LUISS Università Guido Carli

Department of Economics and Finance **Course: Money and Banking**

CRYPTOCURRENCY IN A GLOBALIZED WORLD: A COMPARATIVE ANALYSIS OF BITCOIN AS A FINANCIAL ASSET

SUPERVISOR

Prof. Paolo Paesani

CANDIDATE

Ugo Giorgio Zoli lo Prinzi

Matr. 194051

ANNO ACCADEMICO

2016/2017

Money…
Ranks with love as man's greatest joy.
And it ranks with death as his greatest source of anxiety.

- *John Kenneth Galbraith*

THESIS

Introduction

Historically, since the birth of human exchanges and trade, there has always been an overall trend, in our innovative processes, to lower uncertainty between individuals or parties when exchanging value. Formal institutions such as banks, governments, corporations, as well as legal systems and market places, have progressively arisen in order to ease those forms of exchange. Their main goal being to establish trust in our economies, they relied primarily on people's confidence to ensure and regulate the execution of transactions. But just as third-party intermediation was reaching a peak in the world's financial sector, the Subprime crisis came as the rock making the Financial locomotive to fall. In addition to adding even more uncertainty, creating panic and fear worldwide with devastating withdrawals, the 2007-2008 global Crisis underlined another important problem regarding the very basics of ownership and control over our primary medium of exchange: Money. Indeed, in its most widely spread format, electronic money pretty much comes down to a digital series of numbers on our bank accounts, to which we frequently request access.

Perhaps the most striking example of how our privacy and control are being undermined through this system, is the one of Cyprus Banks raid. In 2013, after suffering from the Crisis' externalities, the national debt of the island had considerably increased, reaching 100% of Cyprus' GDP. Consequently, banks simply decided to retain a percentage on all savings accounts of over 100.000€ in order to repay this national public debt and there is nothing depositors could do about it. Many other cases might suggest that there is a crack in traditional financial systems. While technological progress in software and the Internet are making transactions of money and financial assets faster and more convenient, their circulation still passes through antiquated systems connecting clearinghouses, corresponding banks and central depositories. These circuits imply significant delays for moving funds to another account or for a stock trade to settle, most of the time involving non-negligible fees. In addition to being slow, these systems are expensive and increasingly insecure. Although advances in technologies and Internet based financial services have accelerated the processes of trade and exchange in a context of globalization, our personal information are still kept centrally by single powerful and centralized entities. Paradoxically, in a matter of security our data is given very restricted access but has become increasingly hackable online. As a result, our privacy has been undermined and we lost control over our own money and personal information.

In this climate of fear in the banking sector, primarily driven by uncertainty and over-reliance on unsound third parties, in 2009 a group of programmers known under the name of *Satoshi Nakamoto* responded with a "Peer-2-Peer Electronic cash system": Bitcoin. This crypto-currency takes the form of a bidirectional scheme where money can be used for both virtual and real Goods and Services. Introducing the concept of virtual money, we can now assert that Bitcoin was the first to create actual numerical value, able to short-cut the traditional system of exchanging money. It is completely decentralized with no servers or central authority. Meaning conversion and transfer of money can be proceeded instantly, without the need for any kind of third party intermediation, at any time and place in the world. In that, Bitcoin is a huge deal as, after decades of the "Internet of things" we may be gravitating towards the "Internet of value". What started out as a fringe experiment by anonymous developers has transformed into a multi-billion dollars industry today. But despite controversies regarding Bitcoin's fluctuations and its total lack of supervision, what also draw the attention of the public to this digital currency is the underlying technology allowing the recording of transactions, the Blockchain. This digital distributed public ledger allows for the very existence of cryptocurrencies by recording their transactions chronologically and publicly. Bitcoin was the first decentralized technology built on Blockchain technology. Recently, in the last few years, Bitcoin and cryptocurrencies in general sparked the interest not only from the banking sector but also from governments, companies, consultants, scientists, developers and eventually the wide public. What is found to be so captivating about this new technology is that it cuts away the middle man, eliminates their fees, yet maintains an infrastructure that allows individuals to deal directly with each other. In that, Cryptocurrency bears the promises, among other, to reduce the costs of doing business, to mitigate corruption inside those intermediate institutions, to enlighten the workings of an economic and political system centrally hidden and to shift the control of money and information from powerful elites to the people to whom it belongs, putting them back in charge of their assets. However, those are not the main reasons of Bitcoins' popularity and we cannot talk about a 'cryptocurrency revolution' yet. The general opinion appears to be sceptical to this regard, perhaps sometimes simply not interested, as the press-coverage would mostly relate cryptocurrency to a suspect monetary concept or to the money of the Dark-web, volatile price movements, drugs and money launder. Also, higher institutions worry that it could trigger economic crises because it strips government policymakers the capacity to adjust the money supply and that it may cause significant damages to the financial system.

