows some concrete limitations, raising concerns both among its users and its critics. The major worries are the ones about protocol security, mainly involving forgery, and the possibility of thefts, both at a network and hardware level, and the ones about ethical and ideological issues about

[20] Right now, indeed, the reward is 25 Bitcoin.
[21] Two weeks being the average time needed to add 2016 new blocks, if the average solving time for each block is 10 minutes.

Bitcoin usage, which should not be underestimated since one of the most important drivers leading to Bitcoin success is the ideology behind it.

2.2.1 Forgery, Double Spending and Selfish Mining: Is Honesty Actually Rewarding?

As far as defrauding[22] the system is concerned, the Bitcoin system is a good example of what in mechanism design is called an incentive-compatible mechanism. Whenever designing a certain mechanism of social interaction, the problem of revealing agents' preferences arises. In economic theory, as well as in real life, information asymmetry leads to inefficiency, preventing a system to achieve its optimal allocation. The designer would like the agents to truthfully reveal their type, so that the aim she wants to reach with her mechanism can be fulfilled. In order to make the agents share truthful information, the designer has to build her mechanism in such a way that being honest is rewarding for the agents. In other words, honesty has to be a best response strategy, given rationality and intelligence assumptions[23]. There are two types of incentive-compatible mechanism. One is called dominant strategy incentive compatible, where truth revelation is a dominant strategy for each agent, no matter what the others do. The other is called Bayesian Nash incentive compatible, where truth is the best choice if also the other agents choose to be honest. In the case of the Bitcoin protocol, the mechanism designed to prevent frauds, the mining, is built such that every miner has an incentive to mine honestly, in spite of what other miners do . Therefore, it could be said that the Bitcoin protocol is dominant strategy incentive compatible. This statement is surely strong, but it can be supported as strongly, as it will be done below.

[22] With defrauding the author means all those activities that target the protocol itself to forge or double spend Bitcoin. Theft, meant as hacking the system to get access to users' wallet and steal their Bitcoin or as steeling the physical hardware where the coins are stored, is considered as another type of problem, which will be analysed later on.

[23] On the validity of such assumptions in the real world, many doubts can arise. However, specifically with the Bitcoin case in mind, it can be reasonable to assume that Bitcoin users wants Bitcoin value to be as high as possible, whatever their reason might be, since it is a currency and the utility which comes from it is mainly due to its value and purchasing power. Therefore, they can be considered rational agents in economic terms, meaning that they seek utility maximization.

Simply speaking, all the nodes[24] in the system have an incentive to behave honestly. From an intuitive and simplistic point of view, this is so for two basic reasons:

1. Cheating is extremely difficult, mathematically and in terms of hardware capacity;
2. The Bitcoin system is based on shared trust among its users. If there is no trust, users will leave and the crypto-currency will be worth nothing.

An example can help in making things clearer. Suppose a node wants to cheat the system, i.e. it wants to double spend. In order to do so, it has to build not just one block, but an entire transaction block chain, from the genesis block till the last added block, inserting the false transaction inside it. This means it has to solve an extremely complex proof of work challenge, putting lots of effort into it, since for the fake chain to be accepted by the network, it has to be the longest (the one with the greatest effort). While doing so, the cheater is competing with other miners, honest ones, who instead keep adding new true blocks to the original chain every 10 minutes, thus further complicating the problem she has to face. In order to succeed, the dishonest node should own a computational power greater than the one owned by the rest of the network, considered as a whole. As of today, there is no technology capable of doing so. Let's assume, however, that this cheater actually succeeds into accomplishing this task. The system will rapidly discover the fraud and some nodes may choose to leave the network, because they do not trust it anymore. This will decrease the Bitcoin value. So the cheater will loose wealth. Instead, if a node actually owns such computational power, it would be better off mining honestly, because it would definitely solve the challenge and receive the reward: new Bitcoin plus all the transaction fees. Moreover, since the integrity of the system has not been threatened, its wealth won't be at stake. The same reasoning is valid for forgery. Everything looks fine, however forgery and double spending are not the only temptations, which miners can fall into. The incentive compatibility of the mining process can be put in discussion by a simply selfish behaviour and collusion within pools of miners, without breaking the rules, but simply bending them. As it can be expected, miners' behaviour is the object of a lively debate. Some argue that miners can collude in order

[24] We can talk about nodes more in general and not specifically miners because very node can be a miner and mining is the only channel through which fraud can take place, as it will be explained.

to gain more from their activity, than what is normally expected. Eyal and Sirer, in a white paper published in October 2013, argued that the Bitcoin system, as it is right now, is vulnerable to what is called selfish-mining (Eyal and Sirer 2013). Selfish mining occurs when a pool of miners agrees on not revealing to the network the blocks it mines. Mining pools have been active since the harbours of the Bitcoin network, because joining a pool reduces the income variance for a miner. It is a way for miners to predict more easily their average reward. As the authors state, up until now, pools have been behaving honestly, without any known case of selfish-mining. In their paper, Eyal and Sirer offer a detailed description of what selfish mining is and how it works. For simplicity, they assume the existence in the network of only one pool, which opts for selfish-mining, while the rest of the miners behave honestly (whether they gather in pools or not is irrelevant). The dimension of the dishonest pool does not have to be large: selfish-mining does not require more than 50% of the computational power available in the network to work, and this is probably the main reason why it is so dangerous for Bitcoin, in the authors' opinion. As it was said above, the pool decides not to keep hidden the blocks it mines. Basically, the pool and the rest of the miners start mining a new block. Two situations may occur: the honest miners find the new block and add it to the chain, in which case nothing happens and everyone starts mining the next block; or the pool finds the solution to the proof of work and thus can implement its strategy. There are several situations at this point that can determine the success of selfish-mining:

1. The pool finds the block, keeps it hidden from the network and starts working on the following one. However, it is not able to find this new block before the honest miners publish their solution to the previous challenge. The pool is forced to reveal the block they mined, thus creating a fork in the chain. Obviously the pool mines on its own block, while the rest of the miners will mine either on the pool block or on the honest block. This situation can lead to three outcomes:
   a) The new block is found by honest miners, mining on the honest chain. In this case, the pool makes no profit and its chain is aborted.
   b) The new block is found by honest miners, mining on the pool chain. In this case, the pool chain gets approved, with the pool gaining on the previous block and honest miners gaining on the one they have just added.

c) The new block is found by the pool, mining on its chain. In this case, the pool broadcasts it immediately, winning the rewards for the two blocks it mined. The honest chain is dropped and everyone works on the pool chain.

2. The pool finds the block, keeps it hidden and manages to add new blocks to its dishonest chain, while the rest of the miners work on the public chain. However, since the pool's computational power is not greater than the power owned by the rest of the network, sooner or later the honest chain will catch up with the hidden one. When the pool chain is only one block ahead of the public chain, the dishonest miners reveals their chain, which, being the longest, is the one that the network acknowledges. The pool gets the reward for all the blocks it mined on its chain, gaining a higher profit than it would have gained through honest mining.

It is clear how selfish-mining makes honest miners waste a considerable amount of computational effort, while it allows the pool to increase their expected revenue. Moreover, this practice doesn't go against any specific protocol rule: selfish miners do not forge or steal Bitcoin. According to Eyal and Sirer, the Bitcoin system is completely exposed to this danger, because the computational power owned by the pool needs not to be over 50% of the total one, they found out that only 33% of the mining power is enough for the protocol to be incapable of defending itself from selfish-mining (Eyal and Sirer 2013). In the two authors' opinion, the threshold for the pool size, after which every miner would have an incentive to join such a pool, is basically zero: it's sufficient that a small pool starts selfish-mining for all the other miners to have an incentive to do the same. There is no incentive compatibility: everyone will want to join the dishonest pool, and the system will not be decentralized anymore: the biggest pool will control the mining process and thus the money supply. The proposed solution is to completely randomize the selection on the block to mine on in case of chain forks. This should protect the protocol against attacks from selfish-mining pools, owning less than 25% of the mining resources (Eyal and Sirer 2013). The validity of this analysis, though, is criticized by several Bitcoin enthusiasts, who instead claim that the protocol is indeed incentive compatible, also when taking selfish-mining into account. The arguments in their support are mainly two, one related to game theory considerations, and the other involving past behaviour. Starting from the first one, Cunicola, in a synthetic 2013 paper, specifically addresses the Eyal's and Sirer's paper, nullifying their thesis with basic game theoretic concepts

(Cunicola 2013). In fact, the whole mining process can be seen as an infinitely[25] repeated Prisoner's Dilemma, with two possible actions for every miner: behave honestly, or behave dishonestly, for example as in selfish-mining. The classic, static Prisoner's Dilemma has as its Nash equilibrium a non-efficient allocation: the prisoners would be better off by colluding, but they have no incentive in doing so. If mining were a static game, than it would happen the same: every miner would opt for selfish-mining, since they don't care about what happens next. However, when the game is infinitely repeated, it is possible to solve the dilemma. In a dynamic Prisoner's Dilemma, in fact, each player can adopt in every sub-game what is called a trigger strategy. Given the two possible actions in the game, confess or cooperate, the trigger strategy is:

- Choose cooperate if every other player has cooperated in all the previous sub-game.
- Choose confess if any other player has confessed in the previous sub-game.

With this strategy, if a player acts selfishly, she is punished forever. Such a threat is credible only if the present value of the payoffs of cooperating is greater than the present value of the payoffs of confessing. This depends not only on the payoffs linked to each action, but also on how much each player cares about future outcomes, in other words on their discount rate (Gibbons 1992). Going back to the case of Bitcoin mining, the two actions, honest-mining and selfish-mining, have as payoffs coins and, most importantly their value. Mining honestly or not influences the crypto-currency worth, not only now but also for the future. Under this perspective, the threat of a trigger strategy such as:

- Honest-mining if every other miners have been mining honestly in the past;
- Selfish-mining, if another miner did so in the past.

is indeed credible because

1. Selfish-mining is going to decrease Bitcoin value, making its price drop, so it generally leads to lower payoffs.

[25] It's not sure hoe long Bitcoin will survive, but assuming it will go on at least until 2140 (since mining will keep getting a reward), with the average of one block every 10 minutes, the number of time the mining game is repeated can be approximately close to infinity.

2. Miners do care about future payoffs. In fact, in order to mine, they now have to invest resources into buying specific hardware[26], whose value is proportional to Bitcoin value. If it is worth nothing, also the mining equipment is.

Given these reasons, selfish mining is less profitable than honest mining and the Bitcoin protocol is indeed incentive compatible (Cunicola 2013). The second argument in support of the incentive compatibility of this system only strengthens the reasoning above. Since the beginning of the Bitcoin protocol, several mining pools have been operative, however selfish-mining has never been noticed as a practice among them. Obviously, they must have thought about it, since it is not such a difficult strategy. The only conclusion that can be derived from it, is that they saw it as unprofitable in both the short-run and the long-run.

