
**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ**

**Τμήμα Λογιστικής και Χρηματοοικονομικής**

**Τίτλος διπλωματικής εργασίας: '' The Economics of Digital Currencies: The case of Bitcoin"**

**Ονοματεπώνυμο:** ΑΡΓΥΡΟΥ ΑΛΕΞΑΝΔΡΑ

**Αριθμός Μητρώου:** 1322103

**Κατεύθυνση:** Χρηματοοικονομική

**Εργασία υποβληθείσα στο**

**Τμήμα Λογιστικής και Χρηματοοικονομικής**

**του Οικονομικού Πανεπιστημίου Αθηνών**

**ως μέρος των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης**

**Αθήνα,**

**Αύγουστος 2017**

## CONTENTS

*Julian Assange: There's also a very nice little paper that I've seen in relation to Bitcoin, that... you know about Bitcoin?*

*Eric Schmidt: No.*

*Julian Assange: Okay, Bitcoin is something that evolved out of the cypherpunks a couple of years ago, and it is an alternative... it is a stateless currency.*

*Jared Cohen: Yeah, I was reading about this just yesterday.*

*Julian Assange: And very important, actually. It has a few problems. But its innovations exceed its problems.*

*Secret meeting between Julian Assange, Google CEO Eric Schmidt, and former Secretary of State advisor Jared Cohen, June 23, 2011 Bitcoin was a major innovation in Computer Science that would have significant implications for finance.*

## ***Abstract- A note regarding motivation and disclosure***

In this paper, we provide a deep understanding of decentralized digital currencies, cryptocurrencies and especially the case of bitcoin. In particular, we survey the theory and principles by which the Bitcoin ecosystem operates. Furthermore, we examine Bitcoin's practical aspects and also its current and future interaction with the banking, financial and regulatory systems. But more specifically, we observe how the bitcoin ecosystem can be perceived as a new currency or even monetary system.

In detail, we examine cryptocurrencies as a potentially disruptive sort of payment method in transactions, a feature which can lead to what we call a "*cashless society*". Due to its relative importance, we focus in particular on Bitcoin. It is true that its determinants, is explored, such as the usability, the usefulness that offers, under a subjective norm, could make Bitcoin a game-changer.

The results from the empirical analysis of the Bitcoin system reveal that most stakeholders consider the perceived ease of its use still rather low, with a level of usefulness varying, according to several user groups. However, we cannot deny that the concept behind this system with bitcoin having much future potential as a payment method is confirmed. Interestingly, the underlying technology of the block chain and the whole bitcoin protocol can also be seen as a potential revolutionary and disruptive way to create a more secure transaction environment which would be based on open platforms and open data than the current one.

Bitcoin constitutes a distributed digital currency and payment method that has attracted a lot of attention among consumers. Since the level of interest is continuously increasing, we conduct an in-depth investigation in the way Bitcoin system functions as an economic vehicle and of course as a digital disruption. Nevertheless, we want to understand what made it so successful, while its predecessors couldn't make it. We, also, challenge the current principles concerning the currency and the monetary system in order to examine the potential use of Bitcoin as an official currency. And, in doing so, we identify several issues and attacks in the Bitcoin system.

In this dissertation, we focus on the disruption facing the established financial system and banks in particular. We discuss it in several parts, including electronic payments, digital money management and transactions. The methodology employed for research is exploratory in nature. Specifically, data was collected from several primary and secondary sources like journal articles, research papers, official websites and online social media portals and even official databases such as the DataStream. Furthermore, we present the framework and the design principles of virtual currencies and especially of Bitcoin from an economic and a financial perspective basically, so as to address a non-technical audience. We even tried to pair a careful technical analysis about the background of Bitcoin platform with the relevant economic factors in order to describe its protocol. Through macroeconomic principles, financial practice and theory and academic research, we will try to explain the fundamentals of money and currency and the way they are used in the Bitcoin network.

This research reviews the past, present and the future existence and use of the Bitcoin and its economic determinants, pointing out the possible risks and the regulatory issues it presents. In other words, we observe and show the way that Bitcoin interacts with other official currencies and commodities inside the current, conventional financial system and the real economy and of course the way it disrupts them. At the start, we could say that there are tremendous opportunities in this disruption which has already begun.

Since the virtual currencies and especially the case of Bitcoin constitute an interdisciplinary issue we try not to limit only in one of their aspect but we are looking to cover in our analysis a vast spectrum of their determinants. And as such, the ways and the features which are facilitating the shift towards a "*cashless society*". I hope that this dissertation will be used as a starting point and a good incentive for a further research on the application and the challenges of cryptocurrencies such as the Bitcoin, in a society which heads to a more digital phase and understand the kind of impact they will have in our traditional financial system.

# ***Introduction***

Several economists of the past envisioned or wished for a society without cash or physical money in the near future. Although, such a "*cashless*" world has not emerged yet. But to some extent, their dream has already come true. More precisely, a major step towards "cashlessness", and by "cashlessness" we mean the absence of hard cash in everyday transactions, came with the emergence of Electronic Funds Transfer (EFT) technology. The emergence of EFT happened in the era of credit card and subsequently debit card transactions in the mid-twentieth century. As their use gained momentum, the world saw a shift towards a decrease in the use of hard cash. But, could this fact be enough for a total transformation of retail and investment Banks as we know them today?

In the modern capitalist markets, the banking industry has been around for thousands of centuries. More specifically, Financial such as Banks play a multi-functional role by keeping safe and sound our deposits, by providing us with credit, or by facilitating payments between many parties. Therefore, they are an integral part of our social, economic and political system in a world-wide scale[1].

In today's world, as the Internet has become an integral part of our lives, the application of electronic transactions has transformed the way in which we interact and transact online. In other words, the Internet has provided an increased connectivity between the citizens of the world. This disruption was enough to change the nature of financial transactions. More precisely, with recent developments in Information Technology (IT) and in Information Systems (IS, the concept of money has changed. It currently, extends beyond the traditional and physical tender of government-backed currencies to include mobile payments, digital currencies, and virtual goods.[2]

[1] Banca Monte dei Paschi di Siena, Italy, chartered in 1472.

[2] Villasenor, J., Monk, C., & Bronk, C. (2011). Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-peer Networks, and Mobile Device Payments. Brookings Institution.

On the other side, Banks being influenced by this disruption, are trying to keep up with the commercial and financial innovations driven by the IT sector. More precisely, as a recent financial application which came with the development of IT was the peer-to-peer systems and of course the peer-to-peer lending. This was the first step among users of Internet towards an economic shift to more decentralized forms of networks.

Peer-to-peer lenders provide efficient alternative markets for lending and saving. In other words, Peer-to-peer lending, (P2P), is a method of debt financing that enables individuals to borrow and lend money, but without the use of an official financial institution as an intermediary. Peer-to-peer lending removed the middleman from the process, but it also involved more time, effort and risk than the general brick-and-mortar lending scenarios[3]. Thus, it appeared a new type competition in the payments industry, as IT corporations have begun to act so as to transform the industry.

In the recent period, it is undeniable that something happened which fundamentally changed the way we interact with people on a world-wide scale. More precisely, this fact helped decisively several entire international communities and networks to communicate in a "virtual" way. And now we are able to talk about the creation of "virtual" world. So, why would the creation of a "virtual" economy be far behind it?[4]

On the other side, traditional banks have developed only specific operations over decades and with the emergence of this IT revolution they found it difficult to respond to their customers' new needs. More specifically, it has been hard for banks to cope with their new highly agile competitors coming from the IT industry. Moreover, the game became harder if we take into account the fact that the world's central banks are making continuously serious efforts in order to get their currencies under control, and this fact proves that the next paradigm shift in global finance is not so far.

[3] http://www.investopedia.com/terms/p/peer-to-peer-lending.asp#ixzz4rdVn6UhV

[4] Warwick, D. , Towards a cashless society, The Futurist, (2004).

However, the march towards the era of cashless transactions has not arrived yet. Especially, if we think about the difficulties it faces everyday by its adversaries, the Banks and the established financial system, the road towards cashlessness is not paved with roses. Moreover, the IT innovations have to cope with systemic difficulties because of several challenges that appear, such as the invasion to the personal privacy and the hacking and other security problems on the Internet. In the end, the national governments do not seem willing to display the level of commitment required in order to keep up with these IT changes of our financial system. So, the goal towards cashlessness remains out of reach for now.

## The Banking Industry- How it works

In a barter economy, in order to be able to sell a good, the seller must find a buyer ready to pay with a good or a service in return. These two actions should be compatible with each other. More precisely, if the buyer has opposite endowments with the seller for the specific trade, the exchange cannot be completed. Thus, the buyer needs to find a person who possesses the good he wants to buy and simultaneously the seller should be ready to accept the kind of payment defined by the first. This is referred as "*a double coincidence of wants*", expressed by the economist Stanley Jevons.

Here comes the middleman whose purpose is to find these two parties with "a double coincidence of wants" and that is a role always played by the Banks. More specifically, traditional banks play a major role in our everyday transactions operating as lenders or the opposite. Lending is among the basic reasons which made Banks appear in our current financial system and constitutes a core bank service. Thus, banks are responsible for receiving deposits and for lending some portion of those deposits to borrowers, charging interest to the borrowers and returning interest to the investors[5].

Apart from lending , Banks provide many other financial services to their clients strengthening the viability of the established economic system and simultaneously providing a safe transaction network. A characteristic example is the production of capital through savings and finance or the several operations of the applied payment systems. And these economic processes have existed for thousands of years in all parts of the world.

[5] Federal Reserve Bank of New York,(2013), Household Debt and Credit Report.

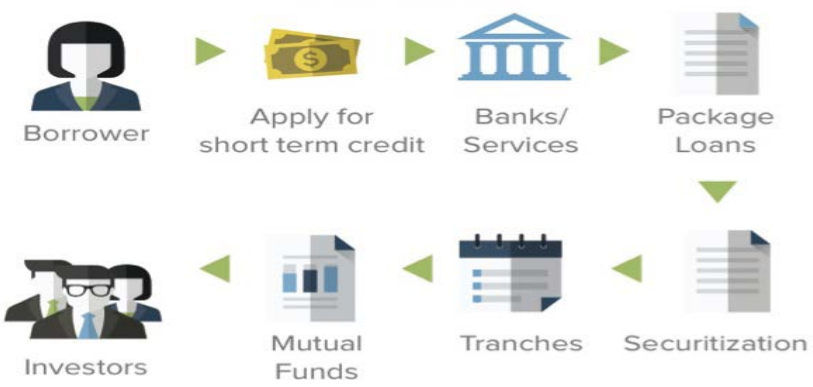



Figure : Retail Lending Layers

Source: Lending Club

We should note that banking, finance and payment services are among the oldest of "industries", with a long history. These commercial services which constitute products of the modern capitalism have emerged even before modern governments[6]. Thus, many of the functions that Banks serve are familiar to us, even if we don't know their origin.

Certainly, Banks, as we have already mentioned, provide the specialized function of securely storing liquid capital and lending it. Put simply, they are able to utilize effectively scale economies associated with providing these services. Metaphorically, banks can be viewed as miniature economies or as organizations in a market which facilitates exchanges[7]. Moreover, these organizations have their own "rules of the game", over which individuals, borrowers or savers can choose to opt in or out.

To complete the metaphor, the banking industry in this sense is a centralized ledger of transactions, whether of capital or payments, which records balances between many different parties.[8] So, a bank, in the modern sense, is an internalized market that

[6] Ferguson, N., (2008),The Ascent of Money: A Financial History of the World, Penguin Books.

[7] Coase, R., H., (1937), The nature of the Firm, Economica.

[8] Buchanan, J. , M. (1990), The domain of constitutional economics, Constitutional Political Economy.

functions as a two-sided market in order to match those with excess supply of capital with those with excess demand for capital[9]. Banks intermediate these two sides of the market. And this kind of intermediation is what the recent entrance of Peer-to-Peer (P2P) finance, especially lending, aims at disrupting.

In sum, we can conclude that the major and basic role of Banks is to operate as third-party intermediating organizations because they are able to internalize substantial, physical and information costs, while using the market to match the supply of and demand for capital and financial transactions.[10] But that does not mean that they do not provide other services too, that are necessary for the existence of our financial ecosystem. However, it seems that these kind of operations cannot serve the updated needs of their clients who now search for new ways of financial services more direct and transparent such as the Peer-to-Peer lending technology.

[9] Rochet, J. , C. and Tirole, J. ,(2003), Platform competition in two-sided markets, Journal of the European Economic Association.

[10] Roth, A., E. and Sotomayor, M. , A., O. (1992), Two-sided matching: A study in game-theoretic modeling and analysis, Cambridge University Press.

# ***The Effects of Peer-to-Peer Lending***


Figure : Marketplace Lending Layers

Source: Lending Club

As we have previously mentioned, Banks intermediate these two sides of the market, the borrower and the investor. And this kind of intermediation is what the recent wave of peer-to-peer (P2P) finance, especially lending, aims at disrupting. More precisely, peer-to-peer (P2P) lenders, also called “marketplace” lenders, compete directly with Banks by offering better rates and a direct kind of experience using a shared marketplace. This process functions by matching sellers of capital, those who would otherwise make deposits in a bank, with buyers of capital who would otherwise seek loans from banks directly.

In this way, the P2P finance threatens to decrease the role of banks in the current economic status quo. More specifically, borrowers and investors pay fees to the Banks, in order to have their financial requests complete. But in a peer-to-peer lending system they

would interact directly, eliminating much of the overhead. If we look at the existing P2P lending mechanisms, we see that the largest P2P lender operating in the US which is the "*Lending Club*", issued $4 billion in loans only in 2014. A snapshot of rates in Q4 2014 includes the following rates, where the letters A through G are used to denote risk categories, with progressively higher expected default rates. The following table is indicative of this fact.

| Risk | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| Interest | 7.32% | 10.82% | 13.63% | 16.25% | 19.20% | 22.99% | 24.42% |
| Expected default rate | 1.74% | 3.54% | 5.04% | 6.60% | 8.24% | 10.36% | 11.41% |
| Return | 4.80% | 6.48% | 7.81% | 8.92% | 10.21% | 11.84% | 12.28% |

Table : Lending Club Risk Categories

In P2P lending, investors have full control over which loans they choose to fund. The minimum investment per loan is $25, allowing investors to spread their risk over a large number of loans[11]. In other words, borrowers pay interest directly to the investors. A large majority of the loans issued are for debt consolidation. Borrowers are attracted by rates that are lower than their credit cards and investors are attracted by rates that are much higher than they can achieve from banks.

Concerning risk assessment in P2P lending we conclude that , P2P lenders differ substantially in how they access and manage risk. Specifically, in the case of Banks, the bank assumes the risk and if the borrower defaults on a loan, it is the bank that loses the

[11] Khayrallah A., Hickey J., Jasvinder S., Radia N., Xu V., (2014), Insights in Engineering Leadership White Paper, Engineering Leadership Professional Program UC Berkeley.

money, not the depositors[12]. However, if the economy experienced a crisis, unfortunately the Banks as the official financial institutions would suffer all the negative consequences and would pay the losses, as we have seen in the crisis of 2009. In fact, the recent financial crisis of 2009 which was caused by poor risk assessment and management practices causing Banks to pay for cascading losses through the industry serves as an indicative example of this case.

On the other hand, P2P lending may serve as an efficient solution given that P2P lenders generally operate on a different model. In this renewed model, the reallocations of capital, including payments and financial assets are undertaken in a decentralized form of market and involves a two-party system rather without the existence of a middleman such as the Bank. This is a financial frame where the interested stakeholders are responsible for assuming the risk. In other words, investors fund individual loans directly and, if a loan defaults, the investor's money is lost.

One of the attractions of P2P lending is that investors can hand-pick the loans that they fund, bringing the knowledge of the crowd to bear on risk assessment[13]. This is what P2P finance is trying to create, but it hasn't quite got there yet. Thus, P2P lending threatens the existence of banks in several ways. First, as we have already noticed, highly efficient online marketplaces for unsecured loans offer far better rates to both borrowers and investors. Second, more effective risk assessment and management practices increase the quality of a lending portfolio. Third, non-bank, P2P lenders are not subject to any kind of banking regulations. Therefore, consumers seem to be more willing to invest in market disruptions such as the P2P lending and turn to other markets, rather than continue to support the obsolete banking practices which are responsible even for the recent economic crisis.

[12] King, Br., (2014), Breaking Banks: The Innovators, Rogues, and Strategists Rebooting Banking. Wiley Publishing.
[13] Khayrallah A., Hickey J., Jasvinder S., Radia N., Xu V., (2014), Insights in Engineering Leadership White Paper, Engineering Leadership Professional Program UC Berkeley.

# A New Era- The Digital Revolution

As P2P lenders are using new technologies which are more capable to help assess their borrowing risk. In the age of the Web 2.0, a large majority of the online public are communicating with each other through broadband Internet connections. In the past few decades, more and more people have been turning to the Internet technology to facilitate certain tasks. Unlike the traditional websites and corporate blogs, the emerging "*social media platforms*" are used by the members to share, engage and collaborate with their peer groups to build lasting relationships in the virtual world[14].

One important task realized on the Internet is the online purchasing via credit cards. Unfortunately, credit cards have been proved not to offer the same security

[14] Boyd, G. (2002). Quatts, Virtual currency for gaming and bartering education on the web. British Journal for Educational Technology.

features as one would get using paper cash. Therefore, this lack of security led to the creation of electronic cash, or e-cash, which is an electronic payment system based on the paper cash system with additional security features.

Due to the loss of trust in the banking sector and the fear of loss of capital, the low interest rates and the uncertainty of existing currencies, the ground for the creation of virtual payment platforms was given. Specifically, since the crisis in the banking sector, there has been noticed a strong loss of trust. Moreover, loss of capital, historically low interest rates for savings and uncertainty over the future of fiat currencies supported a transformation in traditional economic structures. Besides, the economic crisis of 2009, contributed decisively to the emergence of new and especially virtual- electronic economic networks.

This crisis illustrated, essentially, a critical need for new and fundamental changes of the established economic system. The financial crisis, led to several problems affecting the international financial architecture. Some of them included the lack of people's trust to banks due to structural problems and the low financial transparency in leveraging. So, the interplay of these factors has been argued to lead to an accumulation of excesses, whose interaction has led to the creation of electronic, digital forms and ways of transactions[15].

On the other hand, commerce on the Internet, (e-commerce) was continuously rising in a world-wide scale. But, it relied almost exclusively on financial institutions serving as trusted third parties, so as to process electronic payments. Thus, e-commerce required from its clients to process their payments digitally and cashlessly, through debit or credit cards. And entire businesses, founded upon e-commerce, begun to look for new and safe ways to expand their existing payment methods.

In fact, some of the benefits of e-commerce such as it stands for "always on", purchasing 24/7, quick deals, individual responsibility, limited control by authorities and a high degree of anonymity made electronic payments very popular on a worldwide

[15] Roth, F. ,(2009), The effects of the financial crisis on systemic trust, Intereconomics.

scale[16]. They also made more than necessary the appearance of digital, electronic payment methods, functioning in a P2P network. As citizens began to question the conventional banking system they started to think about a new currency, independent from the old system and based on the new technology.

These characteristics, being combined, lead to the emergence of a new phenomenon which occurred for the first time in 2009, the emergence of the "*Virtual Currencies*" (VC), or also called "*cryptocurrencies*". Virtual Currencies constitute math-based peer-to-peer digital currencies that have no central administrating authority and no central monitoring[17]. Currently, there are more than 270 different virtual currencies in use, and the number is increasing steadily. Thus, there were no intermediaries, no service charges, no legal fees and no delays. A total disruption towards the traditional fiat currencies that lacked those benefits. With ease, people of any country was able to send, receive and store value on their digital wallets. Beyond all of this, these new distributed digital coins could compete with governmentally-issued fiat money.

Virtual, or digital currency is a type of online electronic currency which can be used to purchase virtual, or physical goods and also be exchanged to traditional currency. It is possible to provide a more specific definition of what a virtual currency is as the following: " *A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers or users and accepted among the members of a specific virtual community*"[18]. Nevertheless, it presents a new financial field full of opportunities together with some important threats concerning the traditional payment services and providers.

[16] Rennhard, M., & Plattner, B. (2002). MorphMix: Peer-to-Peer based Anonymous Internet Usage with CollusionDetection, Privacy in the Electronic Society.

[17] FATF Report. (2014). Virtual Currencies Key Definitions and Potential AML/CFT Risks. Paris: Financial ActionTask Force on Money Laundering ,OECD.

[18] ECB, (2012), Virtual currency schemes.

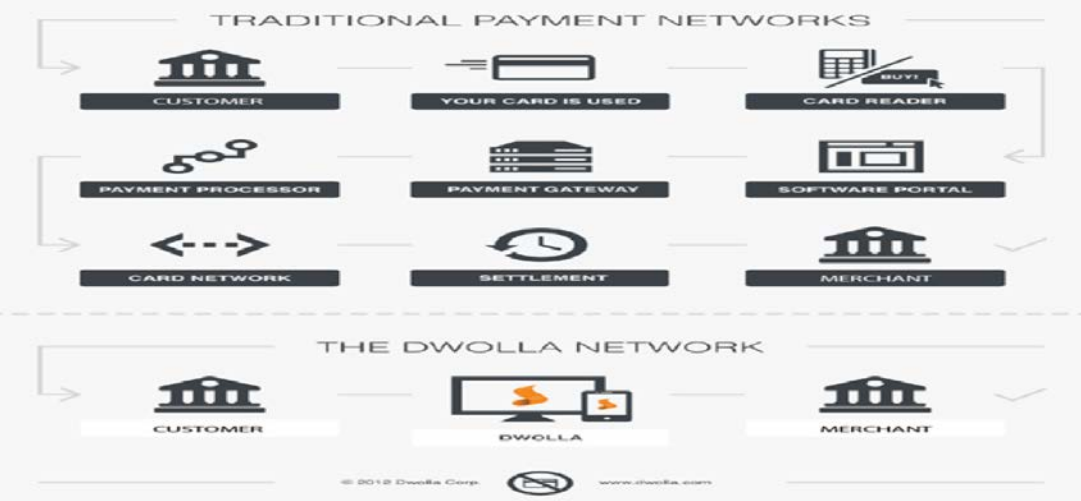



Figure : Traditional Payment Networks versus the Dwolla Network

Source: Dwolla

Recent developments have seen the creation of digital currencies, which combine new currencies with the effects of decentralized payment systems. In fact, the monetary aspects of digital currencies have attracted considerable attention because of their innovative character. Since money and payment systems are intrinsically linked, there needs to exist a secure way for an asset to function as a medium of exchange, or as a way of transferring that asset.

Modern payment systems are computerized and most money exists only as digital records on commercial banks' accounts. More precisely, digital currency schemes combine both new payment systems and new currencies. Users can trade digital currencies with each other in exchange for traditional currency or goods and service. Especially, without the need for any third party like a Bank. And their creation and existence is not controlled by any central bank. Most digital currencies incorporate predetermined supply paths leading to fixed eventual supplies. An overview of how digital currencies work, including the creation of new currency, will give an insight in how they add value to our global economic environment.

Digital currencies are a globally spreading phenomenon which is frequently addressed by media, venture capitalists, financial or even political organizations. More specifically, their development represents a major breakthrough in computer science and especially in cryptography. But also, it solves technical issues which concern the way to establish trust between un-trusted entities in a peer-to-peer system, without the help of Banks[19]. They constitute, undoubtedly, a giant breakthrough in economics and finance too, in as much as they create decentralized, disintermediated and trusted monetary systems. So, this kind of digital innovation proposes a shift away from the established design of financial system infrastructures[20].

Digital currencies are part of a broader group of virtual currencies that include credit card points, air miles, loyalty points and coupons. With the advent of the Internet, mobile devices and companies are increasingly using digital currencies as a marketing tool. As a result, there has been a sharp increase in their use, particularly for application-based coins and tokens, mobile coupons, and personal data exchanged for digital content. So, it is more than important to introduce these alternative innovative concepts which aim to build future currency systems in an effective way to our traditional financial system.

[19] Lamport, L. , Shostak, R., Pease, M., (1982), The Byzantine general's problem, ACM Transactions on Programming Languages and Systems.

[20] Glaser, F. , Haferkorn, M., Weber, M and Zimmermann, K., (2014), How to price a digital currency? Empirical insights on the influence of media coverage on the Bitcoin bubble. Banking and Information Technology.

## ***The Spreading of Virtual Currencies in the Market***

Virtual currency, as we have already mentioned, is a type of online electronic currency which can be used to purchase virtual, digital, or physical goods and may also be exchanged for traditional currency. There is a significant rise of virtual currency in both traditional online games and social networks. Virtual goods are housed within the virtual economy an artificial economy that originally developed within traditional online games but has since expanded to social networks and other online communities.

The virtual goods market has, recently, experienced a significant growth with a growth projected to increase from $ 0.6 billion in 2009 to $ 2.4 billion in the future. Specifically, virtual goods which comprise virtual currency are basically housed within the virtual economy that was originally developed within the traditional online games but has since expanded to social networks and other online communities. The U.S. market for virtual goods, though, is currently estimated at $ 1.6 billion, with social networking sites accounting for around half or double as much a year ago, as it was reported by the research firm "Inside Network Inc"[21].

It is essential to note that the digital currencies and the flows are controlled only online by anonymous groups of volunteers who participate in the digital concept, the so-called peers. Thus, these currencies have the design of a local community currency in a closed environment, as in the case of online games. They are, also, designed to be payment opportunities within these specific environments and every single transaction is documented[22]. Approximately 10, 000 businesses, worldwide, accept payments with digital currencies already and the number is increasing steadily.

[21] Peng, H., & Sun, Y. ,(2009). Network virtual money evolution mode: moneyness, dynamics and trend. InInformation and Automation, International Conference Information and Automation,IEEE.

[22] Kaplanov, N. M. (2012), Money for nothing and bits for free.

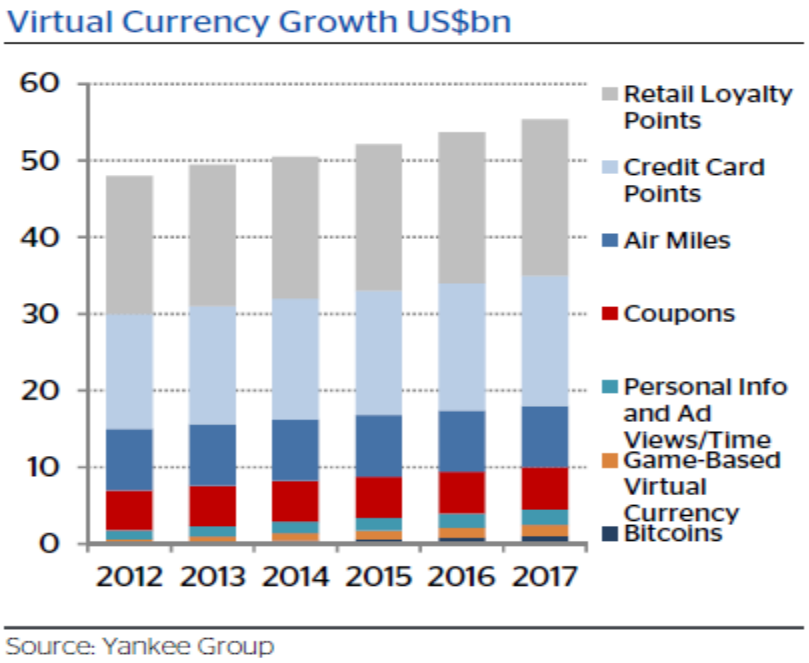



Figure: Percentage growth of Virtual Currencies in USA.

Source: Yankee Group

Virtual, digital currencies are based on the Internet, which has been continuously growing since its launch in 1996 and have no commodity-backed value. Concerning their management, there are typically two ways to obtain them. Firstly, a usual way is to purchase it using real money at a conversion that has been previously established. For example, users in online games or communities can often increase their stock by engaging in specific activities as by responding to an advertisement or by completing an online survey.

By issuing virtual currency credits, it is essentially about creating our own money supply that may be used as a currency for several transactions for goods and services. In fact, this possibility falls within the borders of the new era's virtual community. So, the birth of virtual currencies and their circulation in the market presents both new opportunities and developing threats to traditional payments services and providers.

We couldn't not oversee the fact that virtual currency schemes drew so much attention from the biggest financial institutions that have even published relative reports. These reports were concerning several properties of virtual currencies but most importantly the economic implications coming from them. The first influent paper has been published by the ECB in 2012. Furthermore, both Bank of America Merrill Lynch and Goldman Sachs, though, investigated whether the virtual currency could be interpreted as money or not.

According to the European Central Bank report, the discussion arose about how to define the diffusion of the virtual currencies. So, the ECB concluded that there are three different types of virtual currencies which are known and accepted:

(a) the closed virtual currency schemes, (b) the virtual currency schemes with unidirectional flow and (c) the virtual currency schemes with bidirectional flow.

For this reason from the ECB point of view a distinction between the various forms of coins was needed. In other words, in order to identify the virtual currencies the European Central Bank classified the different digital currencies based on the relation of the latter to the real economy. These three types of currencies are shown in the following figure.

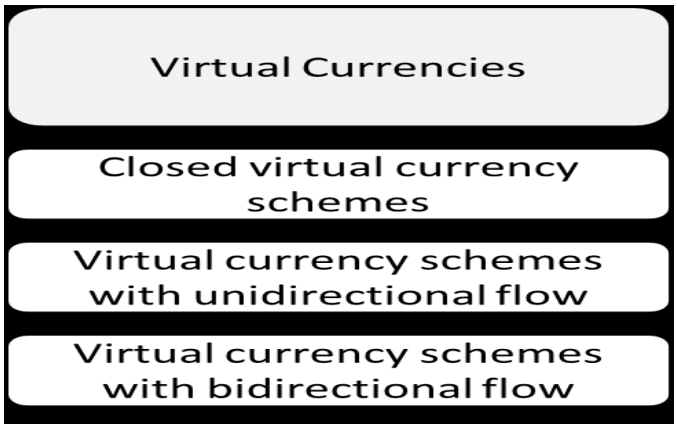



Figure . Different Types Of VC.

Source: European Central Bank

In respects to the first one, there is no link to the real economy. An example of this currency is the one used in the online games and for that reason it is also called "in-game only" scheme. Thus, the holders cannot exchange the game currency into a real currency and the separation to the real economy is well defined[23]. Therefore, the ECB does not account of it.

As far as it concerns the virtual currency scheme with unidirectional flow, there is a one-way relation to the real world. More precisely, in order to purchase this kind of virtual currency the user needs to exchange a real currency at a specific exchange rate. The important feature here is that he cannot exchange it back. The problem in this type of scheme is that the VC cannot be compensated if the owner has a surplus of it. Another problem may be the exchange rate at which it is purchased. The virtual currency's owner decides this rate. Facebook credits, the Nintendo points and the airlines' frequent-flyer miles are associated to this type of scheme.

Probably the most important scheme, because of its strong link with the real economy is the third one: the virtual currency scheme with bidirectional flow. It is defined as the user's possibility to buy or sell virtual money according to the exchange rates of their currency. "*The virtual currency is similar to any other convertible currency with regard to its interoperability with the real world. These schemes allow for the purchase of both virtual and real goods and services.*[24]".

In fact, virtual currency transactions are growing and at the moment the number of transactions realized daily is estimated at 200.000 in comparison to approximately 300 billion transactions in the classic banking procedure[25]. However, the field of digital

[23] Guo, J. , and Chow, A. , (2008), Virtual money systems: a phenomenal analysis. Paper presented at the 10th IEEE Conference.

[24] ECB, (2012), Virtual currency schemes.

[25] ECB, (2012),Virtual Currencies Schemes.

currencies remains very young with the first publications only appearing in the early 2000's, mostly based on theoretical models[26].

There are several reasons for a virtual community to issue its own virtual currency. More precisely, by creating a virtual currency scheme focused on the online world, a company can generate additional revenue. The use of virtual currencies can motivate users by simplifying transactions for virtual goods and services. It can also help lock users in if, for instance, it is possible to earn virtual money by logging in periodically. If users are asked to fill out a survey or to answer other questions in order to earn extra virtual money, users reveal their preferences, thereby providing valuable information for commercial use. So, digital currencies can also be used as an important tool for application developers and advertisers when there is need for designing a specific strategy.

To sum up, the development of digital, virtual currencies began as an idea and from then it followed a more specific and intensive analysis in several scientific directions such as their addition in companies as a loyalty instrument. It has also been used as an essential and disrupting innovation in the financial world posing challenges that we will discuss later. So, bringing together real world with the virtual world of video games was assumed as the starting point of the idea of virtual, digital currencies with payment options for real goods. It followed a movement by several authors writing about development and expansion of virtual currencies in the gaming industry and overviews of them[27].

[26] Irwin, D., Chase, J., Grit, L., & Yumerefendi, A. . (2005). Self-recharging virtual currency, ACM SIGCOMM workshop on Economics of peer-to-peer systems.

[27] Peng, H., and Sun, Y., (2009), Network virtual money evolution mode: moneyness, dynamics and trend. In information and automation, International Conference Information and Automation, IEEE.

## ***THE EMERGENCE OF BITCOIN AS A PEER-TO-PEER VIRTUAL CURRENCY***

## ***The Bitcoin Miracle- History in the Making***

*"You have to really stretch your imagination to infer what the intrinsic value of bitcoin is. I haven't been able to do it. Maybe somebody else can."*

– Alan Greenspan, Bloomberg Interview, 2013

Ever since the first general-purpose charge card debuted in the 1950's, pundits have been predicting the so-called "*cashless society*". Over fifty years later, we may

finally be getting close to that vision, concluding that the shift towards a cashless society with all its features appears to be a beneficial one.

The digital currency which has attracted most attention of the financial press within this context and continues to do it is "Bitcoin". Sold for a fraction of an American cent when it was introduced in 2009, the market value of a bitcoin exceeded four thousand US dollars in 2017. In recent months, though, it was even announced that a few businesses and entities would support transactions in Bitcoins. So, is the Bitcoin system here to stay and become an integral part of our economic lives?

Whatever the outcome of this particular experiment, the Bitcoin innovation made possible by using new technology the potential to revolutionize the current monetary and financial system. Bitcoin constitutes, particularly, an electronic financial mechanism, both a payment system and a currency, proposed by Nakamoto in 2008, that provides features such as its own money creation and transaction regime. Despite its name there is no physical coin! Even though it may not be the first attempt to create an entirely virtual currency, it supports some very interesting features, including anonymity and a decentralized, peer-to-peer network structure that verifies Bitcoin transactions cryptographically.

Bitcoin was born in the midst of the financial crisis of 2008-2009, and its ethos is aligned with much of the political sentiment of that period. It was then that banks have become excessively conservative in their credit policy refusing to provide markets with extra loans. Furthermore, it was publicly shown that traditional banking practices have been proven inefficient to create a stable international economy or a safe ground for potential investors, making most of economists to conclude that this banking model has failed[28]. Even, when Nakamoto's paper came out in 2008, trust in the ability of

[28] Khayrallah A., Hickey J., Jasvinder S., Radia N., Xu V., (2014), Insights in Engineering Leadership White Paper, Engineering Leadership Professional Program UC Berkeley.

governments and banks to manage the economy and the money supply was certaintly at its nadir[29].

According to the history, in 1998, Wei Dai, a member of the "Cypherpunks" which was an online community starting from an electronic mailing list, sought to avoid the need for an intermediary in an electronic payment transaction by proposing the concept of an anonymous digital currency[30]. In his article, Dai described a protocol in which "*untraceable pseudonymous entities . . . [could] cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts*." His idea was to create a currency where government involvement "*is not temporarily destroyed but permanently forbidden and permanently unnecessary*.[31]". However, in 2009, Satoshi Nakamoto effectuated Dai's idea. He designed and developed the idea of an anonymous currency which would be the so-called Bitcoin, the world's first decentralized digital currency, based on his self-published paper.

In the abstract, he would mention that Bitcoin as "*a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through financial institution.[32]*" .The Bitcoin currency and payment system offered an innovative and completely decentralized payment infrastructure based on a peer-to-peer network. So, even though Bitcoin was not based in a central trust authority, its network could provide reliable international money transfer. And that constituted a true innovation[33]. So, bitcoin became a new and unique financial vehicle, unlike anything the world has ever seen.

[29] Wallace, B. , (2011), The Rise and Fall of Bitcoin, Wired.com. Conde Nast Digital.

[30] http:// www.cypherpunks.to/

[31] Wei Dai, B-Money, (1998), http:// weidai.com/bmoney.txt

[32] S. Nakamoto, (2008), Bitcoin: A peer-to-peer electronic cash system.

[33] Krohn- Grimberghe, A. and C. Sorge, (2013), Practical Aspects of bitcoin system.

According to his aforementioned paper, Bitcoin as a payment system required no faith in the politicians or financiers, or even Banks who had wrecked the economy. It only required trust just in Nakamoto's elegant algorithms. The Bitcoin as a currency was created electronically and could be exchanged between users without passing by a financial intermediary. Every transaction made with bitcoins, whether it was a payment for goods and services or a simple transfer between two people was protected by a cryptographic signature which is a private key associated with each wallet. So, enthousiasm and support for bitcoin has gathered investors and investments groups who were willing to pay anything in order to acquire those digital coins.

However, backing the development of the Bitcoin system was a political statement too about the role of government in finance and the economy, making clear that citizens and users of the internet wanted to manage their own affairs by themselves. An indicative example was the fact that particularly in the early months of bitcoin's existence, its functioning as a currency was sustained by individuals who were willing to pay a greater price in exchange for the knowledge that they were using a new technology, more in line with their ideals.

Bitcoin is an online digital currency that relies on peer-to-peer technology for transaction management and distribution[34]. Unlike fiat currencies, whose value is derived through regulation or law and underwritten by the state[35], bitcoins have no intrinsic value and their only real value is based on supply and demand. We have to do with a decentral currency with a peer-to-peer network and control system. So, in bitcoin the entire computer network fulfills the role of the trusted third party for transactions between accounts, where nodes in this network propagate and verify transactions.

What most distinguishes Bitcoin from traditional currencies is that it relies on a decentralized organizational structure. That means that in contrast to the central bank's

[34] http://www.bitcoin.org

[35] J.P., Virtual Currency: Bits and Bob, (2011),The Economist

discretionary decision making, money concept in the Bitcoin system is transparently realized by a distributed and open algorithm, facilitating the reliability of expectations about the future supply of money. As in the case of sharing music files or films, Bitcoin uses a peer-to-peer data transfer protocol. Even several new payment systems like “Google Wallet” or “PayPal” which have simplified fast and even mobile money exchange could not compete with the Bitcoin’s approach to process all the payments without third-party authorities. So, the proper functioning of the network therefore does not rely on any authority, but rests instead on the reliability of its cryptographic protocol.

These characteristics, the decentralized network and the cryptographic security ensure that users do not need to fill out forms with their personal information or pay transaction fees to third parties to process their payments. Even at their current early stage, Bitcoin can  provide economists about a variety of insights and detailed information concerning the general market design and its properties and of course behavioral finance patterns as the behavior of buyers and sellers.


Figure :  BTC-USD, 6-Hour Candles, Bitfinex, Macro Fib. Lines

Source: http://bitcoinmagazine.com/

Bitcoin attempted to overcome the weaknesses of the existing financial system based, in the past, on the rule of gold and nowadays at the fiat currency ‘s rules, presenting itself as an “algorithmic currency” with a deterministic supply and growth rate that are tied to the principles of mathematics. So, no government or other authority could intervene in the supply of bitcoins. Instead, the circulation of them is governed by cryptographic rules that are enforced by transparent computer open-source code, in a decentralized manner. Likewise, the infrastructure behind the bitcoin concept that we will analyze below allows for real-time transactions monitored by the public peer-to-peer network. And the entire transaction history is recorded as a “chain”, in a system frequently referred to as Blockchain which constitutes the heart of the Bitcoin.

That does not make, though, Bitcoin an opaque system. In some ways, it may appear more transparent than the existing monetary system, but its underlying system still suffers from some inherent weaknesses, while processing transactions. These weaknesses often stem from this trust-based model[36]. In particular, it may be difficult to have any recourse in case of fraud, because transactions are irreversible once they have been confirmed in the blockchain. Thus, merchants become more wary of their customers, forcing them to give more information and details about their identity and their economic status. Not to mention that a certain percentage of fraud is accepted as unavoidable in the Bitcoin ecosystem.

We have to note here that the amount of bitcoin is limited to only twenty one billion[37] and no monetary or governmental authority has the right to create bitcoins. Only the integrated peer group, so-called “miners”, are able to create bitcoins and have the responsibility for the currency and the trades. The miners control every single transaction through the block chain[38]. In contrast with real currencies like the euros, the control

[36] S. Nakamoto, (2008), Bitcoin: A peer-to-peer electronic cash system.

[37] Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony & A. Pentland (Eds.), Security and Privacy in Social Networks, Springer New York.

[38] Deloitte. (2014). The new gold rush.

factor is given by the peer group, meaning less central orientation and lower transaction costs. So, Bitcoin with these properties became, undoubtedly, the currency of the Internet: a distributed, worldwide, decentralized digital money.

In fact, the first Bitcoins were transacted in January 2009 and by June 2011 there were 6.5 million of them in circulation among an estimated 10.000 users[39]. The currency has seen, recently, rapid growth in both media attention and market price relative to existing official currencies. However, there have been concerns raised regarding their untraceability and their potential to harm society through tax evasion, money laundering and illegal transactions. The potentil for authorities' ability to regulate and monitor the flow and the implications from the negative use of this virtual currency remains as yet unclear.

[39] Digital Currencies – Bits and Bob, (2011), The Economist.

## ***Making Transactions in the Bitcoin Ecosystem***

Generally, electronic payments involve three different parties: the payer, the payee and a financial network. A payer is the individual who wishes to make a purchase. On the other side, we have the payee who is the merchant from whom the payer wishes to make a purchase. And the financial network is the place where the payer and the payee store their funds, such as the Bank.

The payment system can be performed either online or offline. On an online payment, the payee is in constant communication with the Bank which will verify the validity of a payment by ensuring that money is not being double-spent, before the payee issues the goods to the payer.

On the other hand, in an offline payment, the payee will issue the goods and at a later time will then verify its validity. Unfortunately, in this case it is difficult to ensure that no users double spent their coins. But, the possible fraud would be detected by the Bank.

Concerning the case of Bitcoin now, an individual, wishing to use Bitcoins, needs to use a few simple steps, which are quite similar to obtaining a bank account, in order to get started. In fact, Bitcoin is a completely electronic form of money. Every bitcoin is divided into about one hundred satoshis defined by eight decimal places.

The path is very simple…A new user starts by downloading a wallet from the official Bitcoin website. Once that is complete, the user has to wait for the block chain, which consists of all the previously verified transactions to download. Having checked the block chain, a user can verify the validity of transactions and track the path made by every bitcoin. This process can take a few hours, but does not require any work by the user. Finally, once the wallet and the block chain are downloaded, the user can generate as many public keys, known as Bitcoin addresses, as he wishes.

By using computers intensively and incurring high electricity costs, subsequent participants can mine for bitcoins, of which the total number is 21 million as a fixed supply level. The supply function for the coins is spread out by reducing the size of blocks to be found and via an algorithm that makes finding them dynamically more difficult if they are found too quickly. So, it may take many years to mine them all existing Bitcoins[40].

Bitcoins trade on an online market and anyone can buy them at the going exchange rate on Bitcoin broker platforms such as the “Coinbase”. Bitcoin as a cryptographic currency is based on ideas from Hashcash and b-money and aims to remain completely distributed, free of central authorities or any kind control and anonymous[41].

[40] Goldman Sachs, (2014), All about bitcoin, Top of mind.

