Bitcoin: a new way to understand Payment Systems

by

Javier Iglesias de Ussel

MSc, Person, Society, and Law by University Complutense, Madrid (2009)
Double BA, Business Administration and Law by ICADE, Madrid (2008)

Submitted to the MIT Sloan School of Management in Partial Fulfillment of the Requirements for the Degree of

Master of Business Administration

at the

Massachusetts Institute of Technology

June 2015

Signature of Author Signature redacted

Javier Iglesias de Ussel
MIT Sloan School of Management
May 8, 2015

Certified by Signature redacted

Roberto Rigobón
Professor of Applied Economics
MIT Sloan School of Management
Thesis Supervisor

Accepted by Signature redacted

Maura Herson
Director MBA Program
MIT Sloan School of Management

Bitcoin: a new way to understand Payment Systems

by

Javier Iglesias de Ussel

Submitted to the MIT Sloan School of Management on May 8, 2015 in Partial Fulfillment of the Requirements for the Degree of Master of Business Administration

Abstract

Bitcoin has recently raised substantial attention from a variety of players: media, academia, and regulators. While the price of Bitcoin has continuously and substantially gone down since its peak in December 2013, other metrics indicate a more optimistic prospect. The adoption of Bitcoin is increasing rapidly, even in off-line channels, with companies such as Microsoft, Paypal, EBay, Dell, and Expedia now accepting Bitcoin payments. Venture capitalists are avid for investment opportunities in Bitcoin related opportunities, such as online wallets and remittance payment systems among others. Bitcoin has a prominent present as a payment technology and the potential to grow as a relevant alternative to credit cards and bank transfer. However, some features of its configuration will hinder its future growth. In this paper, I explore what Bitcoin is today and how could it be improved.

Thesis Supervisor: Roberto Rigobón
Title: Professor of Applied Economics
MIT Sloan School of Management

Acknowledgements

I would like to express my sincere gratitude to MIT Sloan School of Management. Its academia, students, and excellence ecosystem have empowered me to write this document. In particular, I would like to assert my deep gratitude to Roberto Rigobón, my professor and thesis supervisor. His energy, passion, and continued support have been instrumental for the genesis of this document.

I am very thankful to professor Christian Catalini for sharing with me his experience on the MIT Bitcoin project and his research on crowd-funding and to Dan Elitzer, president of the MIT Bitcoin club, for organizing several events and building a solid community around Bitcoin in Boston. These events provided me with a privileged access to the ecosystem of users and investors in Bitcoin.

Diego Perez Baudin is the manager at Do Eat, the first restaurant to accept Bitcoin in Madrid. To him I owe my first off-line interaction with Bitcoin. Emilio Ontiveros is the Chairman of Analistas Financieros Internacionales and an expert in the Spanish and Latin American financial sector. In my conversations with him I learnt how traditional financial institutions, particularly those in Latin America, are reacting to Bitcoin.

Finally, I will take this opportunity to thank my parents Julio and Carmen, both university professors, and my brothers Enrique and Ignacio for their permanent encouragement, support and attention.

Without all these people, and many others who have helped me directly and indirectly, the present document would not have been completed.

TABLE OF CONTENTS

List of Figures

Acronyms and Definitions

Bitcoin or bitcoin? Bitcoin refers to the platform, technology, and community around Bitcoin; bitcoin (lowercase "*b*") refers to the unit of that currency. The following quote clarifies the difference: *"Bitcoin with a capital 'B' is a peer-to-peer network that allows for the proof and transfer of ownership without the need for a trusted third party. The unit of that network is bitcoin with a little 'b'"*. Goldman Sachs, March 2014

Blockchain: Unlike cash transactions, where a note or coin does not carry info on the previous transactions that it has been used for, Bitcoin transactions carry a public record with the history of all the previous transactions in chronological order. A new block is incorporated to the chain on average every ten minutes

BTC: Refers to bitcoin

Satoshi Nakamoto: Pseudonym of the creator of Bitcoin and author of its founding paper: "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (published in 2008). The real identity behind Satoshi Nakamoto remains unclear. It is even unclear whether it refers to one or more persons.

Satoshi: Satoshi is the smallest unit of Bitcoin that the network supports today. It is a hundredth millionth of a bitcoin (1/100,000,000 or 0.00000001 bitcoin). In the future this configuration may be changed to allow for further subdivisions.

"Give me control of a nation´s money supply, and I care not who writes its laws"

Mayer Amschel Bauer Rothschild

Introduction

The long story of money until the XX century was characterized by the state's efforts to control the supply money. The ultimate expression of this trend was the quest by the state of the monopoly in the supply of money. Kevin Dowd and Richard Timberlake published in 1998: *"Money and Nation State"*, a book that describes the efforts made by states to accomplish this objective.

One of the central characteristics of the history of money has been the proliferation of centers for the issuance of money. In the past, economic transactions frequently took place in reduced geographic areas. This fueled the use of local money within nearby populations. However, the development of the state in different countries progressively eroded this diversity of money and imposed the money coined by the State.

In the XIX century, the importance of money as a symbol of national unity and sovereignty grew significantly. For the first time in history, money was perceived as a symbol as relevant as the flag or the national hymn. This was precisely one of the reasons that Mrs. Thatcher, Prime Minister of the United Kingdom from 1979 to 1990, used to oppose the integration of the UK in the Euro Area. She refused to give away to the European institutions one of the core values of the sovereignty: the right to issue money.

The relevance of money as a symbol of sovereignty becomes evident at times of high political instability such as wars (particularly civil wars). In this context, one of the typical targets for confrontation is money. Manipulation of money is used as a weapon against the enemy; following the conquest of an area to the enemy, the coin is changed as an evidence of the change in sovereignty over that territory. Several examples exist on this direction. One recent example took place during the Spanish Civil War (1936-1939), immediately after the conquest of a new territory new coins were issued locally and old money was confiscated.

On the other hand, XX century has seen the emergence of different realities of varied nature that have eroded the monopoly of the State in the control, issuance, and usage of coin. The Euro is one example in this direction. The Euro has its origin in an agreement between States. However, these States do not give away political sovereignty to the European Union. Credit cards are another instrument that avoids the direct use of physical money by citizens. Cards have started to become wide spread for small payments (i.e.: in parking, cafeterias, etc.), substituting pocket money; mobile payments (i.e.: M-Pesa in Kenya and Venmo in the US) are also utilized to avoid paying with loose change. E-commerce is an additional tool that avoids the direct usage of money.

Furthermore, the economic crisis has increased the footprint of the barter, the most ancient economic exchange. Exchange of holiday homes for short periods of time, such as summer holidays, is one of its most frequent forms. *"Sharing economy"* is on the rise, with activities such as direct rental of vehicles through internet or shared rental of parking slots for use on different time frames (i.e.: weekdays vs. weekends, or different times within the day), without intermediation.

The reality of money has become so inherent to manhood, that even in the most hostile contexts money-like instrument arise. As illustrated in the brilliant movie: Stalag 17 (1953, directed by Billy Wilder), allied World War II prisoners of war used cigarettes as a substitute of money. That allowed prisoners to trade the goods they received from the Red Cross, such as biscuits, milk, soap, or chocolate, into a common currency. The relatively small value of a single cigarette made it a *"unit of account"*, durability acted as *"store of value"*, and widespread acceptance was instrumental for cigarettes to achieve the status of *"method of payment"*.

These are some of the evidences of the emergence of new modalities of exchange not based in the utilization of coins and notes. The diversion from physical money is testimony of the heterogeneity and pluralism of the developed societies in the XXI century. Money is not only linked with the economic life, but also has social and cultural ramifications.

It is evident that the society of communication, globalization, and internet will also impact money. For this reason, the surge of digital money: the creation by Satoshi Nakamoto of Bitcoin, is a symbol and manifestation of the internet era.

Chapter 1 – What is Bitcoin and how does it work?

1. The Bitcoin Cycle

Bitcoin is a crypto currency. It allows users to measure value (unit of account), pay for goods or services (mean of exchange), and hold it on a virtual or physical wallet therefore allowing to postpone the decision to spend it (deposit of value). These functionalities have many elements in common with those of traditional currency.

On the other hand, Bitcoin does not emulate the traditional system. Transactions take place in the blockchain and away from the traditional financial system (i.e.: credit cards and bank accounts do not act as intermediaries). Furthermore, it has been created without underlying assets or Government backing. In fact, its creators have been vocal about the benefits of being independent from political interferences.

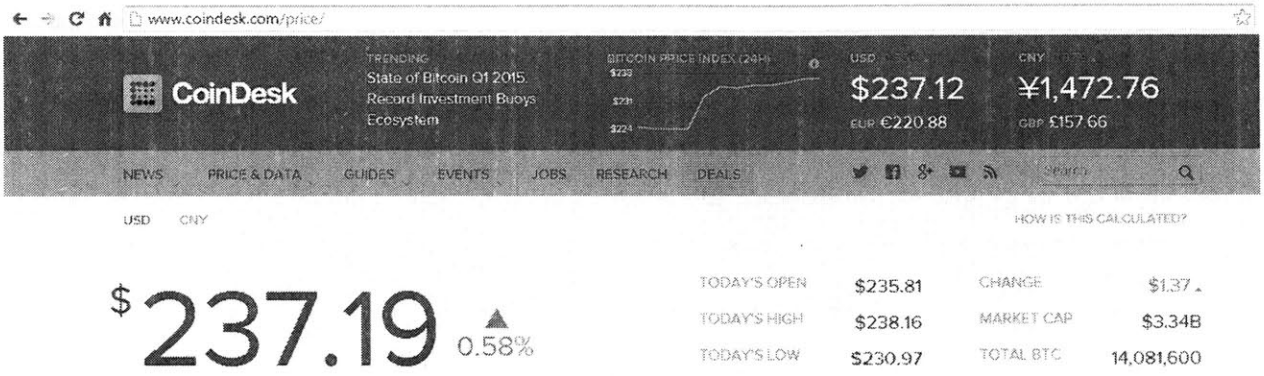
There are two ways for someone to get hold of bitcoin. First and most frequent, a person may directly buy bitcoin at any of the Bitcoin wallets available (i.e.: Coinbase, etc.). Second, a person may mine Bitcoin. In a nutshell, mining consists in verifying a block of transactions through the solution of a complex mathematical problem. The first miner to successfully verify each block gets compensated with a number of newly issued Bitcoin.

The outline of the process is as follows:

2. Buying and selling bitcoin

A person buys bitcoin or sells in exchange of dollars or other currency. For example, as of 22nd April 2015 (14.17pm Eastern Standard Time), the cost of one bitcoin was 237.19 dollars, 220.88 euros, 157.66 GB pounds, or 1,472.76 Chinese Yuan. The table below from Coindesk, one of the most relevant research houses on Bitcoin, shows the actual prices.

Figure 1: Spot price of bitcoin



State of Bitcoin Q1 2015: Record Investment Buoys Ecosystem

$237.12 EUR €220.88

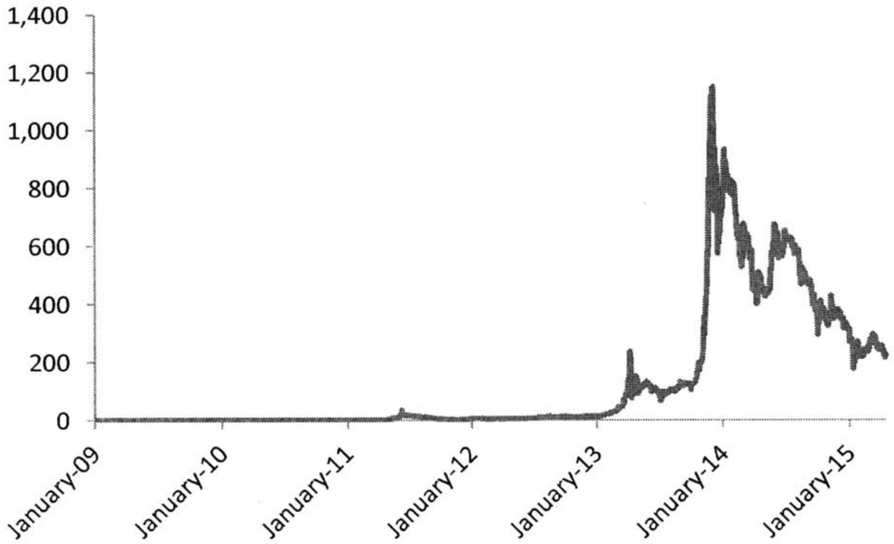
¥1,472.76 GBP £157.66

$237.19 ▲ 0.58%

TODAY'S OPEN	$235.81	CHANGE	$1.37 ▲
TODAY'S HIGH	$238.16	MARKET CAP	$3.34B
TODAY'S LOW	$230.97	TOTAL BTC	14,081,600

Source: Coindesk, 22nd April 2015 at 14.17pm Eastern Standard Time

Figure 2: Bitcoin price evolution, in dollars

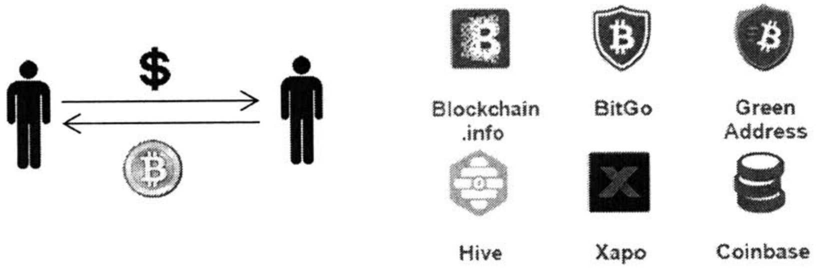


Source: Blockchain.info, as per 22nd April 2015

Bitcoin transactions are executed at the spot trading value at the time of the transaction. The price of bitcoin fluctuates permanently: 24 hours per day, 7 days per week, every day of the year. This is different from the stock market (i.e.: NYSE, etc.) that only accepts trades certain hours of the day and the week, typically 9.30-4pm Monday to Friday.

Bitcoin transactions take place through intermediaries or *"wallets"*. There is no official place to buy bitcoin. Numerous wallets have been established as private companies. They work autonomously and provide the intermediation service. Frequently, they earn a fee from each transaction. For example, Coinbase charges 1% fee per transaction (i.e.: you acquire 100$ worth of bitcoin, Coinbase will charge 1$ upon acquisition). Another intermediary, Circle, does not charge any fee.