The incentive compatibility of the Bitcoin protocol is well proved and rests on solid basis. Thanks to it, cheating the system or trying to turn the protocol mechanism to one's own advantage is practically impossible. However, this doesn't imply that the system is safe from other types of threats. For example, Kroll, Davey and Felten in a recent paper argue that the Bitcoin protocol is vulnerable to an 51% attack that aims to achieve utility outside the Bitcoin economy (Kroll, Davey et al. 2014). The authors call this type of attack Goldfinger attack[27], and hypothesize that a plausible perpetrator of such a move may be the government or other law enforcement institutions, which seek to destroy the Bitcoin system to deter money laundering or achieve other institutional goals. A Goldfinger attack can be modelled as a two-player game, with Auric, who wants to destroy the Bitcoin, and Bond, who stands for the Bitcoin system. If Auric succeeds in its intent, he will get a utility of A. Bond, instead, will get his utility by preserving the value of Bitcoin, B. The game starts with Bond setting a reward for mining, C, which miners will expect from their activities. Then Auric has two choices: either he pays more than C to destroy the cryptocurrency, or he does nothing. If Auric manages to destroy Bitcoin, he will get a payoff of A - C, while Bond's one will be zero, otherwise he does nothing, getting no payoff, and Bond preserves Bitcoin, with a payoff of B - C. The price C each player is willing to pay cannot exceed the amount of their respective utilities. Therefore, if A > B, Auric

[26] See previous paragraph.
[27] The name of the attack comes from the 1964 movie "Goldfinger", the third of the Bond series , where the main villain, Auric Goldfinger, tried to lower the value of U.S. gold reserves by making them radioactive.

will destroy Bitcoin, because Bond is not able to set up a high enough reward for miners; if A < B, then Bond will save Bitcoin, setting a reward C = A. A is therefore a sort of tax Bitcoin has to pay in order to stay alive, in terms of mining equipment and computational effort (Kroll, Davey et al. 2014). The problem is, however, that Bond may not know the value of A: when he bids the reward he has to guess, making assumptions on Auric's utility function, and choosing a bid, x, which maximizes his utility. If he's not able to do so, the currency will die. Moreover, a death spiral scenario can open: if Auric's threat is not sufficiently credible, Bond cannot justify any expense to save Bitcoin, thus making profitable for the attacker to bluff. In this way, Auric can scare off rational agents from the system, without actually launching a real and expensive Goldfinger attack (Kroll, Davey et al. 2014).

Apart from this scenario, in more than one occasion, Bitcoin survival has been threatened, with users' wallets attacked and Bitcoin stolen. Moreover, this crypto-currency is heavily impaired by its dependence on physical hardware storage units. These are other issues highly worth further consideration.

2.2.2 Hiding Bitcoin Under The Mattress: The MtGox's Case

The title of this paragraph wants to be ironic, but it focuses on a true problem for the crypto-currency: thievery. One of the major vulnerability and limitation of Bitcoin is the ease, which they can be stolen with. Beware, a relative ease. Stealing Bitcoin requires either high-level skills in informatics and cryptography, but people with such competences, even though they may be few now, are constantly increasing in our society. Or simply, an extremely good burglar, who can sneak in and steal Bitcoin storage hardware. In these years, we have witnessed several examples of the first type of thefts, none of the second, at least as far as our knowledge goes. In general, the slightest distraction can lead to the loss of Bitcoin wallets, with close to zero chances to recover what has been lost. In order to better understand why thievery is a relevant problem, one thing has to be made clear. That is, how Bitcoin is stored. Maybe some would expect a strange and cryptic system, given the complexity of the Bitcoin protocol. But this is not the case. Bitcoin and their wallets are stored as normal files on the hard disk of the device where the wallet is installed. The point is that Bitcoin,

the currency, is encrypted, its wallets are protected just by password. Hypothetically, if someone had access to someone else's wallet password, which is not that difficult, she could easily transfer the Bitcoin to her own wallet. This is clearly a huge limitation. Also loosing the hard disk storage unit would imply the loss of the coins on it. One of the proposed solutions is to constantly making back-ups of the wallet. But then there is another hardware to worry about. So this is not truly a definitive solution, but it's the best option for now. Another vulnerability is represented by online Bitcoin wallet held by Bitcoin exchanges. Some hackers may succeed (and did) into breaking into the exchange servers and steal users' Bitcoin digitally, not to mention that the software, used by the exchanges to manage its users' wallets, may present technical defaults, further increasing the risk of thefts. On this regard, as of today, the most exemplary case of such an occurrence is the one that involved MtGox. Before discussing this case into further details, it is opportune to describe how a Bitcoin exchange works, so to better understand the events that led to MtGox's collapse. Bitcoin exchanges are intermediaries among Bitcoin users, which work similarly to banks. Similarly, meaning that clients open accounts on the exchange servers in which they deposit either Bitcoin or real currency. It goes without saying that for this to be possible both the exchange and the clients have to be part of the Bitcoin network, meaning that each has their own Bitcoin wallet. The exchange works as an intermediate among its clients, matching their buying and selling orders[28]: users do not buy and sell Bitcoin from and to the exchange, but only among each other. An example can help make things clearer: suppose user A wants to buy Bitcoin with dollars, while user B wants to sell her Bitcoin for dollars. A and B both place their orders[29] on the exchange, and, assuming their bid and ask prices match, the trade takes place. Basically the exchange takes the dollars on A's account on its (the exchange's) e-wallet and transfer them on B's account, always on its e-wallet, and it takes the coins, which B has transferred from her Bitcoin wallet on her account in the exchange Bitcoin wallet, and transfer them on A's account. The Bitcoin is still on the exchange wallet. User A is allowed to make a Bitcoin transaction, transferring her newly acquired coins from the exchange to its own Bitcoin wallet, or she could keep

[28] In general, there are two types of selling and buying orders: limit orders and market orders. Limit orders allow a buyer to place on order at a lower price than the current price and a seller to sell Bitcoin at a higher price. Once a match is found, for this order to be executed the counter parties have to give their approvals. A market order, or instant order, is an order where the issuer specify simply the quantity of Bitcoin she wants to buy or sell. The exchange looks at limit orders and executes the trade with the most convenient match for the issuer; i.e., lowest price when buying, highest price when selling.

[29] Communication between the exchange and its clients happens through a common web browser using a secure SSL connection.

her Bitcoin on the exchange so to have them ready for an eventual selling orders[30]. This is the general mechanism through which a Bitcoin exchange works, then each exchange may present its own peculiarities, which do not affect the mechanism core, though. MtGox, too, worked in this way.

MtGox's case

MtGox was one of the major Bitcoin exchange platforms, counting thousands of users. Based in Tokyo, it was launched in 2009 as an online trading platform for "Magic: The Gathering[31]" cards, a popular card game; however, in 2010, its founder, Jed McCaleb changed the site into a Bitcoin exchange, soon becoming the largest-volume Bitcoin exchange. In March 2011 McCaleb sold the platform to Mark Kerpelès, a French developer who was working in Japan. The problems began some months after that, in June 2011. The site, in fact, was hacked, with the result that many usernames and passwords were leaked. The culprits, then, accessed MtGox through an auditor's account, issuing huge selling order for non-existing coins. This, of course, led to a plummeting in MtGox Bitcoin price, from $17.51 to $0.01 in few minutes. The cause of this security failure seems to be attributed to the change in the platform hashing protocols that left exposed the accounts, which were not accessed into over the past two months. The management response was to reverse all the day transactions and suspend the exchange site to check and fix its security. Still, this attack caused delays of transfers and withdrawals, raising doubts about the solvency of MtGox. These delays, especially those of withdrawals[32], persisted in the following months, together with other minor issues, but apart from occasional complaints, the exchange went on as usual. 2013, though was a problematic year for the platform. In fact, in April 2013, MtGox was the victim of a distributed denial of service[33] (DDoS), suffering of several lags in the trades. Rumours have it that the attacked aimed not to DDoS protected servers, but to a single open server, running both the website and the exchange, which was found by a simple scanning of MtGox's assigned IP block. Then, periodically, users would experience lags or connection problems, especially

[30] It must be remembered that for a Bitcoin transaction to be approved, it has to be included in a block. That takes on average 10 minutes (see the previous paragraph for further clarifications) and this can become an issue, especially for those who want to do arbitrage on Bitcoin.
[31] MtGox is the acronym for Magic: The Gathering Online eXchange.
[32] These withdrawals issues may be one of the reason behind the higher U.S. dollar price on MtGox.
[33] A denial of service is an attempt to make a machine or a network resource unavailable (temporarily or indefinitely) to its intended users. The denial is called distributed when it is conducted by two or more persons or hosts.

during busy market times, resulting in frequent site suspensions. In May 2013, the Department of Homeland Security issued a seizure warrant for MtGox's account at Dwolla[34], their payment provider, because the latter hadn't registered as a money transmitter with FinCEN[35] in the U.S[36], for an amount of $2.9 million. June 2013 saw U.S. Dollar withdrawals temporarily suspended, and overall, the following months were quite problematic for the exchange and especially its clients: only few of them were actually able to sell their Bitcoin for money and always waiting weeks or even months for their orders to be executed. Therefore, when February 2014 came, and MtGox had been registering an increasing backlog of failed Bitcoin transfers, also those got suspended. The reason behind MtGox failure is to be searched in its client software, which managed Bitcoin transactions, specifically in the way it dealt with the so called transaction malleability[37] bug. Transaction malleability is a flaw that lies within the Bitcoin protocol itself. As it was explained in the previous paragraphs, during a Bitcoin transaction the sender digitally signs all the relevant information relative to the transaction itself, mainly the Bitcoin amount, the sender, and the recipient. Then, a transaction ID is generated, which uniquely identify that specific transaction. However, this ID comes also from an unsigned, thus insecure, part of the transaction. Due to this, it is possible to modify[38] the transaction ID, without the sender permission. Obviously, the sensitive information cannot be altered or lost, being digitally signed; still some problems may arise if the sender is expecting the transaction to show up in a block under a particular ID. Transaction malleability has been known since 2011 and can be rendered harmless with software, which accurately reports balances and transactions. As the Bitcoin Foundation[39] stated, "any company dealing with Bitcoin transactions and which have coded their own wallet software should responsibly prepare for this possibility (transaction malleability) and include in their software a way to validate transaction IDs[40]". Unfortunately, in MtGox's case, the implemented software transmitted zero-padded transactions IDs, which other Bitcoin software do not recognize anymore, because sensitive to transaction

[34] Dwolla is a U.S. e-commerce company, which provides an online payment system and mobile payment networks.
[35] The Financial Crimes Enforcement Network is a bureau of the U.S. Department of Treasury that collects and analysed information about financial transactions, in order to fight money laundering, terrorist financiers and other financial crimes.
[36] In February of the same year, MtGox had experienced another trading incidents with Dwolla, due to the implementation of new anti-money laundering requirements by the latter.
[37] Always in February 2014, Silk Road 2.0 reported stolen Bitcoin because of the transaction malleability bug. For further information on Silk Road's case, see next paragraph.
[38] The digital signature consists of two large integers. Any leading zeros should be dropped, but even if they aren't the transaction can still be accepted. Therefore, by simply prepending some zeros, the ID is modified.
[39] A non-profit organization devoted to development and promotion of the currency.
[40] The most adopted solution is that to prevent Bitcoin software to broadcast transactions with leading zeros to the rest of the network.

malleability. This problem was amplified by the fact that the exchange site had a page showing all the failed transactions, as it is explained below. Briefly, this is what happened:

- Whenever a client issued a transaction through MtGox's Bitcoin software, the resulting ID might present leading zeros.
- In this case, the transaction would be denied by other Bitcoin software and thus delayed.
- Because of transaction visibility (in the page above mentioned) and users wanting their transaction to succeed, many of them would retransmit the transaction, simply dropping the zero-padding, without accessing their own wallets.
- This altered transaction would be validated in the public ledger. However, MtGox, unaware of this modified transaction, would consider the operation failed, because its software expected to see the zero-padded transaction ID recognized.
- MtGox, believing the transaction failed, when it had actually succeeded, would try to use those Bitcoin in another transaction, which, of course, would inevitably fail.