[41] Back A. et al., Hashcash-a denial of service counter-measure, http://www.hashcash.org

**Algorithm 1: The first organization.**

**Steps:**

1. The first step is access https://bitcoin.org/en/download and download the Bitcoin Core Software.
2. Install de Bitcoin Core software in the PC.
3. The user must run the Bitcoin Core software and wait for synchronization.
4. The creation of wallet is done by the software.
5. The user must encrypt his wallet assigning a private key
6. The user is now able to make their first

A Bitcoin is a fixed-value cryptographic object represented as a chain of digital signatures over the transactions in which it is used. More precisely, it can be checked for validity simply by checking the cryptographic validity of the signatures that constitute its history.

Each Bitcoin is owned by a Bitcoin address, which consists of a public key[42]. The holder of the corresponding private key constitutes the owner of Bitcoin. He can create a transaction, acting as a sender, by signing an assertion that Bitcoins are being transferred from one address to another. But, a transaction may involve several input and output identities. Occasionally, an extra output value will appear in a transaction for "change" to transfer back to the sender, since fixed-value coins must be transferred in an all-or-nothing manner. Nevertheless, if the total value of the input Bitcoins exceeds the value of the output Bitcoins, the difference is interpreted as a "transaction fee", which is paid to the player who successfully appends that transaction to the Block Chain[43].

[42] Barber S. , Boyen X., Shi E., and Uzun E., (2013), Bitter to Better- How to make Bitcoin a better currency, In proceeding of financial cryptography

[43] Ron D. and Shamir A. , (2013), Quantitative Analysis of the full Bitcoin transaction graph, In proceedings of financial cryptography.

**Algorithm 2: The second organization.**

**Steps:**

1. To access https://blockchain.info/wallet.
2. Inside of website, the user must follow the steps of wallet creation.
3. Then the user must enter the address of his wallet with his private key in the specified fields.
4. The user is now able to make their first transactions.

We should take into account at this point that this digital transfer is very interesting. There is, essentially, an open source key cryptology, one public and one private. In other words, bitcoin transactions transfer ownership of a coin from one public address to another. A private key, though, is required to decrypt the bitcoins and spend them. The cryptographic protocol procedures prevent users from spending other users' funds or double- spending the same coin and of course that new bitcoins are created in accordance to the rules of the system. Furthermore, Bitcoins in the form of public keys are stored in "wallets", on a computer's hard drive and can only be assessed with the private key.

In this way, safety against hacking is increased by the use of off-line "cold-storage" and such services are provided by broker platform intermediaries[44]. More specifically, "wallets" are stored through internet or linked with a smartphone application enabling bitcoin circulation from cold storage to mobile or other wallets.

As we have already mentioned, transactions are recorded in the Block Chain which is the key innovation in Bitcoin technology. More specifically, at the heart of Bitcoin ecosystem lies the blockchain, which is a public transaction ledger on the Internet All transactions are carried out on the network since Bitcoin system began to function are recorded chronologically in the Blockchain. For a transaction to be included in the

[44] Chaum D.,(1982), Blind signatures for untraceable payments. In advances in cryptology: Proceedings of crypto.

blockchain, it must first be validated, which requires the solving of a complex mathematical problem. So, Block Chain constitutes a technology that removes the need for a trusted third party and the following relative intermediary costs.

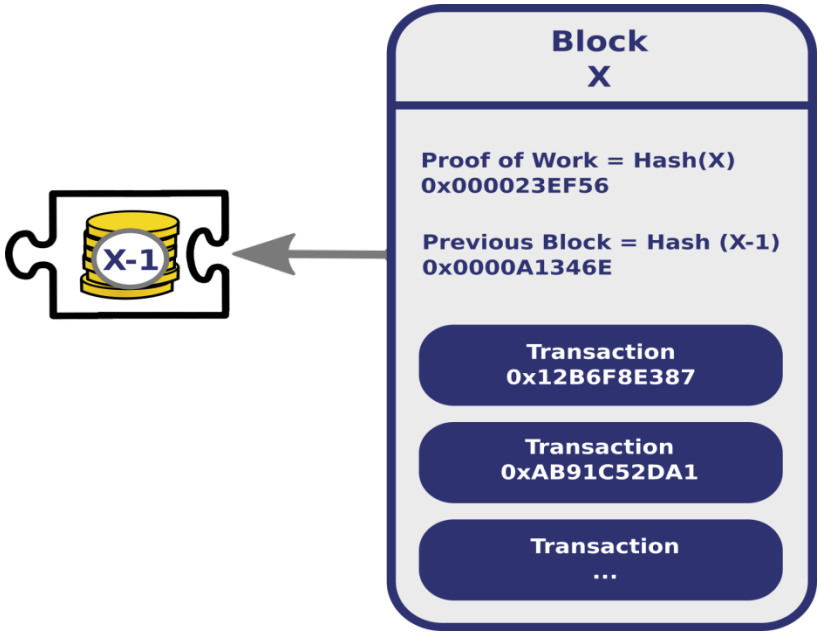



Figure : Each block contains, among other things, a record of some or all recent transactions, and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle , the hash or "Proof of Work" .

Source : https://www.niceideas.ch.

Suppose, for example, that Alice wishes to “send” a number of Bitcoins to Bob. Alice, then, uses a bitcoin client in order to join the Bitcoin peer-to-peer network. Thus, she makes a public transaction which is essentially a declaration stating that she wishes to re- assign one or more identities that contain Bitcoins she controls to Bob. These identities can be verified using public-key cryptography and have Bitcoins assigned to them. So, the participants of the P2P network form a collective consensus regarding the

validity of this transaction by appending it to the public history of previously agreed upon transactions (the blockchain).

Blockchain involves the repeated computation of a cryptographic hash function so that the transaction is “digested”, along with other pending transactions, and an arbitrary nonce too which has a specific form. We can say that this process is designed to require considerable computational effort, from which the security of the Bitcoin mechanism is derived. To encourage users to pay this computational cost, the process is incentivized using newly-generated Bitcoins with transaction fees. There comes the mining game.

The most important aspect in the Bitcoin system is the combination of three essential features. Firstly, the entire history of bitcoin transactions is publicly available in order to validate the transactions and to prevent them from the double- spending problem given that there is no third-party. The second feature of interest is that a transaction can have multiple inputs and multiple outputs. An input of a transaction is either the output of a previous transaction or a sum of newly-generated bitcoins with their transaction fees. Last but not least, the third feature is that the payer and the payee of a transaction are identified through public- keys from public-private key pairs. However, a user can have multiple public keys in order to protect his identity. In this way, he can avoid revealing any identifying information in connection with his public-keys as he can repeatedly send varying fractions of his bitcoins using multiple, newly- generated public keys.

**Algorithm 3: Node Division**

**Steps:**

1. The user must follow the same steps as in Algorithm 1.
2. The user checks the size of the Bitcoin database in the corresponding folder.
3. The user decides in how many parts the database will be divided. Let *n* be the number of parts. According to that, the user groups the *n* parts in *n* computers. Each part will be included in one specific

folder, considering the order of folder creation. That is, folder 1 will be in computer 1, folder 2 in computer 2, and so on.

4. The user must modify the source code of Bitcoin Core. To this end, the following steps must be followed:

a. Download the source code of Bitcoin Core (https://github.com/bitcoin/bitcoin)

b. Edit the source code using QT Project (http://qtproject.org).

i. The parts to be modified are referring to:- How do nodes share the data base together?

- How do nodes share the wallet information together?

5. After the modification of the Bitcoin, the user can start distributing the parts in different computers.

6. The user can execute transactions.

## ***HOW BITCOIN TRULY WORKS?***


Bitcoin's so called money system tries to mimic metallic money. It is not considered and has nothing to do with debt issues. Inspired by the fixed supply of gold, Bitcoin's designers have established a limited stock of twenty-one million "coins". Acquiring these digital coins is very simply as it is realized by downloading a free software that supports the Bitcoin protocol and its processes. Thus, a user acquires a personal wallet installed in his personal computer which allows him to buy, send or receive bitcoins. Each wallet has a distinct alphanumeric address as it happens with a bank account.

To start making transactions by bitcoin, a user needs to install a wallet, which is an application that needs to be run on a computer or smartphone, or on a third party service online. The wallet generates an address to the user, where the user will receive the digital coins. After you install it, you can find your bitcoins in a file called "wallet.dat" at your computer.

An online wallet allows bitcoin owners to store their digital coins in an online account managed by a third party. Alternatively, users can store them on their computers in a personal digital "wallet". Although, in this case they risk losing all of them if the computer is infected with a virus or suffers a physical damage.

There are specialized websites that offer bitcoin wallet services. Specifically, wallets can be useful for storing small amounts of bitcoins and allow mainly for quick online purchases. Some of the more popular wallet services are "Blockchain" and "CoinKite". However, bitcoin exchanges are a somewhat safer place for your bitcoins compared to online wallets because they keep most coins in a "cold storage". Usually over 90% of the bitcoins deposited on an exchange are kept offline. A small 5 to 10% reserve is kept onsite for immediate redemption purposes.

This address has numbers and letters around thirty-three characters in length, and always begins with the digit one or three. However, the user can have more than one address on his wallet. It is often recommended by experts to have plenty of addresses in one wallet in order to increase security and anonymity. Similarly to traditional bank accounts, you can receive bitcoins to your bitcoin address even if you're offline. When you want to "collect" your coins however, you'll have to be online. Once the user has a wallet with an address, he is able to get his very first Bitcoin that he may use in order to exchange things or make investments.

In order to release them in circulation, Bitcoins have to be "*mined*" through a computerized method. This process is also inspired by gold mining and is organized by rewarding nodes, that lie in the Bitcoin system, for volunteering to transmit a successful payment between two or multiple users. Every ten minutes the system releases a certain sum of new Bitcoins from a vault.

If we take into account that the whole Bitcoin process is computerized, we can conclude that people who wish to invest in Bitcoins should firstly invest in computer infrastructure and especially in computer power. Thus, an investor has the capability to

compete efficiently in the network of nodes by obtaining as quickly as possible the newly released digital coins. So, the opportunity to obtain new coins is linked to providing computer power to support this payment system.

Whenever a user wants to send Bitcoins to another user, the system poses a cryptographic puzzle to the network. More analytically, member nodes that have installed the software in order to solve such puzzles can compete for the fastest solution. Initially, the reward limit for solving a block's proof-of-work was fifty new Bitcoins. This amount halves for every 210,000 block of transactions incurred until it becomes virtually impossible to mine other digital coins. When Nakamoto designed the Bitcoin platform, he fixed the money supply at a predetermined limit of twenty-one million Bitcoins[45]. The last Satoshi, or 0.00000001 of a Bitcoin, will allegedly be mined by the 2140. After this, the system will solely rely on transaction fees as an incentive for new users to entry[46].

This process involves the repeated computation of a cryptographic hash function so that the product of the transaction and an arbitrary nonce, have a specific form. This process is designed to require considerable computational infrastructure and effort. Thus, the Bitcoin mechanism is secure and protected against certain technical problems. To encourage users to pay this computational cost, the process is incentivized using newly generated bitcoins or transaction fees in a process referred as "mining" that we will analyze further in the following sections.

Successful solutions print a timestamp on the transaction, something that serves as proof that the transaction is realized and is based on a unique digital coin, not having spent by the same user before. This mechanism prevents the system and its users from the double-spending problem. Afterwards, the proof is added to a public ledger, called Blockchain, which records every transaction in the network. In this way, Blockchain follows all transactions which are realized in Bitcoins in order to avoid inconsistencies in the system, but without revealing the identity of transaction partners.

[45] Wallace, B. (2011). The Rise and Fall of Bitcoin. Wired, http://www.wired.com/magazine/2011/11/mf_bitcoin/.
[46] Brito J., & Castillo, A. (2013). Bitcoin: A Primer for Policymakers,http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf.

The continuously updated public ledger is then checked by all other computers in the mining network for correctness of the solution of the cryptographic puzzle related to each transaction. If confirmed by the community, the updated version of the Blockchain is copied by all network members and serves as a decentralized form of keeping the whole history of all transactions realized within the Bitcoin platform.

As we have previously mentioned, nodes that deliver successful bids for transaction verification are awarded a certain sum of Bitcoins released from the stock. This is what we call in the dictionary of Bitcoin the process of mining. The greater the sum of bitcoins already released, the harder the puzzles become to solve and the smaller the sum of bitcoins awarded to new miners. By rewarding volunteers for payment transfer services with new digital coins, the system links its money predetermined supply to the operation of the payment system.

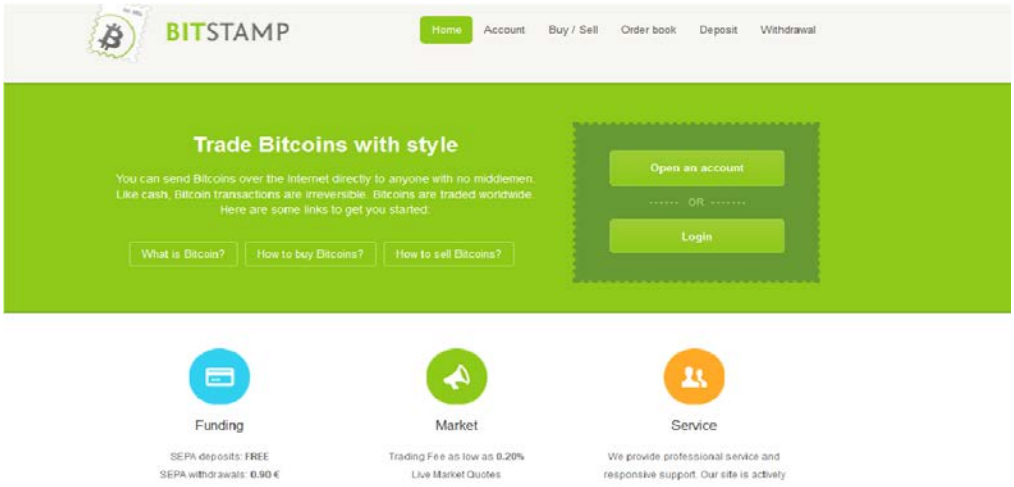
If we want to fully understand the technical process of acquiring and transacting with Bitcoins we can use a simple example. Put simply, suppose Alice wishes to "send" a number of bitcoins to Bob. In practice, Alice uses a bitcoin client to join the bitcoin P2P network and makes a public transaction or declaration stating that one or more (addresses) she controls, wish to reassign those bitcoins to one or more other identities, of which are controlled by Bob. It is important to notice here that these addresses can be verified using public-key cryptography and should have, previously, had a number of bitcoins assigned to them. The participants of the peer-to-peer network form a collective consensus regarding the validity of this transaction by appending it to the BlockChain.

In addition to using mining software in order to obtain bitcoins, users may obtain them from online or even traditional exchanges. More specifically, Bitcoin is currently traded on online exchanges against other national and transnational currencies valued by demand[47]. The largest exchange is the Japanese "Mt Gox", but there exist others as well. Although, different bitcoin exchanges operate in different ways and offer different

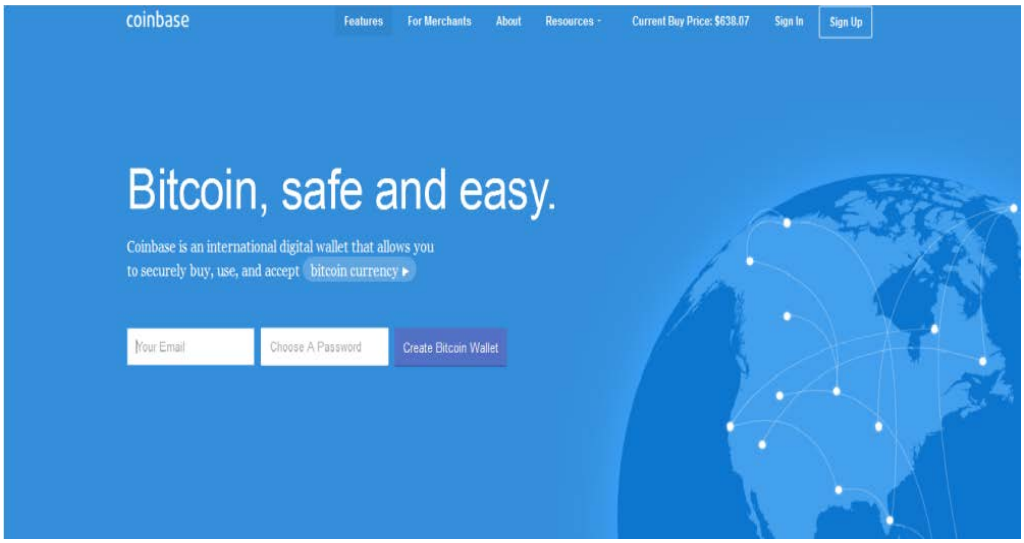
[47] D. , Lyons, (2011), The web's secret cash: a novel version of money is sprouting online, letting people shop in anonymity, Newsweek.

services. On each of these exchanges, users must enter into a service agreement that defines the rights of each party.

Apart from Mt. Gox and exchange sites there are other sites which offer safe and secure solutions for trading bitcoins. There are three major bitcoin exchanges, each of them with their own unique properties and a different fee structure. At first, there is " *Bitstamp.net* " .




In Europe, Bitstamp is a good way to get some bitcoins at a low cost. The company is based in Slovenia. Deposits by SEPA are free, withdrawals are charged a fixed 0.90€ fee once the funds are converted to euros. Because Bitstamp only offers trading in BTC/USD all euro transfers are immediately converted to Dollars. Secondly, there is the "*Coinbase.com*" site which is the easiest and safest way to purchase bitcoins in the U.S.




These sites act as a counter-party to all customer trades. The buy/sell fee is 1% on top of the buy/sell spread. The bid/ask is usually close to where the firm gets its liquidity from. In addition to this, every firm poses daily limits on the amount of Bitcoins bought and sold. These limits are not applied on the individual level. During times of high volatility, users may not be able to buy or sell bitcoins until each firm decides to "refill" their stock. They, also give you the opportunity to link your bank account to them in order to facilitate quick and easy bank transfers. However, all clients should keep in mind that as soon as you connect your bitcoin address to your real identity, by purchasing bitcoins online, the pseudo anonymity provided by bitcoin is lost.

Apart from participating in online or traditional exchanges, a user can obtain bitcoins by purchasing them directly. This can be done by finding someone who is willing to exchange them for cash. Several websites provide contact information for buyers and sellers, allowing them to connect and exchange bitcoins directly. Nevertheless, bitcoins can be transferred to non-miners in exchange for goods and services. But, currently, there are only a few "real world" locations where bitcoins are accepted. However, there are thousands of online merchants that accept them as a

payment for goods like computers or clothes. And the price of these goods is generally determined based on the bitcoin's rate of exchange with another currency.

To sum up, the Bitcoin concept emphasizes the system's ability to operate without the need for trusted third-parties intermediaries and most importantly without inflation. As we have previously cited, bitcoin is an electronic currency with no central authority or issuer. There is no central bank controlling the supply of bitcoins or the transactions realized in the Bitcoin system. Instead, under this general technological frame a user can address an online or traditional exchange in order to acquire the digital coins or even trade them using specialized platforms with specific rules as it happens in the real world with our established fiat currencies.

## ***Anonymity in the Bitcoin Ecosystem***

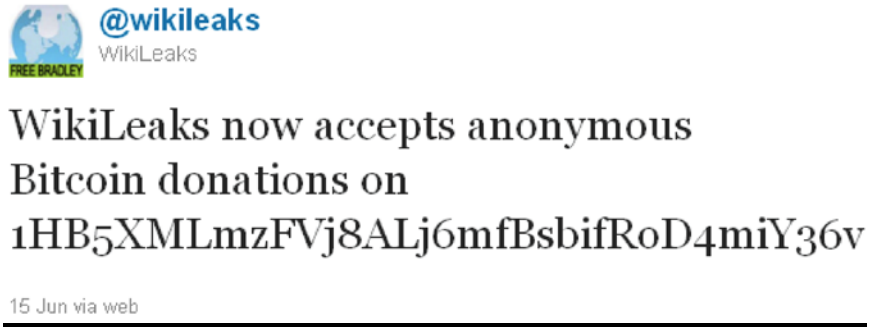



Figure - Screen capture of a tweet from WikiLeaks announcing their acceptance of `anonymous bitcoin donations.

Bitcoin is often described as a way to transact anonymously. But just how anonymous is it, in practice? More precisely, cash or barter are the most intrinsically private and anonymous means of transacting because when transacting they do not require from their owners to give their personal information . In the opposite corner are transactions which are neither anonymous nor private. This may include in this quadrant credit card transactions: although not public knowledge like a campaign contribution, your identity is nevertheless connected to every purchase you make. Not to mention that this information is available to the merchant, to the credit card network, issued by the bank, and maybe to other central authorities.

Unlike bank accounts and most other payment systems, bitcoin addresses are not tied to the identity of users on a protocol level. In other words, anyone can create a new and completely random bitcoin address with the associated private key at any time,

without the need to submit any personal information. So, Bitcoin payment transactions are anonymous and do not require the provision of personal identity information.

In the Bitcoin system, the transactions are not tied to the identity of users either. As long as a miner includes the transaction in a block, anyone can effectively transfer bitcoin from any address whose private keys he controls, to any other address, with no need to reveal any personal information and most importantly without supervision.

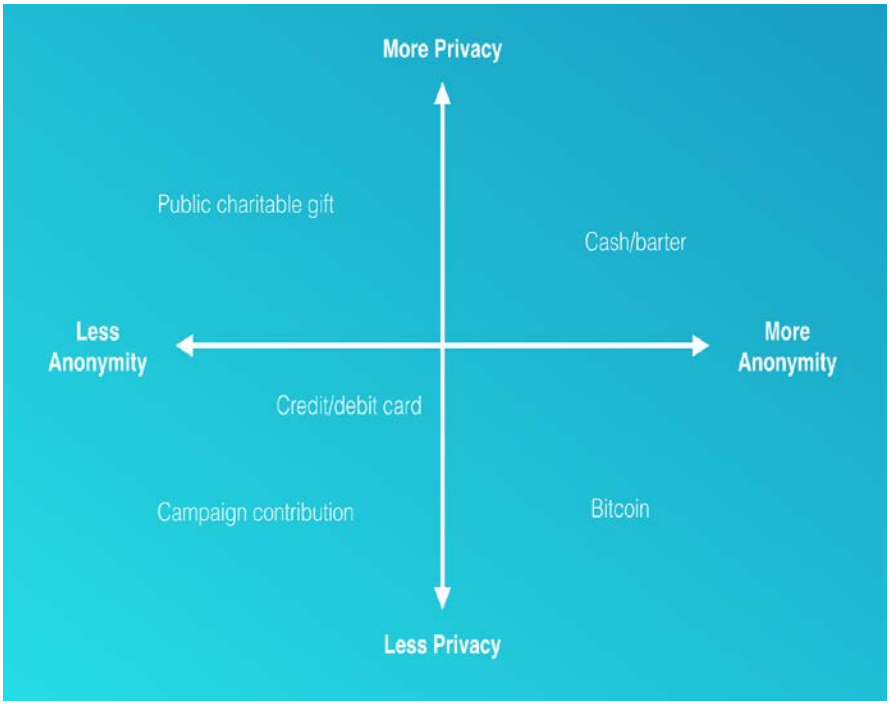



Figure - A matrix containing different financial transactions and their privacy

Like physical cash, not even the receiver needs to know the identity of the sender. Since Bitcoin transactions are peer-to-peer and require just internet access, the bitcoin transaction data is transmitted and forwarded by nodes to a random set of nodes inside the peer-to-peer network. Therefore, with its infrastructure being spread

globally, it is difficult to intercept or track individual transactions While bitcoin nodes do connect to each other using IP-addresses, it's not necessarily clear for nodes whether the transaction data they received was created by the node they connect to. So, for many users, who access the digital coins through online wallet or exchange services, their participation at the outset entails linking their personal identity to their bitcoin holdings.

Bitcoin for these users is no more anonymous than a bank account. We should notice, although, that this loss of anonymity takes place at the point of entry into the Bitcoin system and is not a feature of its architecure. For those who wish to take advantage of bitcoin's intrinsic anonymity, they must find an alternative entry point, such as acquiring bitcoin in a private transaction, as compensation for goods or services rendered.

However, Satoshi upon visualizing Bitcoin protocol claims that the Bitcoin platform remains transparent and public, meaning that anyone is able to follow the chain of transaction. And this is partly true if we think that all BitCoin payments have a traceable history that can be viewed by anyone through Blockchain. In other words, the knowledge of the identity of any user from any transaction allows to track that user's transactions backward and forward through the BlockChain history.

But, it is important to mention that subsequent bitcoin transactions can then be anonymous, since real-world identities are not recorded on the block chain ledger. In other words, the only identifying information recorded are the bitcoin addresses, whose corresponding private keys are held by the owners as proof of ownership[48]. Maintaining one's anonymity from this point forward, however, is in no way guaranteed. There are several options available to overcome the anonymity in the Bitcoin game and make transactions non-traceable. For example, by using new addresses for each payment received, by using different addresses when realizing payments, or using Bitcoin mixer services to break the link between a user and its digital coins.

[48] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2013), "A fistful of bitcoins: characterizing payments among men with no names," In Proceedings of the conference on Internet measurement conference, ACM.

As bitcoin adoption continues to increase, it is not out of the question that a technology arms race could arise between “anonymizers” and “deanonymizers”. On the one hand, increasingly sophisticated data mining schemes are currently being developed, possibly combining transaction graph analysis with IP address discovery. In this way, they will be capable to trace the movement of funds in the Blockchain between individuals in a worldwide scale. On the other hand, improved techniques will be devised to better conceal individual identity and activity[49] and facilitating often illegal transactions with Bitcoins. But unfortunately, this fact can affect negatively the popularity and the use of the Bitcoin system.

[49] http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/

# ***BITCOIN AS A CRYPTOCURRENCY***

## ***Public Key Cryptography behind the Bitcoin***


*"Bitcoin and similar digital currencies are called crypto-currencies by some because the underlying algorithms and security are intimately related to digital cryptographic algorithms." (Dwyer, 2014)*

In fact, paper cash, which has been used for modern trade, serves as a model for the cryptographic application of electronic cash systems such as the debit and the credit card systems. It is not then absurd that cryptographers have been attempting to design a secure form of electronic cash, based on the security properties found in the paper cash system.

Cryptography constitutes a technique developed by computer scientists in order to enable secure transmission of information. In simple terms, it turns information from a readable state into non-sense and then provides a means to unscramble the message. This process is based on sophisticated mathematics and algorithms.

Cryptocurrencies constitute physical pre-computed files utilizing a public or private key pairs generated by a specific encryption algorithm. More specifically, the key assigns ownership of each key pair, or "coin", to the person who owns the private key. These key pairs are stored in a file named "wallet.dat", which resides in a default hidden directory on the owners computer hard drive. And the destination payment address is the public key of the cryptocurrency key pair.

There is a finite amount of each "*cryptocoin*", as they are called, available on the network. The value of each unit is assigned based on supply and demand, as well as the fluctuating difficulty levels required for mining each coin. The "wallet.dat" file is the most important file of the cryptocurrency software architecture and much like cash, if a user loses this file, or has it stolen, the cryptocurrency is lost.

Bitcoin is one of the first implementations of a concept called crypto-currency. It is designed around the idea of using cryptography in order to control the creation and transfer of money, rather than relying on central authorities. Satoshi after creating the cryptocurrency posted the now infamous quote:

*''It might make sense just to get some in case it catches on''*

Satoshi Nakamoto, January 17th, 2009.

In digital cryptography, the original text known as "plaintext" is turned into a coded equivalent called "ciphertext" via an encryption algorithm. The ciphertext is then

decrypted at the receiving end and turned back into plaintext[50]. This is the basic process done by the computers during the transaction processes in the digital currency cryptography system.

In the present market, there are three primary ways of obtaining cryptocurrencies. More precisely, by buying them, accepting them as payment or by mining new ones.

According to the digital cryptocurrency history, in 1976, Diffie and Hellman introduced the concept of "*public key cryptography*", in which a user has both a public and private key. According to this, the receiver of the message publicizes his public key, which can be used then by anyone who wishes to send him a message. The sender simply uses the public key to encrypt his message into ciphertext, and the receiver uses his private key to decrypt the ciphertext into the original message.

In 1982, David Chaum proposed a cryptographic untraceable payment system[51]. After six years, a description of "b-money", which would be an anonymous, distributed electronic cash system was published by Wei Dai[52] that in the near future would form the Bitcoin.

B-money was a personal project and it was more conceptual than practical. After a short period of time, another developer created the "Bit Gold"[53]. In the bit gold scheme, a participant must dedicate computer power in solving cryptographic equations assigned by the system. "Bit Gold" was an electronic currency system which required users to complete a function with solutions being cryptographically put together and published. The solved equations would be sent to the Bit Gold community and the work will be credited to the person who solved it. The solution will then become a part of their computation, thus creating a chain of new property. And this scheme reminds us strongly of the Bitcoin protocol.

---

[50] J. Matonis, "Top 10 Bitcoin Merchant Sites", Forbes.
[51] D. Chaum, "Security without Identification: Transaction Systems to make Big Brother Obsolete", Communications of the ACM, (1985).

[52] W. Dai, "B-Money", (1998), http://www.weidai.com/bmoney.txt .

[53] M.E. Peck, "Bitcoin: The Cryptoanarchists' Answer to Cash", IEE Spectrum, (2012).

Bitcoin, being the first type of decentralized digital currency cryptography introduced in online market, made a worldwide impact. After the emergence of this technology, many other digital currency cryptography have been created, each one offering different features. The majority of them, though, had low market capitalization and did not make it[54].

Bitcoin is one of the first implementations of the concept which was called "*cryprocurrency*", a notion which was first described in 1998 by Wei Dai on the cypherpunks mailing list. More precisely, Bitcoin is considered as a cryptocurrency because it uses cryptography procedures to scramble every financial transaction. In other words, in order to transmit it over the Internet and then unscramble it when it reaches its destination which is the recipient's wallet.

Bitcoin uses a cryptographic hash function in order to accomplish this task. We have to notice, though, that cryptographic tools are very powerful because, "*the secrecy of the encrypted message is preserved even when an attacker knows the encryption key*".[55] So, the scheme of cryptography relies on the fact that encryption is easy but reversing it via decryption is computationally infeasible for anyone other than the intended receiver[56].

In the case of the Bitcoin system, its electronic payment system is based on cryptographic proof instead of trust, allowing any willing parties to transact directly with each other without the need for a trusted third party.[57]. Furthermore, observing its cryptographical architecture, we notice that the encryption which lies behind it generates two mathematically related keys.

---

[54] A. Greenberg,(2011), "Crypto Currency", Covering the worlds of data security, privacy and hacker culture, Forbes .

[55] Katz, J., & Lindell, Y.(2008). Introduction to Modern Cryptography. CRC Press.

[56] Kaliski, B. (2006), The Mathematics of the RSA Public-Key Cryptosystem. *RSA Laboratories*.

[57] S. Nakamoto, (2008), Bitcoin: A peer-to-peer electronic cash system.

One key is retained by the payee of bitcoins and is private like a private password, while the other key is made public like the number of an account location where the funds reside. Thus, the latter is used to receive payments and the funds can only be accessed through the use of the associated private key. At the same time, the payer of bitcoins uses his own private key to approve the payment. Put simply, the public key is like an email address which is something public and available to everyone, while the private key is like the password needed to authorize specific bitcoins to circulate.

Public and private keys are alphanumeric strings based on a sophisticated encryption model. More precisely, they are random numbers and letters which are derived from public keys by the application of a "hash function". Moreover, a hash function constitutes a process that takes an arbitrary block of data and returns a fixed size bit string. For instance, the hash function used for both transactions and block generation in the Bitcoin ecosystem is SHA-256[58].

As far as the privacy of the Bitcoin network is concerned, we can tell that the public keys play a major role in transaction's anonymity. More specifically, from the example of traditional banks, a level of privacy is achieved by limiting access to information provided by the parties involved.

In the Bitcoin system, though, the necessity to announce all transactions publicly precludes this method, but privacy can be still maintained by keeping the public keys anonymous. In other words, the public can see that someone is sending an amount of bitcoins to someone else, but without information linking the transaction to anyone. It is also suggested that a new key pair should be used for each transaction as an additional firewall to keep them from being linked to owners. In the end, some kind of linking remains unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. Unfortunately, the possible risk lies in the fact

[58] FIPS 180-3, (2008), Secure Hash Standard, Federal Information Processing Standards Publication.

that if the owner of a key is revealed, linking could reveal other transactions as well of the same owner[59].

A specific signature algorithm is also used at this level, the elliptic curve digital signature algorithm (ECDSA) which is a cryptographic algorithm in order to ensure that funds can only be spent by the right owners[60]. So, cryptography solves for the problem of maintaining the privacy of the payer and the payee in the bitcoin ecosystem

These cryptographic tools are used in order to prevent possible malicious users from breaking the system and gaining control of it. Thus, Bitcoin overcomes potential attacks especially by relying on the use of public key encryption. In this way, the parties' privacy is secured, solving simultaneously the problem of double-spending through the use of a widely-published peer-to-peer distributed timestamp server[61].

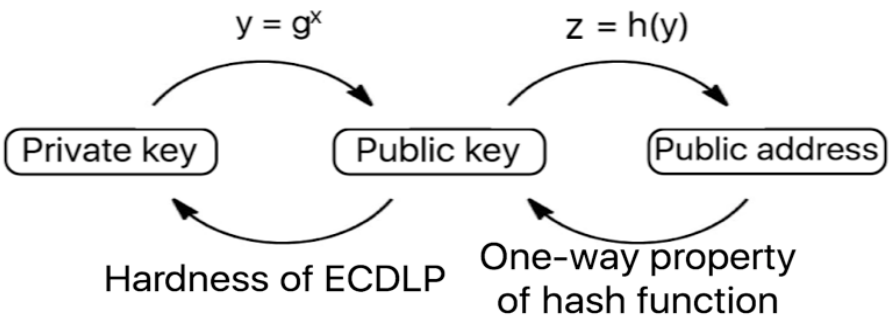



Figure: The arrows along the top show how to produce each piece of data from the previous. The labels on the bottom arrows are known as " hard problems", which cannot feasibly be solved with today's computing power.

Source: https://www.benthamsgaze.org/category/cryptography/

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

[60] https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm

[61] G. Medvinsky and C. Newman, (1993), NetCash: A design for practical electronic currency on the Internet, ACM Conference on Computer and Communications Security.

## ***Hash Function- Timestamp***

Generally, the hash function prevents the creation of a block of data identical to other bitcoin transaction files. It is hard to intervene in hash functions as even in the case of changing a block of data, only slightly changes its hash unpredictably. And this constitutes a feature that provides the necessary security in the Bitcoin system.

Trading of the bitcoin begins with a timestamp whose use is to prove existence of bitcoin data at a specific point of time before development of the hash. The timestamps play an important role in development of the chains through the hashes. More specifically, a cryptographic hash function is a mathematical equation that turns words into numbers. In other words, it takes any worded message and turns it into a unique string of numbers. We have to mention at this point that a hash function constitutes a process which takes a block of data ( transaction files) and transforms it, in an impossible to reverse way, into a large integer[62].

What's unique, though, in hash function is that the message input can be of any length, but the output should be at a fixed length. This characteristic makes sending any message in the network secure and efficient. Therefore, Bitcoin blocks do not require serial numbers because blocks, even by their coding, can be identified by their hash.

In fact, it is proved that the bitcoin software is a really safe way to digitally sign any financial transaction. More precisely, thinking about the digital processes behind it, it is harder to forge a digital signature than a regular written signature. These digital signatures are so unique that the likelihood that someone has the same digital signature is incredibly small. Thus, these feature strengthen the security of the Bitcoin platform.

[62] C. Dwork and M. Naor, (1992), Pricing via processing or combating junk mail, In proceedings of the 12th annual international cryptology conference on advances in cryptology.

We should take into account, though, that storing private identification strings online, while transacting, opens the way for stealing and fraud as with anything where money and Internet is involved. That is why the hash functions and other algorithms were developed. Their aim is essentially to prevent malicious users from stealing and creating their own coins in transactions.

It is important to mention that, while a public- key encryption system is effective in ensuring privacy, as we have described before, it remains useless in preventing digital coins such as Bitcoin from being spent more than once. Moreover, it is necessary to remind that in traditional payment systems, this problem is overcome by relying on a central authority to check each transaction but this does not happen in the case of Bitcoin. So, the identification and the integrity verification requirements for bitcoins need the deveoplment of these cryptographic principles.

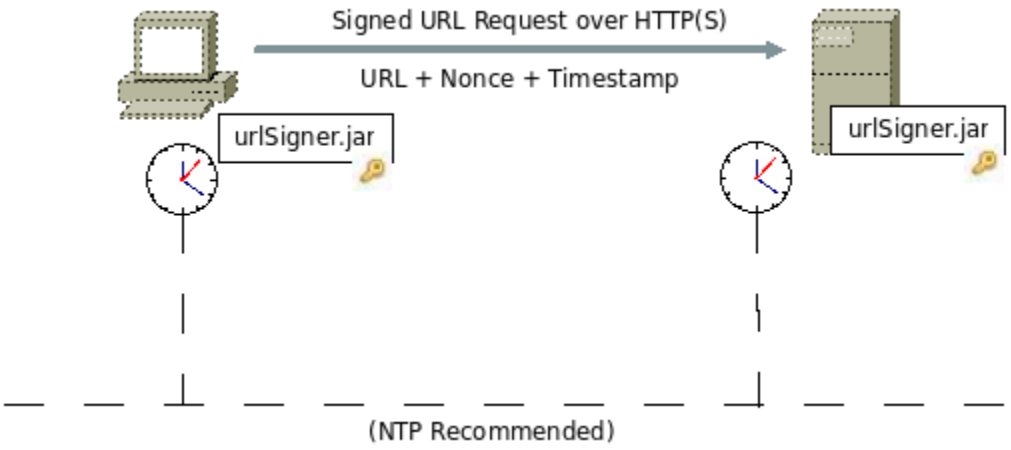



Figure : The sender generates a nonce and a timestamp, using the current date and time, Using its private key it performs a digital signature operation wherein the original URL, the nonce and timestamp are first hashed using the Secure Hash Algorithm (SHA) and then encrypted (using the private key.)

Source: http://urlsigner.sourceforge.net/overview.html

On the other side, there is a timestamp which records the exact time of a transaction. The timestamp comes in two forms: a) the creation of the currency and b) the transaction between two parties. In fact, transactions are organized in the log into blocks, which contain a sequence number, a timestamp, a cryptographic hash of the previous block, some metadata, a nonce and a set of valid bitcoin transactions. In order to prevent double spending, Bitcoin players engage in a peer-to-peer protocol which implements a distributed timestamp service providing a fully serialized log of every realized bitcoin transaction. In this process, Blockchain seems to help secure the transaction since it records all the realized bitcoin transactions.

Essentially, a timestamp server is a network process used to prove that a specific piece of data, in this case bitcoins, must have existed at a certain time in order to get into hash and to create, thus, a chronological order of data movement. According to Satoshi, "*each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it*[63]."

On the other side, digital signatures provide part of the solution, if the problem of double-spending remains. The peer-to-peer network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of work. Thus, a record that cannot be changed easily is formed. In the end, the blocks form a hash chain and each new block contains the cryptographic hash of its predecessor, allowing anyone to verify that no preceding block has been modified[64]. Furthermore, the header contains the hash tree or the "Merkle tree" which depends on the included transactions. This includes the generation transaction, a transaction "out of nowhere" to our own address. In addition to providing the client with incentive to do the work, it also ensures that every client hashes

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

[64] J. Kroll, I. Davey and Ed. Felten, (2013), The twelfth workshop on the economics of information security, Washington DC.

a unique data set. According to results, the hashing process is O(N) and transaction parsing operates at O(*log* (N)**)**, while building the "Merkle tree" O(N2).

The structure of the bitcoin block chain requires that all clients keep a copy of the working hash tree (Merkle tree), which is the longest chain of the agreed blocks. Moreover, the SHA-256 hashing algorithm is used to find possible solutions in order to award Bitcoin users with bitcoins.

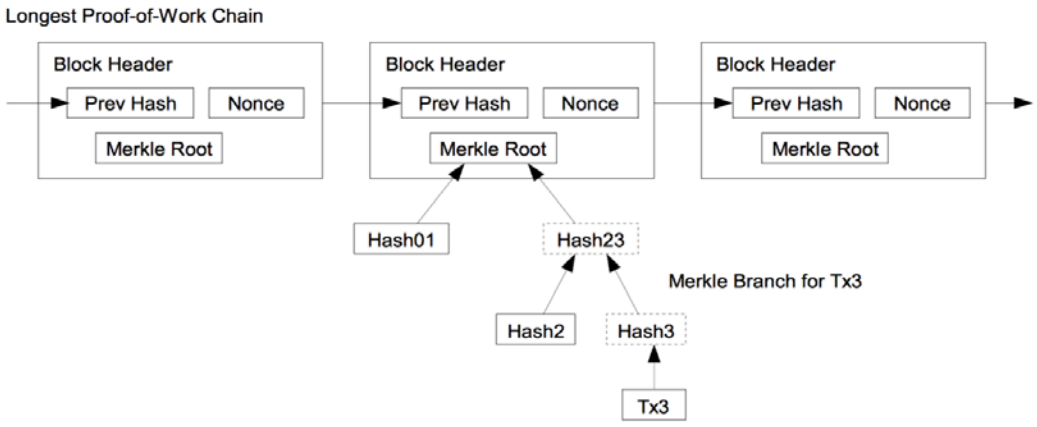



Figure : From the original whitepaper, the schematic view of Satoshi Nakamoto's scheme for validating blockchain changes. Image by Satoshi Nakamoto.

Source: http://www.edgetechcny.com

## ***Digital Signatures***

Another important component of the bitcoin protocol is its digital signatures. More precisely, as we have already stated, identification of the bitcoin is done through chain of "Elliptic Curve Digital Signature Algorithm", (ECDSA) digital signatures. The ECDSA algorithm is used in digital signatures"[65]. Hashes are attached digitally to every digital coin being traded, and the ownership can be determined through the use of digital signatures attached to the coins that have been transacted.

Generally, digital signatures constitute a popular mechanism for message authentication as they have three desirable properties. Firstly, they allow the receiver to validate the correct sender of the message (authentication) Afterwards, they ensure that the sender cannot deny having sent the message (non-repudiation), and thirdly, that the message was not modified in any way by an adversary (integrity)[66] .

To achieve this, the sender computes a digital signature using his private key and sends his "signed" message to the receiver. As long as the receiver knows the sender's public key, he can use a verification algorithm to determine if the message was signed by the original owner. . Rather than encrypting the entire message, it is often more sensible to encrypt a hashed version of the message.

Digital signatures are widely used in electronic transactions because the authenticity of the message can be verified by anyone who has the sender's public key. Another advantage is that digital signatures are publicly verifiable. In other words, if the receiver verifies a given message's signature as legitimate, then all other parties, such as a trusted third party intermediary who receives the same message should also validate it as authentic.

[65] Kogent, (2009), Learning Solutions Inc.

[66] Katz, J., & Lindell, Y.(2008). Introduction to Modern Cryptography. CRC Press.