Figure 3: Acquisition of bitcoin



Source: self-elaborated

A number of platforms exist where bitcoin can be acquired. Given the decentralization spirit of the network, it is the user responsibility to use a wallet that is reputed and secure. In the past, intermediaries have been hacked or engaged in fraudulent activities. The bankruptcy of Mountain Gox in early 2014 is perhaps the most relevant example.

In this context, users should pay attention to the reputation of the intermediary they choose. If you hold cash, it does not make a difference to hold one specific 100$ note or another. Similarly, if you have a bank account, it does not really matter if you have it with one bank or with another, as they are all FDIC insured. However, if you hold bitcoin, more attention should be placed as to what intermediary you are using. Different intermediaries will have different reputation, fees, escale, etc. It is also important to note that Bitcoin do not pay interest. In this sphere, they work like cash or real assets: real estate, art, etc.

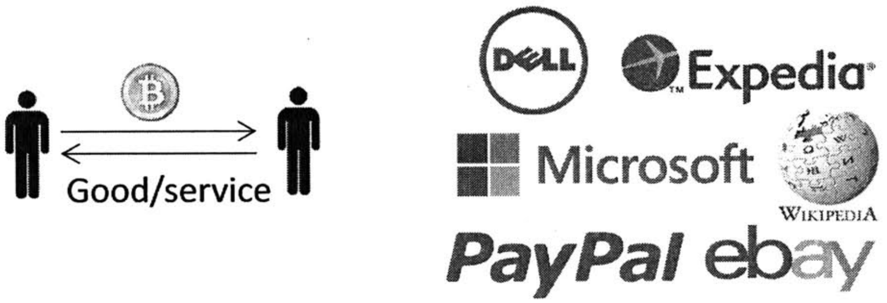
I personally own one bitcoin through Coinbase and a fraction of a bitcoin through Circle, another platform. Coinbase, headquartered in San Francisco, is one of the most active bitcoin companies. In January 2015, it raised 75 million dollar from New York Stock Exchange (NYSE), the Spanish Financial Institution BBVA, and the former CEOs of Citigroup and Reuters. On the other hand, Circle is a Boston based initiative that recently received a capital injection by Goldman Sachs, it provides insurance for its deposits, and does not charge fees for acquisition or disposal of bitcoin. I choose Circle and Coinbase after exploring some of the alternatives. Circle and Coinbase are two of the many valid Bitcoin intermediaries.

3. Paying for goods or services with bitcoin

Once you own a bitcoin, you can either hold or spend it. If you decide to hold it, it will fluctuate in value relative to currencies such as euro, dollar, etc. Alternatively, you may use it to buy assets. A person may buy certain goods or services paying with bitcoins.

The acceptance of bitcoin among merchants (and volume of transactions) is quickly increasing. Companies such as Paypal, EBay, Dell, Expedia, EBay, and Wikipedia already accept transactions denominated in bitcoin. However, in absolute terms the acceptance of bitcoin is far lower than that of credit cards. If Bitcoin is successful, over time, its acceptance will be widespread.

Figure 4: Acquisition of good or service using bitcoin



Source: self-elaborated

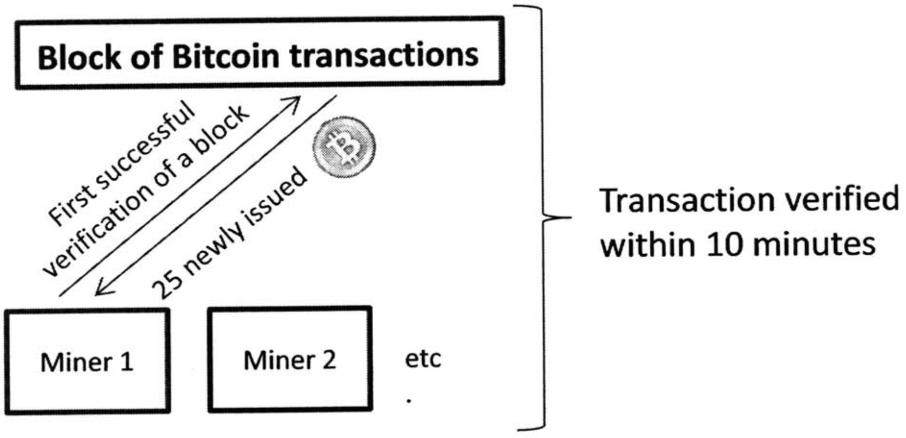
Transaction is executed (and Bitcoin transferred to merchant) within as little as ten minutes and frequently takes place at the market BTC to USD exchange rate. The acquirer can choose whether to pay a transaction fee. If a transaction fee is paid, the transaction will be executed more quickly. On the other hand, the merchant chooses the exchange rate applied to the transaction. In theory they could apply a markup or a discount. In *"Bitcoin as Money?"* S. Lo and J. C. Wang, of the Federal Reserve Bank of Boston, show that on average these two online retailers applied an average 0.2-0.9% discount over the spot foreign exchange rate during May-June 2014. It remains unclear the underlying rationale for this behavior and whether other merchants do the same. However, one possible explanation is that merchants partially share with customers the savings they achieve from accepting Bitcoin. The case of Avalancha, a retailer in Argentina points to this direction (see epigraph 3.1 in chapter 3 for more detail).

It is important to note that the execution of the transaction takes place in the Bitcoin network through the mining process. Unlike other methods of payment (Paypal, Apple Pay, Google Wallet), Bitcoin transactions are not linked to the traditional financial system (i.e.: to bank account, credit or debit card). The only link with the traditional financial system is the acquisition (and disposal) of Bitcoin as they are paid with traditional money. Bitcoin transactions are cleared through mining, a new and innovative process.

4. Mining or verification of transactions

Verification of Bitcoin transactions takes place through mining, a competitive method. A block of transactions is executed on average every ten minutes. Each block of transactions is executed through the competitive solution of a complex mathematical problem by the mining community.

Figure 5: Overview of the mining process

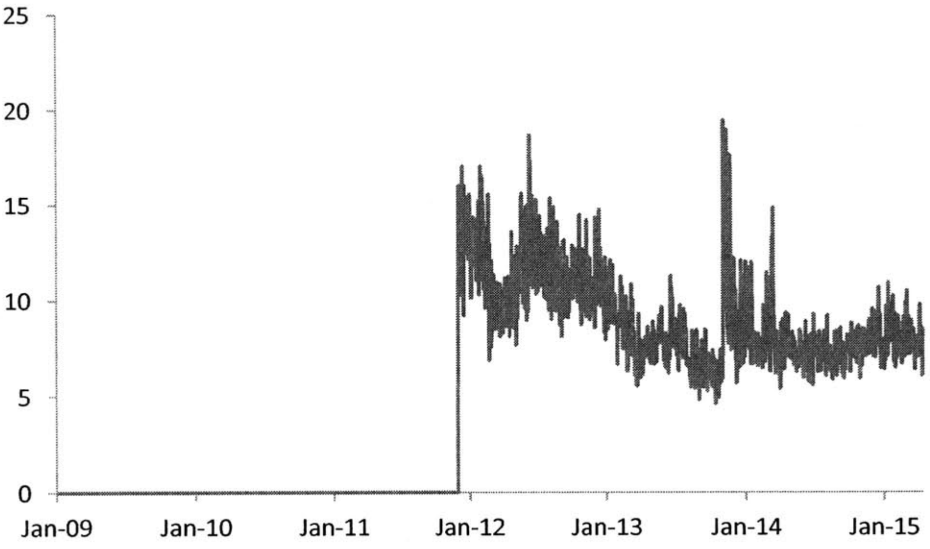

Block of Bitcoin transactions
First successful verification of a block
25 newly issued
Miner 1
Miner 2
etc
Transaction verified within 10 minutes

Source: self-elaborated

Miners are individuals or groups of individuals that join forces and computing power to solve each problem. The first miner to correctly solve each block of transactions and get his solution verified by the broader mining community gets compensated with 25 newly issued bitcoin plus whatever fees users have voluntarily decided to pay to expedite the execution of their transactions (on average around 0.5 bitcoin more per block).

The difficulty of each mathematical problem is adjusted so that on average, a block of transactions is verified every 10 minutes. The graph below shows the average confirmation time of transactions which trends towards 10 minutes. This timing is a convention and could be amended (increased or reduced) in the future.

Figure 6: Average confirmation time of BTC transactions (minutes)



Source: Blockchain.info, as per April 2015

The mining process has two relevant features. On the one hand it is collaborative by nature. On the other, it records each new block of transactions in the context of all the previous blocks in what is usually refered to as blockchain.

The mining process is collaborative by nature. Unlike transactions in the traditional financial system, Bitcoin transactions involve no verification by a central authority. Verification is executed by the community of miners in a competitive process. They compete to successfully verify each block of transactions. The first miner or group of miners to successfully verify a transaction gets compensated (currently receives 25 bitcoins). And the solution is consequently verified by the rest of the community. The mining process is therefore strongly decentralized.

Initially, mining could be executed from a desktop computer. Today, the competition among miners has increased. As a result, expensive computing power (software and hardware) is required to successfully mine.

The record of Bitcoin transactions is held through Blockchain. Each new block of transactions is recorded in the context of all the previous blocks in chronological order. This adds complexity to the Bitcoin mining process. And it facilitates the reconciliation of transactions through the public ledger.

The public ledger is the skeleton of the Bitcoin network. All past transactions are incorporated to the public ledger as long as they are verified by the mining community. On the other hand, all new transactions will be assessed against the public ledger. For example, if someone makes a Bitcoin payment, miners will check whether he has a balance of bitcoin sufficient to support the payment.

The key feature of the blockchain process is that it takes place through mining, a public verification. This is distinct from the traditional payments systems that take place through central verification by banks, whether directly (bank transfers) or indirectly (credit card payments).

The mining process is understood by many experts as one of the greatest innovations that Bitcoin has introduced, with multiple potential applications in areas beyond the transactions payments services. Bill Gates is not an Bitcoin enthusiast. However, he referred to it as *"an exciting new technology"*.

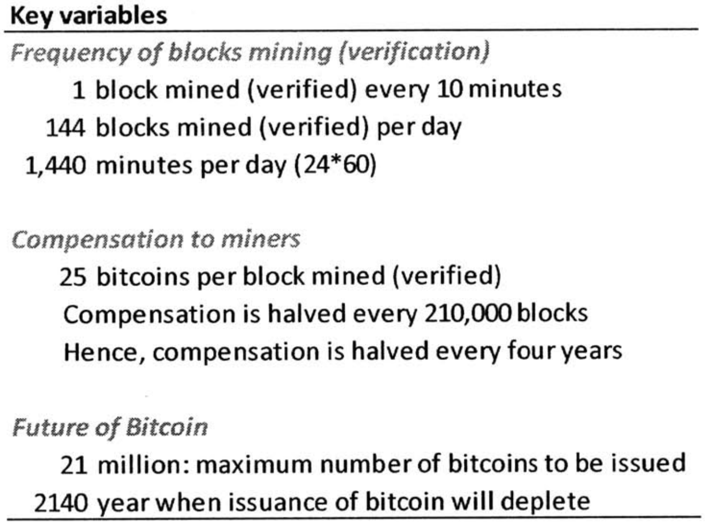
5. Additional considerations

In this epigraph I will cover the issuance of bitcoin through mining and the limitation in the total number of available bitcoins.

Bitcoins are issued as compensation for the first miner or group of miner that verifies a block of transactions. The compensation scheme has been designed in such a way that it is halved approximately every four years. From 2009 to 2013, the compensation was 50 bitcoin/block (remember that a block is verified every ten minutes). The current compensation is 25 bitcoin/block, it will be halved again in 2017, and so on so forth.

The maximum number of bitcoins to be issued is 21 million. At the above described path of issuance, it is expected that this will happen by year 2140. The table and the chart below describes the key mechanism.

Figure 7: Key variables on Bitcoin supply



Key variables

Frequency of blocks mining (verification)

1 block mined (verified) every 10 minutes
144 blocks mined (verified) per day
1,440 minutes per day (24*60)

Compensation to miners

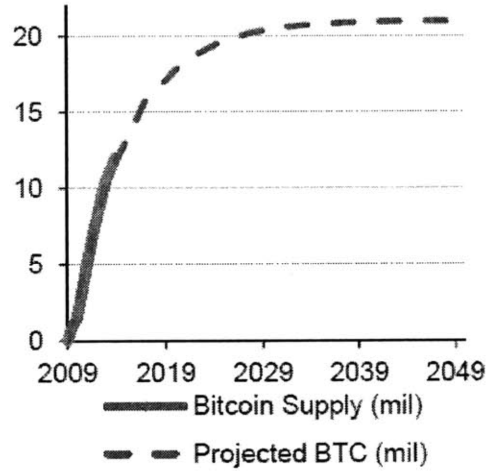
25 bitcoins per block mined (verified)
Compensation is halved every 210,000 blocks
Hence, compensation is halved every four years

Future of Bitcoin

21 million: maximum number of bitcoins to be issued
2140 year when issuance of bitcoin will deplete

Source: self-elaborated

Figure 8: Bitcoin supply over time (million units issued)



Source: Bank of America: *"Bitcoin: a first assessment"*, issued on the 5th of December 2013

The limited supply of bitcoin to 21 million has several consequences. On the one hand, Bitcoin supporters argue that it will result in a price increase over the long run. This would be further fueled by another phenomenon: the potential loss of bitcoins due to loss of passwords or other circumstances (i.e.: holders may die without having passed the details to successors, etc.). These elements would theoretically result in an appreciation of the remaining bitcoin.

On the other hand, the expected downward trend of the compensation for miners has a clear consequence: bitcoin transaction fees will inevitably increase in the medium run to offset the diminished and ultimately eliminated compensation in Bitcoin.

The traditional monopoly by the State in the issuance of money has been substituted for the algorithm complexity of mining Bitcoins.

Chapter 2 – Is Bitcoin money?

1. Historical precedents of money

Before money existed, people had to agree one to one exchanges. This limitation made transaction difficult to execute. For example, if someone owned a cow and wanted to exchange it for five sheep, he had to find someone that had opposite intentions. Obviously, it is not easy to find someone that had five sheep and wanted to exchange them for a cow.