This process went on for months, throwing the exchange into utter chaos, until MtGox shut down all Bitcoin transfers, having no clue of exactly how many Bitcoin they still possessed. Moreover this bug made the exchange easy pray for thieves. Indeed, wanting to withdraw some coins, a client could purposely send an invalid transaction (with padded zeros) and alter it, so that it is validated. Of course, MtGox would be unaware of this validation, thinking the transaction failed. So the user could try that withdrawal again, sending another transaction and fixing it[41]. In this way it is possible to completely drain the exchange wallet. Obviously this bug induced theft wouldn't have been enough for the total collapse MtGox was victim of, however, when considering the U.S. Dollar withdrawals problems and transactions delays the exchange had been experiencing since summer 2013, together with an unjustifiable

[41] The reader should bear in mind that the Bitcoin to be withdrawn are on the exchange Bitcoin wallet, and the client requesting the withdrawal from the change to its own private Bitcoin wallet can do so because she holds a sort of credit towards the exchange. For example, assuming there are only three clients on the exchange, A, B and C, each of them having a deposit of 10 bitcoins on the exchange wallet. The exchange has 30 Bitcoin and knows that it owes 10 to A, 10 to B, and 10 to C, whether any of them requests a withdrawal. Assume A wants to exploit the transaction malleability bug. She issues a transaction, where she withdraws her due 10 Bitcoin. The transaction is zero-padded so she fixes it, and gets her coins. The exchange doesn't know the transaction actually succeeded and thinks to still have 30 Bitcoin on its wallet, while the balance is just 20. So, when A asks to withdraw again, the exchange accepts the transaction, basically allowing the network to move 10 Bitcoin from its wallet to A's wallet. The coins have no owner's name on them, so the network, seeing the exchange has still 20 Bitcoin, authorizes the transaction too, once A has fixed it, without the exchange knowing it. Therefore, the thief gets 10 Bitcoin at the expenses of B or C. The exchange still thinks to have 30 Bitcoin, and the scam can go on, until nothing remains, and B and C have lost their Bitcoin forever.

lax approach to accounting (according to Ryan Selkis, a Bitcoin entrepreneur, sources inside and allied with to the company claimed MtGox has never performed a single audit procedure on its customer's deposit), the tale of the exchange could only have ended as it did: on 28 February 2014, MtGox filed for protected bankruptcy in Tokyo, after Kerpelès' resignation from Bitcoin Foundation's board (on 23 February) and the website going offline (on 24 February).

MtGox's case shows the criticality of carelessness when dealing with Bitcoin online software, as those used by exchanges. These events have also a huge impact on Bitcoin price movements: markets price this risk. However, MtGox's failure must not be considered as a failure of the Bitcoin protocol itself. As it was already said, the transaction malleability has been known since 2011 and other exchanges can perfectly manage it. Failure is physiological to business: just because a mobile company fails, for example, it doesn't mean that mobile phones have failed. Obviously, Bitcoin is not a mobile phone and as an investment, it has a high-risk profile, therefore it should always be approached with due diligence, being as aware as possible of its implications.

2.2.3 Bitcoin: Ethics and Ideology

The Bitcoin network is attracting an increasing number of clients and investors for several reasons. First of all, its growth potential is enormous. Anonymity is a huge incentive, too. It is definitely a winsome feature, together with the transaction time, way more rapid than traditional e-payment systems. Finally, fees are also cheaper, even irrelevant for the time being. Still, as it has been discussed, some problems persists, and it is not just the hacking and thievery issue. It is much more. It is not possible to know whether, in Nakamoto's intentions, what it can be observed now is exactly the development he wished for his Bitcoin project. What can be said for sure is that the effects, the impacts and the reactions to Bitcoin have shaken our reality. This paragraph wants to focus its analysis on less technical issues related to the crypto-currency, trying to sketch a first answer to this question: what does it mean to use Bitcoin? There are many valid responses to such a question, everyone can have

her own. More precisely, this question can be further split into other ones, tackling a different aspect of the matter. For example, what does it mean to use Bitcoin under a taxation profile? Are transactions made in Bitcoin taxable? This is an extremely important issue. As the number of businesses, online and not, that accept the crypto-currency as payment for their services is increasing, Bitcoin taxation is indeed becoming an issue. Not to mention all the people who have invested and gained in Bitcoin. The rising speed, which the crypto is spreading with, has thrown tax authorities into a rushed panic. U.S. Internal Revenue Service (IRS), after many months of silence offering no guidance to U.S. taxpayers about activities involving the virtual world and in particular crypto-currencies (Elwell, Murphy et al. 2013), has just declared that Bitcoin is to be considered as property, defining it as a convertible virtual currency (IRS 2014). Its fair value must be included in taxpayers' gross income report. Meanwhile, market regulators such as U.S. Securities and Exchange Commission, are still debating whether Bitcoin can fall under their jurisdiction (Chaturvedi 2014). On the European front, things seem to be moving faster, even though confusion still persists. Norway and Germany have been the first countries to take a position on this matter. Their tax authorities decided not to consider Bitcoin as a foreign currency, but as an asset, therefore capital gains from buying and selling Bitcoin are taxed, like for any other financial asset (Kollmeyer 2013). Also U.K. is trying to propose a solution to this problem. In these days, HMRC (Her Majesty's Revenue and Customs) is about to issue rules that would treat virtual currencies as regular money, under a taxation profile. According to some indiscretions, virtual currencies, and thus Bitcoin, won't be subject to VAT[42] when purchased, instead a capital-gains tax is likely to be levied on profits made by trading virtual currencies, in a similar fashion as for trading normal currencies and stocks (Chaturvedi 2014). Brazil, instead, in October 2013 passed a law specifically for digital currencies, including Bitcoin. Also China has taken a clear position on the matter, banning Bitcoin from financial institution (Hill 2014). Virtual currencies taxation is an issue that needs to be properly analysed, adjusting regulation on the evolution this phenomenon undertakes. The fact that authorities are still unsure about the approach to take, combined with the decentralized nature of Bitcoin, creates room for usages of the crypto-currency, definitely not legal. Activities such as money-laundering or

[42] Value Added Tax.

weapon and illegal substances trading have, unfortunately, found in Bitcoin an ally, since it is capable of offering an anonymity in transactions, rivalled only by cash. Considering this point of view, another question could be: what does it mean to use Bitcoin for illegal purposes? An answer to it can be given by Silk Road's case, being one of the main examples Bitcoin sceptics bring forward in support of their argument. Silk Road indeed represents one of the darkest sides of Bitcoin, in the specific, but, potentially, of any other digital currencies.

Silk Road's case

Silk Road was an online market for illegal products, especially drugs. It was indeed defined as the "E-bay for drugs". Obviously, accessing to it wasn't that straightforward. Silk Road wasn't the type of website that could be googled. Clients needed to use Tor[43] browser, which guarantees complete anonymity while online, in order to have access to the site. Then, after creating an account on it, and provided the user possesses a Bitcoin wallet, anyone could buy its dangerous products in total anonymity. Silk Road, in fact, resorted to Bitcoin as its only mean of payment, because of the anonymity of transactions and for years authorities had no idea how to close it. The site was launched in February 2011, by Dread Pirate Roberts[44], a pseudonym which, according to what the FBI discovered later on, covered the identity of Ross William Ulbricht, even though there is no concrete proof that ties the two identities. Buyers could register for free, sellers' slots, instead, were limited. In a first time, sellers could win a slot through an auction. Later on, Silk Road introduced a fixed fee to be corresponded by the seller, to avoid the sale of bad quality goods. The price of the merchandise was fixed on the dollar price, independently from how much a Bitcoin was worth: for example, if a certain good cost $200, the price paid was its Bitcoin equivalent. In this way, even if Bitcoin price volatility was high, prices on the site were kept fairly stable. The website took a commission fee on every purchase, and over its two and a half years of business it had accumulated a fortune in bitcoins. Some months before Silk Road's closure, Dread Pirate Roberts released an interview to the magazine Forbes, in which he clarified the motives, the ideology and the role of

[43] It's a web browser which allows access to the so called Deep Web, in other words that part of the World Wide Web which doesn't belong to the Surface Web, which instead is indexed by standard search engines. Deep Web's size is estimated to be far larger than the Surface Web's one.

[44] Dread Pirate Roberts is, originally, a fictional character from the novel "The Princess Bride". As in the story, this title was passed from one person to another, keeping the real identity behind it a secret, so on Silk Road nobody knew who he was and the title may have been passed.

Bitcoin behind the site[45]. About the latter issue, he said that the birth of Bitcoin, together with Tor, has allowed Silk Road project to become a reality. A revolution has started: " It (Bitcoin) already is transforming society. We've won the State's War on Drugs because of Bitcoin, and this is just the beginning. It's really part of a larger transformation, driven by peer-to-peer technology and the Internet as a whole. The people now can control the flow and distribution on information, and the flow of money. Sector by sector the state is being cut out of the equation and power is being returned to the individual. I don't think anyone can comprehend the magnitude of the revolution we are in. I think it will be looked back on as an epoch in the evolution of mankind" (Roberts 2013). On October 2, 2013 the FBI managed to shut down the illegal website and arrest Ulbrich in a joint operation with the IRS Criminal Investigation Division, the ICE Homeland Security Investigation, and the Drug Enforcement Administration, seizing 174,000 Bitcoin, believed to belong to Ulbricht. However, on November 6, 2013 a new website, Silk Road 2.0 opened for business, as a direct successor to the project, led by a new anonymous Dread Pirate Roberts. As of today, this site is still operating, even though it has experienced some problems due to the transaction malleability bug, previously discussed. Silk Road, unfortunately, isn't the only example of this kind of illegal online markets, which can stay on business thanks to Bitcoin or other crypto-currencies. From Dread Pirate Roberts' words, it seems like this trend is only going to increase, if governments and authorities do not take the right precautions and countermeasures. Personally, I don't believe that banning Bitcoin or virtual currencies more in general is the right step in that direction. Instead, a reasonable starting point is trying to better understand the implications and potentialities behind digital currencies, and to conceive a way to integrate them in our realities, for example setting clear rules about taxation and other legal issues concerning them. As Gavin Landresen, Lead Developer of the Bitcoin virtual currency project, said: "Bitcoin is an experiment. Treat it like you would treat a promising Internet start-up company: maybe it will change the world, but realize that investing your money or time in new ideas is always risky[46]".