Bitcoin protocol uses the Elliptic Curve Digital Signature Algorithm (ECDSA), a variant of the Digital Signature Algorithm (DSA). Especially, ECDSA is a group, an abstract mathematical entity "consisting of a set together with an operation * defined on pairs of elements of" [67]. The security of the Digital Signature Algorithm is "based on the intractability of the discrete logarithm problem in prime-order subgroups of z"[68] .

| **Algorithm ECDSA Signature Generation algorithm** [69] |
|---|
| Input: Domain parameters D = (q, P, n, Curve), private key d, message m. |
| Output: Signature (r, s). |
| 1: Select $k \in_R [1, n - 1]$. |
| 2: Compute $kP = (x_1, y_1)$ where $x_1 \in_R [0, q - 1]$ |
| 3: Compute $r = x_1 \bmod n$. If r = 0, then go to Step 1. |
| 4: Compute e = H(m). |
| 5: Compute $s = k^{-1}(e + dr) \bmod n$. If s = 0, then go to Step 1. |
| 6: Return (r, s). |

The operation * must guarantee the following four properties:

**1. Closure**. $a*b \in G$ for all $a, b, \in G$

**2**. **Associativity**. $a*(b*c)=(a*b)*c$ for all $a, b, c \in G$

**3**. **Existence of Identity**. $e*a = a*e = a$ for all $a \in G$ where $e \in G$ is the identity

**4**. **Existence of Inverses**. $\forall a \in G, \exists b \in G$ such that $a*b = b*a = e$ and b is denoted as $a^{-1}$.

[67] Johnson, D. B., & Menezes, A. J. (1998), Elliptic curve DSA (ECDSA): an enhanced DSA. SSYM, 98, 13-13, http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa.pdf.

[68] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security.

[69] D. Hankerson, S. Vanstone, and A. Menezes, (2004), Guide to Elliptic Curve Cryptography,Springer.

To supplement this, the bitcoin protocol also uses a SHA-1 cryptographic hash function. Ideally, the hash function should be one-way. More precisely, given a fixed-length binary output, it would be very difficult to find a string that hashes to the given output[70]. A one-way collision-resistant hash function should make it impossible to forge the signature or modify the original message by attacking the hash function itself. Additionally, the hash function should be collision-resistant, which means that it would be computationally infeasible to find two messages that share the same hash value[71] . In other words, it would be infeasible for any probabilistic polynomial algorithm to find:

$$x, y, \; x \neq y \text{ such that } H(x) = H(x')$$

To sum up, SHA-256 which belongs to SHA family algorithms is a combination of cryptographic hash functions that verifies the transaction and is used especially in bitcoin transactions. Encryption and decryption ensures the privacy of the Bitcoin protocol by preventing adversaries and attackers from accessing the message sent from sender to receiver. Message authentication, however, must also be used in conjunction with public key encryption.

[70] Ius Mentis. (2005). Crash course on cryptography: Digital signatures. .
[71] Katz, J., & Lindell, Y. (2008). Introduction to Modern Cryptography. CRC Press.

## ***Proof of Work (PoW)***

Another characteristic which complements the Bitcoin technological architecture and ensures its safety is the Proof-of-Work (PoW). A proof of work is a piece of data which is difficult and by difficult we mean costly and time-consuming to produce. But, it remains easy for others to verify. Clearly, it satisfies certain requirements.

Bitcoin, as we have already described, uses the "Hashcash" proof of work system. One application of Hashcash as a method to preventing email spam is the requirement of a proof of work on the email's contents. More specifically, Hashcash proofs of work are used in bitcoin in the process of block generation. In order for a block to be accepted by network participants, clients must complete a proof of work which covers all of the data in the block.

The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every ten minutes. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Thus, due to the very low probability of successful generation, this makes it unpredictable for a computer in the network to be able to generate the next block.

For a block to be valid it must have a hash with a value less than the current target and this means that each block indicates that work has been done generating it[72]. As we have already mentioned, PoW is essentially taking the hash of a block of items and broadcasting this hash to the network. The items in question for the PoW block are transactions that need to be verified, the hash of the previous block, and a nonce.

[72] https://en.bitcoin.it/wiki/Proof_of_work

Since each block contains the hash of the previously generated block, the blocks form a chain of hash values along with transactions. The goal is to systematically increase the nonce so that the hash of the block that is currently being generated is less than a predetermined number. The longest chain not only serves as a proof of the sequence of events witnessed, but it also proves that it came from the largest pool of CPU power. As long as the majority of CPU power is controlled by nodes that are not cooperating to attack the network, they will generate the longest chain and outpace attackers[73].

Since each block contains the hash of the preceding block, then it has a chain of blocks that together contain a large amount of work. Changing a block, a work that can only be done by making a new block containing the same predecessor, requires regenerating all successors and redoing the work they contain. This protects the block chain from tampering. The proof-of-work scheme used as a part of bitcoin is based on the algorithm SHA-256[74].

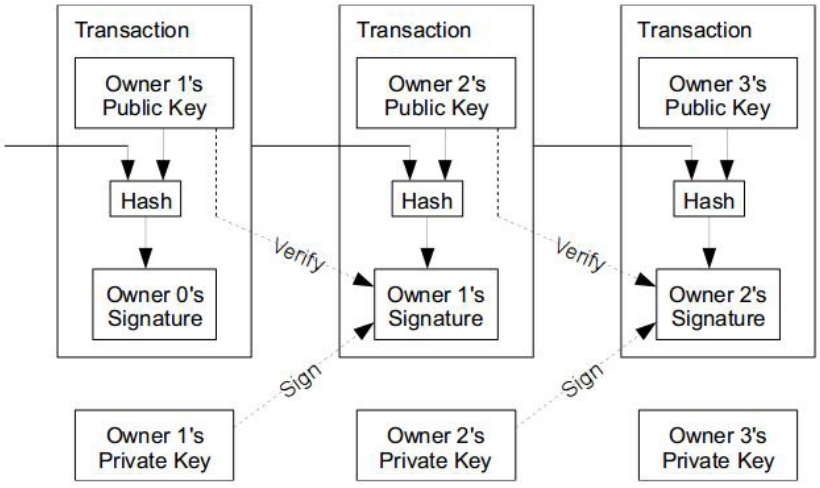



Figure - Block diagram of a typical bitcoin transaction process

[73] S. Nakamoto, (2008), A Peer-to-Peer Electronic Cash System.

[74] https://en.bitcoin.it/wiki/Proof_of_work

In the pictured above, there is the general representation of a transaction inside the bitcoin network. Transactions are the first building block of our global history network and they are composed of a series of "ins" and "outs". An "in" is simply the digital coins going to an owner and an "out" is those leaving an owner.

Proof of work (PoW) functions are constantly being performed by all nodes as part of the bitcoin network. This serves as a critical functionality which replaces the need to have a central entity that assumes the risk of transaction fraud. This orientation of nodes, combined with the randomized methodology that is used to connect to a subset of the other nodes on the network, creates a highly resilient and diversely connected mesh[75].

This target is updated every 2016 blocks to ensure that the time it takes to generate a block is on average ten minutes. This ensures that users will accept a block if all the transactions contained in it are valid and if the coins have not been previously spent. But most importantly, it ensures that the work required to generate all the subsequent blocks is in the PoW chain.

The transactions can be condensed together to save space using a Merkle hash tree. And there is no upper bound to the number of transactions that can be verified in a single block, but there has to be at least one[76].

Creating the Bitcoin ecosystem Satoshi simplified essentially the process of payment verification. As he writes in the original paper, *" It is possible to verify payments without running a full network node. A user only needs to keep copy of the block headers of the longest proof-of –work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch*

[75] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," IEEE P2P Proc., (2013)

[76] Merkle, R., (1980), Protocols for Public Key Cryptosystems. Proceedings of the 1980 IEEE Symposium on Security and Privacy.

*linking the transaction to the block it's timestamped in.*[77]" Thus, it becomes evident that only by linking the transaction to point of the chain a user does see that the network has accepted it. And the verification is reliable as long as honest nodes control the network.

According to Satoshi, in order to implement a distributed timestamp server on a peer-to-peer network, a proof-of-work system is always needed. More precisely, the proof-of-work involves scanning for a value that when hashed, such as with the aforementioned algorithm SHA-256, with a number of zero bits required can be verified by executing a single hash.

When implementing the proof-of-work in the timestamp network, a nonce is incremented in the block until a value is found that gives the block's hash the required zeros bits. Once the effort of the computer's CPU power has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing this work.[78]

Since multiple users in the network are attempting to generate blocks and obtain the reward, there is a possibility that two blocks may be created around the same time and thus creating a fork in the chain. So, it should be noted here that users are not necessarily creating blocks which will verify the same transactions. Therefore, as remedy to the fork, users may have a tendency to trust the prong with the highest level of difficulty, which usually happens to be the longest chain.

The proof-of-work also solves the problem of determining representation in majority decision making. More specifically, if the majority were based on one IP address- one vote, it could be subverted by anyone able to allocate many IP's, given that proof-of-work is essentially one CPU- one vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. Thus, to modify a past block, a possible attacker would have to redo the proof-of-work of the

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

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

block and all blocks after it and then catch up with and surpass the work of the "honest" nodes[79].

We can, also, see how proof-of-work processes in practice in the simple figure below:

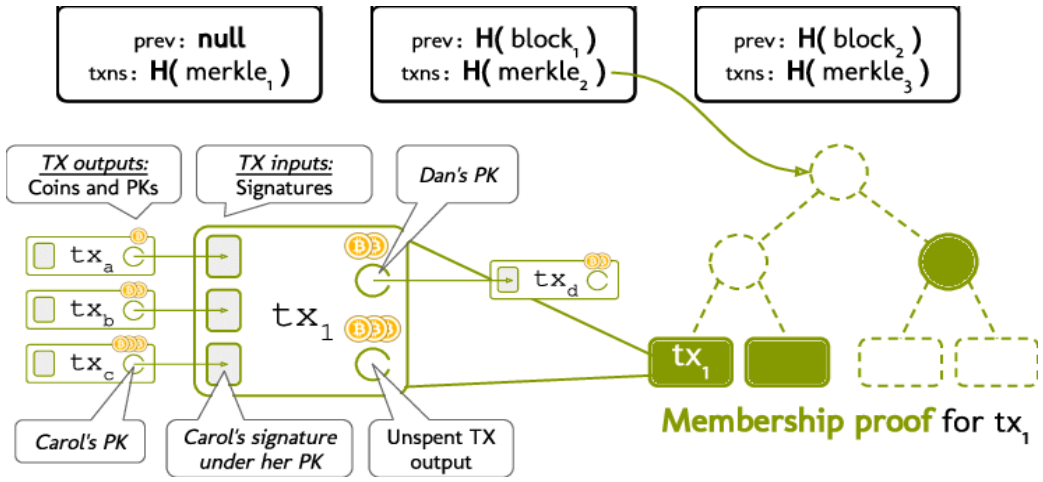



Figure: tx 1 transfers coins from Alice, Bob and Carol to Dan and somebody else .Miners receive a fee of 1 coin.

Source: https://www.researchgate.net/figure/316789505

In this figure is shown what we have already described about the hash function, the block chain and the proof-of-work. More specifically, the Bitcoin block chain is a hash chain of blocks. Each block has a Merkle tree of transactions. Efficient membership proofs of transactions can be constructed with respect to the Merkle root.

[79] FIPS , (2008),Secure Hash Standard, Federal Information Processing Standards Publication , National Institute of Standards and Technology.

We should take into account the fact that the difficulty of the proof-of work puzzle is adjusted periodically by an adaptive algorithm based on the recent block chain history in order to maintain the long-term property that one new block should be mined every ten minutes on average.

## ***BLOCK CHAIN AS THE BITCOIN TRANSACTION LEDGER***

As a specific technology for digital currencies, the blockchain is the technical solution to the double-spending problem. Given that electronic files can easily be duplicated, a digital coin can simultaneously be spent and retained in one's computer files, allowing that coin to be effectively spent twice[80]!

The process of transactions behind bitcoin is powered by an exciting technology known as the Block Chain. The Blockchain, as we have previously described, represents all verified and valid transactions between users of the Bitcoin network. Especially, the block chain is the first concept key about bitcoin. It is bitcoin's public ledger. From a

[80] Katz, J., and Lindell, Y., (2008), Introduction to modern cryptography, CRC Press.

functional standpoint, the block chain provides a decentralized, time stamped, ordered record of all transactions that can be verified at any time.

Blockchain thank to its underlying technology solves this problem using a decentralized database with network-enforced processes which are based on a proof-of-work consensus mechanism[81]. And this is what makes Bitcoin a revolutionary technology. Because for the first time the double spending problem has been solved without the need for a middleman[82].

The block chain provides, for the first time, the infrastructure for a user to directly transfer a piece of property like money, to another user in a secure and safe way where everyone in the network knows about this transfer. It is well known that Bitcoin operates on a list of blocks, the block chain where each block contains a header and transaction data.

The Block Chain initiative constitutes a public database, openly maintained by computers all over the world. Further, each block must meet certain requirements as it passes along the network, in order to make it very difficult to generate a valid block which would fraudulently obtain bitcoins. According to these properties, the 80-byte header should contain the 256-bit hash of the previous block Hi-1, the timestamp Ti, the 32-bit nonce Ni which is used to generate blocks, the hash TXi of the transaction data , and the difficulty parameter di. Currently it must be smaller than 2192, i.e. have its 64 most significant bits equal to zero.

All these conditions are strictly enforced, and a block not conforming to them is discarded immediately[83]. So, faking bitcoin's public record is very difficult as it requires more computer power than the rest of the bitcoin network combined, which is a nearly

[81] Brito J. , (2015), The law of bitcoin, iUniverse.

[82] Brito, J. , and Castillo, A. , (2013), Bitcoin : A primer for policymakers.

[83] https://blockchain.info/charts.

impossible feature that ensures the currency's security[84]. We can see in the following graph from the blocks vectorized how the block chain functions in practice:

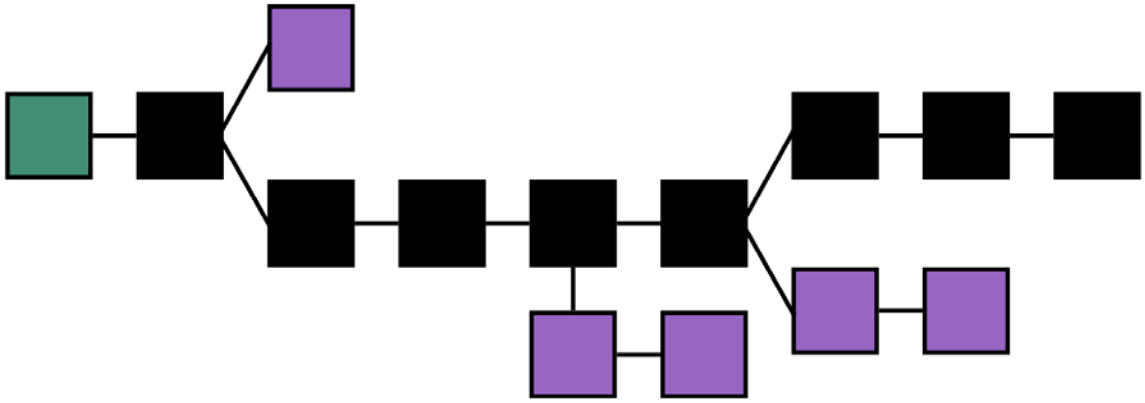


Figure: The main chain (black) consists of the longest series of blocks from the first block which is called "genesis block" (green) which is on the left to the current block. Orphan blocks (purple) exist outside of the main chain.

Source: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe

As we have already stated, in the blockchain in order to be valid, the double-hash of the block header must be smaller than a certain value, which is a linear function of the difficulty parameter:

$$Hi = SHA\text{-}256(SHA\text{-}256(Hi\text{-}1 \,||\, Ti||\, TXi||\, di||\, Ni||\,))) < f(di)$$

[84] J. Aron, (2012), Bitcoin online currency gets new job in web security, New Scientist.

Blockchain is a replicated ledger that keeps track of the account balances, verifies transactions against its current state and updates account balances accordingly. In contrast to other cashless payment systems, Bitcoin transactions are irreversible once they have been accepted by the network. As a consequence, bitcoin has comparatively low transaction fees and no charge-backs. According to the original paper, " *after each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.*[85]" So Block Chain with its innovative technological background seems to solve efficiently this problem.

The system uses asymmetric cryptography to allow the payee to verify that the payer, who must sign the current transaction, is the recipient of the bitcoins in the connected past transactions. Any recipient can check this chain of transactions back to the creation of the bitcoins. This verification process proves that the person paying owns the transferred digital money, something which is not possible in the case of PayPal.

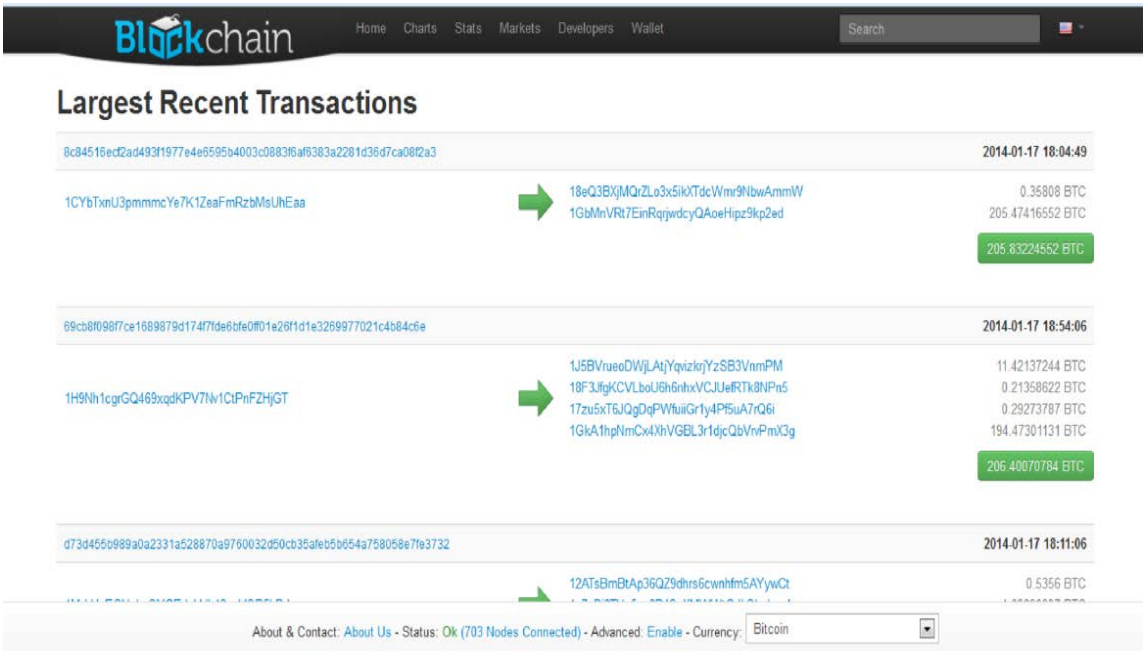
Blockchain constitutes a sequential record of all transactions and current ownership. And this tracking of transactions is supported by the decentralized computer power generated by the activity of "mining". The Blockchain allows essentially participants in the Bitcoin protocol to check whether transfers are coming from actual owners of bitcoins and beats the "double-spending" problem in its root. It doesn't let you spend the same bitcoin fraction more than once! Furthermore, it is important to mention that it contains backwards links, but not forward. Thus, there is a unique path backward from each block to the beginning of the log, the renowned "genesis block". But the forward path from a block might not be unique and that is why the log has the form of the tree whose branches fork as it grows[86].

[85] S. Nakamoto, (2008), A peer-to-peer electronic cash system.

[86] J. Kroll, I. Davey and Ed. Felten, (2013), The twelfth workshop on the economics of information security, Washington DC.

It has to be mentioned that every computer on the bitcoin network has a copy of the entire Block Chain, back to the very first transaction and this information is updated by passing new blocks to other users on the network. Even Satoshi mentions in his paper that, "*we need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions*." And in order to accomplish this goal without a third party he adds, " *transactions must be publicly announced , and we need a system for participants to agree on a single history of the order in which they were received. Furthermore, the payee needs proof that at the time of each transaction , the majority of nodes agreed it was the first received*." So, the solution this problem comes with the technology of the Block Chain assisted by a specific proof-of-work taken from hash cash.

Concerning the transparency of bitcoin, while all bitcoin addresses and transactions are public, the holders of those addresses remain hidden. Let's see an example which will prove the security provided by the block chain in a bitcoin transaction.



The picture above (figure, source: https://blockchain.info/ ) shows some of the recent large transactions recorded in the block chain. The first transaction is for 205 bitcoins (BTC). The long lines of letters and numbers we see in this figure are bitcoin addresses. We notice, though, that there is no name that goes along with the bitcoin address. This is what outside observers mean when they say "*bitcoin is anonymous*".

Bitcoin is in fact "pseudo anonymous". More precisely, the only thing that can be discerned by looking at the Block Chain is that address "1XXxxxXXXxxxxxxXX" sent 205 BTC to address "3XXxxxXXXxxXXxxXX" at a certain time. Who sent the coins, the reason for sending, and the users location remain secrets. However, we should take into account that as soon as you connect your bitcoin address to your real identity for example, by purchasing bitcoins online, the pseudo anonymity provided by bitcoin is lost[87].

The following picture shows the general structure of the blocks, the composition of which form the block chain :

| Field | Description | Size |
|---|---|---|
| Magic no | value always 0xD9B4BEF9 | 4 bytes |
| Block size | number of bytes following up to end of block | 4 bytes |
| Block header | consists of 6 items | 80 bytes |
| | | |
| Transaction | positive integer VI = VarInt | 1 - 9 bytes |

[87] International Journal of Scientific & Engineering Research, (2014).

| | | |
|---|---|---|
| counter | | |
| transactions | the (non empty) list of transactions | <Transaction counter>-many transactions |

Figure – Structure of blocks

Source: https://en.bitcoin.it/wiki/Block

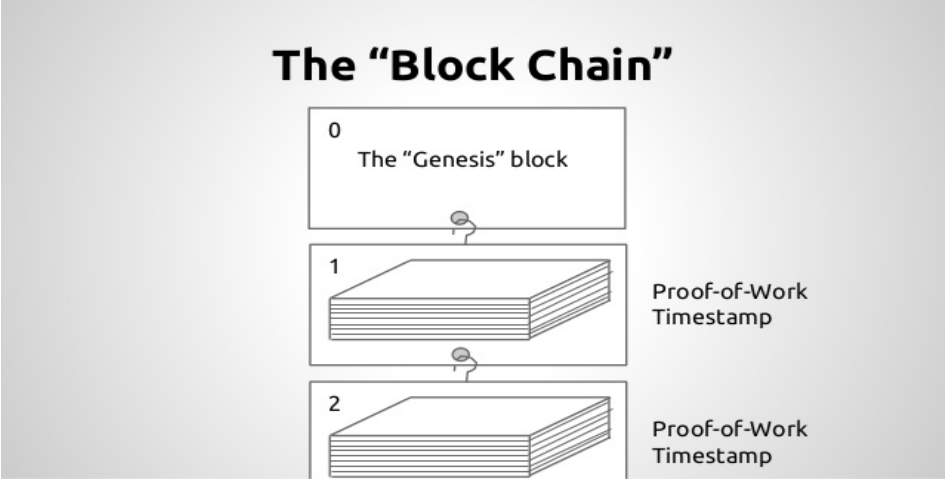
Each block contains, among other things, a record of some or all recent transactions and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle. And the most important is that the answer to which is unique to each block. Therefore, new blocks cannot be submitted to the network without the correct answer!

To sum up, Block chain serves as a digital document ledger for such complex data sharing and storage. Moreover, identity management which constitutes a block chain's feature allows users to create tamper- proof digital identities for themselves by being the "first comprehensive block chain-based identity service." In the Block chain technology, each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known. It is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated. These properties are exactly what make double-spending of bitcoins very difficult and, of course, the block chain the main innovation of bitcoin[88]. The Block Chain technology, though, poses an important scalability problem, related to the computing power required to re-calculate the history of all transactions[89]. In the end, as a new institutional technology because of how they affect transactions in financial markets will fundamentally re-order the governance of the production of banking services and financial assets.

[88] https://en.bitcoin.it/wiki/Block_chain

[89] G. O. Karame, E. Androulaki, and S. Capkun, (2012), Double-spending fast payments in Bitcoin, In proceedings of the 2012 ACM conference on Computer and Communications Security.

The way Block Chain is structured is shown in the following figure.



## ***INTRODUCTION TO BITCOIN MINING***

## ***Mining Process and Economics***

*"A fixed money supply, or a supply altered only in accord with objective and calculable criteria, is a necessary condition to a meaningful just price of money. "*

Fr. Bernard W. Dempsey, S.J. (1903-1960)

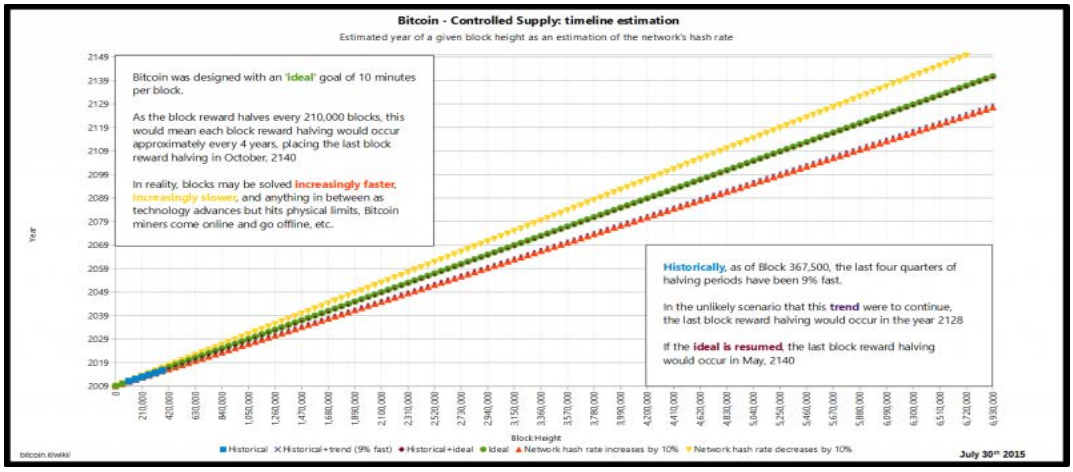



Figure - Graph of bitcoin's controlled supply as an estimate against time, depicting the influence of the network's hash rate (continuously faster versus continuously slower) on that timeline.

Another way to obtain cryptocurrencies such as the Bitcoin is by mining them. More specifically, the Bitcoin digital currency depends for its correctness and stability in a combination of cryptography, distributed algorithms and incentive-driven behavior by

its users. The mining mechanism, as an important aspect of Bitcoin's design, requires consensus between participants who expend resources on solving complicated computational puzzles, in order to collect the digital coins. This is where the "miners" come into play. It is a well-known fact that miners are often rewarded for their services in newly-created bitcoins and with small fees they collect for confirming transactions[90]. This activity is called "mining" by analogy with the extraction of precious metals.

Simply stated, mining is the process of adding transaction records into the cryptocurrency's public ledger of past transactions commonly known as the Blockchain. Mining cryptocurrencies is not an easy task because it was intentionally designed to be resource-intensive and difficult. It takes time and money! Expenses required in this activity are the hardware and software used to run the computers and there may be needed to rent an office space.

The Bitcoin protocol is designed in such a way that new bitcoins are created at a fixed rate that decreases over time, until the creation of new monetary units stops completely once 21 million bitcoins have been put into circulation. More specifically, the number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years. So, the number of bitcoins in existence is not expected to exceed 21 million. This decreasing-supply algorithm was chosen because it approximates the rate at which commodities like gold are mined and miners have to deal here with a computationally difficult problem. However, another reason behind the unintuitive value "21 million" are that it matches a four-year reward halving schedule, or the ultimate total number of satoshis that will be mined is close to the maximum capacity of a 64-bit floating point number. Besides, Nakamoto has never really justified or explained many of these constants[91].

[90] M. Arias and Y. Shin, (2013),There are two sides to every coin – Even to the Bitcoin, a virtual currency, The Regional Economist.

[91] https://en.bitcoin.it/wiki/Controlled_supply

$$\frac{\sum_{i=0}^{32} 210000 \lfloor \frac{50.10^8}{2^i} \rfloor}{10^8}$$

Mining is termed from the software used to create a block, which is called "Bitcoin miner" and is designed to mimic the extraction of minerals. More specifically, anyone is able to obtain bitcoins without purchasing them from other users. He can simply download and run bitcoin's mining program. In fact, the Bitcoin founders seeded the market by providing algorithms to early miners who accumulated the first stock of bitcoins. Thus, these miners benefited from subsequent price increases.

The Bitcoin mining is a program developed by Nakamoto as part of the bitcoin technology .Further, it acts as the clearing house of all bitcoin transactions. More precisely, mining is a process that involves the use of the proof of work after the implementation of the timestamp that is distributed on peer-to-peer server. The value of a coin is known after the use of the longest chain that is a presentation of the most valuable proof of work. It is through bitcoin mining that the value of a coin is formed after hashing.

Users use various types of hardware in order to mine blocks. More precisely, early bitcoin client versions allowed users to use their CPUs to mine. The advent of GPU mining made CPU mining financially unwise as the hash rate of the network grew to such a degree that the amount of bitcoins produced by CPU mining became lower than the cost of power to operate a CPU. The option was therefore removed from the core bitcoin client's user interface. Furthermore, FPGA mining hardware has appeared which is a very efficient and fast way to mine, comparable to GPU mining and drastically outperforming CPU mining. But, there are other mining hardware tools like ASIC mining and cloud mining[92].

During the bitcoin mining there must be honest nodes, and great computing power. The great computing power of the hardware must be supported by the nodes that

[92] https://en.bitcoin.it/wiki/Mining

run over time. That calls for the nodes to be produced on hourly basis. Otherwise, there may arise a problem.

Mining a block is difficult because the SHA-256 hash of a block's header must be lower than or equal to the target in order for the block to be accepted by the network. In other words, the hash of a block must start with a certain number of zeros. The probability of calculating a hash that starts with many zeros is very low, therefore many attempts must be made. In order to generate a new hash each round, a nonce is incremented.

The difficulty is the measure of how difficult it is to find a new block compared to the easiest it can ever be. It is recalculated every 2016 blocks to a value such that the previous 2016 blocks would have been generated in exactly two weeks had everyone been mining at this difficulty. This will yield, on average, one block every ten minutes.

Through mining bitcoin nodes are allowed to reach a secure, tamper-resistant consensus. Mining is also the mechanism used to introduce bitcoins into the system. In other words, miners are paid any transaction fees as well as a subsidy of newly created coins. This both serves the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system.

According to Satoshi's original paper, the steps to run the network are the followings:

"*1. New transactions are broadcast to all nodes; each node collects new transactions into a block*

*2. Each node works on finding a difficult proof-of-work for its block.*

*3. Each node works on finding a difficult proof-of-work for its block.*

*4. When a node finds a proof-of-work, it broadcasts the block to all nodes.*

*5. Nodes accept the block only if all transactions in it are valid and not already spent.*

*6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash."*

The goal remains that nodes, always, consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. Thus, the tie will be broken when the next proof-of-work is found and one branch becomes longer. And the nodes that were working on the other branch will then switch to the longer one[93].

This is why the mining mechanism protects bitcoin against certain technical problems such as inconsistencies in the system's distributed log data structure. It is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady. Individual blocks must contain a proof of work to be considered valid.

Certain transactions contain an incentive of a few Bitcoins that go to the user who generated the block verifying the transactions in question. As an added bonus for spending their computing power for mining, these incentives are added to the reward. Both the reward and the incentives are stored in the block implicating them, in what is called the “coinbase”. Once a block is generated, this creates a transaction from the coinbase to the successful miner.

When a block is discovered, the discoverer may award himself a certain number of bitcoins, which is agreed-upon by everyone in the network. Currently this bounty is 25 bitcoins and this value will halve every 210,000 blocks. Additionally, the miner is awarded the fees paid by users sending transactions. The fee is an incentive for the miner to include the transaction in their block. In the future, as the number of new bitcoin miners is increasing, the fees will make up a much more important percentage of mining income.

The mining mechanism has the property that if there are two branches of the tree, with a separate group of miners growing each branch, then the branch whose miners have more computational power will grow more quickly[94]. In fact, miners vote for a branch by

[93] S. Nakamoto, (2009), Bitcoin: A peer-to-peer electronic cash system.

[94] T. Bauman, (2013), Commerce and Reputation in Online Illegal Drug Markets, Princeton University.

devoting their mining effort to extending it, and the Bitcoin rules say that the longest branch should be treated as the only valid one.

It should be noted that this is the only type of transaction that does not have a traditional input[95]. In the end, to compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour[96].

In fact, as more miners join, the rate of block creation will go up. As the rate of block generation goes up, the difficulty rises to compensate nodes which will push the rate of block creation back down. Any blocks released by malicious miners that do not meet the required difficulty target will simply be rejected by everyone on the network.

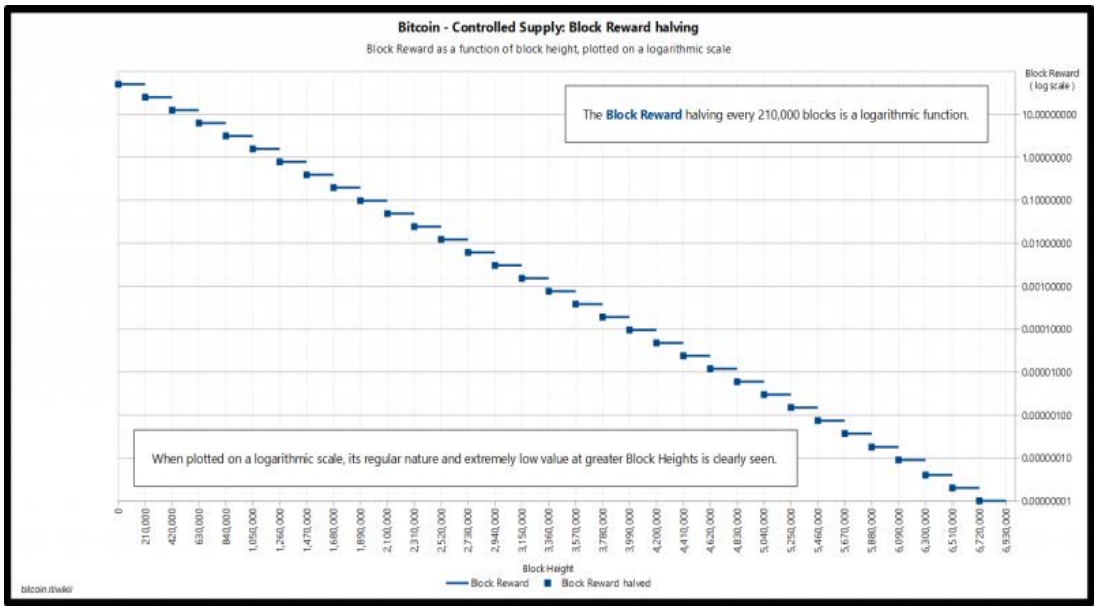



Figure - Graph of the Block Reward halving schedule plotted against a logarithmic scale.

[95] Shor, P., (1997), Polynomial-Time Algorithm for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing.

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

It is very difficult to predict how mining power will evolve into the future. Whether, for example, technological progress will continue to make hardware faster or whether mining will hit a technological wall, or whether or not faster methods of SHA-2 calculation will be discovered. So, putting an exact date or even year on this event is difficult.

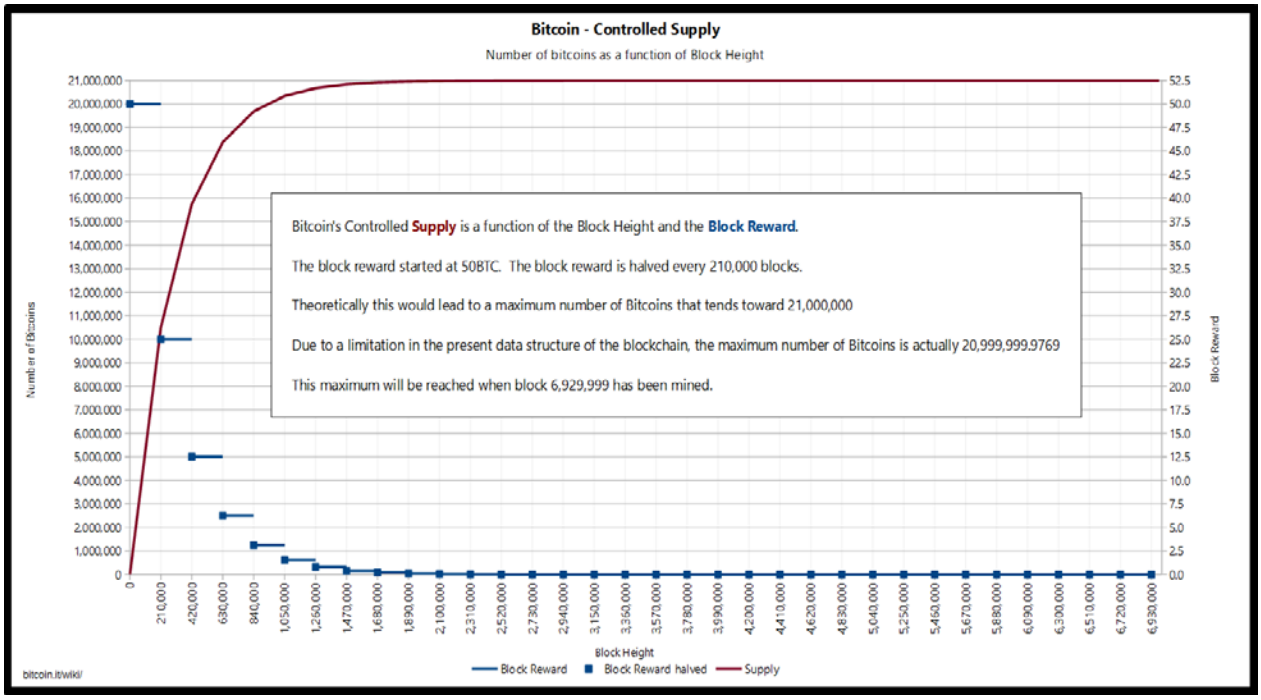



Figure - Graph of Bitcoin's controlled supply, showing the supply as a function of the block height and the block reward.

However, the theoretical total number of 21 million bitcoins, should not be confused with the total spendable supply. The total spendable supply is always lower than the theoretical total supply, and is subject to accidental loss,or destruction, and technical peculiarities.

The algorithm which decides whether a block is valid only checks to verify whether the total amount of the reward exceeds the reward plus available fees. Therefore

it is possible for a miner to deliberately choose to underpay himself by any value. Not only can this destroy the fees involved, but also the reward itself, which can prevent the total number of bitcoins that can come into existence from reaching its theoretical maximum.

Nowadays, thousands of personal computers compute the bitcoin encryption function and the system awards bitcoins to whichever miner happens to compute the proper Block Chain. We should notice here that any player may choose to become a miner and mine new blocks that add new transactions to the log.

Since there is no central company or authority managing the process, Bitcoin miners are essentially volunteering their machines to the bitcoin network in order to solve multiple mathematical problems[97]. The computer which correctly deciphers the problem is rewarded in bitcoins and the bitcoin system continues to operate.

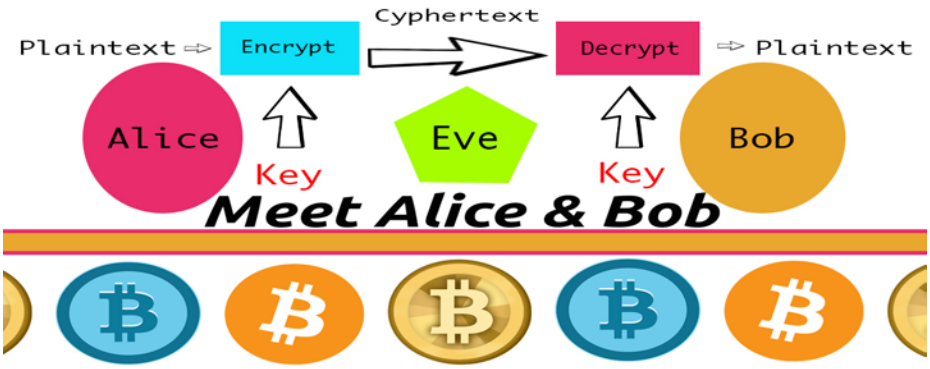


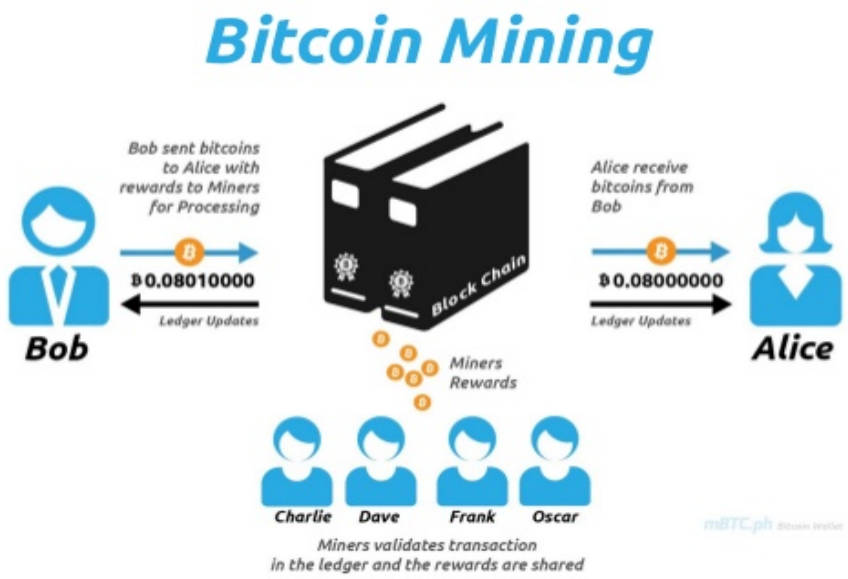

Figure: the actors involved. The consensus is that two people or more are highly involved in the process of the currency's encryption and transaction verification.

Source: https://news.bitcoin.com/meet-alice-bob-the-foundation-of-bitcoins-cryptography/

[97] Al. Harris and C. Conley, (2011), Will Bitcoin kill the dollar?,NVATE.

If we could simply describe the procedure of bitcoin mining we would just tell this. When a user, Bob, wishes to transfer Bitcoins to Alice, he creates and signs a transaction object which he broadcasts to his peers in the Bitcoin P2P network. The peers, then, rebroadcast it effectively by flooding the network with all known pending transactions. So, all of the miners, then, attempt to create a new block with the pending transactions they know about[98].

It is important to note that, in the Bitcoin network new transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. And of course, block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one[99].




[98] J. Becker, D. Breuker, T. Heide, J. Holler, H. Rauer and R. Bohme, (2012), Can we afford integrity by proof-of-work? Scenarios inspired by the bitcoin currency, In workshop on the economics of information security.

[99] S. Nakamoto, (2009), Bitcoin: A peer-to-peer electronic cash system.

Figure : The bitcoin mining process.

Source: https://www.slideshare.net/macoymejia/bitcoin-101-mbtcph

We should not forget that mining as activity does not guarantee a reward. The first miner to find a suitable solution will extend the block chain and will claim the mining reward. Then, all miners start over trying to solve a new puzzle to add yet another block to the blockchain. Moreover, the bitcoin system limits the total number of bitcoins in existence, allowing for bitcoin mining, the process for verifying every bitcoin transaction, where miners receive a reward for the creation of a block[100]. Currently, bitcoin's distribution software automatically slows production over time in order to ensure that there will never be more than twenty one million bitcoins in circulation, which should occur around 2025. Thus, by having this automatic mechanism there is no need for central bank or government intervention.

[100] Sheridan B., (2011), Bitcoins: Currency of the geeks: the untraceable new virtual currency is exploding in usage, notoriety and value, Bloomberg Businessweek.

# ***Modeling Miners and Pools-Incentives and Consensus***

Indeed, conventional wisdom has long asserted that the Bitcoin protocol is incentive-compatible. More precisely, some bitcoin miners combine their computing power and collectively mine bitcoins through pooled mining. Instead of one computer solving a math problem, the problem is broken down into smaller parts and is solved by multiple computers. Because the protocol is believed to reward miners strictly in proportion to the ratio of the overall mining power they control, a miner in a large pool is believed to earn the same revenue as it would in a small pool. Any subsequent reward is shared by all of the computers that participated[101].