Bartering had several limitations. It required double coincidence of needs. A transaction would not take place unless the two parties had something of similar value that the other party wanted. It was difficult of exchange things of different value (i.e.: very high vs very small value). It required simultaneous need for exchange (i.e.: timing can impede an exchange if I want something now but someone can only offer it later). Furthermore, it limited the complexity of the goods that could be transacted. The manufacture of popular goods was incentivized; other goods had difficult access to the market.

In this context, money emerged and Governments, due to its collective dominance, slowly and steadily started gaining terrain in the regulation of money. Initially, money had an underlying value due to its material composition. Coins were made of gold, silver, and copper and that drove their value. Governments minted the coins. But the value of those coins derived from the material composition of those coins.

Over time, this changed. Governments decided to increase their control of money. They took the coins and exchanged them for newly issued notes that had a claim right on the gold. Citizens no longer had the gold on their hands. They had pieces of papers that they could trade with. If they wanted, citizens could also exchange those pieces of paper for gold. Consequently, Governments held large reserves of gold on their coffers.

Finally the gold standard fell. Governments decided not to allow citizens to change the notes for the gold. In this context, the balance changed. Money was still an asset: it was generally accepted for trade. However, it was no longer backed by an asset. This was the birth of the fiat money, where trust and confidence were the key drivers of money.

All over the world, Governments fight companies that engage in monopoly practices. Companies such as Microsoft, Google, and Gazprom have been subject to antitrust cases. The underlying rationale for these actions is that monopolies hinder economic prosperity. In this context, it is surprising that Government have enforced the monopoly in the issuance of money since the end of the 19th century.

In his article: *"Milton Friedman and the Case Against Currency Monopoly"*, George Selgin, a professor of Macroeconomics in the University of Georgia, opens a debate on whether Governments should hold a monopoly in the issuance of money.

George Selgin analyzes the evolution of Milton Friedman view on this subject: *"Despite having been an unflinching champion of classical liberalism and free markets, Milton Friedman at first (Friedman 1960: 4–9) shared the common view concerning the necessity of official currency monopolies".*

Over time, the author notes, Friedman opened his mind to eliminating the monopoly of Governments in the issuance of money: *"Friedman ultimately concluded* (Friedman and Schwartz 1986: 52) *that there is, after all, 'no reason currently to prohibit banks or other groups from issuing hand-to-hand currency' ".*

Bitcoin has emerged as a potential alternative to fiat money. It is still questionable whether it will achieve the mass scale it seeks. Bitcoin' configuration is grounded on free market ideology and aversion towards central regulation. In this context, it is interesting to analyze how regulators over the world address this new reality. Epigraph 3.4 of Chapter 3 covers the regulation in the US and other countries as well as its underlying rationale.

2. Bitcoin and the traditional functions of money

Economic theory has traditionally defined (1) unit of account, (2) mean of exchange, and (3) deposit of value as the three functions for money. In the following epigraph I will define each of these functions and analyze how Bitcoin falls into each of these functions.

The function of unit of account is not exclusive to formal money. Under some circumstances, alternative forms of money have emerged. In his book *"Macroeconomics"*, Greg Mankiw has documented that allied World War II prisoners of war used cigarettes as a substitute of money. The Red Cross distributed goods such as biscuits, milk, soap, cigarettes, and chocolate among prisoners. These packs were distributed to without taking into account their preferences. In this context, many, including non-smokers, choose to trade those goods into cigarettes that acted as a single currency. For example, Mankiw notes that a shirt was worth 80 cigarettes and some prisoners would wash the clothes of others in exchange of 2 cigarettes.

The relatively small value of a single cigarette made it a unit of account, durability acted as store of value, and widespread acceptance was instrumental for cigarettes to achieve the status of method of payment.

In the following epigraph, I will briefly describe the three functions of money and evaluate how Bitcoin fits under each of them.

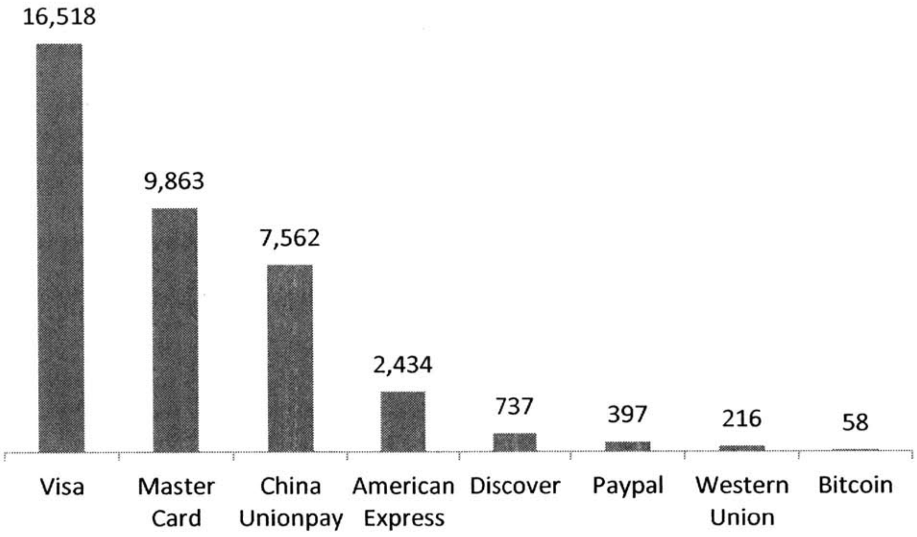
2.1. Unit of account

Unit of account measures to what extent the value of things is measured in a common unit of measure. In the US the value of virtually all goods and services is referenced to the dollar. The price of a bag of chips, a new BMW, and the average salary per hour is around 1$, 35,000$, and 25$ respectively. In the US the dollar is a universal benchmark of value. It is very easy to observe the relative value of different goods and services. Therefore, the dollar complies with the unit of account function of money.

Does Bitcoin comply with this function of money? Only partially.

On the one hand Bitcoin is not yet generally accepted. You can't buy a bag of chips, a new BMW, or get paid in bitcoin. Today, Bitcoin allows you to buy only a limited set of goods and services (some examples are outlined in epigraph 3 of Chapter 2). As a result of this, the magnitude of the transactions is still very small relative to other payment systems. Bitcoin has not yet achieved (and may never achieve) mass adoption.

Figure 9: Average daily payment volume (million dollar)



Source: The Nielsen Report, company websites, Sterne Agee, as per September 2014

On the other hand, even merchants that accept bitcoin most frequently set up prices in their local currency (i.e.: dollar) and then convert to the spot Bitcoin/local currency exchange rate at the time of a transaction. For example, on the 22nd April 2015, the price of a standard laptop in Dell website was 741$. The option to pay Bitcoin was available. You could pay 3.13 bitcoin (at the prevailing exchange rate of 237$/bitcoin). In this context, Bitcoin is only a secondary benchmark of value. Price of goods is set up in dollars and then converted to Bitcoin.

Microsoft is another example of a retailer that accepts Bitcoin payments. However, Microsoft is not yet accepting direct payments for its goods. Today, you can add money to your Microsoft account using your Bitcoin. And then, buy goods at Microsoft online store. The option to pay directly for goods does not yet exist.

This risk averse attitude by merchants is natural. Bitcoin track record has been extremely volatile. The cost base of merchants is in their local currencies (not in Bitcoin). Therefore, they prefer to limit their exposure to this extreme price volatility.

2.2. Mean of exchange

Confidence is the most important asset for fiat money. One will only accept money if he is confident that others will also accept it. General acceptance is a key feature for an instrument to gain the right to be defined as money.

Money is only useful if it allows its holder to buy multiple goods and services. Otherwise, it would not be money but a token or voucher that is only accepted in exchange for a very narrow set of goods or services.

For example, a Starbucks voucher may not be defined as money. It provides you the right to acquire a single good (coffee) in a relatively small set of places (Starbucks shops). With these limitations, clearly a Starbucks voucher is not enough to qualify as a proper mean of exchange.

Different citizen may have different objectives when adopting bitcoin. They may want to buy bitcoin and hold it, putting an emphasis on the store of value that we will visit on the next epigraph. Or they may want to buy and sell bitcoin, putting an emphasis on the mean of exchange.

Does Bitcoin qualify as a mean of exchange? Bitcoin is not backed by an asset (gold) or a sovereign institution (traditional currency). Hence, confidence is the greatest asset. In order for Bitcoin to qualify as mean of exchange, Again, the general acceptance in a broad spectrum of transactions and merchants would be required.

A number of reasons encourage merchants to accept Bitcoin payments. Transactions carry substantially lower fees than credit card transactions. A merchant has two options when accepting bitcoin payment. The merchant can either keep the bitcoin and avoid the volatility risk or automatically convert them to local currency (i.e.: dollar). The former carries a fee of around 0%; the latter would cost the merchant around 1%. In both cases, transactions carry lower fees than debit and credit cards (around 3%).

There are other benefits for merchants of accepting Bitcoin. Some are tangible: merchants receive Bitcoin payments in as little as ten minutes vs. several days or weeks for debit and credit card transactions. Others are intangible. For example, it helps them to attract a specific segment of customers,

Accepting Bitcoin payments is generally attractive for merchants. However, the appeal for end customers to adopt Bitcoin is unclear.

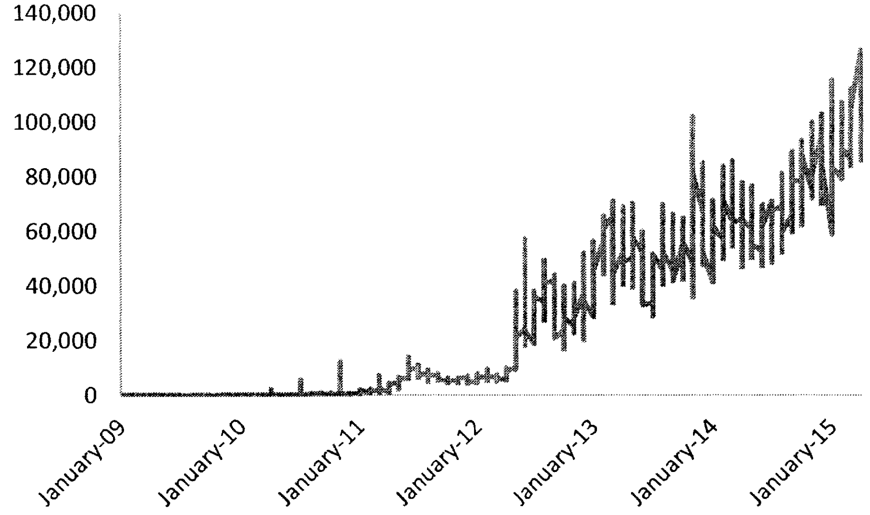
Ideology (absence of central banking authority), privacy (anonymity or pseudonymity of transactions), potential appreciation (albeit with a risk), and ease of use (with potential to bring on board unbanked or underbanked people into the system) are advantages of the adoption of Bitcoin.

On the other hand, Bitcoin presents a number of disadvantages. Bitcoin has been extremely volatile in the past. This makes it risky to hold Bitcoin relative to traditional money. There are no economic incentives (of a similar nature than those of merchant) for individuals to adopt bitcoin, and the payment process may take up to 10 minutes per transaction making it inconvenient to use.

Bitcoin has experimented a strong growth of its adoption to date, measured by the increasing number of daily transactions (97,000 as per 22nd April 2015) and the number of merchants that accept it (over 100,000, as per February 2015). However, the mixed balance of the appetite for individuals to adopt Bitcoin poses a serious threat to the potential for Bitcoin to emerge as a generally accepted currency.

Bitcoin still represents a very limited number of transactions relative to other payment systems (debit and credit cards). However, there is a clear upward trend in the daily number of BTC transactions. Average number of daily transactions has grown from 5,200 (in 2011) to 67,000 (in 2014) and to 97,000 (in 2015 till 22nd April). Should this strong upward trend in the number of Bitcoin transactions continue, there is potential for Bitcoin to emerge as a generally accepted form of transaction.

Figure 10: Daily number of BTC transactions



Source: www.blockchain.info as of April 2015

2.3. Deposit of value

The third traditional function of money is deposit of value. The value of money stays relatively stable in the future. If you hold one dollar today, the purchasing power of that dollar in one day, one month, or one year will be relatively similar. In practice, it may decline (if inflation exists) or increase (if deflation exists). However, these deviations will generally not be significant.

Money allows people to postpone their decision to consume. If a family earns 75,000 and spends 60,000 dollars in a given timeframe, they will save 15,000 dollars. In order for them to save any money, they will need to be confident that they will be able to spend that saved money in the future. In environments with extremely high inflation, families tend not to save any money and to acquire as many durable goods as possible. This has been the case in Venezuela or Zimbabwe in recent periods of high inflation.

In the previous paragraph we discussed money as a mean of exchange. In that context, *"buy and sell"* function, the ability to execute transactions (acquire goods and services paying with money), was paramount. Now we are covering the deposit of value function of money. In this context, a *"buy and hold"* approach is most relevant. Users of money seek capital protection. Speculators will also expect capital appreciation and consequently bear a risk for holding that asset.

Does Bitcoin qualify as an appropriate store of value? In my opinion, today the answer to this question is negative.

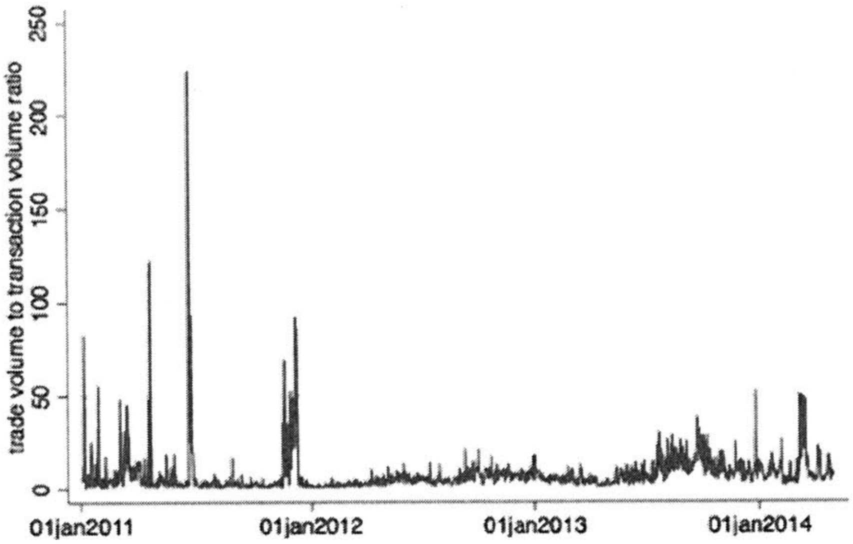
Since its creation in 2009, the price of Bitcoin has been extremely volatile. Figure 2 in page 13 shows the evolution of the price of Bitcoin since its creation in 2009. To name just three three data points, Bitcoin was largely trading under 1 dollar until April 2011, it went up to over 1,000 dollars in December 2013, and is trading at around 237 dollars as of the 22nd of April 2015. These references show the extreme volatility of Bitcoin. The extreme volatility results in

Bitcoin seeks to achieve mass adoption. However, this extreme price volatility is a serious obstacle for Bitcoin to achieve that ambitious objective. All players will take measures to reduce or avoid volatility risk. End users will not feel comfortable holding Bitcoin balances, merchants that accept Bitcoin payments will automatically convert them to their local currencies, and miners will diminish their investment in mining equipment.