This chapter, until now, has been focusing on Bitcoin, from a technical point of view, and on its most direct implications and issues. However, under a monetary and

[45] An Interview With A Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A), by Andy Greenberg, Forbes, 08/14/2013.
[46] http://gavinthink.blogspot.com/2011/06/that-which-does-not-kill-us-makes-us.html

financial point of view, there are other aspects of this cryptocurrency that needs to be discussed. The impact of Bitcoin on markets has been and still is huge, probably not even revealing its full extent yet. A further step into this analysis is required, incorporating Bitcoin in the concept of virtual currency schemes, introduced in the previous chapter, and offering an overview of its role in financial market.

2.3 Bitcoin as a Virtual Currency Scheme

A virtual currency scheme is how a particular virtual currency interacts within the community which it belongs to and, eventually, the real world, thanks to its specific retail payment system (ECB 2012). In this contest, Bitcoin is a virtual currency scheme with bidirectional flows, being consistently exchanged for real currencies and vice versa. To be more specific in classifying Bitcoin as a virtual currency scheme, the first step to take is to look at its retail payment system. The latter is extremely versatile and caterpillar: potentially it can reach everywhere in the world, as long as there is a computer and an internet connection. Being a decentralized digital currency, Bitcoin does not present relevant complexities (aside for the technical ones, relative to its algorithm) when it comes to their usage as a payment system. If two parties agree on using the crypto-currency and acknowledge its value, transactions between them can occur relatively easily and rapidly, without the involvement of a trusted third party. The only trust required is the one among Bitcoin users. A further step can be made, affirming that the Bitcoin retail payment system is its community, its network.. The Bitcoin community is what makes and defines the currency, and every single node is directly involved in the wellbeing and well-functioning of the system, especially miners, who are the ones responsible of the money supply and of the security of transactions: potentially, every node can be a miner. One can decide to accept Bitcoin in exchange for its services or products, allowing its business to cross countries borders and currencies limitations. Bitcoin has no nation, so there is no need of exchange rates if someone from Europe wants to buy something from Australia. This idyllic picture has, however, a dark side. Apart from all the issues and problems related to Bitcoin, that were previously discussed, the currency still needs to define its

purchasing power in relation to real currencies. This is certainly not surprising, still Bitcoin is showing high volatility in its exchange rates, and this aspect surely doesn't appeal to their usage for retail payments. Businesses accepting the crypto-currency, in fact, still need to anchor the Bitcoin prices of their merchandises to some real currency, constantly readjusting them in accordance with the relative exchange rate. Even though this may not be that much of a problem, it still prevents retail payment system to reach its maximum efficiency and autonomy. This scenery can change once Bitcoin becomes more stable, but, as of today, stability still seems unlikely in the short-term. Another characteristic of the Bitcoin retail payment system, which sets it apart from other virtual currency schemes, is that the services or goods, which can be purchased through it, are not specific to the Bitcoin community. It's not like a MMORPG, where the in-game currency is used to buy in-game goods. Bitcoin can buy real things, things you usually pay for with real currencies. This aspect makes the interaction between Bitcoin and fiat currencies even more interesting ad complex. Far from aiming to be a substitute for real currencies, Bitcoin can count on a growing number of supporters, who want to exploit their vast potential. For this reason, the crypto-currency is gaining relevance on financial markets, one day it may even alter the balance between traditional money and the financial environment. Therefore, it could be interesting to see whether the presence of Bitcoin in the monetary scenario is affecting areas, in particular, whether it is posing a risk to areas, which have always been of exclusive competence of fiat currencies and thus central banks: price stability; financial stability; payment system stability.

Price stability

One of the main tasks a central bank deals with is guaranteeing price stability. Maintaining a constant rate of inflation is one of the most important priorities monetary policy pursues. As long as the only money in circulation is the one issued by the central bank, the monetary authority has complete control over the task. Things, however, change when there are other monetary aggregate to consider, which are not under the control of a central bank or a central authority, like Bitcoin is. In general, a virtual currency scheme can have an impact on price stability, if it affects three aspects (ECB 2012):

- Quantity of money: the impact on this aspect consists in whether or not a virtual currency scheme, in this specific case, Bitcoin, is creating new money. In other words, whenever the protocol mint new coins, can those be actual new money, more precisely, does the issuance not depend by the exchange of real money into virtual one, and in the same fashion, does the virtual money not completely disappear once it is exchanged back into real currency? At the present moment, given the current size of the network and the value of each bitcoin, and taking into account the characteristics of the protocol, the following considerations can be achieved. First of all, new coins are issued independently from people wanting to buy them. Coinage is a result of mining, which is basically needed for transactions. Therefore, it could be said that as long as Bitcoin transactions occur, so as long as Bitcoin users attribute worth to the crypto-currency and accept it for transactions (basically, as long as Bitcoin is believed trustworthy and valuable), mining will continue, thus new coins will be created. As far as their re-absorption is concerned, exchanging Bitcoin for real money means that there is a user, or a potential user willing to buy Bitcoin against real money. Otherwise you cannot sell them. Therefore, the coins exchanged don't get re-absorbed "into the system", they don't disappear, they simply change owner. All in all, Bitcoin has an impact on the quantity of money in circulation in our economy; even though, it has still a contained impact. However, if the network keeps growing in size and Bitcoin strengthens its role as an electronic payment alternative, the points here discussed will definitely assume much more relevance.
- Velocity of money: the velocity of money is a measure of how often a unit of currency is spent to purchase goods and services produced in the economy (ECB 2012). It is usually assumed to be constant in the short-term, mainly depending on institutional and technological features. However, given the enormous technological impact Bitcoin has, not only on its own, but also in terms of spurring the development of new related technologies, it cannot be said, for sure, that the velocity of money will remain unaffected. It is still too early to determine whether this impact exists or not, but if Bitcoin popularity, as a payment system, keeps increasing, then such an effect will most likely occur. In an extreme case scenario, if Bitcoin or another virtual currency becomes so widely accepted to the point of replacing fiat money, completely nullifying fiat currency velocity, then central banks could loose most of their ability to influence short-term interest rates.

- Interaction between the virtual currency and the real ones: considerations on this aspect depend on whether the virtual currency is widespread or its diffusion is limited to a single country. In the latter case, the only real money to consider interactions with is the money of the specific country where the digital currency is used. Bitcoin, however, has a global diffusion, it does not affect just one monetary system, therefore its relationship with real money is a complex one and involves more currencies. Another issue to take into account, when performing such an analysis, is that Bitcoin is also used to purchase real goods. This means they have an impact on the real economy, on real GDP (even though now it's still limited and small); this impact needs to be considered, when assessing the relationship between Bitcoin and real money supply (Peng and Sun 2009). However, the most important thing to determine is whether the virtual currency and the real ones are competing; in other words, whether the digital currency can become not only an alternative mean of payment, but also an alternative store of value or unit of account. If this is the case, then such a currency can be considered as proper money, and the monetary authorities should deal with it keeping this consideration in mind.

As of today, Bitcoin is not a threat to price stability. The size of the phenomenon is still contained; however its relevance is growing day by day, therefore the impact of Bitcoin on these aspects discussed above can change completely in the future. For this reason, monetary authorities needs to be ready to deal with such an occurrence, monitoring the development of the crypto-currency, in order to continue to absolve their tasks to the best of their abilities.

Financial stability

Financial stability as the condition in which the financial system (comprising financial intermediaries, markets and market infrastructures) is capable of withstanding shocks, thereby mitigating the likelihood of disruptions in the financial intermediation process which are severe enough to significantly impair the allocation of savings to profitable investment opportunities (ECB 2012). As far as Bitcoin is concerned, the main channel through which it could affect financial stability is its exchange rate with real currencies[47]. These rates are determined by the interaction between demand and

[47] There exists also a market for derivatives on Bitcoin, namely futures and options, but its size and relevance is still negligible.

supply of Bitcoin on the markets, however, since the crypto-currency is not linked to a specific country or economy, the resulting exchange rate is not the expression of economic fundamentals (i.e. it does not reflect trade imbalances, or productivity). For this reason its movement are highly unpredictable and many have been comparing Bitcoin price growth to a speculative bubble. Indeed, the volatility has been high, especially in the last year, and this has started to fuel some concerns of a negative repercussion on the financial markets more in general. Furthermore, since Bitcoin is decentralized, all its financial interactions occur outside the traditional financial and banking system, and this can potentially be a threat to financial stability. But is this truly so? In order to classify an asset, such as Bitcoin, as a risk to financial stability, five aspects need to be examined (ECB 2012):

1. The relationship between the money supply and its exchange rate. In the case of Bitcoin, the rate of inflation is fixed, however no measures has been conceived inside the protocol to keep a fixed or at least stable exchange rate with real currencies.
2. The dimension of the network and eventual externalities. The greater is the network, the higher is the worth of Bitcoin. Moreover, as the number of its users increase, volatility is expected to decrease. As of today, the exact number of Bitcoin users[48] is unknown, some estimations place it around 1 million[49]. It is still a modest size, especially when compared to Bitcoin market capitalization in USD, around $ 8,053,512,189 [50]: even a single transaction can have a great impact on the exchange rate, partly explaining why the volatility is so high.
3. Rules established within the virtual community. Bitcoin is a decentralized system, the only rules are the ones enforced by the algorithm. The latter, as it was previously discussed, is incentive compatible; therefore honest behaviour is encouraged within the network. However, this aspect alone is not enough to shelter the system from external attacks and other misbehaviours.
4. Issuer's reputation. There is no central authority that manages Bitcoin supply. The protocol is set so that money supply is a result of the mining process. Mining is

[48] In this case, the author means relevant users, the ones holding more than 0.0001 BTC, whose transactions actually matter in the total volume.
[49] Source: https://blockchain.info/charts/my-wallet-n-users
[50] Source: http://coinmarketcap.com/

also what guarantees the authenticity of the coins and validity of the transactions. If users don't trust this mechanism, the crypto-currency would fall apart.

5. Conjectures about the future value of the virtual currency, and the possibility of cyber-attacks, given their history. There is a lot of speculation over the value that Bitcoin will assume in the future, greatly affecting the way its exchange rate with real currencies is formed. Moreover, given the several hacker attacks the currency has been suffering, one of the main challenges Bitcoin is going to face is that related to its storage security. If it cannot overcome such an obstacle, its value is likely to drop.

Given these considerations, as of today, Bitcoin cannot be considered a threat to financial stability. However, its weight in financial markets is growing and there are aspects of the crypto-currency, which could indeed become a menace, if they are not dealt in the proper way. For example, there is still no credit system related to Bitcoin, but if loans and debts in Bitcoin start to surface, then the interconnection of the crypto-currency with the financial system will become more complex and risky, especially under a stability point of view.