The best strategy,though, of a rational minority pool is to be honest, and a minority of colluding miners cannot earn disproportionate benefits by deviating from the protocol. Consequently, there is no advantage for colluding miners to organize into continuously increasing pools. Therefore, pool formation by honest rational miners poses no threat to the system[102].

The system is comprised of a set of miners 1,…., n and each miner *i* has a mining power mi, such that $\sum_{i=1}^{n} mi = 1$. Therefore, each miner chooses a chain head to mine, and finds a subsequent block for that head after a time interval that is exponentially distributed with mean $m_i^{-1}$ . We assume that miners are rational, trying to maximize their revenue, and may deviate from the protocol to do so.

On the other hand, a group of miners can form a pool which behaves as single agent with a centralized coordinator, following a specific strategy. The mining power of a pool is the sum of mining power of its members and its revenue is divided among its

[101] https://en.bitcoin.it/wiki/Pooled_mining.

[102] Barber, S., Boyen, X., Shi, E., Uzun, E., (2012), Bitter to better - how to make bitcoin a better currency. In: Financial Cryptography and Data Security, Springer.

members according to their relative mining power. The expected relative revenue, or simply the revenue of a pool is the expected fraction of blocks that were mined by that pool out of the total number of blocks in the longest chain.

As we have previously mentioned, the Bitcoin protocol is incentive-compatible and secure against colluding minority groups. That means it always remains stable, under the assumption that players behave honestly, according to their incentives. In this process, each miner that successfully solves a cryptopuzzle is allowed to record a set of transactions and to collect a reward in Bitcoins. The more mining power a miner applies, the better are the its chances to solve the puzzle first. This reward structure is essential to the currency's decentralized nature.

It has to be mentioned that the bitcoin protocol requires the majority of the miners to be honest. By construction, if a set of colluding miners happens to command the majority of the mining power in the network, the currency stops being decentralized and becomes controlled by them. And this fact can lead to major drawbacks for the participants.

As Satoshi writes on its paper, "*the incentive may help encourage to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth*[103]*."* Even empirical evidence shows that bitcoin miners behave strategically and form pools because rewards are distributed at infrequent, random intervals. Within such pools, all members contribute to the solution of each cryptopuzzle, and share the rewards proportionally to their contributions. And these pools are formed according the Bitcoin protocol.

[103] S. Nakamoto, (2009), Bitcoin: A peer-to-peer electronic cash system.

So the protocol should ensure that the participants are honest so as even a minority of colluding miners could not earn disproportionate benefits by deviating from the protocol[104]. Since the success of the Bitcoin protocol relies on three major principles of consensus, a participant within the Bitcoin system must agree to these principles in order to play the game.

The first one is the consensus about rules. According to this, players must agree on certain criteria to determine which transactions are valid. Only valid transactions will be recorded in the Bitcoin log. Furthermore, that consensus about the rules could be considered as a social process, where participants must come to a common understanding of what is allowed, so that the rules can be encoded into the software each one uses.

The second principle concerns the consensus about state, which is more of a technological problem. Each player can see a part of the state and the players need to cooperate in large numbers and across a potentially unreliable network, to achieve a consistent understanding of the global state. Therefore, players should agree on which transactions are considered valid, which is the history of the bitcoin economy. So, there must exist a common understanding of who owns which coin at any given time. And this technological consensus must be achieved despite the possibility that some players will deviate from the determined rules.

Finally, there must be a consensus about the fact that bitcoins are valuable and about this value. Thus, users should agree that bitcoins have a certain value, so that they continue to accept them as payment. Such value is often modeled as a focal point in a coordination game because players need something to use as a medium of exchange.

These forms of consensus are all mutually dependent upon one another so that the failure of one will hurt the stability of the others. More precisely, in the bitcoin economy,

[104] Barber, S., Boyen, X., Shi, E. , Uzun, E. , (2012), Bitter to better – how to make bitcoin a better currency, Financial cryptography and data security, Springer.

the global equilibrium occurs when the total mining reward in dollars, for example, per second equals the total global cost of mining. A long as this assumption holds, users will continue to participate in the mining process and the Bitcoin system will remain stable. However, it is important to note that users retain the power to enforce or reject any of the rules outlined in Bitcoin's protocol. And that means that a rational user will only participate in a way that maximizes his utility. Therefore, bitcoin's functionality and stability will endure so long as users agree to follow the rules[105].

One critical aspect faced in the bitcoin protocol is that miners must extend the longest branch in the blockchain. But, are all users properly incentivized to do that, or are they more inclined to create forks in the transaction blockchain so as to maximize their own utility? If the second happens, the fork created changes the transaction history leaving the system more vulnerable to the double spending problem.

Looking from another perspective, if we applied the principal of trust assurance from the game theory literature, it would out that there are only two Nash equilibrium outcomes in the system. Either mutual cooperation or mutual defection[106]. And if all the other players cooperate in the mining game by extending the longest chain in the log, then the player who deviates from this established strategy risks having his block rejected from the long-term consensus branch. Consequently, this fact could lead in lowering his expected utility[107].

[105] Barber, S. , Boyen, X., Shi, E., and Uzun, E., (2012), Bitter to better: how to make bitcoin a better currency. In financial cryptography and data security, Springer.

[106] Kroll, J. ,A. , Davey, I., C., and Felten, E., W., (2013), The economics of bitcoin mining or bitcoin in presence of adversaries, In proceedings of WEIS.

[107] The twelfth workshop on the economics of information security,(2013), WEIS.

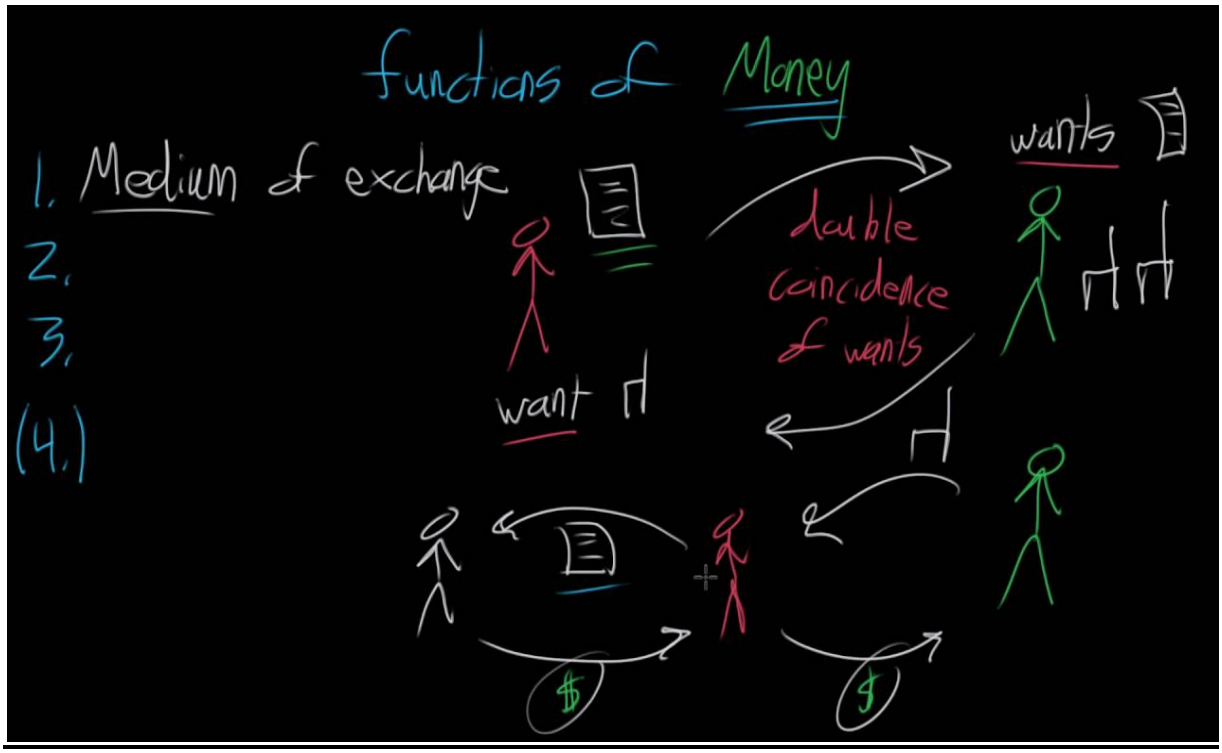
To sum up, any strategy in the bitcoin game can achieve Nash equilibrium as long as all players adopt it, regardless of the strategy itself.[108]. In practice, users follow the rule of extending the longest branch simply because it was stipulated in Nakamoto's paper and as they entry the game they are incentivized to follow the strategy chosen by the majority of existing miners. Overall, the bitcoin protocol is not self- executing. But it relies on the willingness of users to adhere to the already stated consensus principles combined with the economic incentives embedded[109].

[108] Schelling, T., C., (1960),The strategy of conflict, Harvard University Press.

[109] Skyrms, B.,(2003), The stag hunt and the evolution of social structure, Cambridge University Press.

## REQUIREMENTS AND PROPERTIES OF MONEY

## Bitcoin as a currency standard-The intrinsic value of Bitcoin




A significant part of the criticism of bitcoin as a medium of exchange that comes from the Austrian school arises because bitcoin does not seem to follow the regression theorem Mises. In other words, from an Austrian perspective, bitcoin is not considered as money. Bitcoin has been criticized because its fundamental concept does not adhere to the regression theorem from a general viewpoint.

The theorem, laid out by Ludwig von Mises (1912), attempts to explain how media of exchange acquire their prices. From this theorem, it is apparent that Bitcoin

should be possible to trace back the price of a medium of exchange to some origin. And media of exchange arise from a commodity that has inherent uses and is liquid. In short, it states that "*before an economic good begins to function as money it must already possess exchange-value based on some other cause than its monetary function*".

To answer this Ludwig stated that today's demand for money depends on its yesterday's purchasing power. In other words, the prior day's purchasing power of money then determines today's demand for money, which subsequently sets its price. By applying this procedure backwards through time, the Regression Theorem states:

"*We will eventually arrive at a point in time when money was just an ordinary commodity, where demand and supply set its price. The commodity had an exchange value in terms of other commodities…To put it simply, one the day a commodity becomes money it already has an established purchasing power or price in terms of other goods. This purchasing power enables us to set up the demand for this commodity as money. Once the price of money is fixed, it serves as input for the establishment of tomorrow's price of money.*[110]"

The regression theorem states that money has value today because it is expected to have similar value tomorrow. At first glance, this seems like an application of circular logic at best. According this theorem, money derives its value from formerly being a commodity used in barter , before it evolved into a medium of exchange[111]. According to him, money is considered useful because it can be exchanged with other goods and services. In this way, money's sole value is derived from its purchasing power. But, how has its intrinsic value initially been established?

[110] Shostak, F. ,(2004). How does money acquire its value? Ludwig Von Mises Institute.

[111] Shostak, F. (2004). How does money acquire its value? Ludwig Von Mises Institute.

In order, though , to reconcile the different views about the intrinsic value of money , we can conclude that money may have, first, established its value as a physical commodity used in trade of goods and services until it became the official medium of every kind of exchange. Money, then, retained this power through social consensus and government backing, which guaranteed that its function as a store of value and as a unit of account.

The regression theorem, also, states that the expected purchasing power of money gives it value and people are willing to sacrifice goods today in exchange for money that they can use tomorrow. Further, Mises managed to include the element of time in his theory of money. People today (*t*) expect money to keep their value tomorrow (*t+1*) because it had value yesterday (*t-1*) . In this sense, we get a weak notion of money as memory.

This type of regression leads itself to criticism involving the infinite nature of the regression. By using the regression theorem, it is possible to trace the value of money backwards until we get to a point where money first emerged from a pure barter economy. From there it is easy to analyze where the exchange value of money originates, as it is the same process as with any other goods.

Nowadays, the economic definition of money is unambiguous: money works as a widely accepted means of payment. Besides, its main functions are distinguished as a unit of account, a store of value and a medium of exchange. As we all observe in our everyday life, money is used to express the value of all goods and services. In other words, it performs its function as a unit of account in all the economies. Through fulfilling this function, households and businesses are able to make their trade decisions much faster. And this is a benefit that eases making calculations and comparing prices.

When money functions as a store of value, it means that a person is able to save, store and retrieve money over time being sure it retains its value. The value of money , though, is not always constant because of the inflation.

As a medium of exchange, it fulfills its function as a means of payment for goods and services. More precisely, it is the most important and essential function of money since "the double coincidence of wants" no longer needs to be fulfilled. And money itself does not necessarily have to have an intrinsic value as long as the society relies on it being accepted as a trustworthy means of payment.

From this perspective, Bitcoin could be considered as an imperfect form of memory, one which fits somewhere in between commodity money and fiat money, a synthetic commodity money. More precisely, it seems that Bitcoin's price includes a spread over the price in the initial currency, making it impossible to be considered as a unit of account. A this point, though, we should answer, the challenging question: "how does fiat money obtain and retain value?".

According to Hal Varian, a professor of economics, money pumps its value from two sources. As he admits, "*Dollar bills are fiat money. They are valuable because the government in power says so.. . A more profound but unsettling reason that a dollar has value is simply that lots of people are willing to accept it as payment.*[112]".

In fact, Varian admits something we all know but do not say. Specifically, he adds in determining money's intrinsic value the notion of social consensus. While Varian contends that social convention and network effects drive determine money's value, other economists argue that government decree is the key contributor. Given that governments are willing to accept fiat money as payment for tax liabilities this guarantees that there will be a last resort buyer of money if private transactions fail to provide the necessary demand for money[113].

[112] Varian, H. R. (2004), Why is that dollar bill in your pocket worth anything?, The New York Times.

[113] Glasner, D. ,(2011). The paradox of fiat money – Uneasy money.

Money has, also, been described as "general use" by Terrell in 2001, as "industrial commodity" by Korda in 2013[114] and as a "price stability" by North in 2013.[115] By doing so, the economists relied on aggregate variables such as MV=PQ, which created some problems such as trying to account for unstable money velocity and sticky prices. Factors that ultimately make the direct relationship defined in the equation less than perfect. These theories also do not account for the demand of money sufficiently.

The marginal utility theory itself also tried to explain how money begun to have a certain exchange value by referring the fact that people have a marginal utility for money because it has a certain exchange value. While it is true that people have greater marginal utility for money than other goods, which is the essence of how money came in the first place, it does not adequately explain the origin of value. But, this is because money does not derive its value directly from the medium itself but rather its purchasing power.[116]

According to Mises, bitcoin should have amassed demand, long before it acquired value because of its liquidity and convenience. In 2012, the European Central Bank stated that Bitcoin should be considered as a high-risk system for its users from a financial perspective. Taking into account this consideration a question was raised, "what were users' intentions when buying or selling bitcoins? An alternative payment system or a speculative asset?"

Bitcoins are accepted by a growing number of stores and businesses and their use nonetheless remains marginal compared to currencies like the euro and the US dollar. Even recent developments suggest that this use is increasing permanently. One reason is

[114] Korda, P., (2013): Bitcoin Bubble 2.0. Seeking Alpha. http://seekingalpha.com/instablog/7761841-patrik-korda/1616371-bitcoin-bubble-2-0.

[115] Smiling Dave (2013): About a Medium of Exchange Having to Be in Wide Use. Smiling Dave's Blog of Psychology, Economics, and Gentle Sarcasm. http://smilingdavesblog.wordpress.com/2013/10/15/about-a-medium-of-exchange-having-to-be-in-wide-use/

[116] Mises, L. v. (1953). *The Theory of Money and Credit* (1912 ), New Haven: Yale University Press.

that bitcoin investments seem to offer diversification benefits after observing their correlations with other asset classes[117].

In 2009, the so called Genesis Block, which was the first chunk of data in a ledger of bitcoin, was created by Nakamoto. From that moment on, bitcoins have existed as "things". However, a bitcoin was not a good at that time yet.[118] At that time, people didn't know how to use it to satisfy their needs. One of the early adopters, Mike Hearn, explains in an interview in 2013: *"I found [bitcoin] very early on, when no one was using it, so no one, no exchanges, had no exchange rate at all, so they were just completely floating in an abstract space. You know, what was one coin? Well, nothing really.*[119]*"*

As people started to trade bitcoins against the US dollar, bitcoin was considered ay that at that time as a good with a price. As we know the existence of a market exchange is both a sufficient and a necessary requirement for the existence of a price.

A further relevant step in its evolution as a trading asset is the emergence of specialized markets, referred to as "exchanges" to trade bitcoins in 2010. Specifically, the emergence of exchanges created an easily accessible service with the ability to instantaneously trade bitcoin, as well the availability of information about real time pricing and the buy/sell order books. But, since that time, bitcoin was not merely a good with a price, but a liquid good.

What was most observed on the data following the transactions with bitcoins is that users considered them as trading tools on exchanges. Although, the Bitcoin payment system is still predominant in terms of transaction volumes, users' focus is limited to

[117] Briere M., Oosterlinck, K., and Szafarz, A., (2013), Virtual currency, tangible return: portfolio diversification with bitcoins.

[118] Menger, Carl (1871): Principles of Economics. Ludwig von Mises Institute, (2004)

[119] Hearn, Mike (2013): Conference 2013 - Mike Hearn Interview , https://soundcloud.com/mindtomatter/conference-2013-mike-hearn.

trading on exchanges. Its recent dissemination showed that users tend to perceive it as an alternative investment vehicle[120].

Despite the original purpose for bitcoins, many people viewed them as a means to make money rather than to use them as money. This is because their value has rapidly fluctuated in price. But, does bitcoin have the potential to become a form of money that is widely used for day-to-day purchases, on the same level as the other official currencies?

In fact, a currency consists of an asset used regularly to buy goods and services. The value of the currency therefore depends on the utility that people bestow upon it. And this utility depends in turn on users' confidence in the currency and on its adoption by a large number of consumers, investors and merchants. Thus, Bitcoin could even be considered as a hybrid currency satisfying most of the fiat currency properties.

At that time bitcoin was worth little and it wasn't in general use. Yet, it was a liquid good and recognizing this liquidity made the use of as a medium of exchange possible for many goods and services. Since then, the liquidity improved and there are now over a dozen exchanges operating, and sites like "https://localbitcoins.com/" that allow to locate a wiling trader in about 192 countries.[121]

Concluding, it remains unclear whether decentralized cryptographic currencies, such as Bitcoin, can be designed with monetary policies and be considered as fiat currencies. Bitcoin's design embodies a basic version of monetary policy satisfying many properties of the notion of money. But, it is not totally compatible with the state of the real economy. On the other hand, Bitcoin's block chain presents some kind of measure of monetary indicators such as the number of transactions and their nominal amount, but offers no information about what value was actually provided in exchange for payment. Therefore, the block chain lays the groundwork for the development of automatic

[120] Glazer, F., K. Zimmermann, M., Haferkorn, M., C., Weber, and M., Siering, (2014), Bitcoin- Asset or currency? Revealing users' hidden intentions, Proceeding of the 22nd European conference on information systems.

[121] Krugman P., (2011), Golden cybervetters, New York Times.

monetary policy based in nominal data, but does not facilitate any policy based on real economic activity. On the other side, individuals could add information about economic conditions or could introduce discretion by judgment or governance issues about Bitcoin. Thus, further experience in transacting with Bitcoins could illuminate the undiscovered yet aspects of Bitcoin at a monetary policy level.

***Volatility in the Bitcoin ecosystem – Bitcoin as a rival to fiat money or a speculative financial bubble?***

An inelastic supply in the face of volatile demand makes the value of bitcoin unstable relative to established fiat currencies. While a drawback, this does not prohibit bitcoin from spreading as a medium of exchange. Entrepreneurial innovations such as market exchange pricing and exchange facilities enable bitcoin to function as a medium of exchange while allocating the speculative risk of holding it to those who are most willing to tolerate it.

Besides, it is still too early to know how greatly these innovations will widen bitcoin's use. But it is proven that they offer Bitcoin a better chance of becoming a commonly accepted medium of exchange. While bitcoin remains volatile today, it's certainly not the only volatile asset in the world. What about oil? Or gold? Or coal? Even mature assets can experience price fluctuations. Consider also the fact that trading

volume is up in many of the same countries that are likely to benefit the most from bitcoin.

The Bitcoin concept aims at being used as a means of payment. The other functions which are thought to possess derive from the former. Currently, Bitcoin fulfills none of the money functions in the proper sense. More precisely, as long as most of the costs even for producers in the Bitcoin economy occur in different currencies and the digital currency incomes face a volatile value in terms of currencies needed to pay for input, it could not be economical to adopt Bitcoin as a unit of account either.

The domination of speculative over other motives and the complete determination of its value by market governance lead to instability of Bitcoin's price and value.Furthermore, given Bitcoin's current volatility, any seller of goods and services in Bitcoins would incur huge risks. Fortunaltly, in reality, prices of Bitcoin-accepting sellers are fixed in a different currency and the Bitcoin price generally varies with its exchange rate.

The future of bitcoin is unpredictable. However, without any doubt the increased number of bitcoin circulation is a good sign for its further development. More precisely, the number of bitcoins has been increasing for more than two million in one year only. If bitcoin completes growing up, we can assume that its price would be stable and would become a small part of the world economy. However, it has some powerful opponents, such as banks, payments processors and central authorities that might play a great role in controlling or ending the bitcoin era.

By examining Bitcoin economic properties we can tell that it answers the problems of inflation, exchange, fraud prevention, and accessibility. And we should take into account the fact that inflation is an economic phenomenon that is fundamental to fiat currencies. Furthermore, while bitcoin does not offer a complete solution to this issue, it can hedge against currency fluctuations. For example, individuals living in a country with unpredictable and volatile exchange rates can instead invest their money in bitcoin

for hedginfg purposes. Depositing bitcoins, they then can either convert them into other, more stable currencies or simply use them as their transactional currency.

However, will bitcoin become a major medium of exchange? Here the object of consideration is the possibility that, while quantitatively unimportant at present, bitcoin will in the foreseeable future become a major and perhaps main medium of exchange, provided it is not thwarted by legal actions internationally.

A natural way to argue that Bitcoin spreading will grow is to identify some of its major advantages. An optimistic viewpoint has been expressed by Andreessen (2014). Especially, Andreessen emphasized the reduction of transaction costs that bitcoin could bring about[122]. A major example is the case of international remittance: "*Every day, hundreds of millions of low-income people go to work in hard jobs in foreign countries to make money to send back to their families in their home countries, over $400 billion*

On the other side, Grinberg observes that the U.S. Constitution cannot perform strict regulation on Bitcoin because it "*has nothing to say about private parties creating money*," and that the relevant existing federal statutes are the Stamp Payments Act of 1862 and an assortment of federal statutes concerning counterfeiting.[123]. Regarding the first of these, he concludes that it is unlikely that this act would form the basis for a federal attack on bitcoin: "*It is a 150-year-old statute that has outlived its usefulness*." Specifically, "*there has been no published court opinion interpreting the Act since 1899*."

What, then, about the statutes regarding counterfeiting? Grinberg's discussion is highly informative, but does not leave one with much confidence regarding the major issue at hand, namely, whether the U.S. government would permit control of monetary management to pass from the Federal Reserve to a system not under its dominance. So, it

[122] Luther, W. J., and White, L. H. (2014) "Can Bitcoin Become a Major Currency? George Mason University, Department of Economics Working Paper.

[123] Grinberg, R., (2011) "Bitcoin: An Innovative Alternative Digital Currency." Hastings Science and Technology Law Journal.

might be possible for bitcoin to survive and succeed in providing the useful services identified by Andreessen[124].

So, bitcoin must survive in some new context, where it could be considered as the global currency of choice and where there are no fiat currencies operating alongside it. Of course, we know that bitcoin exists in anything but a vacuum, and it must operate in a real economy, dominated by multiple fiat currencies, all of which are controlled by central banks through monetary policy.

However, as far as companies which are financed through institutions touched by inflation-affected interest rates continue to support the development of the bitcoin phenomenon, the bitcoin economy can become the victim of this business cycle. This means that cryptocurrency exchanges, bitcoin-exclusive companies, bitcoin remittance services, bitcoin news websites, and any other bitcoin-driven company may in fact be part of a boom phase that is sure to go bust. Thus, bitcoin is in very close proximity to an unstable economical point with recession and downturns possibility. So it is far from immune.

While nothing theoretically prevents the bitcoin economy from entering a cycle of boom and bubble, it seems unlikely at this point in time that this industry has attracted enough mainstream investors to bring in a significant amount of misallocated capital. So, right now, there probably isn't any reason to worry about. However, as bitcoin's popularity grows, so too will investors' interest in bitcoin-powered companies, which could bring in the boom-and-bust-producing inflation with its negative effects.

Unfortunately, while it is difficult at this stage for a significant boom-and-bust-inflation to happen in the bitcoin business cycle, the truth is that it is hard to know for sure for the future. More specifically, one of the unfortunate parts about the malinvestment theory of the business cycle is that its logical conclusion entails an

[124] Andreessen, M. (2014) "Why Bitcoin Matters." dealbook.nytimes.com/2014/01/21/why bitcoin Matters.

inherent uncertainty in the credit structure. Thus, theoretically, the entire industry could fall down with very little warning.

On the other hand, Bitcoin has an exchange rate volatility, an order of magnitude higher than the volatilities of widely used official fiat currencies. And this is a fact that undermines the bitcoin's usefulness as a unit of account or a store of value. Bitcoin's daily exchange rates exhibit virtually zero correlation with bona fide currencies, making it useless for risk management purposes. Moreover, the high volatility which surrounds the bitcoin ecosystem makes it exceedingly difficult for its owners to hedge. Part of the reason is that Bitcoin lacks access to the central banking system which includes deposit insurance and as a currency, it is not used to denominate consumer credit or loan contracts. Thus, Bitcoin appears to behave more like a speculative investment than like a currency. Foremost, the high exchange rate volatility provides indications that Bitcoin is not utilized as an alternative transaction system, but it is rather considered as a speculative financial asset.

On the bright side, the bitcoin economy is inundated with entrepreneurs and angel investors who adhere to this circulation credit theory of the cycle or are at least sympathetic to it. Generally, entrepreneurs have the ability to preemptively avoid debt-based financing if possible, hopefully shielding the growing industry from the business cycle.

In the end, though, we should not forget that the bitcoin economy, despite its advantages, is far from recession proof, and it can collapse just like any other market. So, economists have a unique opportunity, though, to employ the shared knowledge with older ideologies, theories and practices in order to keep bitcoin true to its original intentions for as long as possible. If they succeed in this, the digital currency will be kept alive long enough to truly flourish and grow, and will not eventually fall victim to the trade cycle[125].

[125] https://news.bitcoin.com/beware-bitcoin-economy-bust/

## ***Monetary Governance in the Bitcoin ecosystem…***

Bitcoin's hypothesized monetary system, as we have already stated, has affinities with the Austrian school of economics. This approach favors a market governance style of economic institutions. With Menger belonging to this historical tradition, the approach holds a commodity theory of money too.

It is true that many Austrian economists favor a return to a gold-based monetary system, outlawing credit-based money creation by private banks. Hayek in his later work favored a competitive solution. Based on the assumption that legal restrictions are the basis of prevailing unit-of-account monopolies, he demanded the abolishment of these restrictions. He thought that once free competition among private and state banknote issuers was allowed, there would be various competitions based on varying backing methods to emerge and those with the most proper monetary management to prevail.

With time passing after the outbreak of the recent crisis and the whole financial and money system was permanently challenged. This observation, though, showed that our prevailing economic environment had to do with a matter of legitimacy crisis. Even though, output standards like Banks' economic goals were accomplished, other targets, more essential were missed. For example, central banks of many European Banks continued keeping interest rates too low or issuing too much credit, undermining the market mechanism[126].

On the other side, Bitcoin has been developed in order to constitute an innovative counterproposal. More specifically, it presented a real alternative monetary and payment

[126] Taylor J., (2009), Getting off track: How government actions and interventions caused prolonged and worsened the financial crisis, Stanford, Hoover Institutions Press.

system and has been the only succesful existing attempt to build a complete digital currency and payment system.

Bitcoin's purpose, thought, seems to be a virtual currency based only on a computer code and for this reason it provides a platform that allows its users to produce what its proponents call money and to transmit payments directly and anonymously among each other. Furthermore, in the framing of Bitcoin governance , designers intended to create an uncontrolled hierarchy lacking input legitimacy which has the power, though, to manipulate its price. In contrast to the current monetary system of fiat currencies, this hierarchy forces the participants of the Bitcoin network to accept an intrinsically worthless money with high volatility.

According to this kind of thinking, Bitcoin was a paradigmatic shift towards a different money which aspired to be based only on the trust of a growing community of members, attracted by its strict anti-inflationary rules. Moreover, it aspired to surpass any arbitrary state controls issued by the general monetary policy.

Bitcoin's ecosystem, essentially, aims at confronting the monetary policy anomalies of our fiat currencies . More specifically, in its attempt to mimic gold, it aspires to create a non-fiat monetary system. Like gold, it has no intrinsic value. The value attributed to gold as a money substitute is based in part on the expectation that other people will value it as a store of wealth and in part on the fact that it is used as a commodity apart from acting as money. And Bitcoin attempts to play in some way the role of gold.

Although, it may mirror the description of some influential mainstream digital currency with several advantages, this perspective is only distortional[127]. According to many economists Bitcoin does not share this feature as it is not considered as a commodity. In the Bitcoin network, there is no linkage to credit and that constitutes a

[127] Leijonhufvud, A.,(2008), Keynes and the crisis, CEPR Policy Insight.

virtue. Its only link to internal value is the computational work of nodes in payment and transfer processing on the Bitcoin system.

To sum up, contrary to official fiat currencies, Bitcoin has neither a link to economic production or other macro- economic indexes, nor value as a means to discharge tax obligations. Its value is based entirely on the subjective evaluation of its users community. The lack of a link to anything representing economic value and especially the lack of a governance mechanism which could keep it stable is a fragile and vulnerable aspect of its input legitimacy. Even, a fact that could also endanger its output legitimacy if trust disappeared[128].

[128] Kaminska I., (2013), Financial Times Alphaville blog bitcoin mania series.

## ***Bitcoin as an Asset***

There is an ongoing discussion whether Bitcoin is primarily an alternative currency or just a speculative asset[129]. According to economists, a currency can be used as a means of trade, or a vehicle to store value or a unit of account in order to compare the value of different goods and services. If we take into account these three features, Bitcoin represents a certain value for every user, either as of today or in the future.

Bitcoin participants who pursue it for its feature as an alternative asset lack a valid evaluation method and are therefore forced to build their own expectations about its future prices based on any information they can acquire from any available source. And these sources can be social media, newspaper articles or internet communities. Given that there is no fundamental pricing methodology available yet, these sources of information are likely to have a higher influence on prices. Thus, negative news announced for Bitcoin ecosystem would push some others to re- evaluate the utility and the usability of Bitcoins or sell them, hence lowering their prices on the exchanges.

It is worth noting, that the negative event of the exchange Mt. Gox's default primarily affected the possibility to withdraw fiat money or Bitcoin from the internal system of the exchange. This event, though, affected the means users were managing their investment and only indirectly related to Bitcoin itself due to the simultaneous announcement of the exploitation via a protocol weakness. This weakness, however, was for long known and according to the Efficient Market Hypothesis was already reflected within Bitcoin prices. .

Contrary to the decisive influence of negative news, positive news seem to exert a positive influence to the Bitcoin prices. On the one hand, they attract new users and on the other hand, positive news assert already invested users to stay invested. So, the

[129] ECB, (2012).

dissemination of news seems to play a major role on Bitcoin prices if users are using Bitcoin as a highly speculative investment.

There is some debate, though, about whether bitcoins qualify as currency, securities, commodities, or a new asset class altogether[130]. Specifically, we should remember that bitcoins fall under the CEA's definition of commodity. The only issue is which category of commodity they fall under.

Bitcoins may be categorized as an excluded commodity if they are viewed as being a type of currency or other financial interest. In addition to being a type of virtual currency, they are also considered as a financial instrument due to their underlying block chain system, which enables financial transactions beyond simple bitcoin transfers[131].

On the other hand, bitcoins may be categorized as a commodity which is exempted if they are viewed like precious metals. Further, like precious metals, bitcoins are limited in supply and capable of being physically delivered, at least in a digital sense. They may also be categorized as exempted commodities, because commodities fail to meet the definition of agricultural commodity.[132] Moreover, the CFTC also recognizes that intangible commodities qualify as exempted commodities "*if ownership of the commodity can be conveyed in some manner and the commodity can be consumed*[133]." Since, then, bitcoins can be owned and can be "consumed" in the sense of being spent, or traded, they may qualify as an exempted intangible commodity.

A further examination of the "commodity" notion may open an argument that bitcoins act like a "commodity," because one can use it, sell it, or make with them. More precisely, most people do purchase bitcoins with money, rather than mine them. Second, the common enterprise could be the network of people who use their computer power to

[130] R. Grinberg, Bitcoin: An Innovative Alternative Digital Currency, 4 Hasting Sci.& Tech. L.J. (2011).

[131] Old Kharif, Bitcoin 2.0 Shows Technology Evolving Beyond Use as Money, Bloomberg, (2014).

[132] CEA, CFTC Glossary, Exempt Commodity.

[133] Fed., (2012), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-18003a.pdf

mine, update the ledger, and thus ensure the value of bitcoins. This argument is furthered by pointing out that as the value of bitcoins increase, each person who holds them is better off.

There is also a strong counter argument in the sense that Bitcoin could be considered as an investment tool. More specifically, the exchanges, the current investment projects or even individuals holding bitcoins in their e-wallets act independently of one another, rather than in a single profit-seeking investment scheme. Furthermore, a strong argument exists that people do expect profits by investing in the Bitcoin system due to the fact that many bitcoin holders believe it is inflation-resistant.

Given the innovative character and the volatile historical price, they are likely to be aware that they invest in a financial instrument with a high price uncertainty. Thus, it would be wise for these users to only invest a small fraction of their total portfolio.

Although, Bitcoin does not provide the feature of an interest rate as traditional currencies do where interest rates are provided by central banks and interest rate term structures are derived from bonds with different maturities. Besides, users who participate in the Bitcoin ecosystem are left to determine the value of Bitcoin themselves, doing so by evaluating information from any area such as news or websites.

Their valuation is reflected in prices of Bitcoin quoted on exchanges. The price and its implicit value are thus determined on exchanges by users who want to buy or sell Bitcoins. And this process is realized under the laws of demand and supply. Furthermore, users considering Bitcoin as an investment asset buy the digital coins at an exchange and store them in a wallet waiting for prices to rise. Though, the three distinguishing features of Bitcoin such as the ease of bilateral transactions, the anonymity and the security it provides are not of interest for them. Besides, as they do not intend to use the network, these users are therefore not affected by negative news regarding security issues or infrastructure failures.

Even, considering that the total supply of these digital coins is deterministic by design, it follows that an increasing growth of the demand side is leading to increased prices. And consequently, sellers can quote higher prices as there are people who are willing to pay higher prices in order to acquire a single coin.

.

Certainly, it is irrelevant which purpose users are pursuing when they decide to buy or sell Bitcoins. For every user who wants to get involved in the Bitcoin game, the starting point is most likely an electronic exchange. Therefore, he will generate trading volume on an exchange by exchanging his current domestic currency into Bitcoin.

If he wants to use the digital coin as a means of trade, we would expect that after he buys Bitcoins at an exchange, he would spend at least some of their newly acquired coins to buy goods or services. Thus, the Bitcoin network transaction volume would increase instantly. But, if the purpose of users is focused on the currency itself, we would expect a strong correlation between the number of new entrants in the Bitcoin system with the Bitcoin network volume. So, an increase in the number of Bitcoin participants would mean an increase in the Bitcoin network volume.

Assuming that an increase in the number of Bitcoin users is associated with an increase in the Bitcoin network volume, we could conclude that users who wish to use Bitcoin as an asset would not leave a footprint in the Blockchain. More precisely, Bitcoin exchanges are handling accounts of their customers in the internal accounting system, which is not other than the Blockchain. The latter guarantees the tracking of all kind of transactions with the digital coins. Thus, we would expect that these Bitcoins would primarily remain within the exchange internal system. So, now it becomes clear that an increase in Bitcoin participants is positively associated with an increase in the Bitcoin exchange volume.

# ***Challenges in the Bitcoin Network***


*"The cause is hidden. The effect is visible to all."*

Publius Ovidius Naso (43 BC – AD 17/18)

The basic risks in payment and settlement systems are related to credit, liquidity, operation and legality[134]. More precisely, virtual currencies, as a form of money, have not avoided being "victims" of malicious activities. But, most of such misdeeds are not new. The phenomenon of money laundering and fraud, for example, has firstly appeared in cash. The question is, however, whether virtual currencies are able to make such abuses easier to carry out or harder to catch.

[134] Federal Reserve Board, (2011).

Concerning Nakamoto's paper, he described his mathematical system that would play the role of a monetary system but he did not refer to the possible weaknesses that it might present in its application. Therefore, Bitcoin may be based on mathematical proofs which seem irrefutable and transparent but its protocol appears to have some critical vulnerabilities.

The problems in the Bitcoin protocol, though, lie in the many uncertainties which characterize its general structure. Given that it is completely decentralized, Bitcoin ecosystem by design favors price instability, lack of regulation and self-policing. Thus, it is not easy for the digital currency to become an official and established monetary tool. But, it could work efficiently as a complementary economic tool to today's current financial structure. In this way, Bitcoin could drive financial institutions and central economic authorities towards becoming more technologically updated and efficient.

Since Bitcoin payments do not involve transfer of credit instruments and they operate on a real-time gross basis, credit and liquidity risks are absent. But legal and operational risks are present, threatening the system's reliability, while increasing use may reveal technical system's scalability limits. Moreover, there is the possibility that individual payments and even the operation of the whole system may be challenged by authorities.

In fact, privacy protection can be undermined too by malevolent hackers who aim at causing instability in the network. while increasing use may reveal technical scalability limits. But, as we all know, in established systems, though, these risks are supposed to be addressed by competition, regulation and oversight of service providers.

The nature of challenges faced by Bitcoin platform can roughly be divided in two streams of research. More specifically, the first stream concerns the several risks arising from its design and its technological architecture and structure underlying the decentralized infrastructure of Bitcoin.

On the surface, the decentralized nature of the network protects it but that could it be enough? In contrast to central banking systems, decentralized systems can better protect themselves against malicious attacks and route around damage. But there are nevertheless theoretical attacks on the networks with many of them having been proven practically. In fact, several techniques based on network and graph theory have been applied in order to conduct analyses regarding transaction anomalies and possibilities of de-anonymizing single entities in the Blockchain.

Due to the anonymous nature of the currency, bitcoin has the foundations to be used for illegal activities such as theft, money laundering and tax evasion. Few governments have set strict capital controls on the currency and many have covered it in tax laws. Central banks around the world have warned consumers on the risks that come with the currency such as lack of consumer protection and high price fluctuations. Research on fraudulent activities with the currency is limited due to the anonymity of the currency making it difficult to obtain data[135].

It has been showed that users and Bitcoin addresses may be mapped passively by the usage of centralized services such as currency exchanges and online wallets[136]. More precisely, on the basis of a day-to-day usage scenario of Bitcoin it is proved that 40% of the users can be profiled passively which therefore makes us willing to reject the anonymity hypothesis regarding Bitcoin[137]. Moreover, it is proved that double spending is possible in the case of a fast payment, given that it cannot be verified in the Blockchain. Therefore, a modification of the current implementation of Bitcoin platform should be taken seriously into consideration by its developers.

[135] European Parliamentary Research Service, (2014).

[136] Reid, F. , and Harrigan, M., (2011), An analysis of anonymity in the bitcoin system.

[137] Karame, G., O., Androulaki, E., and Capkun, S., (2012), Double spending fast payments in bitcoin, Proceedings of the 2012 ACM conference on computer and communications security.

There are diverging opinions concerning the robustness of the Bitcoin architecture. More specifically, there have been reported several hacker attacks which aimed at breaking the anonymity of users[138]. There are reports where Bitcoin wallets have been hacked and some online exchange facilities which have been proven to be fraudulent[139]. According to Bitcoin co-developer Jeff Garzik, "*People have the mistaken impression that virtual currency means you can trust a random person over the Internet*[140]." Finally, there are political and legal risks for anonymity in Bitcoin transactions whose exact nature and impact depend on the future evolution of the political and legal status of the project.

The second research stream on Bitcoin focuses on the risks involved in the Bitcoin governance. Given that there is no regulation about the bitcoin and the other digital cryptocurrencies, they seem vulnerable to speculation and misinformation[141]. If we think that a vital component in the Bitcoin ecosystem are currency- exchanges because they link traditional currencies with the digital ones and the fact that there is no regulation, Bitcoin users can become, thus, subject to risk mitigation.For this reason, bitcoin exchanges should run under some certain governance requirements.

Bitcoin participants can also become vulnerable to default risk caused by several online attacks from hackers or even by systemic weaknesses. Consequently, the percentage of risk default at these exchanges increases dramatically.[142] But, concerning the conversion rate on currency exchanges, researchers show that the price risk, which is referred to the volatility of the currency rate, have a positive effect on price development.

[138] Reid and Harrigan,(2012).

[139] Moore and Christin,(2013).

[140] Wallace, (2011).

[141] Brezo, F. , and Bringas, P., (2012), Issues and risks associated with cryptocurrencies such as bitcoin, The second international conference on social eco-informatics.

[142] Moore, T. ,and Christin, N. , (2012), Beware the middleman: empirical analysis of bitcoin- exchange risk.

In addition to the referred challenges, it should be noticed that Bitcoin is neither regulated, nor is there any designated system manager. Therefore, users are obliged to trust in the power of community to manage these risks. But due to the virtual character and the prevailing anonymity preference of the community, the emergence of trustful relations is de facto discouraged and members are vulnerable to trust abuse.

Not to mention that, currently, the Bitcoin system poses a certain technical challenge for unsophisticated users and payment verification can take several minutes longer than the established payment methods[143]. Since record keeping in the payment transfer system is based on a full list of all historical transactions being continuously updated and held by all network members, the size of the ledger can become substantial, posing scalability issues to the system, over time[144].

There exist other kind of attacks too against the Bitcoin ecosystem. One example is the 51% attack. As we have already mentioned, the Bitcoin protocol measures the level of computing activity on the network in terms of the hash rate. Should one miner or a pool of miners gain control of 51% of the hash rate, then they would theoretically be able to solve their own block of transactions.

The so-called 51% attack also results in a fork, which is where there are two conflicting blocks "battling" for addition to the blockchain. Given that the majority of mining power on the network would support the attacker's block, the malicious one would be sent unfortunately to the blockchain. And the attacker's block could include fraudulent transactions. For example, if the attacker sent bitcoins to a recipient in exchange for a service, blockchain could then record that it had sent the same bitcoins to another bitcoin address that it controlled, in its own block.

[143] ECB (2012).

[144] The Economist,(2013).

In addition, the fact that Bitcoin transactions are irreversible makes them subject of several challenges such as the problem of double spending. More specifically, double spending attacks are mountable in other ways. Given that a block takes around ten minutes to mine, getting even one confirmation of a transaction can take that long. This can facilitate a double spending attack without the significant computing overhead required for a 51% attack. It has, also, been shown by researchers that double spending is possible even by broadcasting a fraudulent transaction to a large number of nodes in the network, while sending the genuine transaction to a service provider. So, the large number of nodes receiving the broadcast makes the network assume that the fraudulent transaction should be accepted into the block, instead of the genuine one.[145]".