In *"Bitcoin as Money?"*, Stephanie Lo and J. Christina Wang, of the Federal Reserve Bank of Boston identify and separate two main uses of Bitcoin. On the one hand, Bitcoin is used for transacting (acquiring goods and services). On the other hand, it is used for investing (acquiring Bitcoin on the hope that its price will go up in the future).

Their analysis defines two metrics to differentiate the use for transacting and investing. The former is defined as *"the estimated number of bitcoin sent over the Bitcoin network"*. The latter is defined as *"number of bitcoin trades on exchanges against fiat currencies"*.

Figure 11: Transacting vs. Investing ratio



Source: *"Bitcoin as Money?"*, Stephanie Lo and Christina Wang, Federal Reserve Bank of Boston

The chart describes the ratio between Bitcoin use for Transacting vs. Investing. The higher the ratio, the more it is used for Transacting (i.e.: mean of exchange) vs. Investing (i.e.: deposit of value). The chart shows a growing (albeit moderately) use of Bitcoin as a mean of exchange.

2.4. Key takeaways

	Comments	**Overall rating**
Unit of account	✓ Prices in Bitcoin available for several goods ✓ Bitcoin is divisible to accommodate transactions of smaller value ✗ Prices are generally set on local currencies, then converted to Bitcoin	◑
Mean of exchange	✓ Low transaction costs ✓ Quicker execution of transactions ✓ Useful instrument for the unbanked ✓ No central authority, independent verification ✗ Bitcoin accepted by a very limited number of merchants	◑
Store of value	✓ Limited supply (21 million); long term value increase? ✓ May be attractive in turmoil periods (EU bailout of Cyprus) or in countries with high inflation (Argentine, Venezuela, etc.) ✗ Extreme price volatility	◔

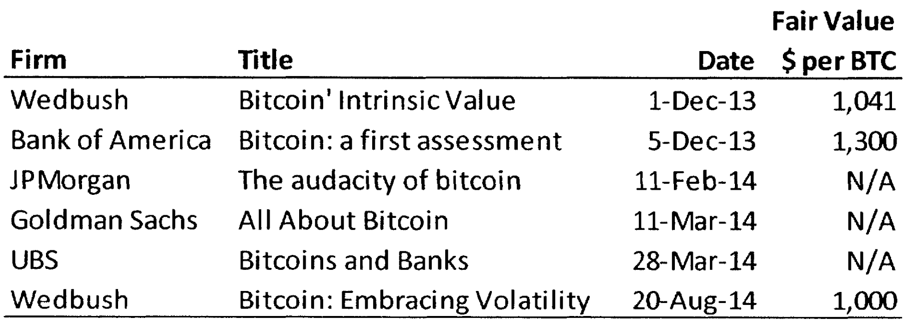
3. Perspectives on the Fair Value of Bitcoin

Bitcoin is a powerful platform for payments and has some elements in common with money. In this context: How much should Bitcoin be worth?

Research departments of Investment banks, such as Goldman Sachs and UBS, issue valuation recommendations of stocks, bonds, and commodities on a daily basis. Typically, they perform an analysis that results into an assessment of the fair value of an asset. Depending on the market trading of the asset relative to the fair value, the resulting recommendation is to Buy/Hold/Sell that asset.

A number of banks have issued research reports on Bitcoins. However, only two have provided a fair value recommendation for Bitcoin. The table below shows some illustrative examples.

Figure 12: Illustrative reports on Bitcoin



			Fair Value
Firm	**Title**	**Date**	**$ per BTC**
Wedbush	Bitcoin' Intrinsic Value	1-Dec-13	1,041
Bank of America	Bitcoin: a first assessment	5-Dec-13	1,300
JPMorgan	The audacity of bitcoin	11-Feb-14	N/A
Goldman Sachs	All About Bitcoin	11-Mar-14	N/A
UBS	Bitcoins and Banks	28-Mar-14	N/A
Wedbush	Bitcoin: Embracing Volatility	20-Aug-14	1,000

Source: Self-elaborated on the basis of selected Broker Research reports on Bitcoin

Wedbush and Bank of America have been determined enough to establish a target valuation for Bitcoin, despite its track record of excessive volatility.

3.1. Wedbush

Wedbush: *"Bitcoin Intrinsic Value"* (published on the 1st of December 2013) valued Bitcoin at 1,041 USD. The analysis identifies three key areas where adoption and usage of Bitcoin may grow exponentially: *"disruptive payment network technology, alternative uncorrelated asset class, and safe haven currency".*

According to the analysis, the success of Bitcoin in the above areas will determine the value drivers for Bitcoin: Penetration of potential demand, and Years to achieve such penetration.

Wedbush established a fair valuation for Bitcoin of 1,041 USD, contingent on Bitcoin transactions achieving a 1% penetration (i.e.: one in one hundred transactions takes place via Bitcoin) over a ten year period time frame. The chart below shows the sensitivity of the valuations of Bitcoin expected by Wedbush depending on the future adoption of Bitcoin as a percentage of the total transactions and on how quickly that adoption happens.

Wedbush identifies three areas where Bitcoin can potentially win market share: global foreign currency reserves, money supply in high inflation countries (such as Venezuela, Iran, Argentina, or Syria), and Gold as a Financial Asset.

Bitcoin thrives in the context of market inefficiencies. Argentina is a clear example: it has extremely high inflation (officially 24% in 2014, unofficial estimates 40%) and currency controls that set artificial obstacles to the free movement of capitals. In order to encourage the use of the local currency (el peso argentino), the government has established rigid currency controls that make it expensive to make payments in international currencies (euro or dollar).

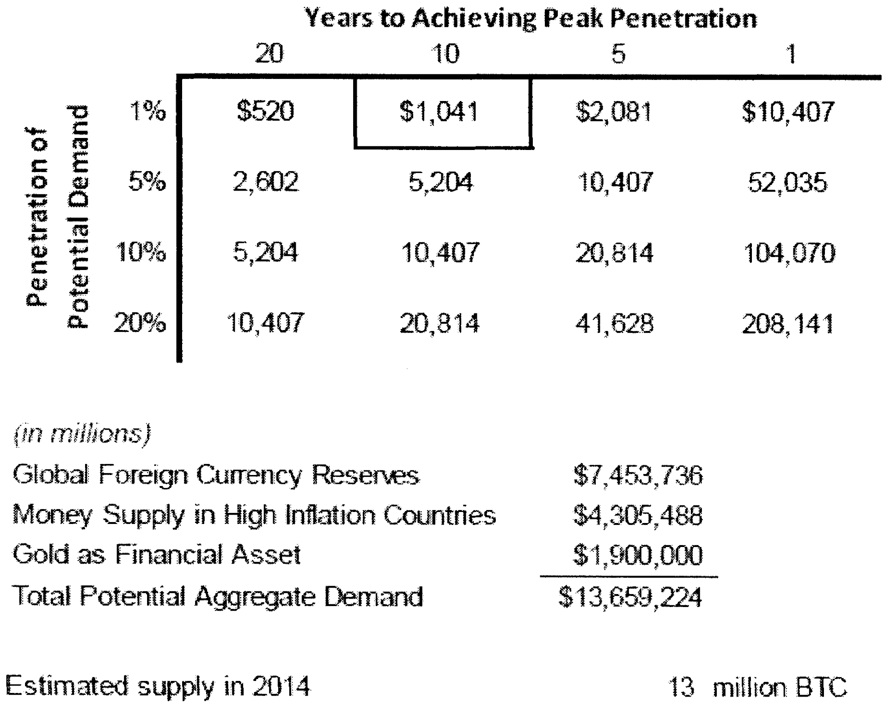
Overall, payments in dollars carry 30% transaction costs in Argentina. This figure incorporates the duties, divergence between the official exchange rate and the black market one, and the credit card fees. Furthermore, it takes an average of 20 days for the international payment to arrive to Argentina. Obviously, these make it burdensome to accept international payments.

An insightful article by the New York Times (Can Bitcoin conquer Argentina, 3rd May 2015) explores the rise in the usage of Bitcoin. Platforms like BitPagos have been very successful in facilitating credit card payments from foreign clients. This enabled merchants (hotels, retailers, etc.) to receive credit card payments from foreign customers moving their money in and out of Argentina via Bitcoin transactions. And hence, avoiding the 30% transaction fees.

Some merchants are starting to pass on part of the savings to customers that pay using Bitcoin. This is the case of Avalancha (www.avalancha.com), an Argentinian online retailer that offers 10% discount to clients that pay using Bitcoin. It is a win-win situation for the company and its customers. The former saves money (30% average transaction fee) and receives the payment sooner (immediately rather than in 20 days). The latter receive a 10% discount.

This example shows the case for companies and customers adopting Bitcoin, particularly in geographic locations where inefficiencies, such as high inflation or foreign currency controls take place.

Figure 13: Bitcoin price drivers as per Wedbush analysis (December 2013)



		Years to Achieving Peak Penetration			
		20	10	5	1
Penetration of Potential Demand	1%	$520	$1,041	$2,081	$10,407
	5%	2,602	5,204	10,407	52,035
	10%	5,204	10,407	20,814	104,070
	20%	10,407	20,814	41,628	208,141

(in millions)	
Global Foreign Currency Reserves	$7,453,736
Money Supply in High Inflation Countries	$4,305,488
Gold as Financial Asset	$1,900,000
Total Potential Aggregate Demand	$13,659,224

Estimated supply in 2014	13 million BTC

Source: Wedbush: *"Bitcoin Intrinsic Value"*, issued on the 1st of December 2013

In August 2014, Wedbush issued another report with another valuation methodology. The report identified three potential scenarios for the valuation of Bitcoin.

In the bearish scenario, Bitcoin is valued at 0 based on: other virtual currency overtakes Bitcoin, fatal error happens, or Bitcoin is made illegal. The document attributes a 50%

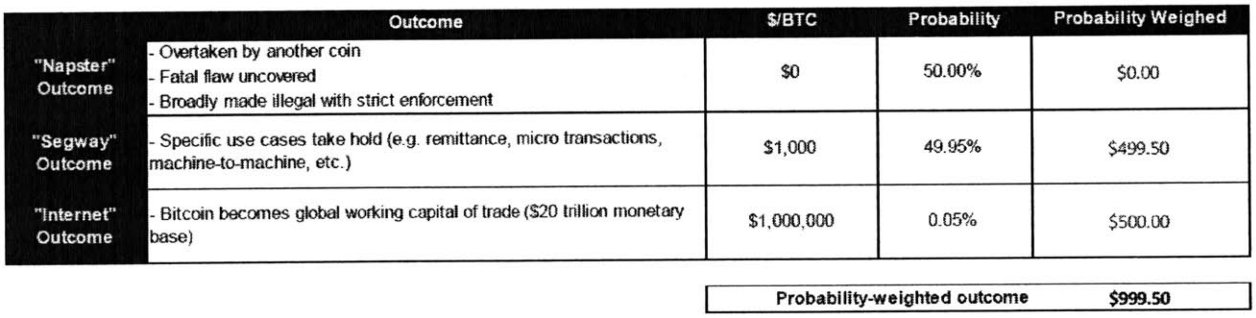
probability to this scenario. Hence, the probability weighted value of Bitcoin in this scenario is 0.

In the base scenario, Bitcoin is valued at 1,000$ based on the crypto currency being successful in niche sectors (remittances, etc.). The document attributes a 49.95% probability to this scenario. Hence, the probability weighted value of Bitcoin in this scenario is 499.50$.

In the bullish scenario, Bitcoin is valued at 1,000,000$ based on the crypto currency becoming the global working capital for trade. The document attributes a 0.05% probability to this scenario. Hence, the probability weighted value of Bitcoin in this scenario is 500$.

According to this theory, the volatility of the price of Bitcoin (see Figure 2 in page 14) is explained by the changing expectations of investors on the likelihood of every scenario. For example, if investors attribute a 0.01% more chances to the bullish scenario, this would result in approximately 100$ more of valuation for Bitcoin. This extreme sensitivity is therefore driving the volatility of the price of Bitcoin.

Figure 14: Bitcoin price drivers as per Wedbush analysis (August 2014)



	Outcome	$/BTC	Probability	Probability Weighed
"Napster" Outcome	- Overtaken by another coin - Fatal flaw uncovered - Broadly made illegal with strict enforcement	$0	50.00%	$0.00
"Segway" Outcome	- Specific use cases take hold (e.g. remittance, micro transactions, machine-to-machine, etc.)	$1,000	49.95%	$499.50
"Internet" Outcome	- Bitcoin becomes global working capital of trade ($20 trillion monetary base)	$1,000,000	0.05%	$500.00
		Probability-weighted outcome		$999.50

Source: Wedbush: *"Embracing Volatility: Trading as Bitcoin's First Killer App"*, issued on the 20th August 2014

3.2. Bank of America

Bank of America: *"Bitcoin: a first assessment"* (published on the 5th of December 2013) valued Bitcoin at 1,300 USD. According to Bank of America, Bitcoin has the potential to *"become a major mean of payment for e-commerce and may emerge as a serious competitor to traditional money transfer providers"*. Furthermore, Bank of America believes that Bitcoins has *"clear potential for growth as a medium of exchange"*.