Payment system stability

Bitcoin is born as an alternative electronic payment system. Bitcoin is used daily to purchase real goods, and the number of businesses accepting bitcoin is growing. Being a payment system, even though a decentralized one, Bitcoin is exposed to the classical risks that threaten the stability of a payment system (ECB 2012):

- Credit risk: It is the risk that the settlement institution managing the payment cannot meet its obligations towards its clients. In the case of Bitcoin, there is not a settlement institution, which guarantees the payments. Users usually have online accounts on Bitcoin Exchanges, so they are exposed to the risk that the exchange does not transfer them the coins or dollar it owes them, as soon as the clients request them. Furthermore, as in MtGox's case, online accounts can be hacked, the coins held in them stolen, and exchange clients have no lender of last resort that can give them back the money they lost.

- Liquidity risk: Users may not be able to convert the crypto-currency into real currency as fast as they like. Since its volume of transaction is not comparable to the one of other payment systems, Bitcoin is still relatively illiquid.
- Operational risk: there may be technical and operational issue when making a Bitcoin transaction, and in general the network may present some occasional glitches.
- Legal risk: Bitcoin does not offer any legal protection or guarantee to its clients.

All the above issues, together with the absence of a settlement institution, make Bitcoin an unstable payment system, in which users bear themselves all the risks related to it. If the number of people resorting to Bitcoin for retail transaction were to increase, then central banks should adopt some measures to protect the traditional payment system from the instability brought forth by the virtual one. As of today, Bitcoin, as a payment system, cannot be considered an actual threat, but this doesn't imply that it could become so in the near future.

The main problem of Bitcoin as a virtual currency scheme, therefore as a new player in the monetary and financial scene, is its lack of regulation. Governments and authorities are having many problems when dealing with Bitcoin mainly because they don't know how to define it and its relationship with real currencies. Still, time is stringent: Bitcoin, and crypto-currencies more in general, have become a widespread reality, which cannot be ignored any longer. Governments and authorities need to lay out some clear guidelines to allow a more aware and responsible usage of virtual currencies.

Chapter 3

Even though Bitcoin is still in its infancy, underestimating its impact on the economy, and in general of crypto-currencies, could be a mistake. Especially for central banks and their fiat money, which could suddenly be faced by a decentralized competitor. Therefore, it could be useful beginning to analyse the interaction between traditional currencies and crypto-currencies, such as Bitcoin, introducing them in classical model of inter-temporal optimization, such as the Ramsey Model, with money in it.

3.1 Money in an optimizing framework

Introducing money in an inter-temporal optimizing model is not a trivial task. As it is modelled, in a Ramsey model there is no need for money: people can hold assets like bonds or capital, which grant a return. Money does not. The first step to take is finding out the reason why people may want to hold money in this economy. Obviously, if agents hold money, it must have some purpose that other assets cannot fulfil. The main characteristic that comes into mind is its liquidity: money is the most liquid asset in existence and this makes money an excellent medium of exchange. Still the problem remains of how to model this liquidity in a Ramsey Economy. The solutions given to this issue by economists are several; as a consequence there are several versions of a Monetary Ramsey Model. The first approach, by Sidrauski (1967), was that of considering money as a source of indirect utility. Basically, the real balances held by the agents had an indirect impact on their utility function, since its usefulness to the holder comes from the fact that it reduces transactions costs and other problems related to trades. The inter-temporal utility function in this model assumes the form:

$$U_t = U(c_t, \frac{m_t}{p_t})$$

Where:

c_t: consumption at time t;

$\frac{m_t}{p_t}$: real money balances;

p_t: price level at time t.

This approach, also known as money-in-the-utility-function, is simple and straightforward enough. Looking at the growth dynamics of this model, it turns out that money is super-neutral: when inflation increases, the amount of capital and the growth process are unaffected. Not only has the amount of money no real effect, but its growth rate as well has no impact on real components. The Sidrauski model however has been subject to several critics, like the one raised by Lucas. Indeed, if real balances provide an indirect utility, which is a result of the optimizing behaviour of the agent in response to several factor, including monetary policy, if this latter changes, then so will the agent's choices, which, being a result of an optimizing decision, shouldn't change. Therefore, Lucas, in 1980, proposed an alternative model, the cash-in-advance (CIA) model, from an idea raised by Clower. In the CIA model the good market operates before the assets and money market. For this reason, people need to hold money ahead of time to be able to purchase consumption goods:

$$m_t \geq p_t c_t$$

There is no reason for money to be source of utility; agents demand it anyways. The problem with this type of model is that money demand function does not depend on the rate of inflation. However, despite this problem, the CIA approach is often used to model monetary economies. Romer (1985), instead, extended the research of the Baumol-Tobin (1957) approach, according to which is expensive exchange money with bonds. As a consequence the consumer goes to the bank once in a while, thus holding a certain amount of money. This model, however, could only be solved in the steady state, so no further research has been conducted on it. Finally, towards the end of the 1980s, a new theory was developed to explain the presence of money in the economy. It is centred on the idea that money is preferred to barter and other types of trading system because it eliminates the so-called coincidence of wants. Suppose there is an agent in the economy that produces shoes and wants trousers, but the agent producing trousers wants hats. The first agent would need to find someone willing to

exchange shoes for hats and only then she could exchange the hats for the trousers she originally wanted. This process can be expensive and time-consuming. Fortunately, money solves such a problem. The pioneers in this field are Kiyotaki and Wright, whose students are continuing the studies on their work. The main limit of this type of model is they are complex to analyse, having abandon the dynamics of a Ramsey Economy and focusing more on agents' interaction finding the related Nash Equilibria.

If modelling money inside traditional Ramsey economies is not an easy task, modelling Bitcoin is even more problematic: its functioning and dynamics are peculiar, moreover the phenomenon is still new, with the majority of its potential largely unexplored. Nevertheless, an attempt is worth trying. Among the above-mentioned approaches, the cash-in-advance model has been chosen as the basis onto which introducing Bitcoin, since its simplicity renders it flexible and versatile. It is highly probable that this model is not the best possible candidate, but, as far as the purpose of this dissertation is concerned, which is proposing a first, basic attempt at modelling Bitcoin in a monetary economics, the CIA model fulfil its task. Before proceeding with the description of the CIA model with Bitcoin, the classical cash-in-advanced model, as proposed by Stockman (1983), will be presented, in order to allow a better comparison between the results of the two models.

3.2 The cash-in-advance model

As explained in the previous paragraph, the utility of money of Sidrauski model is indirect, therefore subject to changes of monetary politics. In order to avoid this shortcoming, Lucas proposed a model where money wouldn't enter as a source of utility, either direct or indirect, but in a cash-in-advance constraint. Indeed, the basic assumption of this economy is that in each period the good market operates before the credit market. Agents cannot exchange their bonds for consumption goods: these latter can be purchased only through money, which individuals save from the previous period. We shall now proceed to describe the CIA model, as in Stockman version

(STOCKMAN, Alan C., 1981), simpler and more transparent version than the original one.

The basic assumptions in this economy are:

- Closed economy with a single physical good;
- The good is produced through a classical constant-return-of-scale production function, using capital and labour;
- There is a continuum of infinitely lived individuals of size 1;
- There are two assets in the economy, one period loans, *A*, and money. The latter pays no interest and it is used for transaction; loans pay a nominal interest rate *i*.
- Firms are financed by loans only;
- The government increases the quantity of money at a fixed rate each period: $M_{t+1} = (1 + \zeta)M_t$, with $\zeta > 0$;
- The increase in money supply is given to individuals through a subsidy, like a helicopter drop[51]: $S_t = M_{t+1} - M_t$;
- There is perfect competition and rational expectations;

In this economy each individual tries to maximize her inter-temporal utility function:

$$U = \sum_{t=0}^{\infty} \beta^t u(c_t)$$

Where:

- $0 < \beta < 1$, is the discount rate, which is higher the more impatient is the agent;
- $u(c_t)$ is a concave standard utility function, such that:
  - $u'(c_t) > 0$
  - $u''(c_t) < 0$
  - $\lim_{c_t \to 0} u'(c_t) = \infty$
  - $\lim_{c_t \to \infty} u'(c_t) = 0$

[51] The expression helicopter drop was firstly used by Milton Friedman.

This maximization problem is subject to two constraints, the budget constraint and the cash-in-advance constraint.

Budget constraint:

$$m_{t+1} + A_{t+1} + p_t c_t = A_t(1 + i_t) + m_t + S_t + p_t w_t$$

This is the nominal budget constraint, where:

- m_t is the demand of nominal balances of each individual at time t;
- A_t is the loan to the firms at time t;
- $p_t w_t$ is the nominal per-capita wage at time t;
- p_t is the price level at time t;
- $p_t c_t$ is consumption in money terms at time t.

CIA constraint:

$$m_t \geq p_t c_t$$

This is the cash-in-advance constraint that requires each agent to hold enough money from the previous period to be able to purchase the consumption good today.

Finally, we add the NPG condition:

$$\lim_{t \to \infty} \frac{A_t}{\prod_{t=0}^{\infty}(1 + i_t)} = 0$$

In order to solve the maximization problem we need to set up the Lagrangian and find the first order conditions (FOCs).

Lagrangian:

$$\mathcal{L}: \sum_{t=0}^{\infty} \beta^t \{u(c_t) + \lambda_t [A_t(1+i_t) + m_t + S_t + p_t w_t - m_{t+1} - A_{t+1} - p_t c_t] + \mu_t [m_t - p_t c_t]\}$$

FOCs:

1. $\frac{\partial \mathcal{L}}{\partial c_t} = 0 \Rightarrow u'(c_t) = p_t(\lambda_t + \mu_t)$

2. $\frac{\partial \mathcal{L}}{\partial m_t} = 0 \Rightarrow \lambda_t = \beta(\lambda_{t+1} + \mu_{t+1})$

3. $\frac{\partial \mathcal{L}}{\partial A_{t+1}} = 0 \Rightarrow \frac{\lambda_t}{\lambda_{t+1}} = \beta(1 + i_{t+1})$

From these three equations we obtain:

$$\frac{u'(c_t)}{u'(c_{t+1})} = \frac{p_t(\lambda_t + \mu_t)}{p_{t+1}(\lambda_{t+1} + \mu_{t+1})} \Rightarrow \frac{u'(c_t)}{u'(c_{t+1})} = \frac{p_t \lambda_{t-1}}{p_{t+1} \lambda_t} \Rightarrow \frac{u'(c_t)}{u'(c_{t+1})} = \beta(1 + i_t) \frac{p_t}{p_{t+1}}$$

The latter equation can be written as:

$$\frac{u'(c_t)}{u'(c_{t+1})} = \beta(1 + r_t) \frac{p_t}{p_{t-1}} \frac{p_t}{p_{t+1}}$$

When inflation is constant, then the equation becomes the standard Euler Equation.
The Euler Equation describes the optimal inter-temporal allocation of consumption. It states that the marginal cost of reducing consumption today must equate the marginal benefit of consuming more tomorrow. In this specific model, since there is money, saving one unit of consumption today means that the agent will get $(1 + i_t) \frac{p_t}{p_{t+1}}$ units of consumption tomorrow, instead of the classical $(1 + r_t)$: consumption requires money, thus inflation need to be included in the benefit-cost relationship; increasing her lifetime utility but with a discount factor of β. In the steady state we will have the classical relation of a Ramsey Plan without money:

$$r^* = \frac{1-\beta}{\beta}$$

This means that in the long run money and inflation should have no impact on optimal consumption choices.