There are other negative aspects of Bitcoin technological architecture too. More precisely, denial of service attacks can be used to compromise the network or to lead to "dust transactions", which include very small transactions that send hardly any bitcoin. Therefore, this kind of attacks can manipulate the blockchain system. Since the minimum fraction of a bitcoin is one Satoshi, there was the possibility to send large numbers of these transactions which would fill up the blocks in the blockchain. And given that each block increases the length of the blockchain , it can end up by bloating the chain[146].

Another potential risk lies within the client's code itself. According to developers, bitcoin network confronts several vulnerabilities such as the attack realized, in 2013, on the voluntary Bitcoin nodes, which are those that relay transaction information around the network but which don't necessarily mine coins.[147] In this attack, hackers exploited an incomplete feature in the source code showing that the software was filled with bugs. Even, bitcoin may have shown signs of improvement, it still faces essential challenges as the network increases.

[145] Karame, Ghassan, Androulaki, Ellie, Capkun, Srdjan, (2013), Two Bitcoins at the price of one? Double spending attacks on fast payments in bitcoin.

[146] Gilson, D., (2013), Bitcoin blockchain grows to 8GB, Coindesk.

[147] Bradbury, D., (2013), Bitcoin network recovering from DDoS attack, Coindesk.

Concerning its economic aspect, an ECB report states that, "*Bitcoin might undergo a deflationary spiral that causes certain individuals or industries to abandon Bitcoin, possibly causing a panic or just a permanent depression in Bitcoin's value*." More specifically, the result of such a spiral is underemployed human capital and other means of production which may lead to destruction of the wealth. Thus, deflationary pressures may impact Bitcoin more than the traditional currencies.

On the other side, Bitcoin proponents have answered criticisms about deflation with declarations that lack evidence. For instance they state that,

"*As deflationary forces may apply, economic factors such as hoarding are offset by human factors that may lessen the chances that a deflationary spiral will occur."*

Other risks exist as well about the credibility of the exchanges stores. More precisely, the Mount Gox, which constitutes the largest exchange of bitcoins with traditional currencies, based in Japan, faced serious problems. Therefore, the Mount Gox case illustrated that it is certainly possible for the bitcoins to be stolen in a digital attack and the exchange shut down, with the strong possibility for all the owners losing their money.

Even, some governments have already moved in some jurisdictions to regulate the Bitcoin system. More specifically, China has banned yuan to Bitcoin deposits into the exchange store "BTC China", which constitutes the largest exchange used to buy real goods and services. Further, Germany, France and Korea have also indicated a repudiation of Bitcoins as a currency. And other countries are yet to follow.

We could not undermine the fact that the use of bitcoins for tax evasion as a potential danger for the public policy . More precisely, Bitcoins, like cash transfers, cannot be traced by third parties and thus are essentially invisible to tax authorities. Thanks to its technological backround, everyone may see the public key accounts and all transactions, they cannot see the identity attached to them. So,similar issues could end up by contributing decisively to money laundering.

Even the Financial Crimes Enforcement Network (FinCen) of the US Treasury stated in 2013 that "*Bitcoins are convertible virtual currencies and should be treated like a currency for the purposes of US anti-money laundering laws in the cases where Bitcoin money service providers could be classified as money-transmitters*." . According to this statement, the digital coin becomes similar to a currency with an exchange rate to the dollar , the gains and the losses from which are taxable.

Another risk for the bitcoin community is the fact that digital currencies are highly susceptible to abuse by criminals. More specifically, many criminals have chosen the digital currencies in order to process their payments. The Silk Road case is an indicative example of their dangerous activity. Before its closure by the FBI in 2013, the Silk Road, which was an online underground market where schedule drugs and narcotics without prescription were sold, relied on Bitcoins for all their transactions. So, criminals have also begun to abuse digital currencies such as Bitcoin as a platform of exchange for illegal activities. As they wanted to register in bank accounts without providing identifying information, they found the new choice of digital coins very interesting. Notably, there has been almost no evidence of criminals using Bitcoin for this purpose on a large scale.

Another risk that Bitcoin faces is the possible collapse in value it may suffer due to the emergence of substitutes of cryptocurrencies and an essential exchange-rate risk. Concerning the latter, it is a fact that the Bitcoin- US dollar exchange rate has fluctuated in the last years widely. During the recent years of its operation its exchange rate fluctuated between $ 5 and $ 15. The currency has only stabilized recently. Consequently, while Bitcoin's rise has benefited early adopters, consumers are fearful of holding or spending the currency because its value can change so rapidly.

Moreover, hackers may benefit from bitcoin system's weaknesses and gain unauthorized access to Bitcoin wallets stealing money from them. The problem becomes bigger if we take into account the fact that several high-profile Bitcoin thefts have

targeted currency exchanges and other entities that hold large amounts of the currency. This becomes significant if we think that many consumers, fearful of taking possession of their Bitcoin assets, choose to leave their newly- acquired currency in the control of the exchanges from which they purchased them. And this fact points to another Bitcoin-specific hazard, the exchange-closure risk.

## ***The promises of the Bitcoin System***

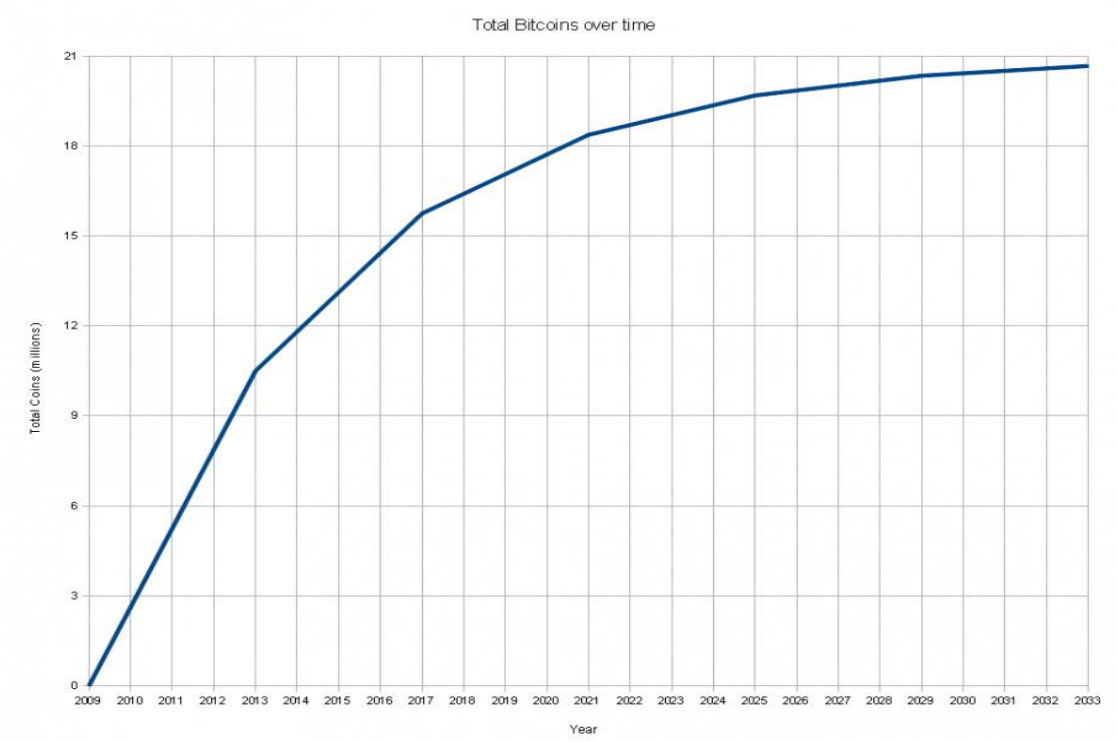



Figure - Expected total quantity of bitcoins over time (2009-2033), measured in millions.

Indeed, there would be many benefits of ending the use of cash, including major reductions in taxes to vastly improved public services. Moreover, a cashless society would result into a lot of benefits[148]. At first, we could have a simpler wallet where we keep just one money card or a digitized, high-security photo identity card. Secondly, there would be the possibility to tax the underground economy, most of which operates through cash money which does not leave any trail. Furthermore, online virtual currencies would make it easier to expose possible transactions concerning government

[148] Bacard, A. (1994). A cashfree society: Nirvana or nightmare? The Humanist.

corruption or bribery because it would make the money path more transparent and of course public.

A cashless society could also eradicate counterfeiters. Since the counterfeiting of currency, stamp papers and negotiable financial papers has become a big business the digital coins would support more transparent transactions between stakeholders. Besides, electronic money would be harder to manufacture than paper money. Digital currencies could even restore accidental losses of cash that happen every day. Nevertheless, given that all transactions take part online, the accounting processes would be more accurate. So, the use of online "virtual currencies" could ultimately help create an economic system without many disadvantages of hard cash.

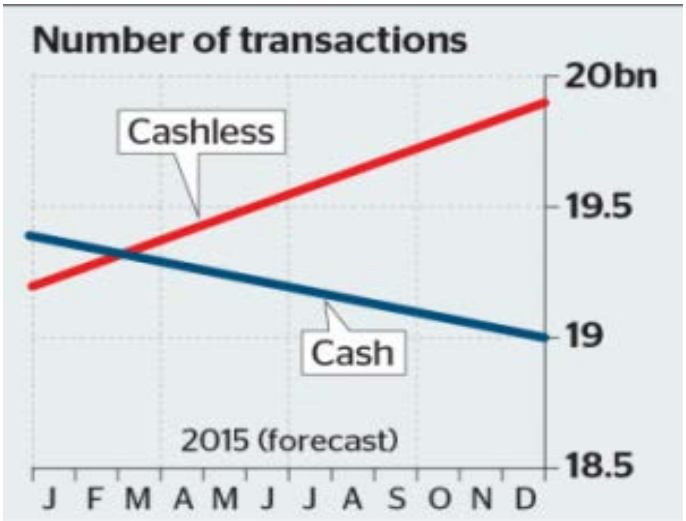



Figure – Cashless vs Cash

On the other side, Bitcoin as a medium of exchange seems to possess all the aforementioned features and many more alluring qualities that are worth mentioning. More precisely, bitcoins are stored on cards or electronic wallets and the payees can

easily recognize them. Their transferability is easy and flexible but most importantly without cost. For example, there are lower transaction costs within the Bitcoin system than there are in transactions with the existing electronic payment methods like PayPal. This can be attributed to the lack of a third-party intermediary. With cheaper transactions and quicker transactions, the possibility of micro-transactions becomes feasible. Bitcoin transactions quickly become irreversible. And this attracts a niche market where vendors are concerned about credit-card fraud and chargebacks. Therefore, the bitcoin verifiers' market currently bears very low transaction fees, which are optional and chosen by the payer. This can be attractive in micropayments where fees can dominate. So, reducing the cost of the transactions, Bitcoins eliminate the added costs to the consumer.

The second major allure of bitcoins is their proven functionality and detachment from central authorities. More precisely, the digital coins become impossible to forge and can be taken and spent across national borders, without the participation of state banking. And this happens under a security frame[149]. Finally, another reason that people are attracted to bitcoin is the anonymity it offers.

While every transaction is publicly logged and available for all to see, the logged information only identifies the location of bitcoins in the system. In other words, the information recorded is the digital address of the digital coins and not the user or the user's account information[150].

Bitcoin works globally and that makes it accepted everywhere and anytime across the world. In addition, since bitcoin doesn't involve a third party, the transactions can be made to anyone with small amount of fees, unlike transactions made through financial institutions such as a Bank, which require a high amount of fees. Moreover, sending bitcoin by its application is simple, easy and doesn't require a lot of information such as expiration date, names, account number or CVV number as it happens with credit cards. The recipient's address is enough to make the transaction.

[149] J. Davis , (2011), The cryptocurrency, Bitcoin and its mysterious inventor, New Yorker.

[150] B. Kerschberg, (2011), Credit card transactions – how safe is your personal information?, Forbes.

The transactions in case of bitcoin are highly secure because of the use of digital signatures and the required technical conformations to identify the transaction. So, Bitcoin offers greater anonymity than credit cards.

In addition, it is not controlled by any government or financial institution, therefore, inflation in bitcoin is unlikely to happen. Its decentralized design is responsible for protecting it against inflation. Traditional currencies rely on a central bank to regulate the money supply, introducing new money into circulation as needed. The quantitative easing policies adopted by the U.S. Federal Reserve have attracted criticism about potentially causing inflation.

Bitcoin, in contrast, uses cryptography to guarantee a relatively fixed money supply, which is allowed to grow at regular intervals. Periodically, the amount of money introduced is halved, until no more bitcoin currency is brought into circulation. Hence, instead of central bank decisions driven by human prognostics, bitcoin relies on an algorithm to limit the growth of the money supply[151].

Owning a bitcoin account doesn't require any amount of deposit, which gives it another advantage compared to traditional bank accounts. So, that's why there appears to be so much interest in digital currencies and especially in bitcoin.

Bitcoin is remarkably flexible partly due to its completely distributed design. The open-source nature of the project entices the creation of new applications and new businesses. Because of its flexibility and openness, a rich extended ecosystem surrounding bitcoin is flourishing. For example, mixer services have spawned to cater to users who need better anonymity guarantees. There are payment processor services that offer gadgets vendors and can embed in their web pages to receive bitcoin payments alongside regular currency.

Last but not the least, in comparison with other digital currency schemes, bitcoin has provided readily available implementations, not only for the desktop computer, but

[151] International journal of critical infrastructure protection, (2013)

also for mobile phones. The open-source project is maintained by a vibrant community and until the time of writing it has a healthy style of development. So, we believe that the reliability and efficiency that surround this technology will create a more efficient economy in which digital coins can flow more freely and securely.

## ***FINANCIAL REGULATION AND TAX TREATMENT***

*"We are at the beginning of a mighty struggle for control of the Internet—the web links everything and very soon it will mediate most human activity—because the Internet has fashioned a new and complicated environment for an age-old dilemma that pits the demands of security with the desire for freedom.*[152]*"*

U.S. laws and regulations have the ability to prohibit or limit the use of bitcoins in the market. Close inspection of the existing laws show that the traditional institutions and mediums of exchange do not contemplate a technology like the bitcoin protocol. Given that bitcoins fall within a gray area under the laws of many countries globally, it remains difficult to provide sincere contractual obligations. Therefore, it becomes necessary to treat them in a different way than authorities do with established fiat currencies. It would be then wiser to treat Bitcoin like a local or a community currency under a specific series of laws. And that would mean receiving full authority as a medium of payment under contract law, requiring taxation on income, and not implicating securities regulations.

The broad scope, though, of an "investment contract" is the best vehicle to bring bitcoins into the jurisdiction of the Securities and Exchange Acts. As analyzed above, applying the definition to bitcoins in general poses problems. Recently, however, a federal court has shown how it is easier to categorize them as an "investment contract" in the context of a specific investment scheme.

[152] Presentation, Misha Glenny, Hire the Hackers!, TED (2011),http://threatpost.com/en_us/blogs/ted-global-misha-glenny-says-hirehackers-091511.

A number of law review articles have addressed the legality of bitcoin[153]. More specifically, due to how novel Bitcoin is, it truly falls into a legal grey area. There are, however, a few laws in the United States that could possibly be used in order to regulate it.

The most obvious argument would be to regulate bitcoin through Congress' constitutional right to control currency[154]. Even though this seems obvious, the Constitution says nothing about private parties making money. However, two federal statutes affect a private party from creating a currency: the Stamp Payments Act of 1862 and federal counterfeiting statutes.

The purpose of the Stamp Payments Act of 1862 is to curb competition with federal currency. More precisely, it states in part, "*Whoever makes, issues, circulates, or pays out any note, check, memorandum, token, or other obligation for a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States, will be fined and/or jailed not more than six months*". Bitcoin does not limit transactions to more than one dollar and some argue that it is intended to compete with official currency. But, the stronger argument is that bitcoins do not fall within the Stamp Payments Act.

Congress goal of the Stamp Payment Act was to prevent competition with federal Currency. And challenging bitcoin would not favor this goal. Bitcoin is only used over the Internet where it competes with credit cards, PayPal and e-wallets. Secondly, the Stamp Payment Act was written long ago and the instruments described inside, were all physical, tangible instruments[155].

---

[153] N., M., Kaplanov, (2012), Nerdy Money: Bitcoin, The Private Digital Currency, and the Case Against its Regulation, 25 Loy. Consumer L. Rev. 111, 130.
[154] Grinberg, supra note 32.

[155] At 189 (noting that Professor Ronald Mann of Columbia Law School, who researches payment systems and electronic commerce, disagrees with a narrow interpretation of "obligations" because he believes the Act would cover a private coin based solely on it's metallic content. Furthermore, he thinks that bitcoins are a "token" and would argue falls within the Act.

Thinking about analogous cases, the most appropriate type of instrument similar to bitcoins is alternative currencies. While local currencies are simply any medium of exchange that is not a traditional currency, a community currency provides the flexibility to participants to make exchanges with multiple parties. Nevertheless, like bitcoins, the denominations in a community currency system are issued by nongovernmental groups and have monetary value accepted for goods and services within the community. So, the substantial purpose of bitcoins, serving as a medium of exchange, is the same as the purpose of community currencies.

The anonymity provided by bitcoin is at once a point of attraction and a challenge for financial regulation. More specifically, up-to-date bitcoin-related regulation has largely been focused on the application of "Know your customer",( KYC), and Anti-Money-Laundering rules (AML), as well as consumer protection licensing, on these new intermediaries. As the adoption of the digital currency grows, Bitcoin system comes more and more under scrutiny by the legal and financial authorities, with regard to compliance with applicable Anti-Money Laundering (AML) statutes and Know-Your-Customer (KYC) controls. So, legal authorities and other interested parties begin to study and discuss about its true level of anonymity and the potential threats it may pose.

The key challenge for prospective regulators is where to impose constraints in the Bitcoin system. Its ecosystem is of high interest to regulators including the new bitcoin-denominated instruments and the completely decentralized markets and exchanges that surround them. Its ecosystem is of high interest to regulators including the new bitcoin-denominated instruments and the completely decentralized markets and exchanges that surround them.

This is due to its open protocol and its decentralized network making no company or central server able to be regulated. Furthermore, since there are a number of emerging new intermediaries operating on the bitcoin network , it appears to be more than necessary for them to become regulated by authorities. These include exchanges, merchant processors and money transmitters that provide bitcoin services to consumers.

Besides, the next major wave of bitcoin regulation should be aimed at financial instruments, including securities and derivatives, as well as prediction markets and even gambling.

Regulators clearly see the bitcoin features of anonymity, decentralization and lack of a central control as detrimental to control. However, it is fair to assume that a complete ban on bitcoin would continue to take place only in totalitarian jurisdictions. Furthermore, it would become infeasible to regulate all peers in the Bitcoin network due to their quantity, their geographic distribution and the privacy protections in the network. Instead, regulators are naturally drawn to key intermediaries. Thus, it is more likely that tax reporting, VAT and other components would be based on some kind of honor systems, in order to protect the consumers of the Bitcoin community. And these members should decide in collaboration with central authorities the creation of a regulatory enforcement.

Needless to say that there are serious risks on further growth of bitcoin as a financial tender type. More precisely, some jurisdictions have deemed bitcoin to be a commodity whereas others treat it as currency. Some countries have outlawed bitcoin altogether and treat the possession of bitcoin as a criminal activity. United States, for example, treats bitcoin as a commodity. Any agency involved in the transfer of bitcoin with fiat currencies comes under the control of banking and money laundering laws and requires licensing in every state. For consumers, the act of purchasing a commodity in bitcoin is a taxable event. This treatment certainly hinders wider adoption.

Given that the first application of the bitcoin technology has been simple payments and money transfers, and given that the technology's censorship-resistance permits transactions that were previously restrained, it is no surprise that the first wave of regulatory activity related to bitcoin has focused on money transmission. More precisely, at the federal level, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued guidance in 2013 advising relatively the Bitcoin exchangers and other related enterprises qualified as money transmitters. According to the guidance, "*such*

*businesses are obligated to register with FinCEN as money services businesses in each state in which they do business and comply with "Know Your Customer" rules, put in place robust Anti-Money-Laundering programs and file Suspicious Activity Reports*."

Money transmitters should be licensed by each state in which they operate. So financial regulators have started to search efficient ways to combine existing money transmission laws and regulations with bitcoin businesses[156]. Even in China, in 2013, policy was broadly similar, requiring that Bitcoin intermediaries implement Know-Your-Customer registrations for account-holders. Furthermore, New York has taken the lead in making these determinations. In August 2013, New York's Department of Financial Services has requested information almost two-dozen bitcoin-related businesses, as well as investors in those businesses.[157]

As we have observed, current law enforcement actions up to date have centered on money laundering and unlicensed money transmission. In 2013, federal agents seized $5 million from accounts belonging to Mt. Gox, which at the time was the world's largest bitcoin exchange[158]. According to the seizure warrant, the company had not registered with FinCEN regulations as a money services businesses.[159] Moreover, in 2014, federal agents arrested Charlie Shrem, CEO of the now-shuttered exchange "BitInstant", on charges of money laundering and operating an unlicensed money transmitter and filed against him suspicious activity reports under FinCEN[160]. And there were plenty other cases too, concerning criminal transactions with bitcoin which raised the need to regulate Bitcoin very high.

---

[156] M. Santori, Bitcoin Law: Money transmission on the state level in the US, CoinDesk, (2013), http://www.coindesk.com/bitcoin-law-moneytransmission-state-level-us/.
[157] G. Farrell, N.Y. Subpoenas Bitcoin Firms in Probe on Criminal Risk, Bloomberg, (2013), http://www.bloomberg.com/news/2013-08-12/n-y-regulator-subpoenasfirms-over-bitcoin-crime-risks.html.
[158] Am. Toor, (2013), US seizes and freezes funds at biggest Bitcoin exchange, The Verge.
[159] Seizure Warrant – In the Matter of the Seizure of The contents of one Dwolla account, (2013), http://cdn.arstechnica.net/wpcontent/uploads/2013/05/

[160] Sealed Complaint – United States of American v. Robert M. Faiella, a/k/a "BTCKing," and Charlie Shrem, No. 14-MAG-0164, (2014), http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR/Faiella, %20Robert%20M.%20and%20Charlie%20Shrem%20Complaint.pdf.

The FBI takedown of Silk Road in 2013 illustrates both the challenges of regulation and regulators' ultimate power. More specifically, Silk Road was hosted as a "hidden service" on Tor, a system which is purpose-built for anonymity of both visitors and operators. Payments in Silk Road, as it was stated, were only accepted in bitcoin. However, the Silk Road domain site was seized by the FBI when the site's alleged operator was arrested on charges of conspiracy to distribute controlled substances, computer hacking and money laundering charges[161].

It is true that Bitcoin is not an obligation. It only has value due to individuals giving it value, not because anyone promised to give something in return for it. On the other hand, there is a counter argument that some hold bitcoins for fun. However, the stronger argument is that they are held for profit.

Given that most bitcoins are purchased through exchanges, if the government wants to curb the illegal activity and money laundering associated with bitcoin, regulating the exchanges will be the starting point.[162]. The best mechanism to regulate this market is the Bank Secrecy Act, (BSA), and Money Laundering Control Act. [163]. According to these regulations, a "money services business" should check cash, dealers in foreign exchange and money transmitters generally.[164]. The Money Laundering Control Act criminalizes money laundering[165].

[161] Greenberg, An., (2013), FBI says it's seized $28.5 million in bitcoins from Ross Ulbricht, alleged owner of Silk Road, Forbes.

[162] Grinberg, supra note 11..

[163] 31 U.S.C. 5330(a)(1).

[164] 31 C.F.R. §1010.100.

[165] 18 U.S.C. §1956.

Recently, FinCEN issued guidelines applying to virtual currency to clarify where they fall under the BSA[166].With regards to virtual currency, a "money services business" was determined as : (a) administrator or exchanger that accepts and transmits virtual currency, or buys or sells virtual currency, (b) brokers and dealers of virtual currency (c) mine and sell virtual currency for money or its equivalent.

These definitions seem to be an attempt to cast a large web over the bitcoin community including e-wallets, exchanges and individual miners[167]. This would require them to implement anti-money laundering procedures, keep records, and report suspicious transactions. Despite the unique nature of bitcoins, they fall within the definition of commodity too, for the purposes of futures regulation. More precisely, any futures contract referencing bitcoins will thus likely be subject to the full scope of regulation under the CEA.

Bitcoin is, also, a very volatile currency so it has very large price fluctuations. For example, in 2013 bitcoin value was around $1200, but on December, 2013 it was around $800. So there is an apparent risk that seller would sell at much lower prices or buyer would buy for much higher prices. Also, with respect to price fluctuations, we can definitely argue, that pricing is hard, because a business must update their pricing almost every day so as to stay on top of the fluctuating exchange rates of the bitcoin.

Fortunately, Bitcoin's electronic form makes it easier to regulate than offline fiat currencies. Consider a possible theft. Once stolen cash enters circulation, little can be done to reclaim it. In contrast, Bitcoin blacklists could let law enforcement claw back all stolen bitcoins.

Concerning the tax treatment of Bitcoin, it remains unsettled and simultaneously complicated. Bitcoin transactions are not currently monitored by any government

[166] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FinCEN, http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html , (2013).

[167] Gruber, supra note 102.

authority. This could make the income reporting difficult. Not to mention that bitcoin price fluctuations make business income reporting even more complicated To correctly claim an income in a tax declaration, business has to convert bitcoins into an official currency. Without doing that, business could confront with several issues with Internal Revenue Service (IRS) . In 2014, the IRS issued guidance that transactions to and from virtual currencies may create taxable events for federal tax purposes.

There is also a serious problem with determination of bitcoins' ownership, because even there is the Blockchain as the underlying technology which records every single transaction with the digital coins, though, there are no official records of ownership of them. Therefore, during transactions it becomes difficult to identify the buyer or the seller. User's identity is encrypted in all transactions but there is a full record of every pair of public and private keys which is preserved on the publicly available ledger.[168] But with all the necessary measures, it can be feasible in the future to identify the actual sender of money who will be taxed.

In many countries, such as Belgium, India, United Kingdom, Canada, Argentina, Chile, France, Greece, Germany and others, there is no specific law or regulation regarding bitcoin at all and it is not illegal in this countries to use them. For instance, in Argentina bitcoin is not a legal currency, because under the Constitution of Argentina the only authority capable of issuing legal currency is the Federal Bank[169] and can be considered under the Civil Code only as a good or thing and so transactions with bitcoins should be governed by rules of the sale of goods under the Civil Code[170]. Furthermore, in 2013, Canada's Revenue Agency stated, that users of bitcoins will have to pay tax transactions in the digital currency, based on two separate tax rules that apply to barter

[168] EPRS Bitcoin. Market, economic and regulation, Http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI%282014%29140793_REV1_EN.pdf

[169] Constitution of the Argentine Nation, section 75, online at http://www.biblioteca.jus.gov.ar/argentina-constitution.pdf

[170] The Argentine Civil Code, art. 2345[2311], http://archive.org/stream/argentinecivilc00whelgoog/argentinecivilc00whelgoog_djvu.txt

transactions and things which are bought and sold for speculative purposes[171]. The European Union, also, has not passed a specific legislation about the status of bitcoin. In 2012, the European Central Bank issued a report, "*Virtual Currency Schemes*" that analyzes the legal status of bitcoin under the EU legislation[172].

According to this report, the bitcoin falls outside the scope of Electronic Money Directive 2007/64/EC because the Directive does not deal with electronic money and because payment institutions introduced by the Directive are not permitted to issue electronic money[173]. As we have mentioned, the EU has not created any specific regulatory laws on bitcoin.

The biggest issue with regulating bitcoin stems from the fact that it cannot be classified as a legal tender or a financial derivative or commodity. More specifically, Japan has announced it as a commodity, the US treats it as property while Germany classifies it as private money.

Currently, law really does not envision a type of technology like bitcoin, which leaves it in a legal gray area. Since people often confront electronic coins as being used for illegal activity, there is likely some interest in trying to limit or ban them. However, a total prohibition on bitcoins would be nearly impossible to accomplish and would not stop the underlying criminal activity. In fact, used correctly, bitcoins could provide much of the information necessary for prosecutors to investigate criminal activity. Therefore, we conclude that policymakers should allow bitcoins to continue in order for their full market capabilities to be realized. So, Bitcoin ecosystem may require the emergence of governance structures, contrary to the commonly held view of Bitcoin community which votes for a digital coin ungovernable, but with certain limits.

[171] Bitcoins aren't tax exempt, Revenue Canada says, http://www.cbc.ca/news/business/bitcoins-aren-t-tax-exempt-revenue-canada-says-1.1395075
[172] ECB, Virtual Currency Schemes (2012)

[173] ECB, Virtual Currency Schemes (2012).

| Scope | Country | Information |
|---|---|---|
| **Prohibited** | China | Banks prohibited from transacting with bitcoins. Citizens allowed to trade. |
| | Russia | Bitcoins prohibited to be used by citizens or banks. |
| | Iceland | All foreign exchange activitie using Bitcoin prohibited. |
| **Protection from illegal activities such as money laundering and illegal financing** | USA | Bitcoin exchanges and miners have an obligation to report any suspicious activities/transactions to the federal government. Selling or trading Bitcoins for real world economic commodities (non-digital) are subject to tax liability |
| **Subject to Taxation** | Japan | Any purchase and revenue from trading with Bitcoins are subject to taxation. Banks and other official entities are prohibited from trading with Bitcoin. |
| | Finland | Any profit made from transacting with foreign currency using Bitcoins is subject to taxation. Profit from increases in Bitcoins value after obtaining it as payment is subject to taxation |
| | Germany | Any profits accrued from mining Bitcoins or trading are subject to capital gains tax. |

Figure - This table shows the regulations on Bitcoin from a few different countries. It seems that this reporting can provide a significant knowledge and experience for the Bitcoin regulation, more efficient than this of fiat currencies.

Source: European Parliamentary Research Service, 2014

# ***CONDUCTING AN EMPIRICAL STATISTICAL RESEARCH***

## ***Data Collection***

The timeframe to be analyzed in this study covers the years from 2009 to 2016 and includes a large fraction of early Bitcoin transaction history and most importantly the growth phase of 2012 until 2013. More analytically, our statistical research includes time series data of Bitcoins, foreign exchange and interest rates and commodities via Datastream and several official websites of Bitcoin such as https://blockchain.info/ and https://bitcoincharts.com/. The time series data comprise open and close prices as well as exchange volumes, transactions and market capitalization in Bitcoin and in other specific fiat currencies.

Since Bitcoin as a digital coin exists exclusively online, every aspect of the system is, in theory, recordable. However, data does not exist or is not readily available, for all the variables in which an economist might be interested. For example, we found no direct measure of the number of users. We obtained information of variables where data exists from a variety of sources mainly from websites given that there is no official bibliography yet for the bitcoin economics. We have, also, gathered detailed information for the currencies, their exchanges rates and for the commodities used in the model from the "DataStream" database. We obtained monthly, mainly, data from 2009 which was the year that bitcoin entered the market until 2016. In other words, our time series variables cover the period from January 2009 through December 2016 for most of our variables. The online sources we utilized were accessed from the official site for bitcoins, http://www.blockchain.info/charts concerning the total number of bitcoins in the market, the number of transactions with bitcoins and many other parameters.

Most importantly, both volumes and prices in Bitcoin are disjoint, meaning that their growth is driven by independent mechanisms and parameters. According, to

Asteriou and Hall, most macro-economic time series are trended and therefore non-stationary. The problem with trended time series is that standars ordinary least-squares regressions can easily be biased in cases where independent and dependent variables share the same trend but share no causal relation. So, in order to check about the existence of stationarity in our variables we perform the Augmented Dickey-Fuller test combined with the Phillips-Perron test. If we observe trends in the variables we take the first-order differences of monthly or daily data points for each variable, which is sufficient in order to reach stationarity according to the Augmented Dickey-Fuller test. Afterwards, we check the correlation between the dependent variables and we omit the ones with levels in order to perform a robust OLS regression. Additionally, the prediction and explanation of time series is prone to time periods of conditional heteroskedasticity which comprise temporal periods of structural volatility changes and autoregressive dependencies which characterize financial time series data. Therefore, we perform an Autoregressive Conditional Heteroskedasticity (ARCH) estimation of the values in order to eliminate such periods within the errors. Certainly, we test the ARCH appropriateness within an auxiliary regression and thus we make some very important conclusions about the economic determinants of Bitcoin. All the dataset was elaborated in Stata.

The variables we used in our analysis are:

- **Total bitcoins** : Bitcoins in circulation- The total number of bitcoins that have already been mined; in other words, the current supply of bitcoins on the network.
- **Market Price(USD)**: Average market price across major bitcoin exchanges expressed in US dollars.
- **Market cap (USD)**: Total Market Capitalization -The total value of bitcoin supply in circulation, as calculated by the daily average market price across major exchanges, expressed in US dollars.

- **Trade volume (USD)**: Exchange Trade Volume- The total value of trading volume on major bitcoin exchanges, expressed in US dollars.
- **N-transactions:** Transaction Volume- The number of daily confirmed Bitcoin transactions. -Total Number of transactions.
- **Estimated Transaction Value (USD):** The Estimated Transaction Value, expressed in US dollars.
- **US Dollar 1-year Deposit Interest Rate:** The interest rate paid by financial institutions to deposit account holders of US dollars.
- **Euro 1-year Deposit Interest Rate:** The interest rate paid by financial institutions to deposit account holders of Euros.
- **Japanese Yen 6-month Deposit Interest Rate:** The interest rate paid by financial institutions to deposit account holders of Yens.
- **UK GBP 1-year Effective Exchange Rate Index:** It describes the strength of the sterling as currency relative to a basket of other currencies.
- **Nikkei 225 1-year Stock Average Price Index:** It is a price-weighted index expressed in yen, and the components are reviewed once a year.
- **Eurostoxx 1-year Price Index:** It is its Europe's leading Blue-chip index for the Eurozone, which provides a Blue-chip representation of supersector leaders in the Eurozone. The index covers 50 stocks from 11 Eurozone countries: Austria, Belgium, Finland, France, Germany, Ireland, Italy, Luxembourg, the Netherlands, Portugal and Spain. The EURO STOXX 50 Index is licensed to financial institutions to serve as underlying for a wide range of investment products such as Exchange Traded Funds (ETF), Futures and Options, and structured products worldwide.
- **Japanese Yen to Euro 1-year Exchange Rate:** The average exchange rate from Yen to Euro.
- **Euro to Japanese Yen 1-year Cross Exchange Rate:** The average exchange rate from Euro to Yen.

- **S&P 500 1-year Composite Price Index:** It is an American stock market index based on the market capitalizations of 500 large companies having common stock listed on the NYSE or NASDAQ.
- **S&P 500 1-year Growth Price Index:** It measures growth stocks using three factors: sales growth, the ratio of earnings change to price, and momentum. It is a style-concentrated index designed to track the performance of stocks that exhibit the strongest growth.
- **Dow Jones Industrials 1-year Price Index:** This is a price-weighted average of 30 significant stocks traded on the New York Stock Exchange (NYSE) and the NASDAQ.
- **Opec Oil 1-year Basket Price:** This is a weighted average of prices for petroleum blends produced by OPEC countries. It is used as an important benchmark for crude oil prices.
- **CMCI WTI Crude Oil 1-year US Dollar Price Index:** This index measures the collateralized returns from WTI Crude oil futures contracts. It is designed to be representative of the entire liquid WTI crude forward curve.
- **CMCI Gold 1-year US Dollar Price Index:** It is a fixed-weight index og gold prices, which may be based on spot or futures prices. It is designed to be representative of the broad commodity asset class or a specific subset of commodities, such as metals. It is an index that tracks a basket of commodities to measure their performance.

From these variables we were also able to develop estimates of the returns of all the variables. Since our sample contains a period when bitcoin was relatively unknown, we were interested in estimating the effects of bitcoins on the market when it became main stream. We decided that the total number on monthly basis of Bitcoins that circulate

would be a good proxy and independent variable in our econometric model because it should be correlated with other official currencies and commodities.

We wanted to estimate the relationship between Bitcoin price, volume and other variables such as the number of transactions, and other official currencies and commodities. Since we had, mainly, monthly observations for Bitcoins, we used Stata's command to calculate all the variables' summary statistics on a monthly basis. This generated thousands observations over the sample period. The summary statistics are shown in the following table for all the variables used in the model:

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| time | 2,802 | 1401.5 | 809.0121 | 1 | 2802 |
| totalbitco~s | 2,810 | 9052326 | 4932344 | 50 | 1.59e+07 |
| marketcap | 2,810 | 2.41e+09 | 3.21e+09 | 0 | 1.39e+10 |
| marketprice | 2,810 | 176.3308 | 232.9846 | 0 | 1151 |
| usdoll6mdepo | 1,999 | .7066083 | .3244166 | .18 | 2.05 |
| usdoll1ydepo | 1,999 | 1.021956 | .3818778 | .45 | 2.65 |
| eurostdepo | 1,999 | .2323512 | .4119558 | -.43 | 2.3 |
| euro1ydepo | 1,999 | .9225963 | .7075425 | -.13 | 3.02 |
| japanyen3m~o | 172 | .6031395 | .1399395 | .3 | .96 |
| japanyenst~o | 172 | .118314 | .0566208 | -.38 | .35 |
| japanyen6m~o | 172 | .7189535 | .2480333 | .23 | 1.25 |
| japanyensw~o | 172 | .1543605 | .0458085 | .08 | .35 |
| ukgbpeffec~x | 91 | 83.53275 | 4.163998 | 77.24 | 93.45 |
| nikkei225s~x | 1,999 | 12672.91 | 3772.388 | 7054.98 | 20868.03 |
| eurostoxxp~x | 1,999 | 282.3067 | 45.01891 | 169.39 | 392.35 |
| japanyento~e | 1,999 | 123.3917 | 13.26279 | 94.53 | 149.3 |
| eurotojapy~r | 1,999 | 123.4365 | 13.2531 | 94.25 | 149.23 |
| eurostoxxP~x | 1,999 | 282.3067 | 45.01891 | 169.39 | 392.35 |
| sp500compo~x | 1,999 | 1530.754 | 406.6814 | 676.53 | 2190.15 |
| dowjonesin~x | 1,999 | 13762.39 | 3130.511 | 6547.05 | 18636.05 |
| nasdaqcomp~x | 1,999 | 3379.506 | 1100.11 | 1268.64 | 5262.02 |
| opecoilbas~e | 1,738 | 85.68411 | 27.20415 | 22.48 | 124.59 |
| cmciwticru~x | 1,738 | 1392.484 | 305.6402 | 771.85 | 1914.24 |
| cmcigold1y~x | 1,738 | 2019.31 | 304.3721 | 1550.53 | 2784.44 |
| date | 2,810 | 19304.5 | 811.3215 | 17900 | 20709 |
| ret_bitcoin | 2,809 | .009403 | .2710643 | 0 | 14 |
| ret_usdoll~t | 1,998 | .0060053 | .1135842 | -.3840579 | .9591836 |
| ret_euro1y~t | 1,987 | -.0014511 | .7040235 | -7 | 19 |
| ret_japany~t | 171 | .0170617 | .2270173 | -.5652174 | 1.3 |
| ret_ukgbpr~e | 90 | .0004217 | .0161914 | -.0656066 | .0438934 |
| ret_nikk~225 | 1,998 | .0004211 | .0143289 | -.1055393 | .0770886 |
| ret_eurost~e | 1,998 | .0002813 | .0133681 | -.0765934 | .0905729 |
| ret_yentoe~e | 1,998 | -.0000163 | .0078852 | -.0535044 | .0400347 |
| ret_euroto~e | 1,998 | -.0000185 | .0079686 | -.0621899 | .0425069 |
| ret_sp500c~p | 1,998 | .0005002 | .0109509 | -.0666345 | .0707575 |
| ret_dowjpr~x | 1,998 | .0004224 | .0100308 | -.0554637 | .0683504 |
| ret_opecoi~p | 1,737 | -.0001863 | .0155793 | -.0847158 | .1140236 |
| ret_cmcic~1y | 1,737 | -.0001901 | .014023 | -.0841151 | .0841201 |
| ret_cmcigo~r | 1,737 | .0001632 | .0106831 | -.0989568 | .0985049 |
| total_ret | 90 | .0180617 | .1061672 | -.0310695 | .989635 |

Furthermore, we have calculated the monthly returns for every variable separately. The tables below are indicative:

**Total Bitcoins sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_bitcoin | 2,809 | .009403 | .2710643 | 0 | 14 |

**US dollar 1-year deposit sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_usdoll~t | 1,998 | .0060053 | .1135842 | -.3840579 | .9591836 |

**Euro 1-year deposit sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_euroly~t | 1,987 | -.0014511 | .7040235 | -7 | 19 |

**Japan Yen 1-year deposit sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_japany~t | 171 | .0170617 | .2270173 | -.5652174 | 1.3 |

**UK GBP Effective Exchange Rate Index sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_ukgbpr~e | 90 | .0004217 | .0161914 | -.0656066 | .0438934 |

**Nikkei225 Stock Average Price Index sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_nikk~225 | 1,998 | .0004211 | .0143289 | -.1055393 | .0770886 |

**Euro Stoxx Price Index sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_eurost~e | 1,998 | .0002813 | .0133681 | -.0765934 | .0905729 |

**Japan Yen to Euro Exchange Rate sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_yentoe~e | 1,998 | -.0000163 | .0078852 | -.0535044 | .0400347 |

**Euro to Japan Yen Fixed Cross Rate Exchange Rate sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_euroto~e | 1,998 | -.0000185 | .0079686 | -.0621899 | .0425069 |

**S&P 500 Composite Price Index sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_sp500c~p | 1,998 | .0005002 | .0109509 | -.0666345 | .0707575 |

**Dow Jones Industrials Price Index sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_dowjpr~x | 1,998 | .0004224 | .0100308 | -.0554637 | .0683504 |

**Opec Oil Basket Price sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_opecoi~p | 1,737 | -.0001863 | .0155793 | -.0847158 | .1140236 |

**CMCI WTI Crude Oil 1-year USD Price Index sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_cmcic~1y | 1,737 | -.0001901 | .014023 | -.0841151 | .0841201 |

**CMCI Gold 1-year USD Price Index sum of returns:**

| Variable | Obs | Mean | Std. Dev. | Min | Max |
|---|---|---|---|---|---|
| ret_cmcigo~r | 1,737 | .0001632 | .0106831 | -.0989568 | .0985049 |

Also with more details,

Total bitcoins

| | Percentiles | Smallest | | |
|---|---|---|---|---|
| 1% | 125550 | 50 | | |
| 5% | 766550 | 50 | | |
| 10% | 1238475 | 50 | Obs | 2,810 |
| 25% | 4801000 | 50 | Sum of Wgt. | 2,810 |
| 50% | 1.04e+07 | | Mean | 9052326 |
| | | Largest | Std. Dev. | 4932344 |
| 75% | 1.34e+07 | 1.59e+07 | | |
| 90% | 1.49e+07 | 1.59e+07 | Variance | 2.43e+13 |
| 95% | 1.55e+07 | 1.59e+07 | Skewness | -.3965831 |
| 99% | 1.58e+07 | 1.59e+07 | Kurtosis | 1.815651 |

US DOLL1Y DEPO(FT/TR)

| | Percentiles | Smallest | | |
|---|---|---|---|---|
| 1% | .51 | .45 | | |
| 5% | .54 | .49 | | |
| 10% | .58 | .49 | Obs | 1,999 |
| 25% | .76 | .5 | Sum of Wgt. | 1,999 |
| 50% | .95 | | Mean | 1.021956 |
| | | Largest | Std. Dev. | .3818778 |
| 75% | 1.21 | 2.48 | | |
| 90% | 1.42 | 2.48 | Variance | .1458307 |
| 95% | 1.77 | 2.55 | Skewness | 1.362331 |
| 99% | 2.41 | 2.65 | Kurtosis | 5.65363 |

EURO1Y DEPO(FT/TR)

| Percentiles | | Smallest | | |
|---|---|---|---|---|
| 1% | -.09 | -.13 | | |
| 5% | -.02 | -.12 | | |
| 10% | .07 | -.12 | Obs | 1,999 |
| 25% | .38 | -.11 | Sum of Wgt. | 1,999 |
| 50% | .6 | | Mean | .9225963 |
| | | Largest | Std. Dev. | .7075425 |
| 75% | 1.42 | 2.93 | | |
| 90% | 2.01 | 2.96 | Variance | .5006163 |
| 95% | 2.19 | 2.99 | Skewness | .4652723 |
| 99% | 2.36 | 3.02 | Kurtosis | 2.129372 |

UK GBP EFFECTIVE EXCHANGE RATE INDEX NADJ

| Percentiles | | Smallest | | |
|---|---|---|---|---|
| 1% | 77.24 | 77.24 | | |
| 5% | 78.88 | 77.28 | | |
| 10% | 79.26 | 77.53 | Obs | 91 |
| 25% | 80.3 | 78.76 | Sum of Wgt. | 91 |
| 50% | 82.64 | | Mean | 83.53275 |
| | | Largest | Std. Dev. | 4.163998 |
| 75% | 86.59 | 92.11 | | |
| 90% | 90.16 | 93.3 | Variance | 17.33888 |
| 95% | 91.8 | 93.36 | Skewness | .7594682 |
| 99% | 93.45 | 93.45 | Kurtosis | 2.638471 |

NIKKEI 225 STOCK AVG -PRICE INDEX

| | Percentiles | Smallest | | |
|---|---|---|---|---|
| 1% | 7682.14 | 7054.98 | | |
| 5% | 8493.77 | 7086.03 | | |
| 10% | 8741.16 | 7173.1 | Obs | 1,999 |
| 25% | 9471.67 | 7198.25 | Sum of Wgt. | 1,999 |
| 50% | 10721.71 | | Mean | 12672.91 |
| | | Largest | Std. Dev. | 3772.388 |
| 75% | 15749.66 | 20808.69 | | |
| 90% | 18264.22 | 20809.42 | Variance | 1.42e+07 |
| 95% | 19698.15 | 20841.97 | Skewness | .5355892 |
| 99% | 20563.15 | 20868.03 | Kurtosis | 1.915006 |

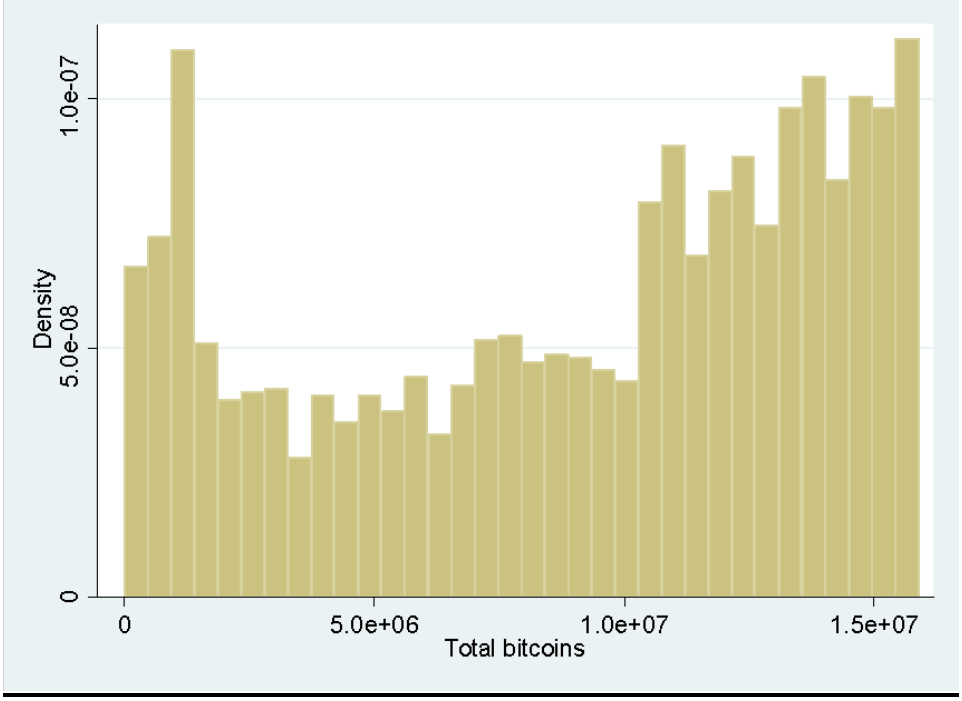
S&P 500 COMPOSITE - PRICE INDEX

| | Percentiles | Smallest | | |
|---|---|---|---|---|
| 1% | 778.94 | 676.53 | | |
| 5% | 903.25 | 682.55 | | |
| 10% | 1049.33 | 683.38 | Obs | 1,999 |
| 25% | 1186.69 | 696.33 | Sum of Wgt. | 1,999 |
| 50% | 1426.19 | | Mean | 1530.754 |
| | | Largest | Std. Dev. | 406.6814 |
| 75% | 1950.79 | 2185.79 | | |
| 90% | 2080.73 | 2186.9 | Variance | 165389.8 |
| 95% | 2104.05 | 2187.02 | Skewness | .0425555 |
| 99% | 2172.47 | 2190.15 | Kurtosis | 1.680894 |

We start by reporting the descriptive statistics in order analyze the nature of data. We clearly show a substantial data variability, highlighting the very prime need to use robust models which may incorporate this nature of the data. The coefficient of kurtosis appears inferior to 3 for all the variables in question indicating that the distribution is less

flattened than the normal distribution. The skewness coefficient is positive for all the time series in question. This implies that the asymmetrical distribution is more plausible. Afterwards, we look at plots of monthly Bitcoin transactions and returns of exchange rates and commodities traded at international stock exchanges in order to check for any evidence of stationarity. So, we look at the graphs of every variable separately in order to see their trends and their movement across the time studied (2009-2016) and we conclude that most of our variables are stationary, a fact which is proved after applying Augmented Dickey Fuller and Phillips Perron tests.