In December 2013, Bitcoin was trading at over 1,000 USD. At that time, Bank of America report established a fair valuation for Bitcoin of 1,300 USD (or market capitalization of 15 billion USD). However, this valuation was contingent on two aggressive statements:

1. Bitcoin becoming a *"major player in both ecommerce and money transfer"*
2. Bitcoin achieving a *"significant store of value with a reputation close to silver"*
3. Ultimately, a valuation of 1,300 USD assumes that Bitcoin captures *"10% of e-commerce or money transfers"*

Despite the high valuation attributed to Bitcoin, the report is cautious. It mentions that the *"100 fold increase in Bitcoin prices this year is at risk of running ahead of its fundamentals"*. In order to explain the value drivers for Bitcoin, Bank of America separately analyzes the value of Bitcoin as a mean of exchange and as a store of value.

Bitcoin attributes two value drivers as a mean of exchange: Bitcoin is used as a mean of payment of e-commerce transactions and for money transfers (i.e.: remittances). These two functions are valued separately.

As a mean of payment for e-commerce transactions, Bank of America observes that on average US families hold 4 cents for every 1$ they spend over the year. Bank of America also notes that B2C e-commerce sales in the US totaled 224$ billion in 2012. In this context, *"households would set aside 10$ billion [around 4% of the B2C e-commerce sales] for their on-line shopping"*.

If we assume that Bitcoin *"will grow to account for the payment of 10% of all on-line shopping, this would suggest that US households would want to have a balance of 1$ billion worth of Bitcoins"*. Bank of America assumes that the US represents a fifth of the world's GDP. And hence the total balance of Bitcoin required in the world would be 5$ billion.

As a mean for sending money (i.e.: remittances), Bank of America makes the assumption that Bitcoin will become one of the top three players in the money transfer industry. *"Given Bitcoin's supply is fixed, when one buys a Bitcoin, one is acquiring not only a medium of exchange but also an investment in the enterprise value of Bitcoin. Bitcoin's market capitalization could be viewed as its enterprise value. With the average market capitalization of Western Union, MoneyGram and Euronet at about 4.5$ billion, we will add this number to the maximum market capitalization of Bitcoin's role as a medium of exchange."*

In this context, Bank of America notes that the maximum market capitalization for Bitcoin's as a medium of exchange =

5$ bn (for B2C e-commerce) + 4.5$ bn (mean for payments) = 9.5$ bn

Today there are 14 million bitcoin issued. Hence, the maximum value for Bitcoin as mean of exchange should be around 650$/bitcoin (9.5$ bn/14m). This is far above the current trading value of 237$/bitcoin as per 22nd April 2015.

On the other hand, Bank of America assesses Bitcoin as store of value. The report notes that Bitcoin does not pay any interest (unlike typical financial instruments). In this context, Bitcoin has some similarities to precious metals or cash, the report notes.

The first potential benchmark for Bitcoin as a store of value is gold. According to Bank of America, *"the current outstanding value of gold bar/coins/ETFs is about 1.3$ trn"*. However, the volatility of Bitcoin is five times larger than that of gold. Hence, Bitcoin as a store of value is worth in the most optimistic scenario five times less than gold: 300$ million.

Furthermore, *"the reputation of gold as a unique and safe store of value has been growing for the past ten thousand years. It will take some time for Bitcoins to acquire that reputation. We don't know how to quantify the value of gold's reputation, but this reputation is probably the main reason that its value is 60 times that of silver"*. In this context, the report states that *"if we were to assume that Bitcoin were to eventually acquire the reputation of silver (which is an extremely ambitious assumption), this suggests that Bitcoin market capitalization for its role as a store of value could reach 5$ billion"*.

As a result of the above, the maximum market capitalization for Bitcoin's as a store of value is 5$ billion.

Bank of America therefore concludes that the maximum overall market capitalization for Bitcoin is 14.5$ billion (9.5$ billion as mean of exchange and 5$ billion as deposit of value). Today, this would suggest a total valuation for Bitcoin of around 1,000$/bitcoin (14.5$ billion/14 million). Again, this is far above the current trading value of 237$/bitcoin as per 22nd April 2015.

3.3. Bitcoin Investment Trust

Bitcoin Investment Trust (*"BIT"*) is a fund that allows investors to gain exposure to Bitcoin in an officially regulated investment vehicle. BIT is listed in the Over the Counter Markets Group with the ticker: GBTC. SecondMarket, a US based broker dealer (registered by US regulator FINRA) acts as marketer, distributor, and custodian for this fund. Ernst & Young is the auditor.

Every share in BIT represents a tenth of a Bitcoin. Therefore, if you own ten shares of BIT, you indirectly own one Bitcoin. This official vehicle opens Bitcoin as an investment option for several people willing to invest in Bitcoin without going through the normal hurdles (opening an account in an intermediary or wallet, keeping the password in a safe place, etc.).

BIT facilitates Bitcoin enthusiasts to invest in Bitcoin their Individual Retirement Accounts, 401ks, and other brokerage and investor accounts. It is an aggressive proposition to invest your pension in Bitcoin given the extreme past volatility. However, it is positive that the option is available for those willing to take the risk.

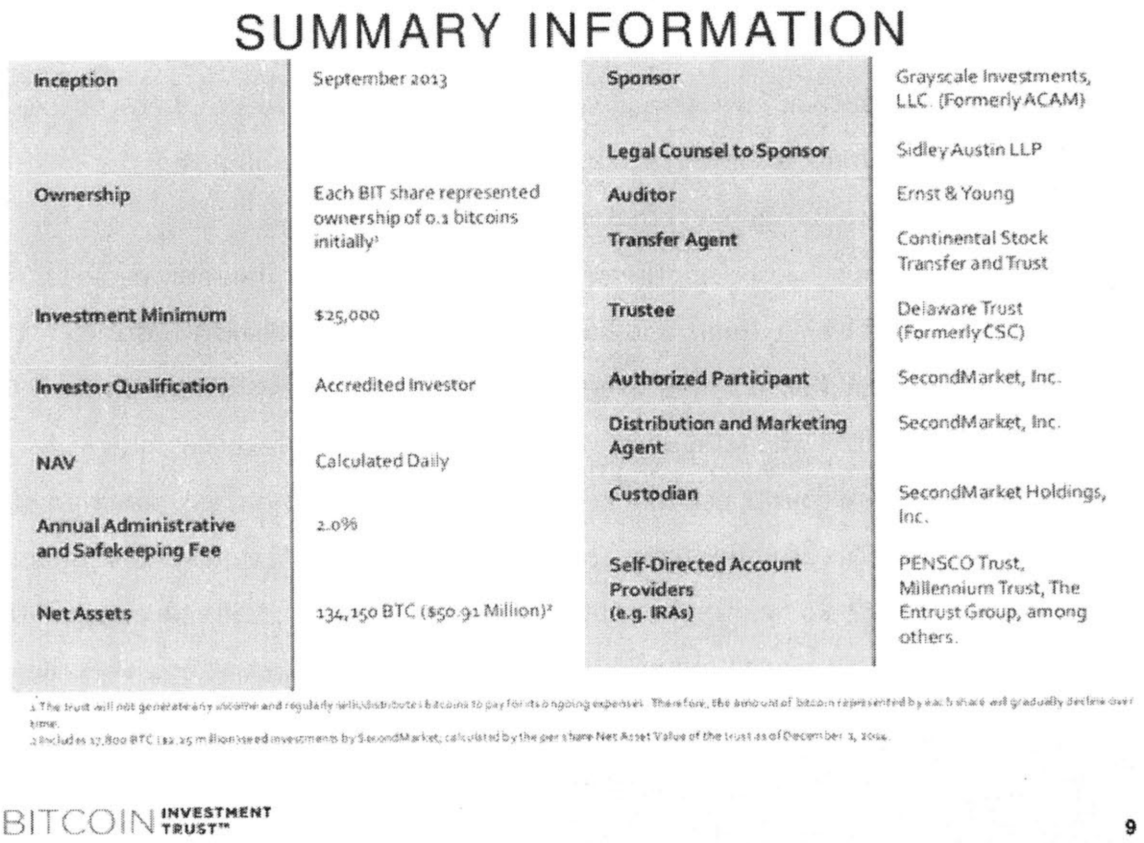
On the negative side, it has a 2% annual administrative and safekeeping fee. This fee is large, in line with the fees that other funds charge for similar services.

A very interesting feature of BIT is that it provides an indirect measure of the value of Bitcoin. Only accredited investors (those with annual income >200,000$ or total assets > 1,000,000$) can invest in BIT. Therefore, the trading value of BIT may be interpreted as the price that institutional investors expect Bitcoin to be worth.

On May 5th, 2015 BIT went public. Over the first two days, BIT had been trading at between 37 and 55$. Remember that every share in BIT represents a tenth of a Bitcoin. This implies a value for one Bitcoin of 370 and 550$ respectively, far above the trading value of 230$ at the time.

It is far too early (and too limited of a data set) to draw conclusions. However, the success of Bitcoin Investment Trust sends a positive signal to the market: accredited investors do not only see Bitcoin as an attractive investment option, but are also keen to pay a premium for it.

Figure 15: Bitcoin Investment Trust key facts



SUMMARY INFORMATION

Inception	September 2013
Ownership	Each BIT share represented ownership of 0.1 bitcoins initially[1]
Investment Minimum	$25,000
Investor Qualification	Accredited Investor
NAV	Calculated Daily
Annual Administrative and Safekeeping Fee	2.0%
Net Assets	134,150 BTC ($50.91 Million)[2]

Sponsor	Grayscale Investments, LLC (Formerly ACAM)
Legal Counsel to Sponsor	Sidley Austin LLP
Auditor	Ernst & Young
Transfer Agent	Continental Stock Transfer and Trust
Trustee	Delaware Trust (Formerly CSC)
Authorized Participant	SecondMarket, Inc.
Distribution and Marketing Agent	SecondMarket, Inc.
Custodian	SecondMarket Holdings, Inc.
Self-Directed Account Providers (e.g. IRAs)	PENSCO Trust, Millennium Trust, The Entrust Group, among others.

[1] The trust will not generate any income and regularly will distribute bitcoins to pay for its ongoing expenses. Therefore, the amount of bitcoin represented by each share will gradually decline over time.
[2] Includes 17,800 BTC ($2.25 million) seed investments by SecondMarket; calculated by the per share Net Asset Value of the trust as of December 1, 2014.

BITCOIN INVESTMENT TRUST™ 9

Source: www.bitcointrust.co

3.4. Key takeaways

Key takeaways from the Broker Research coverage of Bitcoin:

- Almost all the relevant Investment Banks (Goldman Sachs, JPMorgan, UBS, Deutsche Bank, etc.) have issued various research notes on Bitcoin. However, only two (Wedbush and Bank of America) have been determined enough to provide valuation analysis on Bitcoins. This is understandable, given the recent origin of Bitcoin, its innovative nature (and consequently lack of comparable realities), extreme price volatility, and complex underlying drivers. Even Wedbush and Bank of America have not continued providing updates on the valuation of Bitcoin.
- The two reports (Wedbush and Bank of America) that contain explicit valuation analysis were issued in early December 2013, at the time where the valuation of Bitcoin reached over 1,000$/bitcoin, its maximum level since its creation in 2009. Today, Bitcoin trades at a substantially lower level: 237$/bitcoin as of 22nd April 2015. Critics say that equity research analysts are better at explaining what happened in the past than forecasting what will happen in the future. In this case, both Wedbush and Bank of America expressed their concerns about the unsustainably high valuation level that Bitcoin was trading at.
- It is extremely difficult to forecast the price of Bitcoin, even for industry experts. The valuation presented by Wedbush and Bank of America relies on some indirect valuation mechanism. For example, Wedbush estimates the areas where Bitcoin may have a competitive advantage (foreign currency and gold reserves, store of value in high inflation countries), and presents the value of Bitcoin as a function of what share of those areas will Bitcoin achieve (1-20%) and how quickly will Bitcoin achieve that status (1-20 years). On another note, Wedbush presents three potential scenarios for the adoption of Bitcoin (base, bullish, and bearish) and presents the probabilities of each scenario as the key value driver. On the other hand, Bank of America presents a bottom up analysis of the value of Bitcoin on the basis of its attractive as a mean of exchange and deposit of value.

Chapter 3 – Bitcoin as an alternative to payers and merchants

Bitcoin has transformed the process of executing a payment in the same way that email transformed the traditional post services. However, it still lacks sufficient scale among customers (people willing to use Bitcoin in their everyday lives) or merchants (merchants willing to accept Bitcoin payments). In order to become a relevant payment service, Bitcoin should achieve mass adoption.

Overall, Bitcoin transactions cost is extremely low and its execution is substantially quicker relative to traditional payment systems. However, irreversibility, lack of identification, and need for internet access may be inconvenient for certain merchants and end-customers.

Bitcoin is a framework that allows developers to continuously improve its configuration. Individuals, start-ups, and venture capitals have developed applications to improve the functionalities of Bitcoin and overcome its obstacles. For example, apps have been developed to expedite the payment process or allow merchants to immediately convert the bitcoins they receive into other currencies (dollar, euro, etc.).

1. Key features

The following features are crucial when assessing the merits of Bitcoin versus other payment systems.

1.1. Ten minutes delay

On average, it only takes as little as ten minutes to confirm and execute a Bitcoin transaction.

This means that bitcoin payments may go from the sender to the recipient in only ten minutes. This is a remarkably short time lapse relative to other payment systems. For example, it takes two to three weeks for merchants to receive payments from credit cards, and one day (local) to one week (international) for bank transfers to be executed.

On the other hand, ten minutes is too big of a time lapse for the confirmation of an offline transaction. Imagine a restaurant having to wait ten minutes every time a client wants to pay using Bitcoin. That would introduce a big inefficiency in the restaurant: lines of people waiting, lower turnover of tables and customers, etc.

In this context, a number of applications have been designed by independent developers (i.e.: Bitpay, Liberty Teller, and Shopify among others) to tackle this problem. These applications eliminate the time lapse when accepting payments on store. This objective is sometimes achieved through transferring Bitcoin as gift vouchers like e-wallets.

For example, MIT Coop, the store at MIT University that sells textbooks, supplies and school stuff, accepts payments in Bitcoin both on store and online. The solution has been provided by Bitpay, a Bitcoin payment service provider and is getting increasingly popular in an ecosystem that is inclined to technological innovations: MIT itself has a clear technical focus and the city of Cambridge hosts several tech (Google, Microsoft) and healthcare/biotech (Takeda, Pfizer, Sanofi) companies.