At the equilibrium, the following conditions hold:

- Money supply is equal to money demand: $M_t = m_t$;
- The lending market equilibrium is such that $A_t = p_{t-1}k_t$ (asset market clearing);
- Profit maximization: $f'(k_t) + (1-\delta) = (1+r_t)$ and $w_t = f(k_t) - k_t f'(k_t)$.

Substituting these conditions inside the budget constraint and dividing by p_t, to obtain its real terms specification, we have:

$$c_t = f(k_t) + (1-\delta)k_t - k_{t+1}$$

This is the equation shows that the demand for consumption is equal to the real output. It describes a capital accumulation law as the one of the Ramsey Plan without money. In the steady state the equation becomes:

$$c^* = f(k^*) - \delta k^*$$

Therefore, consumption does depend neither on real balances, nor on inflation.

From the CIA constraint we can derive the demand function for real balances:

$$\frac{M_t}{p_t} = c_t = f(k_t) + (1-\delta)k_t - k_{t+1}$$

Which in the steady state becomes:

$$\frac{M_t}{p_t} = f(k^*) - \delta k^*$$

This result implies that real balances are super-neutral, since they do not depend on inflation either in the short-term, or in the long-term. Super-neutrality is the main weakness affecting CIA models.

In the steady state real balances must be constant. This means that:

$$\pi = \zeta$$

Inflation is constant and equal to the money growth rate. Therefore:

$$i = \pi + r = \zeta + r$$

This one-on-one relationship between the nominal interest rate and the inflation rate of money is known as the Fisher Effect. In the long run, the Fisher Effect follows directly from money neutrality. Changes in money supply only affect the inflation rate, not the real interest rate (HORN, Michael, 2008).

After having briefly illustrated the results of a traditional CIA model, we can move onto analysing a slightly modified version of it, in which Bitcoin is introduced.

3.3 Bitcoin in the cash-in-advance model

Bitcoin is a currency completely different from traditional ones. Apart from its digital nature, which may be the first aspect making the difference, there are several characteristics that set Bitcoin apart from traditional money. In particular, Bitcoin is decentralised, without a central authority controlling it. Its growth rate is scheduled by an algorithm, setting a roof for its total supply. Simply these observations make it clear how complicated an attempt at modelling Bitcoin can be, especially inside a

traditional neo-classical framework. Nevertheless, this effort could be a starting point for future analysis, in the event Bitcoin or crypto-currencies more in general shall increase their weight in our economy.

The following model is a variation of the classic Cash-in-advance model. Basically, there is the addition of Bitcoin balances, including the miners' reward and the active fee to the budget constraint; the cash-in-advance constraint holds for Bitcoin too, with a peculiarity: Bitcoin are multiplied by a liquidity incentive, dependant on the active fee, which further specifies Bitcoin holdings' purchasing power and their degree of substitution with traditional money; finally there is the addition of an effort disutility to the lifetime utility function, to represent the cost of mining activity. Furthermore, this effort can be also seen as the probability the agent has to solve the proof of work challenge. The equilibrium conditions are derived and analysed both in the short-term, and in the long-term (steady state). From the model it emerges that: consumption is influenced not by traditional money, but by Bitcoin, as long as their emission is not over; real traditional money balances depends on the amount of Bitcoin in existence; in the steady state, traditional money inflation and Bitcoin inflation are both equal to zero.

The basic assumptions of the classic CIA model still hold:

- Closed economy with a single physical good;
- The good is produced through a classical constant-return-of-scale production function, using capital and labour;
- There is a continuum of infinitely lived individuals of size 1;
- Firms are financed by loans only;
- The government increases the quantity of money at a fixed rate each period: $M_{t+1} = (1 + \zeta)M_t$, with $\zeta > 0$;
- The increase in money supply is given to individuals through a subsidy, like a helicopter drop: $S_t = M_{t+1} - M_t$;
- There is perfect competition and rational expectations.

To these we add some other assumptions to introduce Bitcoin:

- Time is still discrete, but each interval corresponds to the average time of adding a new block to the chain of Bitcoin transaction.
- There are three assets in the economy, one period loans, A, and money, m, and Bitcoin, B. Money and Bitcoin pay no interest and they are used for transaction; loans pay the nominal interest rate i.
- There is no credit market for Bitcoin, therefore loans can be only granted in money: if an agent wants to invest her Bitcoin, she needs to exchange them with traditional currency.
- Every individual is a miner and belongs to a pool. The number of pools is enough to prevent the formation of a dominant pool and to enable everyone to have a fair chance at getting a reward: if a member of a pool solves the proof of work algorithm, everyone belonging to that pool wins a reward proportional to their effort. Therefore, for each agent the cost of mining equipment can be negligible. Each period she tries to add a new block to the chain, spending a certain effort, α_t. This effort is a cost for the agent, therefore is source of dis-utility; however, the greater the effort, the greater the contribution to the pool winning the challenge, thus implying a greater slice of reward.
- The miner's reward is equal to the amount of newly emitted Bitcoin: $X_t = B_{t+1}^S - B_t^S$ (where B_t^S is Bitcoin supply at time t); and a passive fee, f_t^p, which is the sum of all the active fees paid to the miners in each time interval. X_t is decreasing in time, and once $t = T$, Bitcoin supply will reach its maximum and $X_t = 0$. From that point onward, miners will be rewarded only through users' fee.
- Each agent may choose to pay an active fee, f_t^a, to reward the miners for their effort and encourage them to confirm her transaction faster. However, once no more new Bitcoin will be issued, fees will become mandatory, as they will be the only reward for miners' activity.

Having set the assumption, the agent in this economy will have to maximize her utility:

$$\sum_{t=0}^{\infty} \beta^t [u(c_t) - \varphi(\alpha_t)]$$

Where:

- $0 < \beta < 1$
- $0 < \alpha_t < 1$
- $u(c_t)$ and $\varphi(\alpha_t)$ are such that:

$$u'(c_t) > 0 \; ; \; \varphi'(\alpha_t) > 0$$

$$u''(c_t) < 0 \; ; \; \varphi''(\alpha_t) < 0$$

$$\lim_{c_t \to 0} u'(c_t) = \infty \; ; \; \lim_{\alpha_t \to 0} \varphi'(\alpha_t) = \infty$$

$$\lim_{c_t \to \infty} u'(c_t) = 0 \; ; \; \lim_{\alpha_t \to 1} \varphi'(\alpha_t) = 0$$

As in the previous case there are two constraints to the maximization problem.

Budget constraint:

$$m_{t+1} + A_{t+1} + q_t B_{t+1} + p_t c_t + q_t f_t^a = A_t(1 + i_t) + m_t + q_t B_t + S_t + q_t \alpha_t \left(X_t + f_t^p\right) + p_t w_t$$

This is the nominal budget constraint with Bitcoin, where:

- m_t is the demand of nominal balances of each individual at time t;
- A_t is the loan to the firms at time t;
- $p_t w_t$ is the nominal per-capita wage at time t;
- p_t is the price level at time t;
- $p_t c_t$ is consumption in money terms at time t.
- $q_t = \frac{p_t}{p_t^B}$ is the money price of Bitcoin, the exchange rate between traditional money and Bitcoin at time t.
- p_t^B is the price level in Bitcoin at time t.
- $\alpha_t \left(X_t + f_t^p\right)$ is the miner reward at time t, proportional to the effort spent.

CIA constraint:

$$M_t + q_t B_t \psi(f_t^a) \geq p_t c_t$$

Being a cash-in-advance model, the good market operates before the credit market. For this reason, the agent needs to hold in advance enough money and Bitcoin to purchase the consumption good.

$\psi(f_t^a)$ is a liquidity incentive, in order to encourage the payment of the active fee. It is such that:

$$\psi(f_t^a) = \begin{cases} 1 \; for \; f_t^a = \dfrac{f^p}{\alpha} \\ \in (1, 1+\theta) for \; f_t^a > \dfrac{f^p}{\alpha} \\ \in [\varepsilon, 1) for \; 0 \leq f_t^a < \dfrac{f^p}{\alpha} \end{cases}$$

$\frac{f^p}{\alpha}$ is the long-term equilibrium fee[52]; ε is a positive lower bound, θ is a number very close to zero. This liquidity incentive "punish" those users, who pay an active fee lower than its equilibrium value, by reducing the value of their Bitcoin holdings. The closer the fee is to its equilibrium value, the more encouraged miner will be to validate sooner that transaction, thus giving it more purchasing power than to a transaction with a lower fee. The active fee may be higher than its equilibrium value, as well, but the marginal increase in the liquidity incentive would be irrelevant. Indeed:

$$\lim_{f_t^a \to \infty} \psi(f_t^a) = 1 + \theta$$

Which is slighter greater than 1.

Later on, we will explain better the role and the implications of this incentive.

Lastly, we add the NPG condition, as before:

[52] It is obtained by the budget constraint.

$$\lim_{t\to\infty} \frac{A_t}{\prod_{t=0}^{\infty}(1+i_t)} = 0$$

Instead of setting up the usual Lagrangian framework to solve the maximization problem, we can simply insert the budget constraint into the utility function (the consumption one), and taking into account the CIA constraint, we can analyse what happens to consumption utility when $M_{t+1}, B_{t+1}, A_{t+1}, \alpha_t, f_t^a$ change.
We obtain the following equations:

1) $M_{t+1}: \frac{u'(c_t)}{\beta u'(c_{t+1})} = \frac{p_t}{p_{t+1}} + \frac{\lambda_{t+1} p_t}{\beta u'(c_{t+1})}$
2) $B_{t+1}: \frac{u'(c_t)}{\beta u'(c_{t+1})} = \frac{q_{t+1}}{q_t}\left(\frac{p_t}{p_{t+1}} + \frac{\lambda_{t+1} p_t \psi(f_{t+1}^a)}{\beta u'(c_{t+1})}\right)$
3) $A_{t+1}: \frac{u'(c_t)}{\beta u'(c_{t+1})} = \frac{p_t}{p_{t+1}}(1+i_{t+1})$
4) $\alpha_t: \varphi'(\alpha_t) = u'(c_t)\left(X_t + f_t^p\right)\frac{q_t}{p_t}$
5) $f_t^a: \psi'(f_t^a) = \frac{u'(c_t)}{p_t \lambda_t B_t}$

First of all, from equations 1) and 3), given that the nominal interest rate must be positive, λ_t must be positive too. Therefore the CIA constraint is binding.