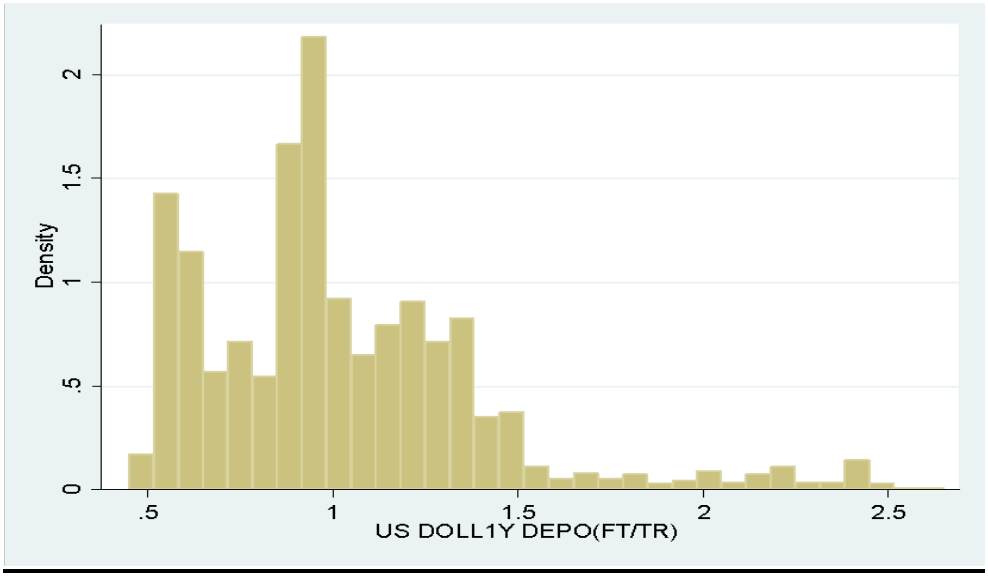
**Histogram for Total Bitcoins**



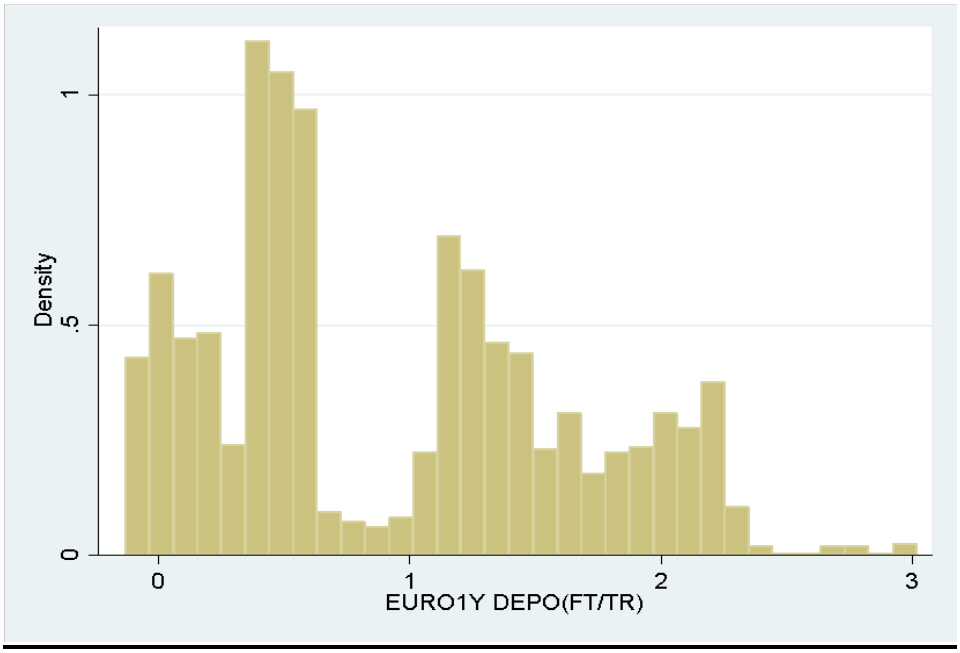
Such extreme high prices and intense fluctuations might be explained by strong inelastic demand and tight supply. Assuming that Bitcoin has some attractive features like the anonymity it provides to its users, the demand can exceed the mining supply. From the perspective of the supply, there are several issues there too. For example, the difficulty of mining might suddenly accelerate, or miners might engage in specific strategies. Alternatively, given the continuously growing investor interest, speculative demand might enter the market, with each trader believing that buying twenty or more times the mining cost doesn't matter, as long as someone else is willing to pay more than that. So judging by the sadden and extreme pick- ups in the volume and the value of trading bitcoins, the "greater fool" theory constitutes probably the best contender for explaining such intense fluctuations.

The price volatility seems to have little to do with fair value. Generally, when valuing cryptocurrencies there are a lot of problems and issues which differentiate their evaluation from other official currencies paths across the time. Such issues can be the technology behind cryptocurrencies like Bitcoin which cannot be easily valued. Thus, attempts to value Bitcoins are highly unsatisfactory and the assumptions that economists should make are inefficient.

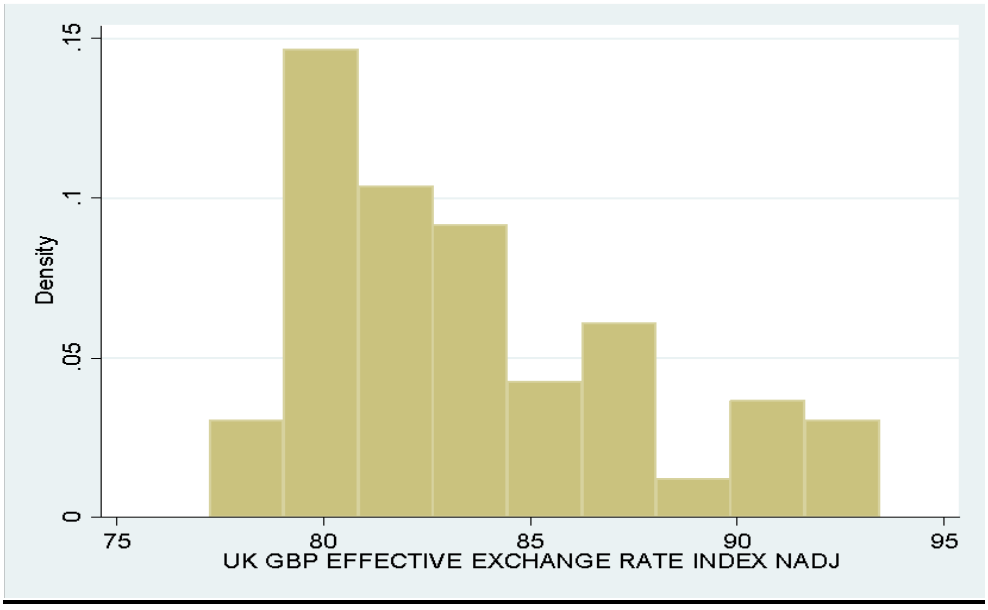
**Histogram of US dollar deposit rate for 1 year**



**Histogram of Euro deposit rate for 1 year**

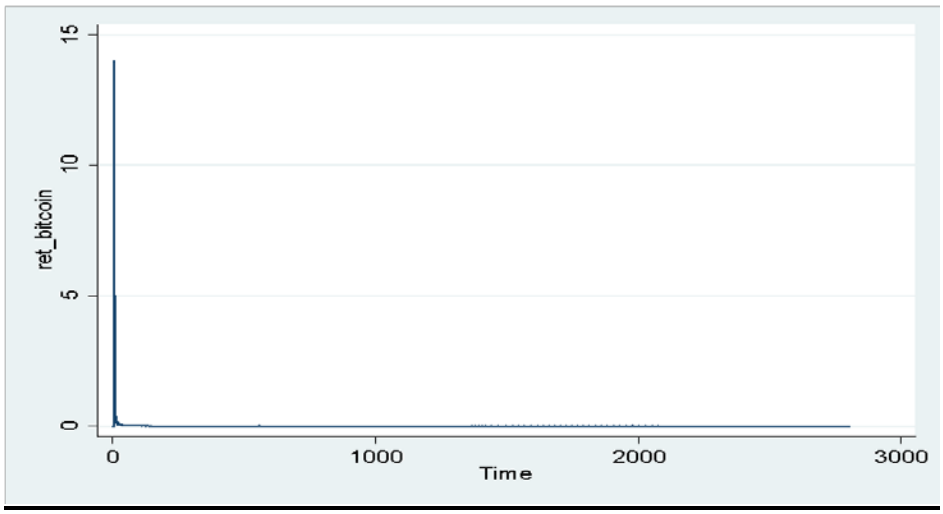



**Histogram of UK GBP exchange rate for 6 months**

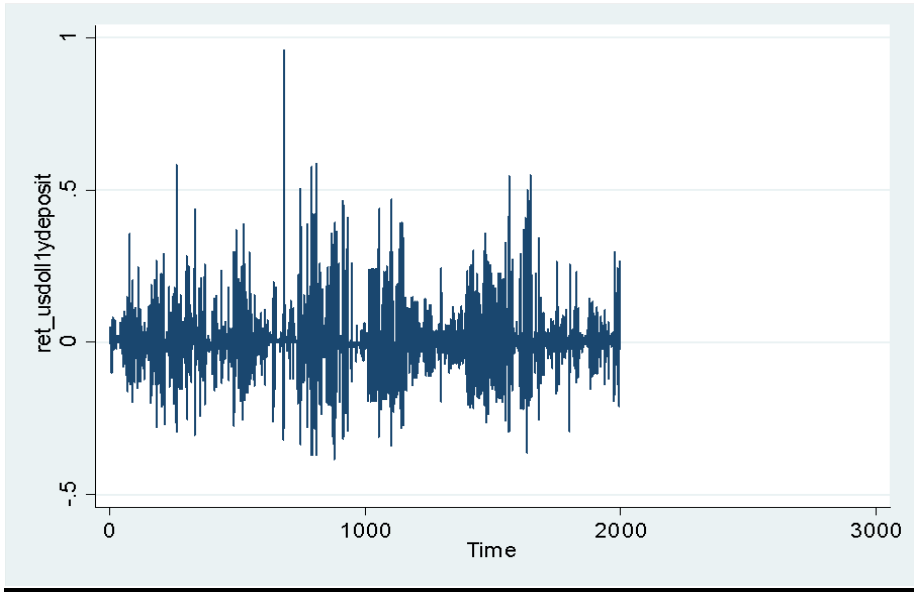


Looking now at the returns of the variables we have generated in Stata we can conclude that they appear to have many fluctuations across the years we examine,

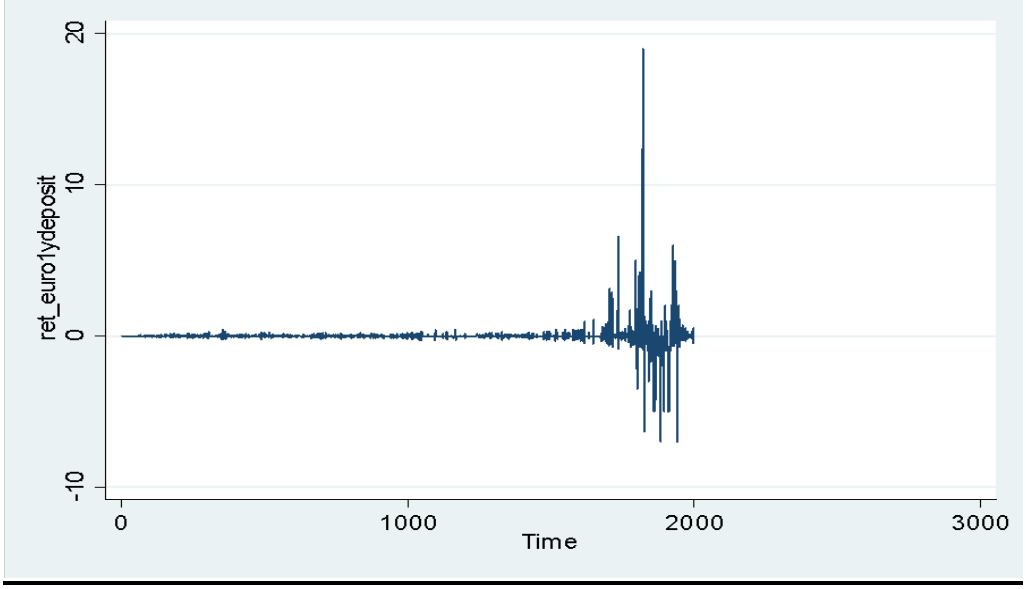
**Histogram of returns of Total Bitcoins**



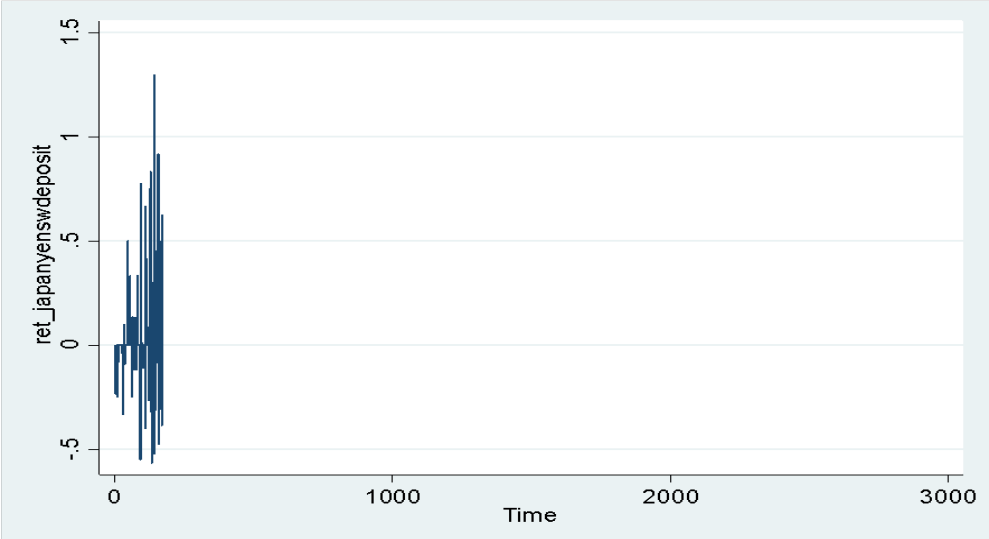

**Histogram of returns of US dollar deposit rate for 1 year**



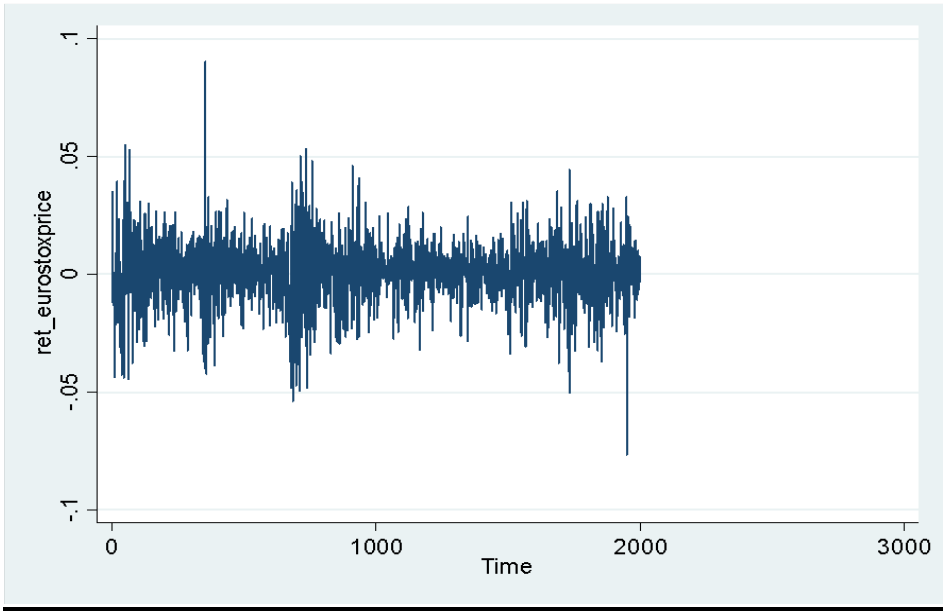
**Histogram of returns of Euro deposit rate for 1 year**



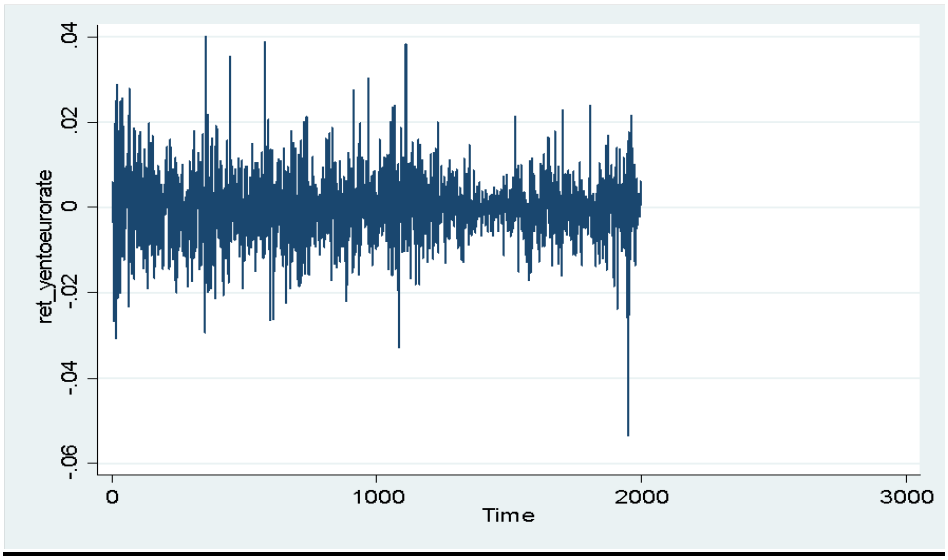

**Histogram of returns of Japanese Yen deposit rate for 6 months**



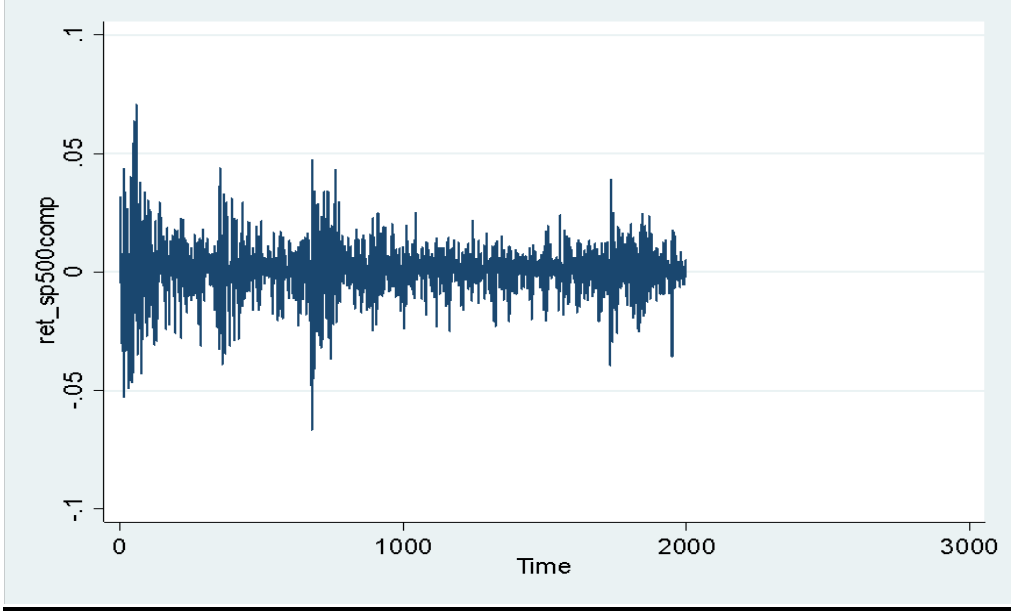
**Histogram for returns of Nikkei 225 stock average price index**




**Histogram of returns of Japanese Yen to Euro exchange rate**



**Histogram of returns of S&P 500 Composite Price Index**



**Augmented Dickey-Fuller test for unit-roots**

To avoid running spurious regressions, we proceeded to determine the appropriate time series model. Following the empirical statistical literature on exchange rate dynamics, we first examine the stationary properties of the time-series data using unit-root tests. In statistics, a unit root test tests whether a time series variable is non-stationary and possesses a unit root. The null hypothesis, (Ho) is generally defined as the presence of a unit root and the alternative hypothesis, (Hi) is either stationarity, or trend stationarity depending on the test used. The order of integration of the time series is assessed using the Augmented Dickey-Fuller Test, (ADF), with the number of lags selected on the basis of information criteria. Most variables exhibit significant evidence of unit-root I(1), which means integration of order 1 while there are certain variables that exhibit I(2).

Due to the existence of non-stationary time series in our case, we cannot directly adopt ordinary time-series regression model,(OLS), in order to analyze the Bitcoin determinants and their effects. More precisely, OLS applied in stationary variables may generate inconsistent estimation and spurious correlation. One way to address non-stationary time series is to apply a first difference model as we did in our sample. The maximum number of lags which is included in our dataset is k=3. Using as basic criterion the p-values we conclude if the variables in both tests are stationary or not. If the p-value of a variable is under the critical value of 0.05 then we reject the Ho and accept the Hi and thus the variable is stationary and vice versa. If our variable is not stationary we take first differences in order to convert it and put it as stationary then in our OLS model as we did in our sample.

Indicatively,

## Total Bitcoins

For lags=1:

Augmented Dickey-Fuller test for unit root  Number of obs = 2808

| | Test Statistic | 1% Critical Value | 5% Critical Value | 10% Critical Value |
|---|---|---|---|---|
| | | Z(t) has t-distribution | | |
| Z(t) | -4.836 | -2.328 | -1.645 | -1.282 |

p-value for Z(t) = 0.0000

For lags=2:

Augmented Dickey-Fuller test for unit root  Number of obs = 2807

| | Test Statistic | 1% Critical Value | 5% Critical Value | 10% Critical Value |
|---|---|---|---|---|
| | | Z(t) has t-distribution | | |
| Z(t) | -4.937 | -2.328 | -1.645 | -1.282 |

p-value for Z(t) = 0.0000

## USdoll 1y- deposit rate

For lags=1:

Augmented Dickey-Fuller test for unit root  Number of obs = 1997

| | Test Statistic | 1% Critical Value | 5% Critical Value | 10% Critical Value |
|---|---|---|---|---|
| | | Z(t) has t-distribution | | |
| Z(t) | -4.451 | -2.328 | -1.646 | -1.282 |

p-value for Z(t) = 0.0000

## Euro 1y- deposit rate

For lags=1:

Augmented Dickey-Fuller test for unit root — Number of obs = 1997

| | Test Statistic | 1% Critical Value | 5% Critical Value | 10% Critical Value |
|---|---|---|---|---|
| | | Z(t) has t-distribution | | |
| Z(t) | -2.651 | -2.328 | -1.646 | -1.282 |

p-value for Z(t) = 0.0040

For lags=2:

Augmented Dickey-Fuller test for unit root — Number of obs = 1996

| | Test Statistic | 1% Critical Value | 5% Critical Value | 10% Critical Value |
|---|---|---|---|---|
| | | Z(t) has t-distribution | | |
| Z(t) | -2.566 | -2.328 | -1.646 | -1.282 |

p-value for Z(t) = 0.0052

## Japan Yen 6-month deposit rate

For lags=1:

Augmented Dickey-Fuller test for unit root — Number of obs = 170

| | Test Statistic | 1% Critical Value | 5% Critical Value | 10% Critical Value |
|---|---|---|---|---|
| | | Z(t) has t-distribution | | |
| Z(t) | -5.290 | -2.349 | -1.654 | -1.287 |

p-value for Z(t) = 0.0000

For lags=2:

```
Augmented Dickey-Fuller test for unit root         Number of obs   =       169

                                 ------------ Z(t) has t-distribution ------------
                       Test         1% Critical       5% Critical      10% Critical
                     Statistic          Value             Value            Value
------------------------------------------------------------------------------
 Z(t)                -5.508            -2.349            -1.654           -1.287
------------------------------------------------------------------------------
p-value for Z(t) = 0.0000
```

## Nikkei 225 Stock Average Price Index

For lags=1:

```
Augmented Dickey-Fuller test for unit root         Number of obs   =      1997

                                 ------------ Z(t) has t-distribution ------------
                       Test         1% Critical       5% Critical      10% Critical
                     Statistic          Value             Value            Value
------------------------------------------------------------------------------
 Z(t)                -1.019            -2.328            -1.646           -1.282
------------------------------------------------------------------------------
p-value for Z(t) = 0.1542
```

For lags=2:

```
Augmented Dickey-Fuller test for unit root         Number of obs   =      1996

                                 ------------ Z(t) has t-distribution ------------
                       Test         1% Critical       5% Critical      10% Critical
                     Statistic          Value             Value            Value
------------------------------------------------------------------------------
 Z(t)                -1.036            -2.328            -1.646           -1.282
------------------------------------------------------------------------------
p-value for Z(t) = 0.1502
```

We then create a correlation matrix of all independent (xi's) variables in order to check if they are highly correlated between them. In the case of a high correlation between two independent variables, according the theory, I see values in the correlation coefficient, r, more than 0.6. Thus, it is a strong sign that I should omit one of them when forming our OLS model. Otherwise I might confront the problem of multicollinearity in the OLS results which will distort the interpretation of the OLS model.

The correlation matrix which was formed is the following,

| | totalb~s | us~ydepo | euro1y~o | ja~wdepo | ukgbpe~x | nikkei~x | eurost.. | japany~e | euroto~r | sp500c~x | sp500g~x | dowjon~x | nasdaq~x | opecoi~e |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| totalbitco~s | 1.0000 | | | | | | | | | | | | | |
| usdoll1ydepo | 0.1842 | 1.0000 | | | | | | | | | | | | |
| euro1ydepo | -0.9431 | -0.3118 | 1.0000 | | | | | | | | | | | |
| japanyensw~o | -0.0835 | -0.2438 | 0.3303 | 1.0000 | | | | | | | | | | |
| ukgbpeffec~x | 0.7516 | 0.0332 | -0.6374 | -0.0182 | 1.0000 | | | | | | | | | |
| nikkei225s~x | 0.3111 | -0.4869 | -0.0478 | 0.6556 | 0.4608 | 1.0000 | | | | | | | | |
| eurostoxxp~x | -0.1039 | -0.6512 | 0.3342 | 0.6144 | 0.1009 | 0.7997 | 1.0000 | | | | | | | |
| japanyento~e | 0.7712 | 0.1738 | -0.6235 | 0.3455 | 0.6103 | 0.5326 | 0.0366 | 1.0000 | | | | | | |
| eurotojapy~r | 0.7656 | 0.1673 | -0.6139 | 0.3580 | 0.5982 | 0.5302 | 0.0331 | 0.9941 | 1.0000 | | | | | |
| sp500compo~x | -0.0450 | -0.6401 | 0.2658 | 0.6433 | 0.1120 | 0.8341 | 0.9654 | 0.1169 | 0.1256 | 1.0000 | | | | |
| sp500growt~x | 0.0709 | -0.5926 | 0.1327 | 0.5698 | 0.1800 | 0.8310 | 0.9406 | 0.1696 | 0.1772 | 0.9848 | 1.0000 | | | |
| dowjonesin~x | -0.2251 | -0.6621 | 0.4363 | 0.6630 | -0.0117 | 0.7745 | 0.9527 | -0.0080 | 0.0031 | 0.9794 | 0.9391 | 1.0000 | | |
| nasdaqcomp~x | 0.4153 | -0.4903 | -0.1900 | 0.5092 | 0.4636 | 0.8848 | 0.8306 | 0.4392 | 0.4445 | 0.8833 | 0.9300 | 0.7809 | 1.0000 | |
| opecoilbas~e | 0.6626 | -0.0447 | -0.4302 | 0.3728 | 0.7421 | 0.6054 | 0.2241 | 0.7665 | 0.7710 | 0.2324 | 0.2499 | 0.1353 | 0.5194 | 1.0000 |
| cmciwticru.. | 0.6396 | -0.1069 | -0.3994 | 0.3677 | 0.7327 | 0.6122 | 0.2871 | 0.7111 | 0.7122 | 0.2812 | 0.2961 | 0.1839 | 0.5543 | 0.9785 |
| cmcigold1y~x | 0.5849 | -0.2299 | -0.3809 | 0.2154 | 0.5560 | 0.5340 | 0.2908 | 0.5549 | 0.5503 | 0.2600 | 0.2716 | 0.1644 | 0.4977 | 0.7921 |

| | cmciwt.. | cmcigo.. |
|---|---|---|
| cmciwticru.. | 1.0000 | |
| cmcigold1y~x | 0.8470 | 1.0000 |

In most variables there is no strong correlation between them so I do not have problem. In some cases, though, we see that the correlation coefficient r is very high, as in the example of the dow jones industrial price with s&p500 composite and s&p500 growth variable with r = 0.9794 and r = 0.9391 respectively. Thus, conforming with the model requirements we should drop one of them when running the OLS regression as we did and omitted the s&p500 growth variable.

After having concluded which are the appropriate independent variables, (xi's), to keep in order to use them in our OLS model against our dependent variable (y) which is being examined and in this case is the total number of Bitcoins, we are able to run the regression.

In fact, according to econometrics theory, the OLS model is based on several assumptions and when these are satisfied, then the regression estimators which are the xi's are optimal. And by optimal we mean unbiased, efficient, and consistent. More precisely, this model expresses the value of a predictand variable which is the y, as a linear function of one or more predictor variables and an error term. The first to check in the OLS model is the coefficient of determination, R-squared.

The explanatory power of the regression is summarized by its R-squared value, also called the coefficient of determination and is often described as the proportion of variance explained by the regression. It is important to bear in mind that a high R-squared does not mean causation. Further, the relative values of the sums-of-squares terms indicate how good the regression is in terms of fitting the calibration data.

So, we take the following output,

| Source | SS | df | MS | | |
|---|---|---|---|---|---|
| Model | 1.3729e+12 | 13 | 1.0561e+11 | Number of obs | = 90 |
| Residual | 6.6494e+11 | 76 | 8.7492e+09 | F(13, 76) | = 12.07 |
| | | | | Prob > F | = 0.0000 |
| | | | | R-squared | = 0.6737 |
| | | | | Adj R-squared | = 0.6179 |
| Total | 2.0378e+12 | 89 | 2.2897e+10 | Root MSE | = 93537 |

| totalbitcoins | Coef. | Std. Err. | t | P>\|t\| | [95% Conf. | Interval] |
|---|---|---|---|---|---|---|
| usdoll1ydepo | 102677.2 | 51434.64 | 2.00 | 0.049 | 236.2298 | 205118.2 |
| euro1ydepo | | | | | | |
| D1. | 127186.7 | 222882.1 | 0.57 | 0.570 | -316721.5 | 571094.9 |
| japanyenswdepo | -153805.9 | 229989.4 | -0.67 | 0.506 | -611869.4 | 304257.6 |
| ukgbpeffectiveexchangerateindex | 28422.45 | 2509.458 | 11.33 | 0.000 | 23424.44 | 33420.47 |
| nikkei225stockavgpriceindex | | | | | | |
| D1. | 137.8015 | 65.0819 | 2.12 | 0.038 | 8.1797 | 267.4234 |
| eurostoxxpriceindex | | | | | | |
| D1. | -2693.215 | 4196.354 | -0.64 | 0.523 | -11050.98 | 5664.549 |
| japanyentoeurexchangerate | | | | | | |
| D1. | 464.6274 | 13964.41 | 0.03 | 0.974 | -27347.91 | 28277.16 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| D1. | 11486.01 | 15540.66 | 0.74 | 0.462 | -19465.89 | 42437.92 |
| sp500compositepriceindex | | | | | | |
| D1. | 2820.6 | 3478.912 | 0.81 | 0.420 | -4108.253 | 9749.453 |
| dowjonesindustrialspriceindex | | | | | | |
| D1. | -261.6092 | 423.6628 | -0.62 | 0.539 | -1105.407 | 582.1884 |
| opecoilbasketprice | | | | | | |
| D1. | -4397.985 | 13979.53 | -0.31 | 0.754 | -32240.64 | 23444.67 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| D1. | -1130.923 | 791.4055 | -1.43 | 0.157 | -2707.143 | 445.2979 |
| cmcigold1ypiusdpriceindex | | | | | | |
| D1. | 1288.953 | 684.8658 | 1.88 | 0.064 | -75.07586 | 2652.981 |
| _cons | -2349827 | 248352.7 | -9.46 | 0.000 | -2844464 | -1855190 |

The Adjusted R-Squared value is always a bit lower than the Multiple R-Squared value, because it reflects model complexity, the number of variables, as it relates to the data and is consequently a more accurate measure of model performance. Thus, adding an additional explanatory variable to the model would increase the Multiple R-Squared value, something that would not be appropriate for the model.

In our statistical sample, the Multiple R-squared value is 0.6737 and the adjusted R-squared value is 0.6179 which show that our model is robust with a good explanatory ability for the whole regression model. More precisely, the independent variables, xi's, seem to explain and describe efficiently the independent variable, y. So, it is proved that the variables we chose for our dataset are the right ones and relate significantly to our independent variable, the Bitcoins, that we are trying to examine. Furthermore, as adj. R-square value is 0.6179 explains approximately 62% of the variation in the value of Bitcoins.

On the other side, the coefficient for each explanatory variable reflects both the strength and type of relationship the explanatory variable has to the dependent variable. When the sign associated with the coefficient is negative, the relationship is negative, while when positive, the relationship is positive.

By looking at the results we see that all the xi's are positive except from the japanyenswdepo, eurostoxxpriceindex, dowjonesindustrialspriceindex, opecoilbasketprice and cmciwticruseoil1ypiusdpriceindex variables that relate with total bitcoins in a negative way. And by negative we mean that the higher the value of Bitcoins the lower the price for these indexes and vice versa. The coefficient reflects the expected change in the dependent variable for every 1 unit change in the associated explanatory variable, holding all other variables constant. For example, if the Bitcoin rises per 1 point then the yearly deposit rate of yen will drop by 153805.8 points along with the stock index rate of euro which will drop by 2693.215, the stock industrial index of Dow Jones that will drop by 261.6092 and so on, but holding all other variables constant.

On the other hand, in the case of Bitcoin rise per 1 unit, we observe according the results that the yearly deposit rate of dollar increases per 102677.2 points, the yearly deposit rate of euro increases per 127186.7 points, the exchange rate of gbp per 28422.45 points, the euro to yen exchange rate per 28422.45 points and so on, holding all other variables constant. So, we can conclude that certain commodities like the oil influence negatively and vice versa the value of Bitcoins while the several exchange and foreign currency interest rates are affecting the Bitcoin's value in a positive way. There is no economic theory behind this relation yet but this result shows that individuals who tend to prefer investing in foreign currencies would invest in Bitcoin because they tend to consider it as a currency too rather than commodity. Although, individuals who prefer investing in commodities do not seem to trust Bitcoin but they could use it as a hedging tool in their portfolio.

In the end, the t- test is used to assess whether or not an explanatory variable is statistically significant against the relative p-values. The null hypothesis is that the coefficient is equal to zero and that the coefficient of the independent variable shows that it is not statistical significant. If Ho is rejected then the independent variable is statistical significant. In our dataset the results of our model show that only the yen interest rate, the euro stock index, the exchange rate of yen to euro, the dow jones industrial stock index, the opec oil basket index and the cmci wti crude oil index are statistical significant for the price of Bitcoin. And from theory ,we know that an explanatory variable associated with a statistically significant coefficient is important to the regression model if the economic theory supports a valid relationship with the dependent variable, if the relationship being modeled is primarily linear, and if the variable is not redundant to any other explanatory variables in the model.

We have, also, performed the Johansen test in our dataset in order to formally test for the existence of a cointegrating vector.

The results of the Johansen tests are the following,

Johansen tests for cointegration

Trend: constant — Number of obs = 88
Sample: 4 - 91 — Lags = 2

| maximum rank | parms | LL | eigenvalue | trace statistic | 5% critical value |
|---|---|---|---|---|---|
| 0 | 210 | -2898.3192 | . | 575.0533* | . |
| 1 | 237 | -2851.7753 | 0.65279 | 481.9654 | . |
| 2 | 262 | -2807.0433 | 0.63819 | 392.5014 | . |
| 3 | 285 | -2775.8751 | 0.50755 | 330.1652 | 277.71 |
| 4 | 306 | -2746.2687 | 0.48976 | 270.9522 | 233.13 |
| 5 | 325 | -2717.9151 | 0.47502 | 214.2451 | 192.89 |
| 6 | 342 | -2691.8227 | 0.44734 | 162.0602 | 156.00 |
| 7 | 357 | -2670.388 | 0.38563 | 119.1908 | 124.24 |
| 8 | 370 | -2650.7913 | 0.35942 | 79.9974 | 94.15 |
| 9 | 381 | -2636.9206 | 0.27039 | 52.2562 | 68.52 |
| 10 | 390 | -2625.6402 | 0.22615 | 29.6953 | 47.21 |
| 11 | 397 | -2618.6936 | 0.14605 | 15.8021 | 29.68 |
| 12 | 402 | -2614.241 | 0.09624 | 6.8969 | 15.41 |
| 13 | 405 | -2610.8711 | 0.07373 | 0.1571 | 3.76 |
| 14 | 406 | -2610.7926 | 0.00178 | | |

| maximum rank | parms | LL | eigenvalue | max statistic | 5% critical value |
|---|---|---|---|---|---|
| 0 | 210 | -2898.3192 | . | 93.0879 | . |
| 1 | 237 | -2851.7753 | 0.65279 | 89.4640 | . |
| 2 | 262 | -2807.0433 | 0.63819 | 62.3362 | . |
| 3 | 285 | -2775.8751 | 0.50755 | 59.2130 | 68.83 |
| 4 | 306 | -2746.2687 | 0.48976 | 56.7071 | 62.81 |
| 5 | 325 | -2717.9151 | 0.47502 | 52.1849 | 57.12 |
| 6 | 342 | -2691.8227 | 0.44734 | 42.8694 | 51.42 |
| 7 | 357 | -2670.388 | 0.38563 | 39.1934 | 45.28 |
| 8 | 370 | -2650.7913 | 0.35942 | 27.7412 | 39.37 |
| 9 | 381 | -2636.9206 | 0.27039 | 22.5609 | 33.46 |
| 10 | 390 | -2625.6402 | 0.22615 | 13.8932 | 27.07 |
| 11 | 397 | -2618.6936 | 0.14605 | 8.9052 | 20.97 |
| 12 | 402 | -2614.241 | 0.09624 | 6.7398 | 14.07 |
| 13 | 405 | -2610.8711 | 0.07373 | 0.1571 | 3.76 |
| 14 | 406 | -2610.7926 | 0.00178 | | |

.