1.2. Irreversibility

Unlike debit and credit card payments, Bitcoin transactions may not be reversed. Once a Bitcoin transaction has been verified it is final. This presents unbalanced implications for merchant and customer. More specifically, merchants receive too much power relative to end customers.

Recently, I was checking my credit card statement when I noticed that I had been charged twice for a hotel stay. I called my credit card provider, explained the situation, and got an immediate refund of my overpayment. This quick fix would not have been possible if the payment had been done through Bitcoin.

Irreversibility of Bitcoin transactions introduces hassles for both merchant (it adds process complexity, refunds have to be implemented as new transactions of opposite signs) and customer (uncertainty, customer protection).

What if a transaction is sent to a wrong destination? What if the transaction is sent for the incorrect amount (i.e.: 10 bitcoin instead of 1.0 bitcoin)? The solution to these potential problems relies on the merchant (or the recipient of the transfer) to act *bona fide* and issue a new transaction correcting for the difference.

1.3. Pseudonym identification

The nature of Bitcoin is in grey ground: It is not anonymous (like cash) but is not easily identifiable (like bank transfers).

Bitcoin transactions are pseudonymous. Each transaction is linked to a single-use address. The address is a succession of between 26 and 35 case-sensitive alphanumeric characters that always begins with numbers 1 or 3. This is an example of address: 1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp. Addresses are not directly linked to the identity of payers.

On the other hand, all Bitcoin transactions once verified (mined) immediately form part of the public ledger and stay public forever. Therefore, Bitcoin transactions are publicly traceable. The flow of payments across different addresses is completely public: it belongs to the Blockchain and anyone can check it in www.blockchain.info.

The pseudonymous nature of Bitcoin arises two implications: First, it leaves trace of consumption history that could be used for data analytics purposes. Second, it is sometimes used by people willing to hide their identity due to legitimate (i.e.: ideological) or illegitimate (i.e.: crime related, money laundering, etc.) reasons.

The person behind a Bitcoin transaction can be identified during the purchase (in order to complete the transaction) or following an investigation. However, the latter is extremely difficult and time consuming to execute. Consequently, Bitcoin has attracted regulatory attention in order to avoid the risk of money laundering. In some jurisdictions, such as Russia, Ecuador, and Indonesia, Bitcoin has been banned.

Upon creation of a Bitcoin account, certain wallets such as Coinbase, require authentication by text message (mobile number) and initial transfer by credit card or bank transfer (i.e.: linked to an account). This type of identification is frequent but is not mandatory. And

1.4. Internet access required

Internet access for both merchant and customer is frequently required in order to complete Bitcoin transactions. In this, Bitcoin is similar to credit card payments. However, this puts a constraint in the use of Bitcoin relative to other payment services. For example, credit card transactions require merchants, but not customers, to have internet access. I can pay using my credit card even if I don't have access to internet. Bitcoin transactions frequently require the end customer to have access to internet too.

This limitation may be inconvenient (i.e.: a customer may not have access to internet, or may run out of mobile battery in the middle of a transaction). However, it is not very relevant in developed countries where the penetration of internet among merchants and customers is widespread.

On the other hand, this requirement may be significantly limitation the growth of Bitcoin in emerging markets. VCs and Start/ups are already working to address this issue. A number of initiatives, such as Square, have been released that allow end customers to execute Bitcoin payments without the need of internet access. Frequently, they rely on a password but lack other authentication measures (such as email or text message authentication).

2. Advantages

Overall, it Bitcoin payments are more customer friendly than traditional alternatives for both merchants and end customers. The following are the main advantages of using Bitcoin.

2.1. Low cost

Today, Bitcoin transactions are virtually free. Successful miners get compensated in newly issued Bitcoin (25 Bitcoins per block, every ten minutes). Therefore, people executing transactions hardly pay any fees at all. This makes Bitcoin extremely attractive to both merchants and end customers.

Merchants avoid debit/credit card fees (typically as high as 1-3% per transaction) and foreign exchange fees (for transactions in different currencies). Merchants often decide not to hold a balance of Bitcoin. Instead, they automatically convert any payment they receive in Bitcoin to their local currencies (i.e.: dollar, euro, etc.). By doing this, they reduce the price volatility risk. The cost thid *"hedge"* is around 1% of the transaction volume, still lower than other payment systems.

End customers also save money. Most credit and debit cards charge an annual fee. With Bitcoin payments, most providers (such as Circle) do not charge any annual fee.

Remittances, particularly international remittances, are another field where Bitcoin has a strong potential to capture a share of the market. Traditional options are generally too expensive. For example, sending 3,000 euros from Spain to USA with my traditional bank costs me around 4.5%: 2% fixed fee plus a 2.5% mark up on the market exchange rate. With Bitcoin, I can do this for free (if I choose to receive Bitcoin) or I could pay a fee of around 1% if I choose to convert to dollars. There is a strong potential for Bitcoin to grow in this segment. Venture Capital firms are supporting many projects that tackle this need.

The benefit of the low transaction costs may dilute in the future. The configuration of Bitcoin contemplates that miners are compensated in 25 Bitcoins per block. However, this compensation is scheduled to be halved every four years. Hence, in the future, a growing portion of the cost of mining Bitcoin will be borne by people carrying out transactions (instead of by the network).

2.2. Quicker

Bitcoin transactions are executed and settled in as little as ten minutes. Traditional alternatives take far more time. For example, local bank transfers typically take 1-2 days to settle, international bank transfers take up to a week, and credit cards payments may take up to a month.

In this context, Bitcoin is extremely attractive. It improves the working capital position for merchants relative to other payment systems. While at the same time providing other benefits of credit cards: secured transactions, efficiency, automatic exchange rate, etc.

Some merchants have started to share some of the benefits of accepting Bitcoin with the end customer. For example, Avalancha, an Argentinian online retailer (similar to Amazon) offers 10% discount to those customers that pay with Bitcoin. See epigraph 3.1 in chapter 3 for more detail.

2.3. Security of the transactions

Bitcoin has a solid verification process. The security of Bitcoin transactions is higher than that of other online transactions because it is built on the mining process, a global and competitive clearing system for Bitcoin payments.

UBS report *"Bitcoin and Banks"* dated 28 March 2014 states that: *"Bitcoin has already demonstrated the potential to transfer large sums securely. While there are issues relating to Bitcoin's volatility, the underlying technology clearly works, and could provide the basis for faster transfers that are settled throughout the day at comparable, if not lower costs, than current alternatives. In this sense we see Bitcoin as a flawed first take on such a technology, which could be used to move existing currencies and securities".*

The Bitcoin Blockchain has been praised almost unanimously. In theory, a 51% attack would be possible. If a miner or group of miners could join forces that represent 51% of the mining power in the Bitcoin network, they could theoretically collude and agree to confirm false transactions. This would corrupt the Bitcoin network with horrible consequences. Trust in Bitcoin would disappear and price of Bitcoin would probably plummet.

There are strong reasons that make a 51% attack scenario highly unlikely: Incentives and Game Theory (cost and benefit analysis).

The competitive tension and the financial compensation (25 Bitcoin every ten minutes as of today) introduced in the mining process of Bitcoin makes it inefficient for miners to carry out a 51% attack. Doing so would require an extraordinarily high upfront cost: the cost of putting together such a large share of mining computing power, with a very uncertain potential win: the price of Bitcoin would almost certainly plummet in that event.

Furthermore, any player carrying out a 51% attack would have another cost: the opportunity cost of continuing operating within the rules of the Bitcoin network and earning the majority of the legitimate revenues (25 Bitcoin every ten minutes as of today) from the ongoing running of Bitcoin.

This is too high of a cost for a too uncertain potential return. It is better and more profitable to act within the platform.

2.4. Potential to attract niche customers

There is a small but growing number of Bitcoin enthusiasts. Merchant have the potential to attract that niche of customers if they accept Bitcoin payments. This is one of the reasons that merchants frequently mention when they speak about the drivers that took them to accept Bitcoin payments.

I will mention one example. Moksa is a restaurant in Massachusetts Avenue, in Cambridge. There are dozens of similar restaurants in that street. Moksa accepts Bitcoin payments and also has an on-store Bitcoin Automated Teller Machine. By doing so, Moksa has managed to attract a loyal customer base.

MIT Bitcoin club meets every Wednesday evening at Moksa. This meeting brings about 15-20 people to the restaurant on a regular basis. They get together, discuss recent developments around Bitcoin, brainstorm ideas, seek funding for those ideas, etc. Of course, they also eat and drink, and pay for that using Bitcoin.

Something similar happens with Do Eat, a restaurant in Maria de Molina (Madrid) and one of the pioneers in accepting Bitcoin in Spain. His owner, Diego has managed to attract a clientele of Bitcoin enthusiasts. Furthermore, he has appeared several times on the local press and television.

Accepting Bitcoin can be an efficient and cheap marketing campaign.

2.5. Bitcoin momentum

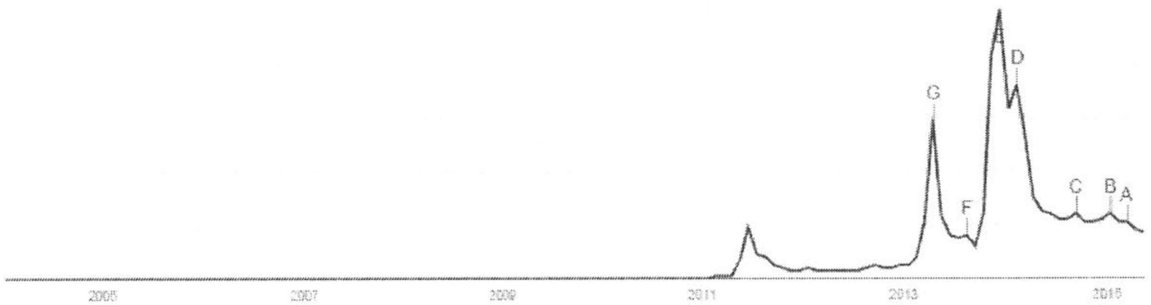
Despite the continued decrease of Bitcoin price since its peak in December 2013, other data points suggest a more positive outlook for the crypto currency.

First, the number of transactions is still small relative to other payment services. See Figure 9: Average daily payment volume for detail. However, it has substantially and steadily increased as can be seen in Figure 10: Daily number of BTC transactions. The number of Bitcoin transactions is growing on a regular basis.

Second, has attracted relevant attention by several players. Papers have been published on the topic by traditional banks (Goldman Sachs, Bank of America, JPMorgan), consulting firms (Deloitte, PwC), regulators (Chicago Fed, Finma, Bank of England), academic institutions (MIT, Berkeley, NBER).

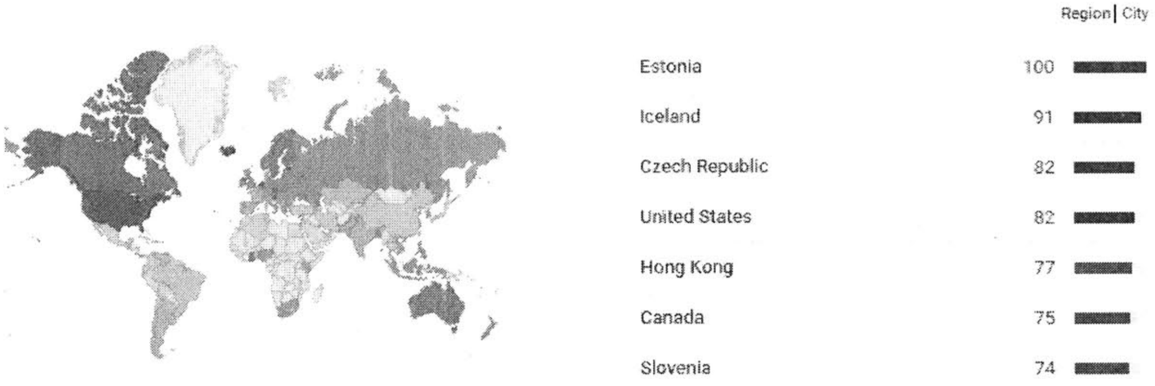
The charts below show the evolution of the number of Google searches on Bitcoin over time and its geographic concentration. The peaks relate to specific moments: Cyprus bailout and subsequent price increase of Bitcoin (March 2013), historical maximum price of Bitcoin (December 2013), and Mountain Gox bankruptcy (February 2014). However, the chart shows a relevant increase in the overall attention devoted to Bitcoin since 2011.

Figure 16: Google searches on Bitcoin over time



Source: Google Trends, as of May 2015

Figure 17: Regional breakdown of Google searches on Bitcoin



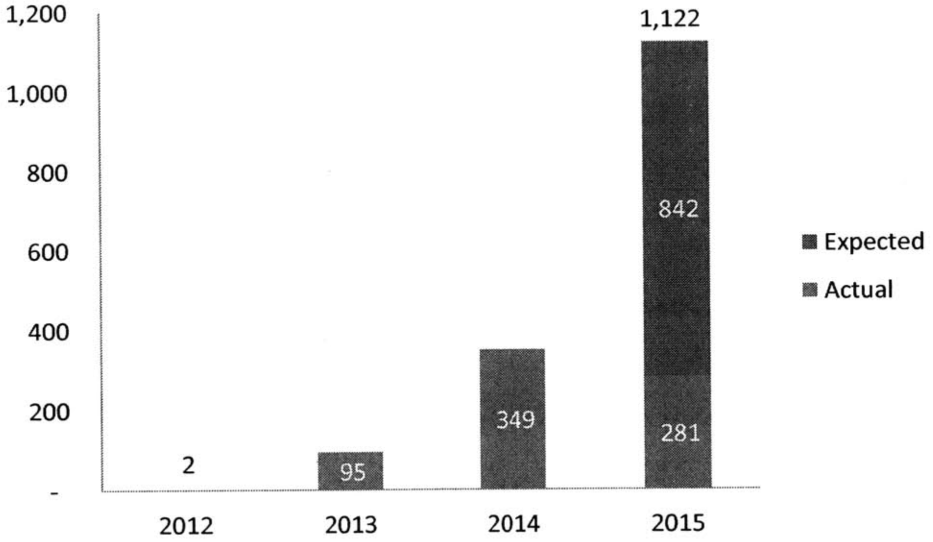
Estonia	100
Iceland	91
Czech Republic	82
United States	82
Hong Kong	77
Canada	75
Slovenia	74

Source: Google Trends, as of May 2015

Third, the investment by Venture Capital funds on Bitcoin projects has increased substantially. It was almost inexistent in 2012, and it has grown at a huge path, both measured from qualitative and quantitative metrics.