Then, combining 1) and 2) together we obtain:

$$\frac{p_t}{p_{t+1}} + \frac{\lambda_{t+1} p_t}{\beta u'(c_{t+1})} = \frac{q_{t+1}}{q_t}\left(\frac{p_t}{p_{t+1}} + \frac{\lambda_{t+1} p_t \psi(f_{t+1}^a)}{\beta u'(c_{t+1})}\right)$$

Knowing that λ_{t+1} is positive, depending on whether the liquidity incentive is lower or equal to one, we can have three possible scenarios:

a) $0 < \psi(f_{t+1}^a) < 1$: it is a likely scenario, at least until Bitcoin supply is not over, since the fee payment is optional. Given this, we have:

$$\frac{\lambda_{t+1}p_t}{\beta u'(c_{t+1})} > \frac{\lambda_{t+1}p_t\psi(f^a_{t+1})}{\beta u'(c_{t+1})} \Rightarrow \frac{\frac{\lambda_{t+1}p_t}{\beta u'(c_{t+1})}}{\frac{\lambda_{t+1}p_t\psi(f^a_{t+1})}{\beta u'(c_{t+1})}} > 1$$

Therefore

$$\frac{q_{t+1}}{q_t} > 1 \Rightarrow q_{t+1} > q_t$$

Given that $q_t = \frac{p_t}{p^B_t}$, we have:

$$\frac{p_{t+1}}{p^B_{t+1}} > \frac{p_t}{p^B_t} \Rightarrow \pi_{t+1} > \pi^B_{t+1}$$

This result states that in presence of the liquidity incentive, which in this circumstance is smaller than 1, Bitcoin have less purchasing power than they could (in the CIA constraint Bitcoin holdings are lowered in value by the incentive), thus they are weaker than traditional money. For this reason, in order to avoid a crowding out of Bitcoin in favour of traditional currency, money inflation needs to be higher than Bitcoin inflation. The more the active fee is closer to its equilibrium value, the lower the gap between the two inflations needs to be. Therefore, we could look at the active fee also as the price Bitcoin users are willing to pay to promote Bitcoin and to make it an alternative to traditional money. Basically, the more they believe in Bitcoin potential as a currency, the higher active fee they will pay, since they want miner to keep playing their role as best as they can, guaranteeing the whole system functioning.

b) $\psi(f^a_{t+1}) = 1$: this is the long-term scenario, in which the active fee is equal to its equilibrium value. Thus we have:

$$\frac{q_{t+1}}{q_t} = 1 \Rightarrow q_{t+1} = q_t$$
$$\frac{p_{t+1}}{p^B_{t+1}} = \frac{p_t}{p^B_t} \Rightarrow \pi_{t+1} = \pi^B_{t+1}$$

Bitcoin and traditional money are substitutes, therefore any slight change in the inflations equivalence would imply a shift to the most valuable currency. In the steady state, since the active fee is going to be equal to its equilibrium value, $f^a = \frac{f^p}{\alpha}$, then Bitcoin inflation and money inflation will be equal. This means that monetary policy, in particular money emission, needs to take into account Bitcoin supply, as it will be shown later.

c) $\psi(f_{t+1}^a) > 1$: in this case, the active fee is higher than its equilibrium value. This implies:

$$\frac{q_{t+1}}{q_t} < 1 \Rightarrow q_{t+1} < q_t$$
$$\frac{p_{t+1}}{p_{t+1}^B} < \frac{p_t}{p_t^B} \Rightarrow \pi_{t+1} < \pi_{t+1}^B$$

The liquidity incentive makes Bitcoin more appealing than traditional money, therefore Bitcoin inflation needs to be higher than money inflation. However, Bitcoin users will not be willing to pay a fee higher than the equilibrium one. In fact, they face a trade-off between the liquidity incentive and the Bitcoin inflation. The higher the incentive, the higher is the inflation (thus Bitcoin looses purchasing power compared to traditional money). If, as we said before, one of the aims of the active fee is that of supporting the Bitcoin system and Bitcoin role as an alternative currency, once the fee is higher than the equilibrium fee, the liquidity advantage is compensated by the loss of competitiveness with real money in terms of inflation gap. The equilibrium fee, $\frac{f^p}{\alpha}$, is the fee that maximizes the marginal liquidity incentive, $\psi'(f_t^a)$; it is a saddle point for $\psi(f_t^a)$. More specifically:

$$\psi''(f_t^a) = \begin{cases} \geq 0 \; for \; f_t^a \in \left[0, \frac{f^p}{\alpha}\right] \\ < 0 \; for \; f_t^a > \frac{f^p}{\alpha} \end{cases}$$

From equations 2) and 3) we obtain:

$$1 + i_{t+1} = \frac{q_{t+1}}{q_t}\left(1 + \frac{\lambda_{t+1} p_{t+1} \psi(f^a_{t+1})}{\beta u'(c_{t+1})}\right)$$

From 5):

$$\lambda_{t+1} = \frac{u'(c_{t+1})}{p_{t+1} B_{t+1} \psi'(f^a_{t+1})}$$

Substituting this latter equation into the previous one, we have:

$$1 + i_{t+1} = \frac{1+\pi_{t+1}}{1+\pi^B_{t+1}}\left(1 + \frac{\psi(f^a_{t+1})}{\beta B_{t+1} \psi'(f^a_{t+1})}\right) \quad (1)$$

As predictable, the nominal interest rate depends positively from the rate of inflation of traditional money: the higher the inflation, the higher the nominal interest rate. However, it depends negatively from the inflation rate of Bitcoin. Indeed, the nominal interest rate refers to loans in traditional money. Therefore, one should first exchange Bitcoin for traditional money and then lend that money to the firms, at the rate i_t. In doing so, there is a trade-off between Bitcoin purchasing power and the rate paid by the loans. When Bitcoin inflation rises, Bitcoin looses purchasing power, therefore, *ceteris paribus*, the nominal interest rate goes down; otherwise everyone would exchange Bitcoin for loans. A similar reasoning can be applied to the relationship between the nominal interest rate and the active fee, which determines the liquidity incentive, $\psi(f^a_{t+1})$. If the latter increase, the nominal interest rate needs to increase as well, to keep loans competitive. However, looking at the marginal liquidity incentive, the effect depends on whether the increase is under the equilibrium value or above it. In the first case, the increase in the fee determines an increase in the marginal liquidity incentive. Bitcoin haven't reached their full potential yet, thus the nominal interest rate can be lower. However, the effect of $\frac{\psi(f^a_{t+1})}{\psi'(f^a_{t+1})}$ on i_{t+1}will depend on which variation is stronger. In the case of an increase of the active fee increasing above the equilibrium fee, than $\psi'(f^a_{t+1})$ goes down. Indeed, when the fee is higher than its equilibrium level, it means that Bitcoin have surpassed money as a currency, thus the interest rate offered needs to rise, for loans to be competitive. As a consequence, the

total impact of $\frac{\psi(f_{t+1}^a)}{\psi\prime(f_{t+1}^a)}$ on the nominal interest rate is positive. Lastly, the effect of Bitcoin holdings is a negative one: when they increase, the agent has more resources to invest; therefore the nominal interest rate can be lower.

From equations 3) and 4), we have:

$$\frac{\varphi'(\alpha_t)}{\varphi'(\alpha_{t+1})} = \beta \frac{(1+r_{t+1})}{(1+\gamma_{t+1})}(1+\pi_t^B) \quad (2)$$

Where $(1+\gamma_{t+1}) = \frac{(X_{t+1}+f_{t+1}^p)}{(X_t+f_t^p)}$ is the gross rate of growth of miners' reward.

This equation defines a sort of Euler Equation for the effort, α_t. We can see that the marginal rate of substitution for the effort, depends negatively on the rate of growth of the miner reward, meaning that if tomorrow the reward is going to be smaller (a reasonable assumption for Bitcoin, since their growth rate is decreasing), it pays off more spending a greater effort today to obtain the present reward, which is higher. On the other hand, the marginal rate of substitution is positively correlated to the real interest rate (the higher is the rate, which I can lend Bitcoin at, the higher is the marginal utility of the effort today, since I can invest the obtained reward) and to the inflation for Bitcoin prices (if Bitcoin are going to have less purchasing power tomorrow, I'd rather win a reward today).

Equation 3) gives us the classic Euler Equation:

$$\frac{u\prime(c_t)}{u\prime(c_{t+1})} = \beta(1+r_{t+1}) \quad (3)$$

From the supply side of the economy we have:

- $M_{t+1} = (1+\zeta)M_t$
- $B_{t+1}^S = (1+\kappa_{t+1})B_t^S$
- $S_t = M_{t+1} - M_t$

- $X_t = B_{t+1}^S - B_t^S$

At the equilibrium:

- Money supply is equal to money demand: $M_t = m_t$;
- Bitcoin supply is equal to Bitcoin demand: $B_t^S = B_t$
- The lending market equilibrium is such that $A_t = p_{t-1}k_t$ (asset market clearing);
- Profit maximization: $f'(k_t) + (1 - \delta) = (1 + r_t)$ and $w_t = f(k_t) - k_t f'(k_t)$.
- Fees equilibrium: $f_t^a = \frac{f_t^p}{\alpha_t}$

Substituting these conditions inside the budget constraint and dividing by p_t, to obtain its real terms specification, we obtain:

$$c_t = f(k_t) + k_t - \delta k_t - k_{t+1} - (1 - \alpha_t)\frac{X_t}{p_t^B}$$

In this model with Bitcoin, consumption is not the same to the consumption of a Ramsey Model without money in it. The amount of Bitcoin emitted each period influences it. Each agent will consume the output minus the part of newly emitted Bitcoin, which she didn't get. Solving the proof-of-work challenge, the effort spent in mining increases the possibilities of consumption. Traditional money instead is still super-neutral. Indeed, in this economy money is given by the government for free, as a subsidy; on the contrary Bitcoin are "earned" and "issued" by the agents themselves. They are both used for transaction purposes, but, as far as Bitcoin are concerned, agents can choose if they want them or not, if they are valuable or not. This reflects in their consumption possibilities. The above result holds until Bitcoin supply is over, at which point the consumption goes back to its Ramsey Plan without money counterpart:

$$c_t = f(k_t) + k_t - \delta k_t - k_{t+1}$$

At this point, it is interesting seeing what happens to the traditional money balances demand function, expressed in real terms. From the CIA constraint we have:

$$\frac{M_t}{p_t} = c_t - \frac{B_t}{p_t^B}\psi(f_t^a)$$

Money balances have now found competition in Bitcoin. The more Bitcoin demand is, the lower is traditional money demand. Moreover, the liquidity incentive determines the rate of substitution between the two currencies. For $f_t^a = \frac{f^p}{\alpha}$, $\psi(f_t^a) = 1$, there is perfect substitution.

To conclude this brief analysis, we shall now look at the steady state of this economy.

From (3), we obtain:

$$r^* = \frac{1-\beta}{\beta}$$

This is the real interest rate of a Ramsey Plan without money.