According to the results taken from the Johansen test, we can conclude that we strongly reject the null hypothesis, Ho, of no cointegrating vector. Therefore, the Johansen tests confirms what we have assumed from the beginning, the presence of cointegration in most of our variables. We have also calculated the returns of our variables which if put in a portfolio with a percentage of Bitcoins could create a certain profit.

We, also, use the ARCH and GARCH models in order to estimate the effects of volatility on Bitcoin price. We first set the data up for the ARCH(1,1) model after making the non-stationary variables stationary with first differences since Standard ARCH and GARCH models assume stationarity. Not to mention that before performing these models we should have run the OLS model. At the OLS model, we compare the results with the p-values and thus we reject the null hypothesis. So, we are able then to run the ARCH and GARCH models. The results show that there may be ARCH effects and especially extreme volatility in the value of our variables.

Finally, we perform a VAR model. More precisely, vector autoregression (VAR) is a stochastic process model used to capture the linear interdependencies among multiple time series. VAR models generalize the univariate autoregressive model (AR model) by allowing for more than one evolving variable. All variables in a VAR enter the model in the same way: each variable has an equation explaining its evolution based on its own lagged values, the lagged values of the other model variables, and an error term. VAR modeling does not require as much knowledge about the forces influencing a variable as do structural models with simultaneous equations: the only prior knowledge required is a list of variables which can be hypothesized to affect each other intertemporally.

A VAR model describes the evolution of a set of $k$ variables over the same sample period ($t = 1, ..., T$) as a linear function of only their past values. The variables are collected in a $k \times 1$ vector $y_t$, which has as the $i^{th}$ element, $y_{i,t}$, the observation at time "t"

of the $i^{th}$ variable. Moreover, the properties of the VAR model are usually summarized using structural analysis using Granger causality test, impulse responses, and forecast error variance decompositions.

In our dataset the results are the following,

Vector autoregression

| | | | |
|---|---|---|---|
| Sample: 3 - 91 | | Number of obs | = 89 |
| Log likelihood = | -2923.405 | AIC | = 73.58214 |
| FPE = | 1.11e+16 | HQIC | = 77.53818 |
| Det(Sigma_ml) = | 3.23e+12 | SBIC | = 83.39687 |

| Equation | Parms | RMSE | R-sq | chi2 | P>chi2 |
|---|---|---|---|---|---|
| totalbitcoins | 27 | 797.331 | 1.0000 | 4480069 | 0.0000 |
| usdoll1ydepo | 27 | .115767 | 0.7969 | 349.2296 | 0.0000 |
| euro1ydepo | 27 | .043295 | 0.9894 | 8269.073 | 0.0000 |
| ukgbpeffective~x | 27 | 1.113 | 0.9488 | 1650.36 | 0.0000 |
| nikkei225stock~x | 27 | 125.445 | 0.9692 | 2800.663 | 0.0000 |
| eurostoxxprice~x | 27 | 4.04512 | 0.9519 | 1761.57 | 0.0000 |
| japanyentoeure~e | 27 | 1.36426 | 0.9666 | 2574.871 | 0.0000 |
| eurotojapyenfx~r | 27 | 1.40474 | 0.9639 | 2378.021 | 0.0000 |
| sp500composite~x | 27 | 16.8847 | 0.9399 | 1391.127 | 0.0000 |
| dowjonesindust~x | 27 | 144.044 | 0.9480 | 1622.943 | 0.0000 |
| opecoilbasketp~e | 27 | .665779 | 0.9802 | 4406.943 | 0.0000 |
| cmciwticrudeoi~x | 27 | 18.393 | 0.9489 | 1652.076 | 0.0000 |
| cmcigold1ypius~x | 27 | 16.0419 | 0.9073 | 871.0066 | 0.0000 |

| | Coef. | Std. Err. | z | P>\|z\| | [95% Conf. | Interval] |
|---|---|---|---|---|---|---|
| totalbitcoins | | | | | | |
| totalbitcoins | | | | | | |
| L1. | 1.329425 | .0819859 | 16.22 | 0.000 | 1.168736 | 1.490115 |
| L2. | -.3451876 | .0822354 | -4.20 | 0.000 | -.5063659 | -.1840092 |
| usdoll1ydepo | | | | | | |
| L1. | 798.1974 | 679.2678 | 1.18 | 0.240 | -533.143 | 2129.538 |
| L2. | -1270.533 | 621.4034 | -2.04 | 0.041 | -2488.462 | -52.60504 |
| euro1ydepo | | | | | | |
| L1. | -4739.696 | 1973.426 | -2.40 | 0.016 | -8607.539 | -871.8522 |
| L2. | -2059.644 | 1956.36 | -1.05 | 0.292 | -5894.039 | 1774.752 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | -355.9483 | 73.71872 | -4.83 | 0.000 | -500.4344 | -211.4623 |
| L2. | 379.4033 | 75.49715 | 5.03 | 0.000 | 231.4316 | 527.375 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .4418419 | .7427755 | 0.59 | 0.552 | -1.013971 | 1.897655 |
| L2. | 1.129783 | .6350988 | 1.78 | 0.075 | -.1149879 | 2.374554 |
| eurostoxxpriceindex | | | | | | |
| L1. | -83.36047 | 36.09275 | -2.31 | 0.021 | -154.101 | -12.61998 |
| L2. | 50.46466 | 36.58784 | 1.38 | 0.168 | -21.24618 | 122.1755 |
| japanyentoeurexchangerate | | | | | | |
| L1. | 299.8645 | 163.6338 | 1.83 | 0.067 | -20.85178 | 620.5808 |
| L2. | -243.7453 | 149.7012 | -1.63 | 0.103 | -537.1543 | 49.66376 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | -200.2126 | 160.6802 | -1.25 | 0.213 | -515.1399 | 114.7147 |
| L2. | 33.34463 | 169.5453 | 0.20 | 0.844 | -298.958 | 365.6473 |
| sp500compositepriceindex | | | | | | |
| L1. | -80.47128 | 28.19799 | -2.85 | 0.004 | -135.7383 | -25.20424 |
| L2. | 107.2078 | 29.72991 | 3.61 | 0.000 | 48.93828 | 165.4774 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | 9.641973 | 3.336123 | 2.89 | 0.004 | 3.103292 | 16.18065 |
| L2. | -12.64267 | 3.5651 | -3.55 | 0.000 | -19.63014 | -5.655205 |
| opecoilbasketprice | | | | | | |
| L1. | 55.71596 | 203.3039 | 0.27 | 0.784 | -342.7524 | 454.1843 |
| L2. | 281.3337 | 136.9589 | 2.05 | 0.040 | 12.89915 | 549.7682 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | -13.93365 | 8.740786 | -1.59 | 0.111 | -31.06527 | 3.197978 |
| L2. | -9.94467 | 11.57406 | -0.86 | 0.390 | -32.6294 | 12.74006 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | 10.90428 | 6.644147 | 1.64 | 0.101 | -2.118014 | 23.92657 |
| L2. | 1.121657 | 7.352283 | 0.15 | 0.879 | -13.28855 | 15.53187 |
| _cons | 18317.26 | 10155.19 | 1.80 | 0.071 | -1586.553 | 38221.06 |

| | | | | | | |
|---|---|---|---|---|---|---|
| usdoll1ydepo | | | | | | |
| totalbitcoins | | | | | | |
| L1. | -.0000242 | .0000119 | -2.03 | 0.042 | -.0000475 | -8.35e-07 |
| L2. | .0000269 | .0000119 | 2.25 | 0.024 | 3.52e-06 | .0000503 |
| usdoll1ydepo | | | | | | |
| L1. | .3190864 | .0986254 | 3.24 | 0.001 | .1257842 | .5123886 |
| L2. | -.0126073 | .0902239 | -0.14 | 0.889 | -.1894428 | .1642282 |
| euro1ydepo | | | | | | |
| L1. | -.1089135 | .286529 | -0.38 | 0.704 | -.6704999 | .452673 |
| L2. | .9123821 | .2840512 | 3.21 | 0.001 | .355652 | 1.469112 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .002918 | .0107035 | 0.27 | 0.785 | -.0180604 | .0238965 |
| L2. | -.0008753 | .0109617 | -0.08 | 0.936 | -.0223598 | .0206093 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .00008 | .0001078 | 0.74 | 0.458 | -.0001314 | .0002914 |
| L2. | 2.44e-07 | .0000922 | 0.00 | 0.998 | -.0001805 | .000181 |
| eurostoxxpriceindex | | | | | | |
| L1. | -.0072941 | .0052404 | -1.39 | 0.164 | -.0175651 | .002977 |
| L2. | .0051226 | .0053123 | 0.96 | 0.335 | -.0052893 | .0155346 |
| japanyentoeurexchangerate | | | | | | |
| L1. | .0028925 | .0237586 | 0.12 | 0.903 | -.0436735 | .0494584 |
| L2. | -.015935 | .0217357 | -0.73 | 0.463 | -.0585362 | .0266661 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | .0032182 | .0233297 | 0.14 | 0.890 | -.0425072 | .0489437 |
| L2. | .0079492 | .0246169 | 0.32 | 0.747 | -.040299 | .0561975 |
| sp500compositepriceindex | | | | | | |
| L1. | .0028405 | .0040942 | 0.69 | 0.488 | -.0051839 | .0108649 |
| L2. | -.0055238 | .0043166 | -1.28 | 0.201 | -.0139841 | .0029366 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | -.0005009 | .0004844 | -1.03 | 0.301 | -.0014503 | .0004485 |
| L2. | .0005148 | .0005176 | 0.99 | 0.320 | -.0004998 | .0015293 |
| opecoilbasketprice | | | | | | |
| L1. | .0142699 | .0295184 | 0.48 | 0.629 | -.0435852 | .0721249 |
| L2. | -.0726673 | .0198856 | -3.65 | 0.000 | -.1116423 | -.0336923 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | -.0000344 | .0012691 | -0.03 | 0.978 | -.0025218 | .002453 |
| L2. | .0023759 | .0016805 | 1.41 | 0.157 | -.0009177 | .0056696 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | -.000614 | .0009647 | -0.64 | 0.524 | -.0025047 | .0012768 |
| L2. | -.0021204 | .0010675 | -1.99 | 0.047 | -.0042126 | -.0000281 |
| _cons | 6.947749 | 1.47447 | 4.71 | 0.000 | 4.057842 | 9.837656 |

| | | | | | | |
|---|---|---|---|---|---|---|
| euro1ydepo | | | | | | |
| totalbitcoins | | | | | | |
| L1. | -5.60e-06 | 4.45e-06 | -1.26 | 0.209 | -.0000143 | 3.13e-06 |
| L2. | 4.39e-06 | 4.47e-06 | 0.98 | 0.325 | -4.36e-06 | .0000131 |
| usdoll1ydepo | | | | | | |
| L1. | .0075735 | .0368843 | 0.21 | 0.837 | -.0647185 | .0798655 |
| L2. | -.0010533 | .0337423 | -0.03 | 0.975 | -.067187 | .0650804 |
| euro1ydepo | | | | | | |
| L1. | .4784501 | .1071573 | 4.46 | 0.000 | .2684256 | .6884746 |
| L2. | .071617 | .1062307 | 0.67 | 0.500 | -.1365913 | .2798253 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .003111 | .0040029 | 0.78 | 0.437 | -.0047346 | .0109566 |
| L2. | -.0008757 | .0040995 | -0.21 | 0.831 | -.0089106 | .0071592 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .0000115 | .0000403 | 0.29 | 0.775 | -.0000675 | .0000906 |
| L2. | -.0000513 | .0000345 | -1.49 | 0.137 | -.0001189 | .0000163 |
| eurostoxxpriceindex | | | | | | |
| L1. | .0012119 | .0019598 | 0.62 | 0.536 | -.0026293 | .0050532 |
| L2. | -.0002211 | .0019867 | -0.11 | 0.911 | -.004115 | .0036729 |
| japanyentoeurexchangerate | | | | | | |
| L1. | -.0149231 | .0088853 | -1.68 | 0.093 | -.032338 | .0024918 |
| L2. | .0153334 | .0081288 | 1.89 | 0.059 | -.0005988 | .0312655 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | .0125786 | .008725 | 1.44 | 0.149 | -.004522 | .0296792 |
| L2. | -.0099687 | .0092063 | -1.08 | 0.279 | -.0280128 | .0080754 |
| sp500compositepriceindex | | | | | | |
| L1. | -.0001903 | .0015312 | -0.12 | 0.901 | -.0031913 | .0028108 |
| L2. | .0007143 | .0016143 | 0.44 | 0.658 | -.0024498 | .0038783 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | 4.93e-06 | .0001812 | 0.03 | 0.978 | -.0003501 | .00036 |
| L2. | -.0000328 | .0001936 | -0.17 | 0.866 | -.0004122 | .0003466 |
| opecoilbasketprice | | | | | | |
| L1. | -.0161177 | .0110394 | -1.46 | 0.144 | -.0377546 | .0055192 |
| L2. | .0080213 | .0074369 | 1.08 | 0.281 | -.0065548 | .0225973 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | .0012713 | .0004746 | 2.68 | 0.007 | .0003411 | .0022016 |
| L2. | -.0001022 | .0006285 | -0.16 | 0.871 | -.0013339 | .0011296 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | .0000797 | .0003608 | 0.22 | 0.825 | -.0006274 | .0007868 |
| L2. | -.0003925 | .0003992 | -0.98 | 0.326 | -.001175 | .00039 |
| _cons | .0389923 | .5514285 | 0.07 | 0.944 | -1.041788 | 1.119772 |

| | | | | | | |
|---|---|---|---|---|---|---|
| ukgbpeffectiveexchangerateindex | | | | | | |
| totalbitcoins | | | | | | |
| L1. | .0001979 | .0001144 | 1.73 | 0.084 | -.0000264 | .0004223 |
| L2. | -.0002178 | .0001148 | -1.90 | 0.058 | -.0004428 | 7.18e-06 |
| usdoll1ydepo | | | | | | |
| L1. | 1.020496 | .9481984 | 1.08 | 0.282 | -.837939 | 2.87893 |
| L2. | -2.410266 | .8674248 | -2.78 | 0.005 | -4.110387 | -.7101444 |
| euro1ydepo | | | | | | |
| L1. | -5.158442 | 2.75473 | -1.87 | 0.061 | -10.55761 | .2407292 |
| L2. | 2.271857 | 2.730908 | 0.83 | 0.405 | -3.080625 | 7.624338 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .9126326 | .1029049 | 8.87 | 0.000 | .7109427 | 1.114322 |
| L2. | -.0596804 | .1053874 | -0.57 | 0.571 | -.266236 | .1468751 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .0031406 | .0010368 | 3.03 | 0.002 | .0011084 | .0051727 |
| L2. | .0002437 | .0008865 | 0.27 | 0.783 | -.0014939 | .0019813 |
| eurostoxxpriceindex | | | | | | |
| L1. | .0046369 | .0503823 | 0.09 | 0.927 | -.0941107 | .1033844 |
| L2. | -.0923659 | .0510734 | -1.81 | 0.071 | -.192468 | .0077362 |
| japanyentoeurexchangerate | | | | | | |
| L1. | -.4132324 | .2284184 | -1.81 | 0.070 | -.8609243 | .0344594 |
| L2. | -.0250267 | .2089698 | -0.12 | 0.905 | -.4346 | .3845467 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | .5096581 | .2242954 | 2.27 | 0.023 | .0700471 | .9492691 |
| L2. | -.1412372 | .2366704 | -0.60 | 0.551 | -.6051027 | .3226283 |
| sp500compositepriceindex | | | | | | |
| L1. | .1464432 | .0393619 | 3.72 | 0.000 | .0692953 | .2235912 |
| L2. | -.0384249 | .0415004 | -0.93 | 0.355 | -.1197641 | .0429143 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | -.0193305 | .0046569 | -4.15 | 0.000 | -.0284579 | -.0102031 |
| L2. | .0068099 | .0049766 | 1.37 | 0.171 | -.002944 | .0165638 |
| opecoilbasketprice | | | | | | |
| L1. | .8171819 | .2837945 | 2.88 | 0.004 | .260955 | 1.373409 |
| L2. | -.4384902 | .1911827 | -2.29 | 0.022 | -.8132013 | -.0637791 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | -.0247108 | .0122014 | -2.03 | 0.043 | -.048625 | -.0007965 |
| L2. | .0248115 | .0161564 | 1.54 | 0.125 | -.0068544 | .0564774 |



| | | | | | | |
|---|---|---|---|---|---|---|
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | .0092089 | .0092746 | 0.99 | 0.321 | -.0089691 | .0273868 |
| L2. | -.0263159 | .0102631 | -2.56 | 0.010 | -.0464313 | -.0062006 |

| | | | | | | |
|---|---|---|---|---|---|---|
| nikkei225stockavgpriceindex | | | | | | |
| totalbitcoins | | | | | | |
| L1. | -.0002686 | .012899 | -0.02 | 0.983 | -.0255501 | .0250129 |
| L2. | .0021977 | .0129382 | 0.17 | 0.865 | -.0231607 | .0275561 |
| usdoll1ydepo | | | | | | |
| L1. | -267.7414 | 106.8702 | -2.51 | 0.012 | -477.2032 | -58.27962 |
| L2. | 62.03766 | 97.76635 | 0.63 | 0.526 | -129.5809 | 253.6562 |
| euro1ydepo | | | | | | |
| L1. | 537.8993 | 310.4821 | 1.73 | 0.083 | -70.63436 | 1146.433 |
| L2. | -105.3294 | 307.7971 | -0.34 | 0.732 | -708.6007 | 497.9419 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | 17.33073 | 11.59828 | 1.49 | 0.135 | -5.40148 | 40.06293 |
| L2. | -11.60291 | 11.87808 | -0.98 | 0.329 | -34.88352 | 11.67771 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .2207657 | .116862 | 1.89 | 0.059 | -.0082796 | .449811 |
| L2. | .0640402 | .0999211 | 0.64 | 0.522 | -.1318014 | .2598819 |
| eurostoxxpriceindex | | | | | | |
| L1. | 12.65203 | 5.678527 | 2.23 | 0.026 | 1.522324 | 23.78174 |
| L2. | -14.35697 | 5.75642 | -2.49 | 0.013 | -25.63934 | -3.074592 |
| japanyentoeurexchangerate | | | | | | |
| L1. | 31.99737 | 25.74475 | 1.24 | 0.214 | -18.46141 | 82.45615 |
| L2. | 42.31845 | 23.55272 | 1.80 | 0.072 | -3.844036 | 88.48094 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | -8.852652 | 25.28005 | -0.35 | 0.726 | -58.40064 | 40.69534 |
| L2. | -42.81388 | 26.67482 | -1.61 | 0.108 | -95.09557 | 9.4678 |
| sp500compositepriceindex | | | | | | |
| L1. | -1.211167 | 4.436432 | -0.27 | 0.785 | -9.906415 | 7.48408 |
| L2. | -2.430821 | 4.677452 | -0.52 | 0.603 | -11.59846 | 6.736816 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | .6639815 | .5248773 | 1.27 | 0.206 | -.364759 | 1.692722 |
| L2. | .3116576 | .5609026 | 0.56 | 0.578 | -.7876913 | 1.411006 |
| opecoilbasketprice | | | | | | |
| L1. | 18.85402 | 31.98611 | 0.59 | 0.556 | -43.8376 | 81.54565 |
| L2. | 14.39367 | 21.54795 | 0.67 | 0.504 | -27.83955 | 56.62688 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | .2180651 | 1.375201 | 0.16 | 0.874 | -2.47728 | 2.91341 |
| L2. | -1.979352 | 1.820964 | -1.09 | 0.277 | -5.548375 | 1.589672 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | -.9461177 | 1.045334 | -0.91 | 0.365 | -2.994934 | 1.102699 |
| L2. | .4297779 | 1.156746 | 0.37 | 0.710 | -1.837402 | 2.696958 |
| _cons | -1829.459 | 1597.732 | -1.15 | 0.252 | -4960.955 | 1302.038 |

| | | | | | | |
|---|---|---|---|---|---|---|
| eurostoxxpriceindex | | | | | | |
| totalbitcoins | | | | | | |
| L1. | -.0005335 | .0004159 | -1.28 | 0.200 | -.0013488 | .0002817 |
| L2. | .0005904 | .0004172 | 1.42 | 0.157 | -.0002274 | .0014081 |
| usdoll1ydepo | | | | | | |
| L1. | -1.272501 | 3.446149 | -0.37 | 0.712 | -8.026828 | 5.481827 |
| L2. | 4.615012 | 3.152584 | 1.46 | 0.143 | -1.563939 | 10.79396 |
| euro1ydepo | | | | | | |
| L1. | -.3128681 | 10.01184 | -0.03 | 0.975 | -19.93571 | 19.30997 |
| L2. | 10.2463 | 9.925259 | 1.03 | 0.302 | -9.206845 | 29.69945 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .2660841 | .3739993 | 0.71 | 0.477 | -.466941 | .9991091 |
| L2. | -.4021553 | .3830219 | -1.05 | 0.294 | -1.152864 | .3485537 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | -.0010405 | .0037683 | -0.28 | 0.782 | -.0084263 | .0063454 |
| L2. | -.0007883 | .0032221 | -0.24 | 0.807 | -.0071034 | .0055269 |
| eurostoxxpriceindex | | | | | | |
| L1. | .5043372 | .1831104 | 2.75 | 0.006 | .1454475 | .8632269 |
| L2. | .0289374 | .1856221 | 0.16 | 0.876 | -.3348752 | .3927501 |
| japanyentoeurexchangerate | | | | | | |
| L1. | .4571493 | .8301678 | 0.55 | 0.582 | -1.16995 | 2.084248 |
| L2. | .7793356 | .7594835 | 1.03 | 0.305 | -.7092247 | 2.267896 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | .0342995 | .8151832 | 0.04 | 0.966 | -1.56343 | 1.632029 |
| L2. | -1.585021 | .860159 | -1.84 | 0.065 | -3.270902 | .1008594 |
| sp500compositepriceindex | | | | | | |
| L1. | -.0431857 | .1430577 | -0.30 | 0.763 | -.3235736 | .2372021 |
| L2. | -.0378715 | .1508296 | -0.25 | 0.802 | -.3334921 | .2577491 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | .0119915 | .0169252 | 0.71 | 0.479 | -.0211813 | .0451644 |
| L2. | .0102599 | .0180869 | 0.57 | 0.571 | -.0251898 | .0457096 |
| opecoilbasketprice | | | | | | |
| L1. | -1.371533 | 1.031427 | -1.33 | 0.184 | -3.393094 | .6500278 |
| L2. | -.2138905 | .6948376 | -0.31 | 0.758 | -1.575747 | 1.147966 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | .0595695 | .0443449 | 1.34 | 0.179 | -.0273448 | .1464839 |
| L2. | .0658767 | .058719 | 1.12 | 0.262 | -.0492104 | .1809639 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | -.0452861 | .0337079 | -1.34 | 0.179 | -.1113525 | .0207802 |
| L2. | -.0079861 | .0373005 | -0.21 | 0.830 | -.0810938 | .0651216 |
| _cons | 44.86551 | 51.52062 | 0.87 | 0.384 | -56.11305 | 145.8441 |

| | | | | | | |
|---|---|---|---|---|---|---|
| japanyentoeurexchangerate | | | | | | |
| totalbitcoins | | | | | | |
| L1. | -.0000994 | .0001403 | -0.71 | 0.479 | -.0003744 | .0001755 |
| L2. | .0001159 | .0001407 | 0.82 | 0.410 | -.0001599 | .0003916 |
| usdoll1ydepo | | | | | | |
| L1. | -2.535387 | 1.162247 | -2.18 | 0.029 | -4.813349 | -.2574248 |
| L2. | 2.961165 | 1.063239 | 2.79 | 0.005 | .8772548 | 5.045076 |
| euro1ydepo | | | | | | |
| L1. | 3.612608 | 3.376589 | 1.07 | 0.285 | -3.005384 | 10.2306 |
| L2. | -1.895697 | 3.347389 | -0.57 | 0.571 | -8.456459 | 4.665065 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .0582884 | .1261349 | 0.46 | 0.644 | -.1889314 | .3055081 |
| L2. | -.2348808 | .1291778 | -1.82 | 0.069 | -.4880646 | .0183031 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | -.0001904 | .0012709 | -0.15 | 0.881 | -.0026813 | .0023006 |
| L2. | -.000327 | .0010867 | -0.30 | 0.763 | -.0024569 | .0018028 |
| eurostoxxpriceindex | | | | | | |
| L1. | -.0447579 | .0617557 | -0.72 | 0.469 | -.1657969 | .0762811 |
| L2. | -.0071728 | .0626028 | -0.11 | 0.909 | -.1298721 | .1155265 |
| japanyentoeurexchangerate | | | | | | |
| L1. | -.0215253 | .2799821 | -0.08 | 0.939 | -.5702801 | .5272295 |
| L2. | .1600815 | .2561431 | 0.62 | 0.532 | -.3419498 | .6621128 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | .9771323 | .2749284 | 3.55 | 0.000 | .4382826 | 1.515982 |
| L2. | -.3550044 | .2900969 | -1.22 | 0.221 | -.9235839 | .2135751 |
| sp500compositepriceindex | | | | | | |
| L1. | -.0038912 | .0482476 | -0.08 | 0.936 | -.0984547 | .0906723 |
| L2. | -.0040222 | .0508687 | -0.08 | 0.937 | -.1037231 | .0956787 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | -.0003671 | .0057082 | -0.06 | 0.949 | -.0115549 | .0108208 |
| L2. | .0027115 | .0061 | 0.44 | 0.657 | -.0092443 | .0146673 |
| opecoilbasketprice | | | | | | |
| L1. | .021121 | .3478588 | 0.06 | 0.952 | -.6606698 | .7029118 |
| L2. | .3983089 | .2343407 | 1.70 | 0.089 | -.0609904 | .8576081 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | .0151773 | .0149557 | 1.01 | 0.310 | -.0141354 | .04449 |
| L2. | -.027115 | .0198035 | -1.37 | 0.171 | -.0659292 | .0116993 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | -.005595 | .0113683 | -0.49 | 0.623 | -.0278765 | .0166865 |
| L2. | -.0047098 | .01258 | -0.37 | 0.708 | -.0293661 | .0199465 |
| _cons | 41.45919 | 17.37583 | 2.39 | 0.017 | 7.4032 | 75.51518 |

| | | | | | | |
|---|---|---|---|---|---|---|
| eurotojapyenfxcrossrateexchanger | | | | | | |
| totalbitcoins | | | | | | |
| L1. | -.0000443 | .0001444 | -0.31 | 0.759 | -.0003274 | .0002388 |
| L2. | .0000755 | .0001449 | 0.52 | 0.603 | -.0002085 | .0003594 |
| usdoll1ydepo | | | | | | |
| L1. | -2.788372 | 1.19674 | -2.33 | 0.020 | -5.133939 | -.4428045 |
| L2. | 3.082319 | 1.094794 | 2.82 | 0.005 | .9365617 | 5.228076 |
| euro1ydepo | | | | | | |
| L1. | 6.860318 | 3.476799 | 1.97 | 0.048 | .0459166 | 13.67472 |
| L2. | -1.990692 | 3.446733 | -0.58 | 0.564 | -8.746165 | 4.764781 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .081257 | .1298783 | 0.63 | 0.532 | -.1732998 | .3358138 |
| L2. | -.3282349 | .1330116 | -2.47 | 0.014 | -.5889328 | -.0675371 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .0003932 | .0013086 | 0.30 | 0.764 | -.0021717 | .002958 |
| L2. | -.0013694 | .0011189 | -1.22 | 0.221 | -.0035625 | .0008236 |
| eurostoxxpriceindex | | | | | | |
| L1. | -.053589 | .0635885 | -0.84 | 0.399 | -.1782203 | .0710422 |
| L2. | -.0299699 | .0644608 | -0.46 | 0.642 | -.1563107 | .0963709 |
| japanyentoeurexchangerate | | | | | | |
| L1. | -.0165693 | .2882914 | -0.06 | 0.954 | -.5816101 | .5484715 |
| L2. | .6353841 | .263745 | 2.41 | 0.016 | .1184535 | 1.152315 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | .8993319 | .2830877 | 3.18 | 0.001 | .3444902 | 1.454174 |
| L2. | -.8641163 | .2987064 | -2.89 | 0.004 | -1.44957 | -.2786625 |
| sp500compositepriceindex | | | | | | |
| L1. | -.0397375 | .0496795 | -0.80 | 0.424 | -.1371074 | .0576325 |
| L2. | -.0152391 | .0523784 | -0.29 | 0.771 | -.1178989 | .0874207 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | .0027322 | .0058776 | 0.46 | 0.642 | -.0087877 | .0142521 |
| L2. | .0059221 | .006281 | 0.94 | 0.346 | -.0063885 | .0182327 |
| opecoilbasketprice | | | | | | |
| L1. | .1849214 | .3581826 | 0.52 | 0.606 | -.5171037 | .8869464 |
| L2. | .536101 | .2412954 | 2.22 | 0.026 | .0631707 | 1.009031 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | .0167339 | .0153996 | 1.09 | 0.277 | -.0134487 | .0469166 |
| L2. | -.0391691 | .0203913 | -1.92 | 0.055 | -.0791353 | .0007971 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | -.0194921 | .0117057 | -1.67 | 0.096 | -.0424348 | .0034507 |
| L2. | .0017792 | .0129533 | 0.14 | 0.891 | -.0236089 | .0271672 |
| _cons | 54.19423 | 17.89151 | 3.03 | 0.002 | 19.12752 | 89.26093 |

| | | | | | | |
|---|---|---|---|---|---|---|
| sp500compositepriceindex | | | | | | |
| totalbitcoins | | | | | | |
| L1. | -.0010562 | .0017362 | -0.61 | 0.543 | -.004459 | .0023467 |
| L2. | .0014404 | .0017415 | 0.83 | 0.408 | -.0019728 | .0048536 |
| usdoll1ydepo | | | | | | |
| L1. | -23.11134 | 14.38454 | -1.61 | 0.108 | -51.30452 | 5.081846 |
| L2. | 25.25276 | 13.15918 | 1.92 | 0.055 | -.5387511 | 51.04427 |
| euro1ydepo | | | | | | |
| L1. | 31.94497 | 41.79033 | 0.76 | 0.445 | -49.96257 | 113.8525 |
| L2. | 10.96782 | 41.42894 | 0.26 | 0.791 | -70.23141 | 92.16706 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .1416973 | 1.561107 | 0.09 | 0.928 | -2.918017 | 3.201412 |
| L2. | -3.697043 | 1.598768 | -2.31 | 0.021 | -6.830572 | -.5635143 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .0200941 | .0157294 | 1.28 | 0.201 | -.010735 | .0509232 |
| L2. | .0001717 | .0134492 | 0.01 | 0.990 | -.0261883 | .0265316 |
| eurostoxxpriceindex | | | | | | |
| L1. | .7372123 | .7643196 | 0.96 | 0.335 | -.7608265 | 2.235251 |
| L2. | -.8246825 | .7748038 | -1.06 | 0.287 | -2.34327 | .6939051 |
| japanyentoeurexchangerate | | | | | | |
| L1. | 5.366523 | 3.465197 | 1.55 | 0.121 | -1.425138 | 12.15818 |
| L2. | 6.672509 | 3.170154 | 2.10 | 0.035 | .459121 | 12.8859 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | -2.884605 | 3.40265 | -0.85 | 0.397 | -9.553676 | 3.784466 |
| L2. | -13.07464 | 3.590383 | -3.64 | 0.000 | -20.11166 | -6.037617 |
| sp500compositepriceindex | | | | | | |
| L1. | -.424079 | .5971358 | -0.71 | 0.478 | -1.594444 | .7462858 |
| L2. | -.4143548 | .6295766 | -0.66 | 0.510 | -1.648302 | .8195928 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | .0895936 | .0706475 | 1.27 | 0.205 | -.0488731 | .2280602 |
| L2. | .0934496 | .0754965 | 1.24 | 0.216 | -.0545207 | .24142 |
| opecoilbasketprice | | | | | | |
| L1. | -.8245197 | 4.305273 | -0.19 | 0.848 | -9.2627 | 7.613661 |
| L2. | 3.643588 | 2.900316 | 1.26 | 0.209 | -2.040927 | 9.328103 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | .1660121 | .1850996 | 0.90 | 0.370 | -.1967765 | .5288007 |
| L2. | -.038142 | .2450985 | -0.16 | 0.876 | -.5185262 | .4422422 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | -.2841447 | .1407001 | -2.02 | 0.043 | -.5599117 | -.0083777 |
| L2. | -.1219859 | .1556959 | -0.78 | 0.433 | -.4271443 | .1831725 |
| _cons | 808.4826 | 215.0518 | 3.76 | 0.000 | 386.9887 | 1229.976 |

| | | | | | | |
|---|---|---|---|---|---|---|
| dowjonesindustrialspriceindex | | | | | | |
| totalbitcoins | | | | | | |
| L1. | -.0071951 | .0148114 | -0.49 | 0.627 | -.0362249 | .0218348 |
| L2. | .0105851 | .0148565 | 0.71 | 0.476 | -.0185331 | .0397033 |
| usdoll1ydepo | | | | | | |
| L1. | -221.3183 | 122.7154 | -1.80 | 0.071 | -461.8361 | 19.19952 |
| L2. | 207.715 | 112.2618 | 1.85 | 0.064 | -12.314 | 427.744 |
| euro1ydepo | | | | | | |
| L1. | 258.7773 | 356.516 | 0.73 | 0.468 | -439.9811 | 957.5358 |
| L2. | 253.837 | 353.4329 | 0.72 | 0.473 | -438.8788 | 946.5528 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | 2.439966 | 13.31791 | 0.18 | 0.855 | -23.66265 | 28.54258 |
| L2. | -28.26159 | 13.63919 | -2.07 | 0.038 | -54.99392 | -1.529257 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .1358254 | .1341886 | 1.01 | 0.311 | -.1271795 | .3988303 |
| L2. | -.009971 | .1147359 | -0.09 | 0.931 | -.2348493 | .2149073 |
| eurostoxxpriceindex | | | | | | |
| L1. | 4.885703 | 6.520459 | 0.75 | 0.454 | -7.894161 | 17.66557 |
| L2. | -8.162598 | 6.6099 | -1.23 | 0.217 | -21.11776 | 4.792568 |
| japanyentoeurexchangerate | | | | | | |
| L1. | 51.38021 | 29.56181 | 1.74 | 0.082 | -6.559884 | 109.3203 |
| L2. | 64.18538 | 27.04479 | 2.37 | 0.018 | 11.17857 | 117.1922 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | -30.39156 | 29.02822 | -1.05 | 0.295 | -87.28583 | 26.50271 |
| L2. | -115.6682 | 30.62978 | -3.78 | 0.000 | -175.7015 | -55.63497 |
| sp500compositepriceindex | | | | | | |
| L1. | -9.220189 | 5.094204 | -1.81 | 0.070 | -19.20464 | .7642666 |
| L2. | -3.996612 | 5.370958 | -0.74 | 0.457 | -14.5235 | 6.530272 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | 1.474204 | .6026986 | 2.45 | 0.014 | .2929366 | 2.655472 |
| L2. | .8907093 | .6440653 | 1.38 | 0.167 | -.3716354 | 2.153054 |
| opecoilbasketprice | | | | | | |
| L1. | -9.333797 | 36.72856 | -0.25 | 0.799 | -81.32045 | 62.65285 |
| L2. | 32.52684 | 24.74278 | 1.31 | 0.189 | -15.96811 | 81.0218 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | 1.395212 | 1.579096 | 0.88 | 0.377 | -1.69976 | 4.490184 |
| L2. | -.3104095 | 2.090951 | -0.15 | 0.882 | -4.408597 | 3.787778 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | -2.381339 | 1.200321 | -1.98 | 0.047 | -4.733925 | -.0287532 |
| L2. | -1.20502 | 1.328252 | -0.91 | 0.364 | -3.808346 | 1.398305 |
| _cons | 6561.175 | 1834.621 | 3.58 | 0.000 | 2965.385 | 10156.97 |

| | | | | | | |
|---|---|---|---|---|---|---|
| opecoilbasketprice | | | | | | |
| totalbitcoins | | | | | | |
| L1. | .0001266 | .0000685 | 1.85 | 0.064 | -7.57e-06 | .0002608 |
| L2. | -.0001232 | .0000687 | -1.79 | 0.073 | -.0002578 | .0000114 |
| usdoll1ydepo | | | | | | |
| L1. | -.2889568 | .5671949 | -0.51 | 0.610 | -1.400638 | .8227247 |
| L2. | .6921444 | .5188776 | 1.33 | 0.182 | -.324837 | 1.709126 |
| euro1ydepo | | | | | | |
| L1. | 4.002434 | 1.647829 | 2.43 | 0.015 | .7727485 | 7.232119 |
| L2. | -2.121436 | 1.633579 | -1.30 | 0.194 | -5.323192 | 1.08032 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .1645339 | .0615558 | 2.67 | 0.008 | .0438867 | .2851811 |
| L2. | -.0819068 | .0630408 | -1.30 | 0.194 | -.2054646 | .0416509 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | .0004422 | .0006202 | 0.71 | 0.476 | -.0007734 | .0016578 |
| L2. | -.0001062 | .0005303 | -0.20 | 0.841 | -.0011456 | .0009332 |
| eurostoxxpriceindex | | | | | | |
| L1. | .0448495 | .0301378 | 1.49 | 0.137 | -.0142194 | .1039185 |
| L2. | -.020225 | .0305512 | -0.66 | 0.508 | -.0801042 | .0396542 |
| japanyentoeurexchangerate | | | | | | |
| L1. | -.1429264 | .1366357 | -1.05 | 0.296 | -.4107274 | .1248747 |
| L2. | .0064059 | .1250019 | 0.05 | 0.959 | -.2385934 | .2514051 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | .3518588 | .1341694 | 2.62 | 0.009 | .0888916 | .614826 |
| L2. | -.1400506 | .1415719 | -0.99 | 0.323 | -.4175264 | .1374252 |
| sp500compositepriceindex | | | | | | |
| L1. | .0036942 | .0235456 | 0.16 | 0.875 | -.0424542 | .0498427 |
| L2. | -.0310175 | .0248248 | -1.25 | 0.211 | -.0796731 | .0176381 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | -.0042686 | .0027857 | -1.53 | 0.125 | -.0097285 | .0011912 |
| L2. | .0058877 | .0029769 | 1.98 | 0.048 | .0000531 | .0117223 |
| opecoilbasketprice | | | | | | |
| L1. | .5153762 | .1697606 | 3.04 | 0.002 | .1826515 | .848101 |
| L2. | -.0719582 | .114362 | -0.63 | 0.529 | -.2961035 | .1521871 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | .0368455 | .0072986 | 5.05 | 0.000 | .0225405 | .0511506 |
| L2. | -.0063515 | .0096644 | -0.66 | 0.511 | -.0252934 | .0125905 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | .0082137 | .0055479 | 1.48 | 0.139 | -.00266 | .0190874 |
| L2. | -.0228346 | .0061392 | -3.72 | 0.000 | -.0348673 | -.010802 |
| _cons | 2.810366 | 8.479679 | 0.33 | 0.740 | -13.8095 | 19.43023 |

| | | | | | | |
|---|---|---|---|---|---|---|
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| totalbitcoins | | | | | | |
| L1. | .0024647 | .0018913 | 1.30 | 0.193 | -.0012421 | .0061715 |
| L2. | -.0022463 | .001897 | -1.18 | 0.236 | -.0059644 | .0014718 |
| usdoll1ydepo | | | | | | |
| L1. | 2.283 | 15.6695 | 0.15 | 0.884 | -28.42866 | 32.99466 |
| L2. | 7.941775 | 14.33467 | 0.55 | 0.580 | -20.15367 | 36.03722 |
| euro1ydepo | | | | | | |
| L1. | 63.95364 | 45.52343 | 1.40 | 0.160 | -25.27065 | 153.1779 |
| L2. | 14.20005 | 45.12976 | 0.31 | 0.753 | -74.25266 | 102.6528 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | 3.422357 | 1.70056 | 2.01 | 0.044 | .0893204 | 6.755393 |
| L2. | -.6525964 | 1.741585 | -0.37 | 0.708 | -4.066041 | 2.760848 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | -.0070529 | .0171345 | -0.41 | 0.681 | -.0406359 | .0265301 |
| L2. | -.0064194 | .0146506 | -0.44 | 0.661 | -.0351341 | .0222952 |
| eurostoxxpriceindex | | | | | | |
| L1. | .8395889 | .8325957 | 1.01 | 0.313 | -.7922687 | 2.471446 |
| L2. | .0965018 | .8440165 | 0.11 | 0.909 | -1.55774 | 1.750744 |
| japanyentoeurexchangerate | | | | | | |
| L1. | -.5882138 | 3.77474 | -0.16 | 0.876 | -7.986569 | 6.810141 |
| L2. | -2.912914 | 3.453342 | -0.84 | 0.399 | -9.68134 | 3.855511 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | 4.605837 | 3.706606 | 1.24 | 0.214 | -2.658977 | 11.87065 |
| L2. | .1952915 | 3.911109 | 0.05 | 0.960 | -7.470342 | 7.860924 |
| sp500compositepriceindex | | | | | | |
| L1. | -.6082882 | .6504776 | -0.94 | 0.350 | -1.883201 | .6666244 |
| L2. | -.1217409 | .6858163 | -0.18 | 0.859 | -1.465916 | 1.222434 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | -.0067601 | .0769584 | -0.09 | 0.930 | -.1575959 | .1440756 |
| L2. | .0700597 | .0822405 | 0.85 | 0.394 | -.0911288 | .2312481 |
| opecoilbasketprice | | | | | | |
| L1. | 2.853352 | 4.68986 | 0.61 | 0.543 | -6.338605 | 12.04531 |
| L2. | 1.797524 | 3.159399 | 0.57 | 0.569 | -4.394785 | 7.989832 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | .6545844 | .2016344 | 3.25 | 0.001 | .2593882 | 1.049781 |
| L2. | -.1399387 | .2669929 | -0.52 | 0.600 | -.6632353 | .3833579 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | .3208038 | .1532687 | 2.09 | 0.036 | .0204026 | .6212049 |
| L2. | -.4357092 | .1696041 | -2.57 | 0.010 | -.7681271 | -.1032912 |
| _cons | -95.65268 | 234.2622 | -0.41 | 0.683 | -554.7982 | 363.4929 |

| | | | | | | |
|---|---|---|---|---|---|---|
| cmcigold1ypiusdpriceindex | | | | | | |
| totalbitcoins | | | | | | |
| L1. | .0015731 | .0016495 | 0.95 | 0.340 | -.0016599 | .0048061 |
| L2. | -.0011592 | .0016545 | -0.70 | 0.484 | -.004402 | .0020836 |
| usdoll1ydepo | | | | | | |
| L1. | -8.321928 | 13.66653 | -0.61 | 0.543 | -35.10784 | 18.46399 |
| L2. | 4.908606 | 12.50233 | 0.39 | 0.695 | -19.59551 | 29.41273 |
| euro1ydepo | | | | | | |
| L1. | 95.96809 | 39.70436 | 2.42 | 0.016 | 18.14898 | 173.7872 |
| L2. | 25.08953 | 39.36101 | 0.64 | 0.524 | -52.05663 | 102.2357 |
| ukgbpeffectiveexchangerateindex | | | | | | |
| L1. | .5086948 | 1.483184 | 0.34 | 0.732 | -2.398293 | 3.415683 |
| L2. | 1.19143 | 1.518966 | 0.78 | 0.433 | -1.785688 | 4.168547 |
| nikkei225stockavgpriceindex | | | | | | |
| L1. | -.0418353 | .0149443 | -2.80 | 0.005 | -.0711255 | -.012545 |
| L2. | -.0104853 | .0127779 | -0.82 | 0.412 | -.0355295 | .0145589 |
| eurostoxxpriceindex | | | | | | |
| L1. | .1049675 | .7261684 | 0.14 | 0.885 | -1.318296 | 1.528231 |
| L2. | 1.419259 | .7361293 | 1.93 | 0.054 | -.0235274 | 2.862046 |
| japanyentoeurexchangerate | | | | | | |
| L1. | 7.00248 | 3.292231 | 2.13 | 0.033 | .5498259 | 13.45513 |
| L2. | -.8171992 | 3.011915 | -0.27 | 0.786 | -6.720445 | 5.086046 |
| eurotojapyenfxcrossrateexchanger | | | | | | |
| L1. | -3.701881 | 3.232806 | -1.15 | 0.252 | -10.03806 | 2.634302 |
| L2. | .1798874 | 3.411168 | 0.05 | 0.958 | -6.505879 | 6.865654 |
| sp500compositepriceindex | | | | | | |
| L1. | .0316345 | .5673297 | 0.06 | 0.956 | -1.080311 | 1.14358 |
| L2. | -.9664703 | .5981512 | -1.62 | 0.106 | -2.138825 | .2058845 |
| dowjonesindustrialspriceindex | | | | | | |
| L1. | -.0216323 | .0671212 | -0.32 | 0.747 | -.1531873 | .1099228 |
| L2. | .1293283 | .0717281 | 1.80 | 0.071 | -.0112561 | .2699127 |
| opecoilbasketprice | | | | | | |
| L1. | -.532423 | 4.090375 | -0.13 | 0.896 | -8.54941 | 7.484564 |
| L2. | 7.434149 | 2.755546 | 2.70 | 0.007 | 2.033378 | 12.83492 |
| cmciwticrudeoil1ypiusdpriceindex | | | | | | |
| L1. | -.1362579 | .1758603 | -0.77 | 0.438 | -.4809378 | .208422 |
| L2. | -.5260663 | .2328643 | -2.26 | 0.024 | -.982472 | -.0696606 |
| cmcigold1ypiusdpriceindex | | | | | | |
| L1. | .8722083 | .133677 | 6.52 | 0.000 | .6102062 | 1.13421 |
| L2. | .02111 | .1479243 | 0.14 | 0.887 | -.2688163 | .3110364 |
| _cons | -187.5709 | 204.3175 | -0.92 | 0.359 | -588.0258 | 212.884 |