All these colourful elements are worth taking into consideration to understand this disruptive innovation, but should be seen as incentives to dig further into what could change our future economic landscape. Because in the end, disruptive innovation is associated to

technological progress, which is a factor of economic growth and can potentially improve the general wealth of nations, all else being equal. This does not mean it will be painless, people always prefer improvement to change. If virtual currencies keep up and become our primary money of exchange or source of investment, it will create uncertainty at least for a certain time period. There will be economic and political clashes of major importance and a considerable amount of people will find their jobs at risk. Nevertheless, there is a growing majority of individuals who support this shift from the old system. From the investment banker who stores his profits in Bitcoins and sees an investment opportunity, the entrepreneur who offers Blockchain solutions, to those who simply are interested in the currency itself, cryptocurrency is reaching people from all around the globe. As the US- Senator Thomas Carper said, "Virtual currencies, perhaps most notably Bitcoin, have captured the imagination of some, struck fear among others, and confused the heck out of the rest of us".

But what exactly is Bitcoin? From a terminological point of view, we will refer to *Bitcoin* (with a capital 'B') as the technology or the system's protocol which allows computers to communicate with each other and exchange. While the digital units of value that are used to in exchange for goods and services or other currencies will be referred as *bitcoin*, the currency (BTC). Bitcoin as well as all the other cryptocurrencies, is not an organization, does not have a CEO neither can it go bankrupt. It can view simply as an open source software that allows people to transfer value over the internet, or as a digital currency and an international payment system. This thesis aims at providing an in-depth analysis of cryptocurrencies to understand how and why the shift from fiat and electronic money was made, what are the major challenges cryptocurrencies face in order to integrate our economy and what it implies for the future of our exchanges. Considering the roller-coaster fluctuations the prices of crypto-values are subject to, we will also investigate bitcoin's abnormal pattern of growth and size the presence of speculative bubbles in BTC trading exchange markets.

I. PURPOSE AND FUNCTIONNING OF CRYPTOCURRENCIES

1. From the traditional banking system to Cryptocurrency

1.1. The birth of intermediation

When expressing his concerns about our modern economy which will keep involving ever more exchanges, former U.S. treasury secretary Larry Summer explained that an "exchange, unless it can be literally simultaneous, always has issues of trust". What he meant is that time delay and every other factor or person involved in a transaction can cause serious issues of trust by adding uncertainty and asymmetries of information. Hence, this is where with the invention of money as a medium of exchange, payment and store of value, the need for intermediation rose. It is important to keep in mind that the existence of intermediary institutions answers a strong demand for safety and for several services regulating financial exchanges, in order to minimize risk. Intermediaries such as Banks are addressing this issue of trust by bringing their expertise, time and knowledge, in exchange of a fee which is a cost for any debtor, investor or consumer in need of those services. Taking in charge the wide range of costs direct finance would imply, financial intermediaries act as centralize agents performing activities of screening, selection, monitoring, and diversification of risk, while simultaneously providing credit and liquidity services to fund suppliers. The constant need for liquidity and guarantees made the traditional system of financial intermediation a bank-centred system. In this model of intermediation, Banks perform the activities of what is usually performed by separate entities: not only they are the *loan originator*, but they are also the implicit *issuers* and *underwriters* of the loan portfolio to its own investors, depositors and equity holders. In addition to that, Banks perform the role of *trustees* acting as agents backing the transactions of their clients, and that of *servicers* who collect the revenue streams. Eventually, Banks are also here to provide further liquidity and *credit enhancement* to debt holders. (Nicola Cetorelli s.d.)