The amount invested in Bitcoin projects in 2014 was almost 350$ million. And in 2015, the investment in Bitcoin is expected to grow even more.

Figure 18: Bitcoin Venture Capital funding by year



Source: http://www.coindesk.com/bitcoin-venture-capital as of May 1st, 2015; Expected investment (in red) in 2015 assumes the same monthly investment for (May to December 2015) as in the first quarter of the year (January to April)

From a qualitative perspective, this growing investment appeal of Bitcoin is very important. Robust investments in the Bitcoin network result in an improved experience for Bitcoin users and enhanced applications for merchants, customers, international remittances, etc.

Furthermore, some of the world most reputed investors have interest in Bitcoin. VC investors such as Marc Andreessen, founder of Andreessen Horowit, Peter Thiel and Max Levchin, cofounders of Paypal participated in a 116$ million investment round for 21 Inc, a Bitcoin start-up. Traditional financial institutions have also been very active. New York Stock Exchange, BBVA (the second largest Spanish bank), USAA (a Texas domiciled bank) invested 75$ million in Coinbase, a Bitcoin wallet and exchange service. In April 2015, Goldman Sachs along with other investors injected 50$ million in Circle, a Boston based Bitcoin financial service start up. This large appetite from qualified investors provides a stamp of approval for Bitcoin. Traditional banks are growing increasingly aware of the opportunities and risks that FinTech brings to the table. They are starting to realize that if they are not ready to cannibalize their business and explore innovative solutions, other players will take the lead in this front (payment services, peer to peer lending, credit scores based on big data, etc.).

2.6. Flexibility

Several applications and functionalities for Bitcoin have been released largely as a result of the relevant investments by VCs mentioned in the previous epigraph. This talks about the dynamic environment of the Bitcoin platform.

The community as a whole, students, developers, venture capitalist can contribute to enhance and improve Bitcoin. Today Bitcoin is more modern, robust, and tailored to customers and merchant needs than it was two months ago. And in two months, it will be even more so.

The lack of political interference or central authority that is inherent to the Bitcoin is liked by many on the basis of ideological reasons (i.e.: libertarian reasons). However, that ideological sphere is irrelevant when compared with the magnitude of the opportunity to improve and support the Bitcoin network through the collaboration of the broad Bitcoin community.

Bitcoin applications have already introduced relevant improvements: transactions can be confirmed immediately (BitPay), Bitcoin can be sent internationally (Coinbase), released from Automated Teller Machines (Liberty Teller), or people can invest in a listed Bitcoin vehicle (Bitcoin Invested Trust).

In the future, applications will be developed to continue improving the ecosystem of Bitcoin. For example, Bitcoin transactions are irreversible but an app could be released that would fix this problem. Every week there are innovations in Bitcoin as opposed to traditional payment systems that have essentially worked in the same way (slow, costly, and inefficient) for decades.

2.7. MIT Bitcoin Project

Boston is one of the most important technology hubs in the world. The city hosts leading technology institutions in the academic, Technology, and Biotech sectors. Massachusetts Technology Institute (MIT), Google, Microsoft, and Takedo are some examples. The fluid links with healthcare innovation and technology entrepreneurship are evident throughout the city.

It is not surprising that the Bitcoin ecosystem is more present in Boston than in other regions. Conferences, entrepreneurship around Bitcoin, and Bitcoin specific events abound. Furthermore, the usage of bitcoin is accepted in a number of offline spots, such as the MIT Book and clothes stores (The Coop), restaurants (Thelonious Monkfish), night clubs (Moksa), etc. Some of these places even have Bitcoin tellers (developed by Liberty Teller) where you can buy bitcoin the same way you would get money from an ATM. Prominent Bitcoin start-ups are based in Boston, such as Circle Internet Financial, a digital currency company that raised 50$ million from Goldman Sachs and IDG Capital Partners.

In this privileged ecosystem, Massachusetts Technology Institute (MIT) has launched the Bitcoin Initiative (http://www.mitbitcoinproject.org). In November 2014 the Institute offered each of its 4,500 undergraduate students the option to receive 100$ worth of bitcoin for free. In exchange, a group of MIT experts would study and analyze on an aggregated basis the diffusion of Bitcoin.

Over 70% of the students choose to participate in the MIT Bitcoin Project. This involved more than 3,000 students receiving over 300,000$ worth of bitcoin, in total. The onboarding process took around 45 minutes, with students answering several questions and generating a wallet that they choose.

The objective of the project is to observe the diffusion of Bitcoin and identify direct effect and indirect effects. The evolution to date has been fascinating. In the first 12 hours one MIT undergrad student already tried unsuccessfully to hack the system. Curious trends have been identified. 1st year students and US citizen have generally been more active. On the other hand, Biology students showed less interest. A relevant percentage (15-20%) cashed out in the first month of the project.

The project was led by two MIT students: Dan Elitzer and Jeremy Rubin. Dan is an MBA student at MIT Sloan School of Management and founder of the MIT Bitcoin club; Jeremy is studying Electrical Engineering and Computer Science at MIT. They jointly raised over 500,000$ of funding between MIT alumni and the Bitcoin community.

The MIT Bitcoin project had a number of consequences. First, it strengthened the position of MIT as institution in the vanguard of technology and Bitcoin related research. Second, it contributed to the consolidation of a bitcoin ecosystem around Cambridge and Boston. The adoption of Bitcoin substantially in the community increased substantially as a result, both between end customers and merchants. Third, it sets the example for other institutions to run similar examples.

3. Challenges

Bitcoin faces relevant challenges that may undermine its future viability. In order to succeed and realize its full potential, Bitcoin needs to address these key challenges and mitigate its main risks (price volatility, regulation, usage by criminals, etc.).

3.1. Rigid supply of Bitcoin

According to Macroeconomics theory, the formulation of monetary policy is the role of Central Banks. Issuance of money is one of the instruments available to Central Banks to execute this policy. They decide when and how much money to issue depending on the state of the economy in the region.

The main Structural challenge for Bitcoin is the lack of backing by a Central Bank. Today, Bitcoin is designed in such a way that the issuance of money is automatic depending on certain automatic parameters.

What challenges does this design raise for Bitcoins?

Under the current design, the supply of Bitcoin is not flexible. The founders of Bitcoin opted for a model with a steady supply of Bitcoins. The supply of Bitcoin is automatic and independent of the broader circumstances. Currently 25 Bitcoins are issued every ten minutes. In the future this number will be smaller and even disappear. Epigraph 5 of chapter 2 gives more detail in this process.

This steady and limited supply of Bitcoins leaves all the power to the market and is at the heart of the extreme volatility observed in the trading of Bitcoin.

Certain Bitcoin enthusiasts claim that central banking authorities are polluted by political motivations and that the monetary policy followed during the recent crisis by Central Banks has been erratic. Fiat money is based on the reputation of the issuer, not on the underlying material value of the currency or the reserves of the country.

This allows for Quantitative Easing to be executed in times of crisis. Governments have no limit to the amount of money they can print. Governments from all over the world have been taking advantage of this since the beginning of the crisis.

This has resulted in inflation. More money is available for the same assets in the economy, therefore, the face value of those assets increases. Inflation has harmed savers and benefited indebted players. Some people see Bitcoin as a solution to this erratic monetary policy. However, Bitcoin is not a magical solution.

The expansionary monetary policy followed by several countries throughout the recent crisis may have been wrong. However, if Bitcoin has the aspiration to become a relevant currency in the world, it should also address the macroeconomic questions.

Who is the lender of last resourt? If Bitcoin was the only currency used in the world, how would it react in case countries or individuals have the need to access provisional financing? If extra Bitcoins were issued, who would act as a Central Bank and receive the proceeds from those issuances? What would be the use of those proceeds? Unfortunately, Bitcoin does not have answers for these questions today.

3.2. Lack of a credit system

Bitcoin is pseudonymous. This characteristic is covered in detail in epigraph 1.3 of Chapter 3. As a direct result of the pseudonymous nature of Bitcoin it is very difficult for credit to exist in the Bitcoin platform.

Bitcoin transactions and ownership can't easily be traced to the underlying person or institution. If I tell you that I own a Bitcoin, it is very difficult (almost impossible) for you to be able to confirm my statement. Therefore, it would be highly unlikely that you will be able to facilitate me credit.

In this aspect, real estate and traditional financial systems work better than Bitcoin. I can check the ownership of a real estate property in the central register. Bank accounts, loans, and deposits are intrinsically linked to the identity of the holders.

Unless this lack of identification is removed, it will be extremely difficult for a credit system to grow in the Bitcoin ecosystem. With Bitcoin, you don´t know who is your counterparty, where is it based, what assets does it hold, and how solvent it is. In these circumstances, it is almost impossible that lending activity will emerge.

If Bitcoin really had the ambition to grow as an alternative currency, credit would be one necessary factor for this to happen.

3.3. Role of Bitcoin in illegal transactions

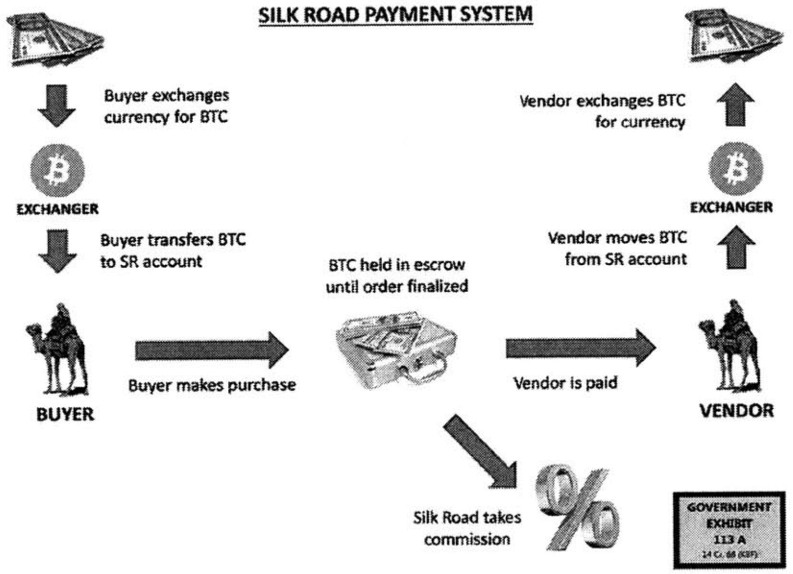
The quasi anonymous nature of Bitcoin makes it a natural channel that criminals will try to conduct their illegal activities.

In early October 2013, Silk Road market was shut down by the FBI. Silk Road market was an online black market that facilitated the trade of illegal drugs, weapons, child pornography, and other disgusting products. Even the commission of murder was freely traded in that illegal market. Bitcoin was the only currency accepted in that market.

Ross William Ulbricht was arrested under charges of being the manager of the site, known with the pseudonymous of Dread Pirate Roberts. 144,000 bitcoins were seized as part of the operation and the price of bitcoin went down 30%, from 125$ to 87$, immediately after the news was made public (first week of October 2013).

On February 2015, Ulbricht was convicted of the following charges: engaging in a continuing criminal enterprise, narcotics trafficking, money laundering, and computer hacking, among others. He will be sentenced on the 15th of May 2015 for up to 30 years in prison.

Figure 19: Silk Road payment system


SILK ROAD PAYMENT SYSTEM
Buyer exchanges currency for BTC
EXCHANGER
Buyer transfers BTC to SR account
BUYER
Buyer makes purchase
BTC held in escrow until order finalized
Vendor exchanges BTC for currency
EXCHANGER
Vendor moves BTC from SR account
Vendor is paid
VENDOR
Silk Road takes commission
%
GOVERNMENT EXHIBIT 113 A 14 Cr. 68 (KBF)

Source: Evidence used by the Government in the case against Ulrich

Bitcoin has and will occasionally be used for illegal actions. That does not mean that Bitcoin itself is illegal. Cash is also used for illegal transactions and this does not mean that cash is illegal.

Still, the use of Bitcoin for illegal transactions presents a challenge to the diffusion of Bitcoin. It raises sensitivities and concerns among potential legitimate users.

What is the solution to significantly diminish the illegal activity around Bitcoin? The solution is to mandate the disclosure of the identity for the users of Bitcoin. If Know your Customer procedures similar to those that Banks follow were implemented, Bitcoin would lose its attractive as a channel for illegal transactions. However, this would bring increased complexity and cost of operations of Bitcoin.

3.4. Increasing regulation of Bitcoin

In order to protect customers and more broadly the society, Governments are increasing the focus on regulation in several jurisdictions throughout the world. Different countries are taking different approaches in this process.

Why is Bitcoin regulated?

The impulse for Governments to regulate (and in some cases prohibit) the use of Bitcoin is driven by: 1. Protection of customers from fraud and excessive price risk, 2. Protection of society from potential money laundering and terrorism financing.

First, **Governments seek to protect Bitcoin customers**. There are two areas that merit the protection of customers: the excessive price fluctuations of Bitcoin and the solvency of the Bitcoin intermediaries.

The price of Bitcoin has been fluctuating very aggressively. Initially, it grew continuously for several years. It traded under 1$ till February 2011. By January 2013, it went for the first time over 20$, some months later, in April it went past 100$, and by December it had traded at over 1,000$, its maximum valuation. Since January 2014, the value of Bitcoin has consistently decreased till its current level of 237$ (22nd April 2015).

It is impossible to predict whether the price of Bitcoin in the future will go up or down and its volatility will stay as high or decrease to moderate levels. However, it is clear that Bitcoin is a risky investment. Bitcoin investors must acknowledge the inherent risks of that position. Only risk seeking investors should be allowed to trade Bitcoin as an investment.

The traditional financial sector is heavily regulated. As a result of this heavy regulation, the Government provides protection in case financial institutions go bankrupt. Federal Deposit Insurance Corporation (FDIC) is an independent agency of the United States government that protects the funds depositors place in banks and savings associations. Unlike, activity in the traditional financial sector, ownership of Bitcoin does not count with Government backed insurance or protection.