Finally, we perform the Granger causality test in order to determine whether one time series is useful in forecasting another. Generally, the causality in economics could be tested for by measuring the ability to predict the future values of a time series using prior values of another time series. Time series X is said to Granger-cause Y if it can be shown, usually through a series of t-tests and F-tests on lagged values of X and with lagged values of Y, that those X values provide statistically significant information about future values of Y. In our test the results are the following,

| Equation | Excluded | chi2 | df | Prob > chi2 |
|---|---|---|---|---|
| totalbitcoins | usdolllydepo | 4.2371 | 2 | 0.120 |
| totalbitcoins | eurolydepo | 12.064 | 2 | 0.002 |
| totalbitcoins | ukgbpeffectivee~x | 27.099 | 2 | 0.000 |
| totalbitcoins | nikkei225stocka~x | 3.743 | 2 | 0.154 |
| totalbitcoins | eurostoxxpricei~x | 5.3544 | 2 | 0.069 |
| totalbitcoins | japanyentoeurex~e | 6.1401 | 2 | 0.046 |
| totalbitcoins | eurotojapyenfxc~r | 1.6089 | 2 | 0.447 |
| totalbitcoins | sp500compositep~x | 13.375 | 2 | 0.001 |
| totalbitcoins | dowjonesindustr~x | 12.73 | 2 | 0.002 |
| totalbitcoins | opecoilbasketpr~e | 4.2198 | 2 | 0.121 |
| totalbitcoins | cmciwticrudeoil~x | 3.2252 | 2 | 0.199 |
| totalbitcoins | cmcigoldlypiusd~x | 5.7451 | 2 | 0.057 |
| totalbitcoins | ALL | 114.05 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| usdolllydepo | totalbitcoins | 13.392 | 2 | 0.001 |
| usdolllydepo | eurolydepo | 12.056 | 2 | 0.002 |
| usdolllydepo | ukgbpeffectivee~x | .12649 | 2 | 0.939 |
| usdolllydepo | nikkei225stocka~x | .55537 | 2 | 0.758 |
| usdolllydepo | eurostoxxpricei~x | 1.9969 | 2 | 0.368 |
| usdolllydepo | japanyentoeurex~e | .55638 | 2 | 0.757 |
| usdolllydepo | eurotojapyenfxc~r | .12054 | 2 | 0.942 |
| usdolllydepo | sp500compositep~x | 1.682 | 2 | 0.431 |
| usdolllydepo | dowjonesindustr~x | 1.1851 | 2 | 0.553 |
| usdolllydepo | opecoilbasketpr~e | 14.372 | 2 | 0.001 |
| usdolllydepo | cmciwticrudeoil~x | 2.0021 | 2 | 0.367 |
| usdolllydepo | cmcigoldlypiusd~x | 11.416 | 2 | 0.003 |
| usdolllydepo | ALL | 89.06 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| eurolydepo | totalbitcoins | 14.275 | 2 | 0.001 |
| eurolydepo | usdolllydepo | .04772 | 2 | 0.976 |
| eurolydepo | ukgbpeffectivee~x | 1.0588 | 2 | 0.589 |
| eurolydepo | nikkei225stocka~x | 2.233 | 2 | 0.327 |
| eurolydepo | eurostoxxpricei~x | .45533 | 2 | 0.796 |
| eurolydepo | japanyentoeurex~e | 6.5178 | 2 | 0.038 |
| eurolydepo | eurotojapyenfxc~r | 3.3557 | 2 | 0.187 |
| eurolydepo | sp500compositep~x | .24763 | 2 | 0.884 |
| eurolydepo | dowjonesindustr~x | .05002 | 2 | 0.975 |
| eurolydepo | opecoilbasketpr~e | 3.8155 | 2 | 0.148 |
| eurolydepo | cmciwticrudeoil~x | 7.2221 | 2 | 0.027 |
| eurolydepo | cmcigoldlypiusd~x | 1.3492 | 2 | 0.509 |
| eurolydepo | ALL | 43.45 | 24 | 0.009 |

| | | | | |
|---|---|---|---|---|
| ukgbpeffectivee~x | totalbitcoins | 8.1918 | 2 | 0.017 |
| ukgbpeffectivee~x | usdolllydepo | 7.7923 | 2 | 0.020 |
| ukgbpeffectivee~x | eurolydepo | 3.512 | 2 | 0.173 |
| ukgbpeffectivee~x | nikkei225stocka~x | 9.4813 | 2 | 0.009 |
| ukgbpeffectivee~x | eurostoxxpricei~x | 4.412 | 2 | 0.110 |
| ukgbpeffectivee~x | japanyentoeurex~e | 3.2794 | 2 | 0.194 |
| ukgbpeffectivee~x | eurotojapyenfxc~r | 5.6131 | 2 | 0.060 |
| ukgbpeffectivee~x | sp500compositep~x | 18.145 | 2 | 0.000 |
| ukgbpeffectivee~x | dowjonesindustr~x | 23.677 | 2 | 0.000 |
| ukgbpeffectivee~x | opecoilbasketpr~e | 15.73 | 2 | 0.000 |
| ukgbpeffectivee~x | cmciwticrudeoil~x | 6.5888 | 2 | 0.037 |
| ukgbpeffectivee~x | cmcigoldlypiusd~x | 7.6603 | 2 | 0.022 |
| ukgbpeffectivee~x | ALL | 85.829 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| nikkei225stocka~x | totalbitcoins | 3.8758 | 2 | 0.144 |
| nikkei225stocka~x | usdolllydepo | 6.6632 | 2 | 0.036 |
| nikkei225stocka~x | eurolydepo | 3.3095 | 2 | 0.191 |
| nikkei225stocka~x | ukgbpeffectivee~x | 2.3605 | 2 | 0.307 |
| nikkei225stocka~x | eurostoxxpricei~x | 7.2903 | 2 | 0.026 |
| nikkei225stocka~x | japanyentoeurex~e | 4.6794 | 2 | 0.096 |
| nikkei225stocka~x | eurotojapyenfxc~r | 2.6651 | 2 | 0.264 |
| nikkei225stocka~x | sp500compositep~x | .95668 | 2 | 0.620 |
| nikkei225stocka~x | dowjonesindustr~x | 6.5354 | 2 | 0.038 |
| nikkei225stocka~x | opecoilbasketpr~e | .69637 | 2 | 0.706 |
| nikkei225stocka~x | cmciwticrudeoil~x | 1.2142 | 2 | 0.545 |
| nikkei225stocka~x | cmcigoldlypiusd~x | .93405 | 2 | 0.627 |
| nikkei225stocka~x | ALL | 180.99 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| eurostoxxpricei~x | totalbitcoins | 4.8681 | 2 | 0.088 |
| eurostoxxpricei~x | usdolllydepo | 2.2763 | 2 | 0.320 |
| eurostoxxpricei~x | eurolydepo | 1.3439 | 2 | 0.511 |
| eurostoxxpricei~x | ukgbpeffectivee~x | 1.1463 | 2 | 0.564 |
| eurostoxxpricei~x | nikkei225stocka~x | .14968 | 2 | 0.928 |
| eurostoxxpricei~x | japanyentoeurex~e | 1.3326 | 2 | 0.514 |
| eurostoxxpricei~x | eurotojapyenfxc~r | 3.4059 | 2 | 0.182 |
| eurostoxxpricei~x | sp500compositep~x | .45741 | 2 | 0.796 |
| eurostoxxpricei~x | dowjonesindustr~x | 3.1436 | 2 | 0.208 |
| eurostoxxpricei~x | opecoilbasketpr~e | 1.7829 | 2 | 0.410 |
| eurostoxxpricei~x | cmciwticrudeoil~x | 3.0033 | 2 | 0.223 |
| eurostoxxpricei~x | cmcigoldlypiusd~x | 4.2145 | 2 | 0.122 |
| eurostoxxpricei~x | ALL | 37.445 | 24 | 0.039 |

| | | | | |
|---|---|---|---|---|
| japanyentoeurex~e | totalbitcoins | 2.8762 | 2 | 0.237 |
| japanyentoeurex~e | usdolllydepo | 8.7229 | 2 | 0.013 |
| japanyentoeurex~e | eurolydepo | 1.1485 | 2 | 0.563 |
| japanyentoeurex~e | ukgbpeffectivee~x | 5.9963 | 2 | 0.050 |
| japanyentoeurex~e | nikkei225stocka~x | .12227 | 2 | 0.941 |
| japanyentoeurex~e | eurostoxxpricei~x | .89604 | 2 | 0.639 |
| japanyentoeurex~e | eurotojapyenfxc~r | 14.427 | 2 | 0.001 |
| japanyentoeurex~e | sp500compositep~x | .0381 | 2 | 0.981 |
| japanyentoeurex~e | dowjonesindustr~x | .35306 | 2 | 0.838 |
| japanyentoeurex~e | opecoilbasketpr~e | 2.9217 | 2 | 0.232 |
| japanyentoeurex~e | cmciwticrudeoil~x | 2.9621 | 2 | 0.227 |
| japanyentoeurex~e | cmcigoldlypiusd~x | 1.1913 | 2 | 0.551 |
| japanyentoeurex~e | ALL | 82.776 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| eurotojapyenfxc~r | totalbitcoins | 8.1693 | 2 | 0.017 |
| eurotojapyenfxc~r | usdolllydepo | 9.2155 | 2 | 0.010 |
| eurotojapyenfxc~r | eurolydepo | 4.0683 | 2 | 0.131 |
| eurotojapyenfxc~r | ukgbpeffectivee~x | 11.056 | 2 | 0.004 |
| eurotojapyenfxc~r | nikkei225stocka~x | 1.5338 | 2 | 0.464 |
| eurotojapyenfxc~r | eurostoxxpricei~x | 1.9289 | 2 | 0.381 |
| eurotojapyenfxc~r | japanyentoeurex~e | 5.8156 | 2 | 0.055 |
| eurotojapyenfxc~r | sp500compositep~x | 1.8548 | 2 | 0.396 |
| eurotojapyenfxc~r | dowjonesindustr~x | 3.8862 | 2 | 0.143 |
| eurotojapyenfxc~r | opecoilbasketpr~e | 4.9781 | 2 | 0.083 |
| eurotojapyenfxc~r | cmciwticrudeoil~x | 4.9572 | 2 | 0.084 |
| eurotojapyenfxc~r | cmcigoldlypiusd~x | 4.6554 | 2 | 0.098 |
| eurotojapyenfxc~r | ALL | 68.032 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| sp500compositep~x | totalbitcoins | 8.8483 | 2 | 0.012 |
| sp500compositep~x | usdolllydepo | 4.3144 | 2 | 0.116 |
| sp500compositep~x | eurolydepo | 1.1005 | 2 | 0.577 |
| sp500compositep~x | ukgbpeffectivee~x | 13.817 | 2 | 0.001 |
| sp500compositep~x | nikkei225stocka~x | 1.6489 | 2 | 0.438 |
| sp500compositep~x | eurostoxxpricei~x | 1.3424 | 2 | 0.511 |
| sp500compositep~x | japanyentoeurex~e | 6.6918 | 2 | 0.035 |
| sp500compositep~x | eurotojapyenfxc~r | 13.794 | 2 | 0.001 |
| sp500compositep~x | dowjonesindustr~x | 12.108 | 2 | 0.002 |
| sp500compositep~x | opecoilbasketpr~e | 1.717 | 2 | 0.424 |
| sp500compositep~x | cmciwticrudeoil~x | .83461 | 2 | 0.659 |
| sp500compositep~x | cmcigoldlypiusd~x | 12.876 | 2 | 0.002 |
| sp500compositep~x | ALL | 67.252 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| dowjonesindustr~x | totalbitcoins | 9.3066 | 2 | 0.010 |
| dowjonesindustr~x | usdollydepo | 4.5364 | 2 | 0.103 |
| dowjonesindustr~x | eurolydepo | 2.0005 | 2 | 0.368 |
| dowjonesindustr~x | ukgbpeffectivee~x | 10.241 | 2 | 0.006 |
| dowjonesindustr~x | nikkei225stocka~x | 1.0246 | 2 | 0.599 |
| dowjonesindustr~x | eurostoxxpricei~x | 1.533 | 2 | 0.465 |
| dowjonesindustr~x | japanyentoeurex~e | 8.4804 | 2 | 0.014 |
| dowjonesindustr~x | eurotojapyenfxc~r | 15.116 | 2 | 0.001 |
| dowjonesindustr~x | sp500compositep~x | 10.083 | 2 | 0.006 |
| dowjonesindustr~x | opecoilbasketpr~e | 1.9254 | 2 | 0.382 |
| dowjonesindustr~x | cmciwticrudeoil~x | .80835 | 2 | 0.668 |
| dowjonesindustr~x | cmcigoldlypiusd~x | 13.56 | 2 | 0.001 |
| dowjonesindustr~x | ALL | 60.402 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| opecoilbasketpr~e | totalbitcoins | 3.8554 | 2 | 0.145 |
| opecoilbasketpr~e | usdolllydepo | 1.798 | 2 | 0.407 |
| opecoilbasketpr~e | eurolydepo | 5.9235 | 2 | 0.052 |
| opecoilbasketpr~e | ukgbpeffectivee~x | 9.0562 | 2 | 0.011 |
| opecoilbasketpr~e | nikkei225stocka~x | .52672 | 2 | 0.768 |
| opecoilbasketpr~e | eurostoxxpricei~x | 2.2468 | 2 | 0.325 |
| opecoilbasketpr~e | japanyentoeurex~e | 1.0996 | 2 | 0.577 |
| opecoilbasketpr~e | eurotojapyenfxc~r | 8.0328 | 2 | 0.018 |
| opecoilbasketpr~e | sp500compositep~x | 2.3765 | 2 | 0.305 |
| opecoilbasketpr~e | dowjonesindustr~x | 3.9217 | 2 | 0.141 |
| opecoilbasketpr~e | cmciwticrudeoil~x | 26.062 | 2 | 0.000 |
| opecoilbasketpr~e | cmcigoldlypiusd~x | 15.955 | 2 | 0.000 |
| opecoilbasketpr~e | ALL | 177.04 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| cmciwticrudeoil~x | totalbitcoins | 4.0176 | 2 | 0.134 |
| cmciwticrudeoil~x | usdolllydepo | .52037 | 2 | 0.771 |
| cmciwticrudeoil~x | eurolydepo | 3.2383 | 2 | 0.198 |
| cmciwticrudeoil~x | ukgbpeffectivee~x | 8.2208 | 2 | 0.016 |
| cmciwticrudeoil~x | nikkei225stocka~x | .3977 | 2 | 0.820 |
| cmciwticrudeoil~x | eurostoxxpricei~x | 1.6464 | 2 | 0.439 |
| cmciwticrudeoil~x | japanyentoeurex~e | .73048 | 2 | 0.694 |
| cmciwticrudeoil~x | eurotojapyenfxc~r | 1.5442 | 2 | 0.462 |
| cmciwticrudeoil~x | sp500compositep~x | 2.0212 | 2 | 0.364 |
| cmciwticrudeoil~x | dowjonesindustr~x | 1.3792 | 2 | 0.502 |
| cmciwticrudeoil~x | opecoilbasketpr~e | .60826 | 2 | 0.738 |
| cmciwticrudeoil~x | cmcigoldlypiusd~x | 6.8123 | 2 | 0.033 |
| cmciwticrudeoil~x | ALL | 67.719 | 24 | 0.000 |

| | | | | |
|---|---|---|---|---|
| cmcigoldlypiusd~x | totalbitcoins | 11.83 | 2 | 0.003 |
| cmcigoldlypiusd~x | usdolllydepo | .38502 | 2 | 0.825 |
| cmcigoldlypiusd~x | eurolydepo | 10.021 | 2 | 0.007 |
| cmcigoldlypiusd~x | ukgbpeffectivee~x | 3.1984 | 2 | 0.202 |
| cmcigoldlypiusd~x | nikkei225stocka~x | 9.005 | 2 | 0.011 |
| cmcigoldlypiusd~x | eurostoxxpricei~x | 5.758 | 2 | 0.056 |
| cmcigoldlypiusd~x | japanyentoeurex~e | 4.6245 | 2 | 0.099 |
| cmcigoldlypiusd~x | eurotojapyenfxc~r | 1.3193 | 2 | 0.517 |
| cmcigoldlypiusd~x | sp500compositep~x | 4.4733 | 2 | 0.107 |
| cmcigoldlypiusd~x | dowjonesindustr~x | 5.5248 | 2 | 0.063 |
| cmcigoldlypiusd~x | opecoilbasketpr~e | 7.545 | 2 | 0.023 |
| cmcigoldlypiusd~x | cmciwticrudeoil~x | 5.6353 | 2 | 0.060 |
| cmcigoldlypiusd~x | ALL | 72.391 | 24 | 0.000 |

## ***FINDINGS AND CONCLUSIONS***

For the half-century futurists have predicted the advent of a cashless society[174]. Many of their predictions have been realized concerning the on- line and real-time payment system features without the intermediation of middlemen such as the Banks. However, cash as a form of payment is not dead yet. Bitcoin may constitute an electronic analog with attractive and competitive characteristics but it is not established in our everyday transactions. And for instance, it seems that its domination as currency is not an easy task.

Bitcoin constitutes a decentralized form of electronic payment because there is no central authority responsible for the issuance of electronic coins and there is no need to involve a trusted third-party when making online transactions. And this flexibility comes at a price if we take into account that the entire history of bitcoin transactions is publicly available.

In contrast to early electronic forms of payment which are connected with central institutions for money supply, such as Paypal and several others which are limited to certain communities, especially in the online games, Bitcoin represents a decentralized currency. This feature seems to be one of the main reasons that Bitcoin has gained popularity within the media and attracted a large user base, especially if we think about the generalized disappointment of people after the economic crisis of 2008.

In this dissertation we tried to examine the economic determinants in combination with the technical aspects that surround the development of Bitcoin ecosystem within the current international financial frame. Most importantly, apart from

[174] A. Anderson, D. Cannell, T. Gibbons, G. Grote, J. Henn, J. Kennedy, M. Muir, N. Potter and R. Whitby, (1996), An electronic cash and credit system, American Management Association.

assessing Bitcoin's added value and use we tried to understand whether its value and use in order to buy or sell goods increases over the time and of course to discover which factors influence its path.

In order to conduct this research empirically, we collected a set of trading data from recorded bitcoin exchanges, transaction data from the Bitcoin Blockchain and trading data for several official foreign currencies along with specific interest rates and stock indexes taken from official databases. Our research structure was based on two streams. Firstly, we gathered the theoretical background behind banking activity, disrupting innovations such as the digital cryptocurrencies and especially of Bitcoin from a vast spectrum and secondly, we conducted an empirical research concerning the financial and macro-economic effects which affect Bitcoin's price and trading volume, using econometrics principles.

In fact, money is one of the most valuable and sought after commodities in the world, affecting people in almost every facet of their life. One of the most controversial new innovations in this field are cryptocurrencies. The first cryptocurrency created and the most widely used, is Bitcoin. More precisely, bitcoin is a cryptocurrency that is not protected by governmental regulations or law, making it a challenge for central and financial authorities. The currency is fully decentralized, and unlike fiat money the government cannot affect its value. Its value is only affected by the members of the community it belongs.

On the other side, there is a significant innovation, a ledger called the block chain, publicly records all transactions with bitcoin keeping the users completely anonymous. And we believe that Blockchain will play a major role in reforming the banking activity and the nature of transactions, in the near future. Furthermore, the supply of bitcoins comes from a community activity, the "mining", a process which involves computing complex algorithm with increased difficulty over time, making it more expensive and resource intensive and thus less profitable as time go by.

The demand for bitcoin comes mainly from its decentralization and anonymity. But, also, from low transaction costs, its role as an investment vehicle which can lead to significant profit from its price volatility or its use in order to diversify a portfolio. Other possible uses for bitcoin include measures to avoid currency controls or other sources of governmental interference and even for tax evasion as it remains in most countries unregulated. There are, however, several disadvantages associated with this cryptocurrency.

As far as it concerns its decentralized feature, there is very little consumer protection in the case of fraud or theft. Moreover, stolen bitcoins are lost forever and bitcoins are also highly susceptible to code-based attacks by hackers. In addition, the Bitcoin price is very volatile and thus it is highly risky to hold on to many digital coins in a wallet because this may cause a lack of liquidity. In contrast, this fact does not constitute a serious risk for the official currencies. Moreover, the currency is also subject to taxation in many countries such as the US, Japan and Germany. In the end, technical members of the bitcoin community, have, also, cautioned that strong anonymity is not as beneficial as it seems for the sustainability of bitcoin system.

We must admit that the rise of the Bitcoin phenomenon has caused everyone from financial regulators to law enforcement globally to start observing the relative changes. Although, the Bitcoin community insists on keeping an ungovernable frame around the Bitcoin platform. Furthermore, Bitcoin's fans are convinced that bitcoin's real value is not in providing the world with a currency free from government intervention, but in the technology which is revolutionary. In fact, Bitcoin platform provides a secure system of verifying transactions, the Blockchain which has the potential to disrupt the way we exchange goods and services around the world.

The Block chain ensures that anyone who holds bitcoins also has an exact copy of the block chain, making it virtually impossible to create a forgery. This eliminates the need for trusted third parties, like PayPal and Visa, or even Banks to take part in financial transactions. So, Bitcoin's metagovernance design eliminates the need for trust in other

parties for processing payments and replaces it by the need to trust in the robustness of its own design.

Bitcoin also solves the so called “double-spending problem” which affects digital goods. It solves this by maintaining a P2P network and recording every single transaction. As a cryptocurrency, Bitcoin uses cryptography to control the creation and transfer of money.After an in-depth investigation of bitcoin, we found that although bitcoin uses no fancy cryptography, its design actually reflects a surprising amount of ingenuity and sophistication.

Most importantly, it addresses the problems of consensus more efficiently. It assumes that the majority of nodes in its network are honest and promotes a majority vote mechanism for dispute resolution. This feature greatly appeals to individuals who wish for a freely-traded currency, in a spirit similar to the original motivation for a distributed Internet.

There are many arguments, though, on whether the new virtual currency will succeed or fail to be established in the international Market. Despite the fact that bitcoin has several negative aspects such as fluctuations in the prices and other risks it has survived being the most popular and the most used among the existing digital currencies. Since the value of the bitcoin depends on hypothesis that other people will accept it in financial transactions we cannot be sure about its dominance yet. For instance, the digital currency is still too much in its infancy to have proven if its economic model is sustainable and if it is able to add value in our current financial system. In the end, the bitcoin system has provided a novel method of value exchange that could potentially serve as the foundation of further innovations concerning even the fiat currencies.

Any regulatory response towards Bitcoin or other digital currencies, then, should initially be limited and carefully measured. More precisely, as virtual currencies continue to evolve, incentives of users will change. Some abuses may disappear, while others may surge and it is still unknown on how the community is able to adapt to its technology and ready to confront the challenges of today’s traditional financial system.

Even if prohibition eventually proves to be a logical choice, it would likely never come close to addressing the real problems for which it was enacted. While ensuring that the exchanges with Bitcoins comply with the existing statutory scheme, they may only achieve the desired result on a domestic level, until the direction of the bitcoin economy is more fully realized. Thus, we conclude that for further development of bitcoin, an appropriate legal and regulatory framework is necessary to be adopted in order to mitigate the risks mentioned.

On the other side, there are economists who support that bitcoin is unlikely to succeed as an official currency for the general public as it has too many risks. For an innovation in currency to be successful, it needs to improve the properties of the already existing. However the technologies and innovation found within bitcoin as a cryptocurrency can still be applied to other technology and innovations too.

To sum up, Bitcoin might not be perfect but we notice that bitcoins are in essential circulation. More specifically, we predict that new applications will be built which will provide more use cases for different clients. But bitcoin is seven years old and it will take many more years for the infrastructure to be exploited and for these applications to be wide- spread worldwide. To imagine bitcoin's true potential, we need to think in decades, not in months or years. So, we can conclude that achieving a perfect cashless society needs a lot of time, but we surely have begun, in many ways mentioned, the shift towards it. In the end, as this is a completely new phenomenon, many questions in this dissertation remain unanswered. So, what is in store for Bitcoin, only time can tell.

# ***REFERENCES- BIBLIOGRAPHY-LINKS***


[2]Villasenor, J., Monk, C., & Bronk, C. (2011). Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-peer Networks, and Mobile Device Payments. Brookings Institution.

[3] http://www.investopedia.com/terms/p/peer-to-peer-lending.asp#ixzz4rdVn6UhV.

[4]Warwick, D. , Towards a cashless society, The Futurist, (2004).

[5] Federal Reserve Bank of New York,(2013), Household Debt and Credit Report.

[6] Ferguson, N., (2008),The Ascent of Money: A Financial History of the World, Penguin Books.

[7] Coase, R., H., (1937), The nature of the Firm, Economica.

[8]Buchanan, J. , M. (1990), The domain of constitutional economics, Constitutional Political Economy.

[9]Rochet, J. , C. and Tirole, J. ,(2003), Platform competition in two-sided markets, Journal of the European Economic Association.

[10] Roth, A., E. and Sotomayor, M. , A., O. (1992), Two-sided matching: A study in game-theoretic modeling and analysis, Cambridge University Press.

[11] Khayrallah A., Hickey J., Jasvinder S., Radia N., Xu V., (2014), Insights in Engineering Leadership White Paper, Engineering Leadership Professional Program UC Berkeley.

[12] King, Br., (2014), Breaking Banks: The Innovators, Rogues, and Strategists Rebooting Banking. Wiley Publishing.

[13]Khayrallah A., Hickey J., Jasvinder S., Radia N., Xu V., (2014), Insights in Engineering Leadership White Paper, Engineering Leadership Professional Program UC Berkeley.

[14] Boyd, G. (2002). Quatts, Virtual currency for gaming and bartering education on the web. British Journal for Educational Technology.

[15] Roth, F. ,(2009), The effects of the financial crisis on systemic trust, Intereconomics.

[16] Rennhard, M., & Plattner, B. (2002). MorphMix: Peer-to-Peer based Anonymous Internet Usage with CollusionDetection, Privacy in the Electronic Society.

[17] FATF Report. (2014). Virtual Currencies Key Definitions and Potential AML/CFT Risks. Paris: Financial ActionTask Force on Money Laundering ,OECD.

[18] ECB, (2012), Virtual currency schemes.

[19] Lamport, L. , Shostak, R., Pease, M., (1982), The Byzantine general's problem, ACM Transactions on Programming Languages and Systems.

[20] Glaser, F. , Haferkorn, M., Weber, M and Zimmermann, K., (2014), How to price a digital currency? Empirical insights on the influence of media coverage on the Bitcoin bubble. Banking and Information Technology.

[21] Peng, H., & Sun, Y. ,(2009). Network virtual money evolution mode: moneyness, dynamics and trend. InInformation and Automation, International Conference Information and Automation,IEEE.

[22] Kaplanov, N. M. (2012), Money for nothing and bits for free.

[23] Guo, J. , and Chow, A. , (2008), Virtual money systems: a phenomenal analysis. Paper presented at the 10th IEEE Conference.

[24] ECB, (2012), Virtual currency schemes.

[26] Irwin, D., Chase, J., Grit, L., & Yumerefendi, A. . (2005). Self-recharging virtual currency, ACM SIGCOMM workshop on Economics of peer-to-peer systems.

[27]Peng, H., and Sun, Y., (2009), Network virtual money evolution mode: moneyness, dynamics and trend. In information and automation, International Conference Information and Automation, IEEE.

[29] Wallace, B. , (2011), The Rise and Fall of Bitcoin, Wired.com. Conde Nast Digital.

[30] http:// www.cypherpunks.to/

[31] Wei Dai, B-Money, (1998), http:// weidai.com/bmoney.txt

[32] S. Nakamoto, (2008), Bitcoin: A peer-to-peer electronic cash system.

[33] Krohn- Grimberghe, A. and C. Sorge, (2013), Practical Aspects of bitcoin system.

[34] http://www.bitcoin.org

[35] J.P., Virtual Currency: Bits and Bob, (2011),The Economist

[37] Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony & A. Pentland (Eds.), Security and Privacy in Social Networks, Springer New York.

[38] Deloitte. (2014). The new gold rush.

[39] Digital Currencies – Bits and Bob, (2011), The Economist

[40] Goldman Sachs, (2014), All about bitcoin, Top of mind.

[41] Back A. et al., Hashcash-a denial of service counter-measure, http://www.hashcash.org

[42] Barber S. , Boyen X., Shi E., and Uzun E., (2013), Bitter to Better- How to make Bitcoin a better currency, In proceeding of financial cryptography

[43] Ron D. and Shamir A. , (2013), Quantitative Analysis of the full Bitcoin transaction graph, In proceedings of financial cryptography

[44] Chaum D.,(1982), Blind signatures for untraceable payments. In advances in cryptology: Proceedings of crypto.

[45] Wallace, B. (2011). The Rise and Fall of Bitcoin. Wired, http://www.wired.com/magazine/2011/11/mf_bitcoin/.
[46] Brito J., & Castillo, A. (2013). Bitcoin: A Primer for Policymakers,http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf.

[47] D. , Lyons, (2011), The web's secret cash: a novel version of money is sprouting online, letting people shop in anonymity, Newsweek.

[48] D. , Lyons, (2011), The web's secret cash: a novel version of money is sprouting online, letting people shop in anonymity, Newsweek.

[49] http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/

[50] Matonis, "Top 10 Bitcoin Merchant Sites", Forbes.
[51] D. Chaum, "Security without Identification: Transaction Systems to make Big Brother Obsolete",
Communications of the ACM, (1985).

[52] W. Dai, "B-Money", (1998), http://www.weidai.com/bmoney.txt .

[53] M.E. Peck, "Bitcoin: The Cryptoanarchists' Answer to Cash", IEE Spectrum, (2012).

[54] A. Greenberg,(2011), "Crypto Currency", Covering the worlds of data security, privacy and hacker culture, Forbes .
[55] Katz, J., & Lindell, Y.(2008). Introduction to Modern Cryptography. CRC Press.

[56] Kaliski, B. (2006), The Mathematics of the RSA Public-Key Cryptosystem. *RSA Laboratories*.

[58] FIPS 180-3, (2008), Secure Hash Standard, Federal Information Processing Standards Publication.

[60] https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm

[61] G. Medvinsky and C. Newman, (1993), NetCash: A design for practical electronic currency on the Internet, ACM Conference on Computer and Communications Security.

[62] C. Dwork and M. Naor, (1992), Pricing via processing or combating junk mail, In proceedings of the 12th annual international cryptology conference on advances in cryptology.

[64] J. Kroll, I. Davey and Ed. Felten, (2013), The twelfth workshop on the economics of information security, Washington DC.

[65] Kogent, (2009), Learning Solutions Inc.

[66] Katz, J., & Lindell, Y.(2008). Introduction to Modern Cryptography. CRC Press.

[67] Johnson, D. B., & Menezes, A. J. (1998), Elliptic curve DSA (ECDSA): an enhanced DSA. SSYM, 98, 13-13, http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa.pdf.

[68] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security.
[69] D. Hankerson, S. Vanstone, and A. Menezes, (2004), Guide to Elliptic Curve Cryptography,Springer.

[70] Johnson, D. B., & Menezes, A. J. (1998), Elliptic curve DSA (ECDSA): an enhanced DSA. SSYM, 98, 13-13, http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa.pdf.

[71] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security.
[72] D. Hankerson, S. Vanstone, and A. Menezes, (2004), Guide to Elliptic Curve Cryptography,Springer.

[75] C. Decker and R. Wattenhofer, “Information propagation in the Bitcoin network,” IEEE P2P Proc., (2013)

[76] Merkle, R., (1980), Protocols for Public Key Cryptosystems. Proceedings of the 1980 IEEE Symposium on Security and Privacy.

[79] FIPS , (2008),Secure Hash Standard, Federal Information Processing Standards Publication , National Institute of Standards and Technology.

[81] Brito J. , (2015), The law of bitcoin, iUniverse.

[82] Brito, J. , and Castillo, A. , (2013), Bitcoin : A primer for policymakers.

[83] https://blockchain.info/charts.

[84] J. Aron, (2012), Bitcoin online currency gets new job in web security, New Scientist.

[86] J. Kroll, I. Davey and Ed. Felten, (2013), The twelfth workshop on the economics of information security, Washington DC.

[87] International Journal of Scientific & Engineering Research, (2014).

[88] https://en.bitcoin.it/wiki/Block_chain

[89] G. O. Karame, E. Androulaki, and S. Capkun, (2012), Double-spending fast payments in Bitcoin, In proceedings of the 2012 ACM conference on Computer and Communications Security.

[90] M. Arias and Y. Shin, (2013),There are two sides to every coin – Even to the Bitcoin, a virtual currency, The Regional Economist.

[91] https://en.bitcoin.it/wiki/Controlled_supply

[92] https://en.bitcoin.it/wiki/Mining

[94] T. Bauman, (2013), Commerce and Reputation in Online Illegal Drug Markets, Princeton University.

[95] Shor, P., (1997), Polynomial-Time Algorithm for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing.

[97] Al. Harris and C. Conley, (2011), Will Bitcoin kill the dollar?,NVATE.

[98] J. Becker, D. Breuker, T. Heide, J. Holler, H. Rauer and R. Bohme, (2012), Can we afford integrity by proof-of-work? Scenarios inspired by the bitcoin currency, In workshop on the economics of information security.

[100] Sheridan B., (2011), Bitcoins: Currency of the geeks: the untraceable new virtual currency is exploding in usage, notoriety and value, Bloomberg Businessweek.

[102] Barber, S., Boyen, X., Shi, E., Uzun, E., (2012), Bitter to better - how to make bitcoin a better currency. In: Financial Cryptography and Data Security, Springer.

[106] Kroll, J. ,A. , Davey, I., C., and Felten, E., W., (2013), The economics of bitcoin mining or bitcoin in presence of adversaries, In proceedings of WEIS.

[107] The twelfth workshop on the economics of information security,(2013), WEIS.

[108] Schelling, T., C., (1960),The strategy of conflict, Harvard University Press.

[109] Skyrms, B.,(2003), The stag hunt and the evolution of social structure, Cambridge University Press.

[110] Shostak, F. ,(2004). How does money acquire its value? Ludwig Von Mises Institute.

[112] Varian, H. R. (2004), Why is that dollar bill in your pocket worth anything?, The New York Times.

[113] Glasner, D. ,(2011). The paradox of fiat money – Uneasy money.

[114] Korda, P., (2013): Bitcoin Bubble 2.0. Seeking Alpha. http://seekingalpha.com/instablog/7761841-patrik-korda/1616371-bitcoin-bubble-2-0.

[115] Smiling Dave (2013): About a Medium of Exchange Having to Be in Wide Use. Smiling Dave's Blog of Psychology, Economics, and Gentle Sarcasm. http://smilingdavesblog.wordpress.com/2013/10/15/ about-a-medium-of-exchange-having-to-be-in-wide-use/

[116] Mises, L. v. (1953). *The Theory of Money and Credit* (1912 ), New Haven: Yale University Press.

[117] Briere M., Oosterlinck, K., and Szafarz, A., (2013), Virtual currency, tangible return: portfolio diversification with bitcoins.

[118] Menger, Carl (1871): Principles of Economics. Ludwig von Mises Institute, (2004)

[119] Hearn, Mike (2013): Conference 2013 - Mike Hearn Interview , https://soundcloud.com/mindtomatter/conference-2013-mike-hearn.

[120] Glazer, F., K. Zimmermann, M., Haferkorn, M., C., Weber, and M., Siering, (2014), Bitcoin- Asset or currency? Revealing users' hidden intentions, Proceeding of the 22nd European conference on information systems.

[121] Krugman P., (2011), Golden cybervetters, New York Times.

[122] Luther, W. J., and White, L. H. (2014) "Can Bitcoin Become a Major Currency? George Mason University, Department of Economics Working Paper.

[123] Grinberg, R., (2011) "Bitcoin: An Innovative Alternative Digital Currency." Hastings Science and Technology Law Journal.

[124] Andreessen, M. (2014) "Why Bitcoin Matters." dealbook.nytimes.com/2014/01/21/why bitcoin Matters.

[125] https://news.bitcoin.com/beware-bitcoin-economy-bust/

[126] Taylor J., (2009), Getting off track: How government actions and interventions caused prolonged and worsened the financial crisis, Stanford, Hoover Institutions Press.

[127] Leijonhufvud, A.,(2008), Keynes and the crisis, CEPR Policy Insight.

[128] Kaminska I., (2013), Financial Times Alphaville blog bitcoin mania series.

[130] R. Grinberg, Bitcoin: An Innovative Alternative Digital Currency, 4 Hasting Sci.& Tech. L.J. (2011).

[131] Old Kharif, Bitcoin 2.0 Shows Technology Evolving Beyond Use as Money, Bloomberg, (2014).

[132] CEA, CFTC Glossary, Exempt Commodity.

[133] Fed., (2012), http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-18003a.pdf

[134] Federal Reserve Board, (2011).

[135] European Parliamentary Research Service, (2014).

[136] Reid, F. , and Harrigan, M., (2011), An analysis of anonymity in the bitcoin system.

[141] Brezo, F. , and Bringas, P., (2012), Issues and risks associated with cryptocurrencies such as bitcoin, The second international conference on social eco-informatics.

[142] Moore, T. ,and Christin, N. , (2012), Beware the middleman: empirical analysis of bitcoin-exchange risk.

[146] Gilson, D., (2013), Bitcoin blockchain grows to 8GB, Coindesk.

[147] Bradbury, D., (2013), Bitcoin network recovering from DDoS attack, Coindesk.

[148] Bacard, A. (1994). A cashfree society: Nirvana or nightmare? The Humanist.

[142] Moore, T. ,and Christin, N. , (2012), Beware the middleman: empirical analysis of bitcoin-exchange risk.

[147] Bradbury, D., (2013), Bitcoin network recovering from DDoS attack, Coindesk.

[149] J. Davis , (2011), The cryptocurrency, Bitcoin and its mysterious inventor, New Yorker.

[150] B. Kerschberg, (2011), Credit card transactions – how safe is your personal information?, Forbes.

[151] International journal of critical infrastructure protection, (2013)

[152] Presentation, Misha Glenny, Hire the Hackers!, TED (2011),http://threatpost.com/en_us/blogs/ted-global-misha-glenny-says-hirehackers-091511.

[153] N., M., Kaplanov, (2012), Nerdy Money: Bitcoin, The Private Digital Currency, and the Case
[156] Against its Regulation, 25 Loy. Consumer L. Rev. 111, 130.

[157] M. Santori, Bitcoin Law: Money transmission on the state level in the US, CoinDesk, (2013), http://www.coindesk.com/bitcoin-law-moneytransmission-state-level-us/.

[158] G. Farrell, N.Y. Subpoenas Bitcoin Firms in Probe on Criminal Risk, Bloomberg, (2013), http://www.bloomberg.com/news/2013-08-12/n-y-regulator-subpoenasfirms-over-bitcoin-crime-risks.html.

[159] Am. Toor, (2013), US seizes and freezes funds at biggest Bitcoin exchange, The Verge.

[160] Seizure Warrant – In the Matter of the Seizure of The contents of one Dwolla account, (2013), http://cdn.arstechnica.net/wpcontent/uploads/2013/05/

[161] Sealed Complaint – United States of American v. Robert M. Faiella, a/k/a "BTCKing," and Charlie Shrem, No. 14-MAG-0164, (2014), http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR/Faiella, %20Robert%20M.%20and%20Charlie%20Shrem%20Complaint.pdf.

[161] Greenberg, An., (2013), FBI says it's seized $28.5 million in bitcoins from Ross Ulbricht, alleged owner of Silk Road, Forbes.

[162] 31 U.S.C. 5330(a)(1).

[163] 31 C.F.R. §1010.100.

[164] 18 U.S.C. §1956.

[166] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FinCEN, http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html , (2013).

[167] Gruber, supra note 102.

[168] EPRS Bitcoin. Market, economic and regulation, Http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI%282014%29140793_REV1_EN.pdf

[169] Constitution of the Argentine Nation, section 75, online at http://www.biblioteca.jus.gov.ar/argentina-constitution.pdf

[170] The Argentine Civil Code, art. 2345[2311], http://archive.org/stream/argentinecivilc00whelgoog/argentinecivilc00whelgoog_djvu.txt

[171] Bitcoins aren't tax exempt, Revenue Canada says, http://www.cbc.ca/news/business/bitcoins-aren-t-tax-exempt-revenue-canada-says-1.1395075