From (2)

$$1 = \frac{(1+\pi_t^B)}{(1+\gamma_{t+1})} \Rightarrow \pi_t^B = \gamma_{t+1}$$

Since at the steady state $X_t = 0$ and $f_t^p = f_{t+1}^p$, $\gamma_{t+1} = 0$, therefore also $\pi^B = 0$. Once no more Bitcoin are introduced in the economy, Bitcoin inflation stops. This result comes out also from the steady state requirement of real balances being constant. In order to be so, the inflation rate, must be equal to the growth rate of the Bitcoin supply, which is zero. Moreover, given that at the steady state $f^a = \frac{f^p}{\alpha}$, from the previous result we have:

$$\pi = \pi^B = 0$$

Money inflation goes to zero as well, otherwise traditional money would be less competitive than Bitcoin. And since, for the same reason as above, real balances need to be constant, the inflation rate is equal to the growth rate, so:

$$\zeta = \pi = 0$$

Government need to stop issuing new money, for inflation to be equal to zero. This is a rather strong result: Bitcoin can stop money inflation. The crypto-currency has a strong impact on traditional money emission, and also demand. In fact:

$$\frac{M}{p} = c^* - \frac{B}{p^B}$$

Where $c^* = f(k^*) - \delta k^*$, which is the classic Ramsey Plan specification. In the long run consumption is influenced neither by money, nor by Bitcoin. Real money balances demand instead is not influenced by their own inflation, but by real Bitcoin holdings.

From the model, it appears that the presence of Bitcoin in the economy can affect traditional money demand and therefore monetary policy. There can be competition between traditional currency and crypto-currency. This competition, if appropriately studied and understood, can actually bring benefits for the users: they are "in control" of Bitcoin and thus they have an instrument to react to monetary policy decisions. In particular, thanks to the liquidity incentive, they can show their support to the crypto-currency, their trust in it. Moreover, in the long-term inflation goes to zero, even the traditional money one. This occurs given the model assumption and specifications, but it can still imply a corrective effect on excessive inflationary monetary politics. Maybe it can have the beneficial effects of private money competition, advocated by Hayek. Ignoring the phenomenon can be a mistake, as well as reacting to it with rigidity. As it was said before, this is not the best model to fully capture the interactions between traditional currencies and crypto-currencies. A decentralized currency is not something easy to model, especially with traditional theories, inside a

neo-classical framework, but nevertheless, I personally believe it is an effort worth some time. I also believe crypto-currencies interactions in real economies can become an interesting field of studying, opening the doors to new theories and solutions.

Conclusions

Whether for better or for worse, Bitcoin and crypto-currencies have the potential to deeply affect our economy, and probably they have already. This is why it is extremely important beginning to pay serious attention to them, in particular from an economic point of view. Some studies on the interaction between virtual economies and real ones have been pursued, since the digital component in our lives is increasing fast, on a daily basis. Crypto-currencies, being the most recent product of the digitalization of economy, have just started to catch the interest of some part of the academic community and of the relevant authorities, but probably still too little is being done in an attempt to truly understand the phenomenon. Ignorance is not bliss. The complexity of their working mechanism is definitely off-putting. In the second chapter there is a brief explanation of Bitcoin system functioning, which tries to keep technicalities to a minimum, that minimum impossible to omit to grasp the mechanism. From the technical aspect of Bitcoin, many concerns rise, about security, legality, ethics and other more, related to daily usage. Cases like those of MtGox and Silk Road were exploited by media, only to highlight Bitcoin's negative aspects. Then, there are the economic implications of Bitcoin as a virtual currency scheme, interacting with real currencies. Obviously, as for now, Bitcoin does not represent a threat to price stability, financial market stability and payment system stability, but in the future this situation may change and central bank may be forced to change their usual monetary policy strategies. Therefore, in this optic of a more relevant weight of Bitcoin, and crypto-currencies more in general, on the economy, it may be interesting to try to model the interactions of Bitcoin and traditional money in a neo-classical framework: the cash-in-advance model. Bitcoin holdings are introduced both in the budget constraint and in the CIA constraint. In this latter, Bitcoin balances are multiplied by a liquidity incentive, function of the active fee, which determines its true purchasing power, but, most importantly, its degree of substitution with traditional money (the liquidity incentive can be seen as the way in which Bitcoin users can support the crypto-currency and show their trust in it). From the model it emerges that: consumption is influenced not by traditional money, but by Bitcoin, as

long as its emission is not over; real traditional money balances depends on the amount of Bitcoin in existence; in the steady state, traditional money inflation and Bitcoin inflation are both equal to zero. Therefore, there can be competition between traditional currency and crypto-currency. This competition, if appropriately studied and understood, can actually bring benefits for the users: they are “in control” of Bitcoin and thus they have an instrument to react to monetary policy decisions. In conclusion, I believe that crypto-currency have the potential to change the status quo. Whether for better or for worse, it depends on how much we understand them and the choice we take about them.

Bibliography

BLANCHARD, Olivier. 2005. *Introducing Money*.

BRAY, David A. and Benn R. KONSYNSKI. 2006. *Virtual Worlds, Virtual Economies, Virtual Institutions*.

BUITER, Willem H. 2007. *Is Numerarology the Future of Monetary Economics? Unbundling Numeraire and Medium of Exchange through a Virtual Currency and a Shadow Exchange Rate*. National Bureau of Economic Research.

CUNICOLA. 2013. *Cunicula's Game Theory Primer for Computer Scientists invovled in Bitcoin*.

CASTRONOVA, Edward. 2002. *On Virtual Economies*.

CASTRONOVA, Edward. 2003. *Theory of the Avatar*.

CHAUM, David. 1998. *Blind Signature For Untraceable Payments*.

CHATURVEDI, Neelabh. 2014. *U.K. Nears Rule on Taxing Bitcoin*. [online]. Available from World Wide Web: <http://online.wsj.com/news/articles/SB10001424052702304360704579415352635879152>

EYAL, Ittay and Emin Gün SIRER. 2013. *Majority is not Enough: Bitcoin Mining is Vulnerable*.

ECB. 2012. *Virtual Currency Schemes*.

EICHENGREEN, Berry. 1992. *Golden Fetters: The Gold Standard and the Great Depression, 1919–1939*. Oxford University Press.

ELWELL, Craig K., M. Maureen MURPHY, and Michael V. SEITZINGER. 2013. *Bitcoin: Questions, Answers, and Analysis of Legal Issues*.

DEPARTMENT OF THE TREASURY FINANCIAL CRIMES ENFORCEMENT. 2013. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*.

DOPPELHOFER, Gernot. 2009. *Intertemporal Macroeconomics*.

GERVAIS, Arthur, Ghassan O. KARAME, Srdjan CAPKUN, and Vedran CAPKUN. 2013. *Is Bitcoin a Decentralized Currency?*.

GIBBONS, Robert. 1992. *Game Theory for Applied Economists*. Princeton: Princeton University Press.

GRUBER, Sarah. 2013. *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*.

IRS. 2014. *Notice 2014-21*.

HAYEK, F.A. 1990. *Denationalization of Money- The Argument Refined: An Analysis of the Theory and Practice of Concurrent Currencies*. London: The Institute of Economic Affairs.

HARRIS, Billy and Andy NOVOBILSKI. 2008. Real Currency Economies: Using Real Money in Virtual Worlds. *In*: *2008 International Conference on Frontiers in Education: Computer Science and Computer Engineering*., pp.241-246.

HERN, Alex. 2014. How a bug in Bitcoin led to MtGox's collapse. *The Guardian*, 27 February.

HERNANDEZ-VERME, Paula L. and Ruy A. VALDES BENAVIDES. 2013. *Virtual Currencies, Micropayments and the Payments Systems: a Challenge to Fiat Money and Monetary Policy?*.

HILL, Kashmir. 2014. *Bitcoin's Legality Around the World*. [online]. Available from World Wide Web: <http://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world/>

HORN, Michael. 2008. *Explain the Fisher effect and analyse its role in linking the nominal and real rate of interest. Can interest rates be negative? Critically discuss in the context of the Japanese experience of de ation since the early 1990s*.

KIYOTAKI, Nobuhiro and Randall WRIGHT. 1989. On Money as a Medium of Exchange. *Journal of Political Economy*. **97**(4), pp.927-954.

KOLLMEYER, Barbara. 2013. *Bitcoins aren't real, but they are taxable, Norway says*. [online]. Available from World Wide Web: <http://blogs.marketwatch.com/thetell/2013/12/16/bitcoins-arent-real-but-theyre-taxable-norway-says/>

KROLL, Joshua A., Ian C. DAVEY, and Edward W. FELTEN. 2013. *The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries*.

LEHDONVIRTA, Vili. 2005. *Virtual Economics: Applying Economics to The Study of Game Worlds*.

LOYO, Eduardo. 2002. Imaginary money against sticky relative prices. *European Economic Review*., pp.1073-1092.

NAKAMOTO, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

NARAHARI, Y. 2012. *Incentive Compatibility and Revelation Theorem*.

NILSSON, Anders. 2014. *The Troublesome History of the Bitcoin Exchange MtGox*. [online]. Available from World Wide Web: <https://anders.io/the-troublesome-history-of-the-bitcoin-exchange-mtgox/>

MCKEE, Jordan. 2013. *Redefining Virtual Currency*.

MOORE, Tyler and Christin NICOLAS. 2013. *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*.

ORMAN, Levent V. 2010. *Virtual Money in Electronic Markets and Communities*.

PARKER, Jonathan A. 2007. *Euler Equations*.

PENG, Hui and Yanli SUN. 2009. The Theoretic and Empirical Analysis on the Impact of Network Virtual Money on Real Money Supply. *In*: *International Conference on Future Computer and Communication*. Kuala Lumpar.

SALOMON, Mandy. 2010. Why Virtual-World Economies Matter. *Journal of Virtual Worlds Research*. **II**(4).

SIDRAUSKI, Miguel. 1967. Rational Choice and Patterns of Growth in a Monetary Economy. *The American Economic Review*. **57**(2), pp.534-544.

STOCKMAN, Alan C. 1981. Anticipated inflation and the capital stock in a cash in-advance economy. *Journal of Monetary Economics*. **8**(3), pp.387-393.

STOCKMAN, Alan C. 1981. Anticipated Inflation and the Capital Stock in a Cash-In-Advance Economy. *Journal of Monetary Economics*. **8**(3), pp.387-393.

STOKES, Robert. 2012. *Virtual money laundering: the case of Bitcoin and the Linden dollar*. Information & Communications Technology Law.

REICHLIN, Pietro. 2012. *Notes on Advanced Macroeconomics*.

ROBBINS, Tyler S. 2013. *A Primer on Bitcoin Taxation*.

ROBERTS, Dread Pirate. 2013.

VILLASENOR, John, Cody MONK, and Christopher BRONK. 2011. *Shadowy Figures: Tracking Illicit Financial Transaction in the Murky World of Digital Currency, Peer-To-Peer Network, and Mobile Device Payments*.

VISHNUMURTHY, Vivek, Chandrakumar, Sangeeth and Emin Gün SIRER. 2003. *KARMA : A Secure Economic Framework for Peer-to-Peer Resource Sharing*.

YAMAGUCHI, Hiroshi. 2004. *An Analysis of Virtual Currencies in Online Games*.

YERMACK, David. 2013. *Is Bitcoin a Real Currency?*.

ZEIRA, Joseph. 2013. *Money and Inflation*.