The second area where customers may need protection is in order to guarantee the solvency of the Bitcoin intermediaries. In practice this objective is very difficult (if not impossible) to achieve. The Bitcoin network is based on the collaboration and private initiative of the broad Bitcoin community. In this context, some projects are extremely helpful to improve the functionalities of Bitcoin. While others, are not successful.

It is important to select solvent intermediaries with strong management teams and access to funds when buying Bitcoin. In February 2014, Mountain Gox, the largest bitcoin intermediary at the time went bankrupt and 850k bitcoin worth almost 500$ million that belonged to its customers disappeared. Today, the reasons for that situation are still unclear. However, the magnitude of this event is enormous.

The open nature of the Bitcoin community encourages innovation of Bitcoin and continued enhancement of its functionalities. However, this open nature also makes it easier for evil people to conduct fraud. Some people argue that Bitcoin would merit increased regulation to protect investors. In practice, it is very difficult, impractical, and costly to design and enforce a tougher regulation.

Figure 20: Market share of Bitcoin exchanges (March 2012-March 2014)

Exchange	Volume (million BTC)	Market share
Mtgox	41.6	51.7%
Btcchina	9.9	12.3%
Huobi	9.2	11.4%
Bitstamp	8.6	10.7%
Btce	6.9	8.5%
Bitfinex	2.0	2.5%
Bitcoin24	0.8	1.0%
Campbx	0.6	0.8%
Localbitcoins	0.5	0.6%
Others	0.4	0.5%

Source: *"Bitcoin as Money?"* S. Lo and J. C. Wang, of the Federal Reserve Bank of Boston

Second, **Governments seek to protect the society** from money laundering, terrorism financing and other illegal activities. In the past, Bitcoin has been used for this purpose. Criminals tend to transfer money through channels that are not easy to trace. Bitcoin, cash, and precious metals have frequently been used by criminals.

Governments continuously make it difficult for criminals to act within the financial system. For example, the US Secretary of State holds a list of States that sponsor the Terrorism. Currently, there are four countries designated: Cuba, Iran, Sudan, and Syria. US will penalize with heavy fines individuals, companies, or States trading with those countries.

Traditional banks are obliged to establish strong and costly Anti Money Laundering (*"AML"*) systems. These procedures include extensive requirements, record keeping, reporting procedures, communications and training for employees, etc.

When these banks fail to comply with AML procedures, they suffer long and burdensome investigations that frequently result in strong fines. In January 2014, JPMorgan paid a 2.6$ billion settlement for failed AML compliance that aided Madoff. In July 2013, a judge approved HSBC 1.9$ billion settlement for failed AML compliance that facilitated drug money to flow through Mexico and Colombia. These two example clarify the magnitude of the consequences that banks face if they don´t comply with AML regulation.

In this context, there is pressure from Banks asking Governments to force Bitcoin to comply with the same AML standards that Banks face. If these attempts are successful, the very existence of Bitcoin would be at risk.

How is Bitcoin regulated in the US?

In the US and in most other jurisdictions across the world, it is legal to acquire, sell, mine, and trade Bitcoin.

In March 2014 the US tax authority (IRS) released a notice covering how Bitcoin and other *"virtual currencies"* should be treated. Full statement is available as Notice 2014-21 in the IRS website: http://www.irs.gov/pub/irs-drop/n-14-21.pdf

First, the IRS acknowledges that *"virtual currency may be used to pay for goods or services, or held for investment"*. This statement clearly recognizes that operating with Bitcoin is legal.

Second, it establishes that: *"For federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency"*. In this context, Bitcoin is treated as property, not currency. Therefore:

- According to this IRS notice, disclosure of all Bitcoin transactions is mandatory, even if the transaction is small. In practice, this will be difficult to enforce this regulation for small transactions (should I disclose that I bought a coffee paying with Bitcoin?). However, this rule provides legal ground for the IRS to go after people that don´t disclose their trading in Bitcoin.
- Gains or losses from the trading of Bitcoin must be declared and taxed through capital gains or income tax. This applies to any transaction using bitcoin. For example: buying and selling Bitcoin, or buying Bitcoin and then acquiring goods in exchange of Bitcoin. More specifically, capital gains (i.e.: buying a Bitcoin for 200$ and selling it for 300$ is a 100$ capital gain) from trading with Bitcoin will be subject to ordinary income tax if they are realized in the short term (less than a year), or the capital gains tax (if they are realized in over a year).
- Gains from mining must be declared as income and subject to tax. For example, an individual miner that earns 5,000$ equivalent in Bitcoin over a year should pay income tax for that amount. The tax payable will vary (usually between 10 and 40%) depending on the specific marginal tax rate applicable.

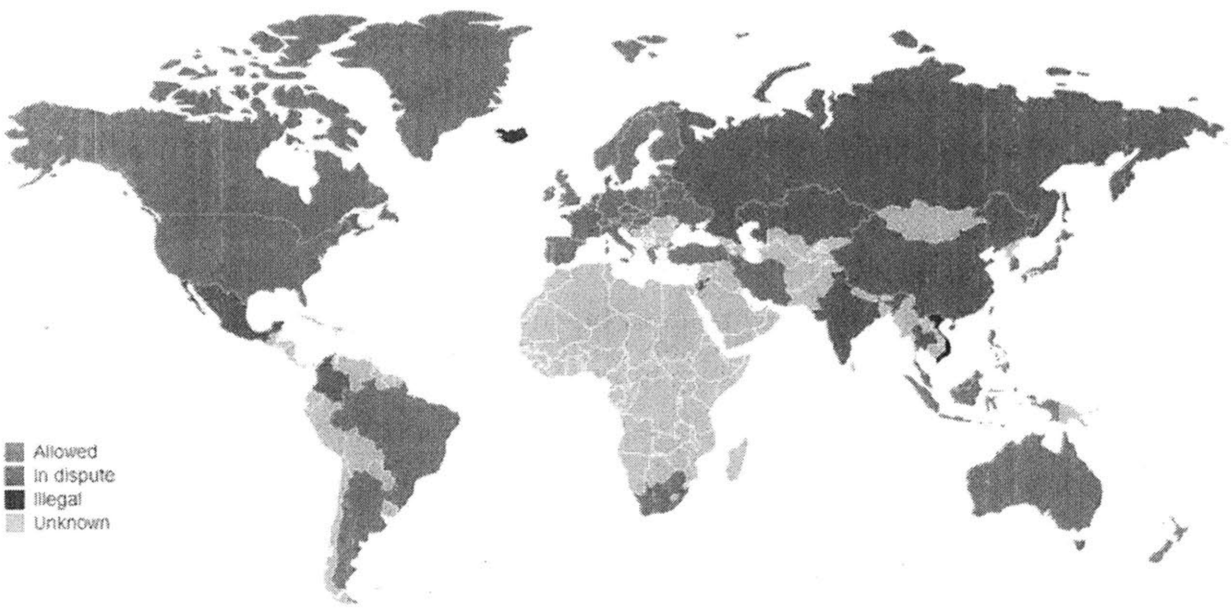
How is Bitcoin regulated in other geographies of the world?

Most countries have taken a similar instance than the US. They have formally or informally declared Bitcoin legal, allowed its use, and regulated for Bitcoin transactions to be subject to taxes in a similar manner than credit card or other transactions. Some countries have also defined the tax treatment relevant for situations when the acquisition or disposal of Bitcoin results in capital gains or losses.

On the other side of the spectrum, Ecuador, Bolivia, and Kyrgyzstan have completely banned Bitcoin, China has prohibited its financial institutions to buy or sell Bitcoin, and Russia appears to be planning a similar ban. And Indonesia has theoretically banned Bitcoin too, but to date has not been enforcing this measure.

The following map shows an overview of the regulation of Bitcoin across different geographies.

Figure 21: Regulation of Bitcoin by country



Source: http://en.bitcoinwiki.org/

Can regulation keep pace with innovation?

The answer to this question is NO. The world changes continuously. Governments and policy makers are slow moving giants. It is very difficult to articulate the right balance of regulation that protects customers and the broader society, while at the same time allowing for the innovation that the society demands.

3.5. Compensation to miners through fees

It would be ideal if compensation to miners came entirely from transaction fees, instead of from newly issued Bitcoin. Under the current configuration of Bitcoin this will only happen from 2140 onwards. At that date the supply of newly issued Bitcoin is scheduled to end.

It signals lack of ambition for Bitcoin to set a date 125 years from now (2140) in order to consider Bitcoin developed enough to stop issuing new Bitcoin and start compensating miners entirely with transaction fees. The natural way to pay for the transaction fee is directly. The current system where almost no fees are paid but 25 Bitcoin is issued seems artificial and theoretically has a similar indirect cost through inflation.

In my opinion, Bitcoin should be prepared to transition to a system where fees are paid for directly as soon as it achieves a relevant scale. It is difficult to predict when that will happen.

4. Future

American and Canadian economist John Kenneth Galbraith said: *"There are two kinds of forecasters: those who don't know, and those who don't know they don't know"*. The future of Bitcoin is an expression of the Age of Uncertainty, an expression that Galbraith and other economists have used to refer to the modern society.

The future will be determined by internal and external factors. Internally, there is room to continue improving its reliability, validity, and accessibility, and consequently, increasing its penetration in the everyday life of the population. But this will not be enough: external factors will also be crucial. The broader context of the monetary system will play a significant role. The stability of the hegemonic currencies (dollar, pound, euro), the pressure by emerging countries such as China against the hegemonic currencies, and the regulatory environment may encourage the use and diffusion of Bitcoin.

Bitcoin has dramatically transformed the payment systems sector. The Blockchain allows for payments to go through substantially quicker and cheaper than in traditional transactions. It has eliminated the need for a central authority that verifies and clears transactions. This role has been taking by a community, the miners, that continuously compete to verify transactions in exchange for compensation. Miners are in charge of eliminating the risk of double spending and clearing transactions in the Bitcoin network.

This new technology has important consequences in the world. It has the potential to provide an improved access to the financial system for the un-banked and under-banked, particularly in developing countries where inefficiencies are greater (high inflation, high transaction costs, etc). To date, the focus has been on the developed world, but I expect this to change in the future. The center of gravity will increasingly move to emerging economies.

Bitcoin is an evolving and dynamic reality. While the technology and functionalities of traditional payment systems (bank transfers, credit and debit card payments) have stayed stable for decades, Bitcoin ecosystem of Developers, Start-ups, and Venture Capitalists introduce innovations every day. This makes it an extremely agile vehicle to improve and pose solutions to most of the problems that it faces.

Will Bitcoin achieve mass adoption? Only time will tell. It certainly has the potential to continue growing and capturing market share as a payment system. It facilitates quicker and cheaper transactions (both commerce transactions and remittances) and given its limited supply (capped at 21 million bitcoin) price may increase in the future if penetration and scale of Bitcoin continues to grow.

Since the creation of Bitcoin, it has experimented extreme volatility. As time goes by it would be optimal if the volatility of Bitcoin decreased to moderate levels, even if it meant that the price stabilized at a lower level relative to the current trading (237$/Bitcoin as per 22nd April 2015).

Volatility is the single most important factor that may undermine the potential success of Bitcoin. A more balanced supply and demand of Bitcoin would dramatically reduce volatility. This would help Bitcoin mature as an asset, boosting confidence for customers and merchants to accept Bitcoin, transact in Bitcoin, and hold Bitcoin in their balance sheets.

The number of transactions and merchants that accept Bitcoin has grown substantially and continuously since its creation. However, both metrics are still really small relative to other payment systems. It would be important for Bitcoin to reach scale among merchants and end consumers, ideally to a level at least as high as credit cards. Again, this would stimulate an increased usage of Bitcoin by end customers.

Bitcoin has democratized the payment services industry. It has shifted the focus to the Bitcoin community. Miners collaboratively take the role of the Central Bank, developers transform and improve the applications and functionalities available, and users enjoy the benefits of transacting with Bitcoin. This is a solid ground for a prominent future.

Bibliography and sources

Bank of America: *"Bitcoin: a first assessment"*, published on the 5th of December 2013

Bank of England, 2014, *"The economics of digital currencies"*, Quarterly Bulletin 2014 Q3

Bank of England, 2014, *"Innovations in payment technologies and the emergence of digital currencies"*, Quarterly Bulletin 2014 Q3

Eicheengren, Barry and Kawai, Masahiro, 2015, *"Renminbi Internationalization: Achievements, Prospects, and Challenges"*, Brookings Institution Press and the Asian Development Bank Institute

Dowd, Kevin and Timberlake, Richard, 1998, *"Money and Nation State"*, Transaction Publishers

Galbraith, John Kenneth, 1977, *"The Age of Uncertainty"*, British Broadcasting Corporation

Global Legal Research Center, 2014, *"Regulation of Bitcoin in Selected Jurisdictions"*, The Law Library of Congress

Gloudeman, Lauren, 2014, *"Bitcoin's Uncertain Future in China"*, USCC Economic Issue Brief

Goldman Sachs: *"All About Bitcoin"*, published on the 11th of March 2014

IRS Notice 2014-21 on the tax treatment of Bitcoin in US, released in March 2014. Full statement: http://www.irs.gov/pub/irs-drop/n-14-21.pdf

Frankel, Jeffrey, 2012, *"Internationalization of the RMB and Historical Precedents"*, Harvard University

Krugman, Paul, *"Bitcoin is Evil"*, published on the 28th December 2013, in the New York Times

Lo, Stephanie and Wang , J. Christina, 2014, *"Bitcoin as Money?"*, Federal Reserve Bank of Boston

Mankiw, Gregory, 2013, *"Macroeconomics"*, 8th edition, Harvard University

Nakamoto, Satoshi, 2008, *"Bitcoin: A Peer-to-Peer Electronic Cash System,"* retrieved on November 2014 at "https://bitcoin.org/bitcoin.pdf"

New York Times: *"Can Bitcoin conquer Argentina"*, published on the 3rd May 2015

Selgin, George, 2008, *"Milton Friedman and the Case Against Currency Monopoly"*, Cato Journal

UBS: *"Bitcoin and Banks"*, published on the 28th of March 2014

Wedbush: *"Embracing Volatility: Trading as Bitcoin's First Killer App"*, published on the 20th August 2014

Wedbush: *"Bitcoin Intrinsic Value"*, published on the 1st of December 2013

www.blockchain.info

www.usebitcoins.info

www.bitcointrust.co

Yermack, David, 2013, *"Is Bitcoin a real currency? An economic appraisal"*, NBER Working Paper No. 19747