But as the variety and dimension of services Banks had to provide was growing at a significant rate, we acknowledged over the years a segmentation of the intermediation chain. Different external entities government-backed or not, started carrying out one or more of the above activities in order to keep fast flows of money, high level of security and more consumer tailored services. It is undeniable that this division of tasks to manage money happened to be correlated with people's lack of faith in the financial system. Nowadays, even private entrepreneurs are launching new activities related to that matter, such as peer-to-peer lending which is boom in the U.K. and where both debtors and creditors can meet directly on a platform to make loans without the need

for any intermediary. But while the system has become slightly more decentralized and complex with the emergence of new entities performing services related to the circulation of money, financial intermediation still resides at its core. Everything is related to our money and our information which are held centrally in our bank accounts and managed by governments and central banks. We may wonder what is it that people dislike about having a 3rd party protecting our information and carrying all the activities we do not want to take care of ourselves. Well people in-satisfaction resides in the fact that those entities proved not to be as sound as they claimed and that technological progress will soon offer an alternative.

1.2. Digital money for a digital age

Back in the 90s, exploring the potential of the internet, a group of programmers known as the *Cypherpunk* made a series of experiments which could be considered as the foundation of cryptocurrency. What the crisis showed is that the existing system which nearly collapsed had some serious flaws and this made people furious and hungry for an alternative. The global financial crisis did, in a way, legitimate those ideas and gave them the possibility to become reality. More than simple computer coding protocols, virtual currencies come from a very politically engaged background. Since the beginning, Bitcoin took the form of an open source project, creating a true sense of culture and community who believe in a new system. Through the discovery of cryptography, some people started to think about a new world, one that could lie outside the structures of power and the hierarchies. Being very concerned about privacy and personal liberty, they evoked the need and the possibility for a digital currency that could be anonymized using cryptography. Digicash, the digital currency David Chaum tried to create, was based on the idea that privacy of payments was essential for democracy. The Cypherpunk movement took his philosophy to translate it into something that could disempower the government and empower the individuals (Bitcoin 2016). A few years later, it's a whole community who shares these values.

"What is needed is an electronic payment system based on cryptographic proof instead of trust" (Nakamoto 2009)

In 2009, Satoshi Nakamoto took these projects and ideas, and eventually made them work by publishing a paper on an encryption-based protocol, that wasn't really a currency yet. It allows for many kinds of transactions to occur, utilizing a distributed ledger called the Blockchain and a system of consensus where multiple computers participate in the management of this digital document that keeps track of all the payments.

1.3. Updating the concepts of money, exchanges and payment

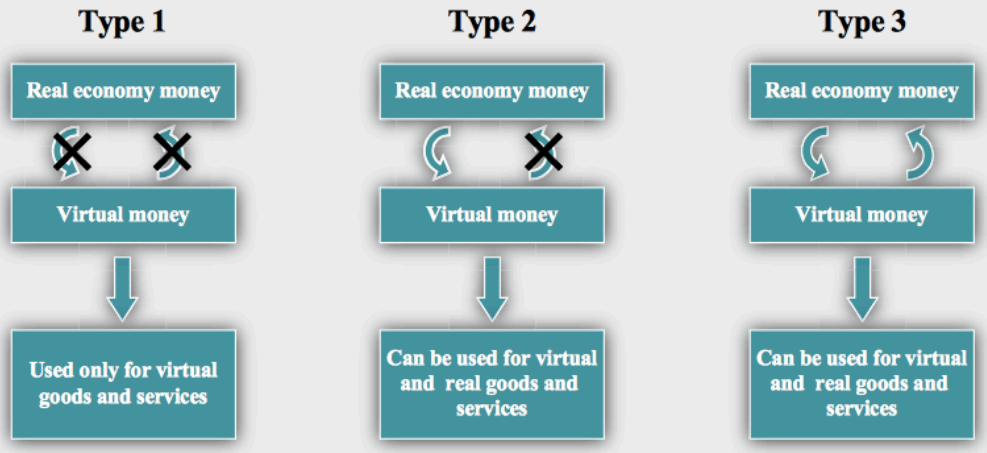
Money is basically an accounting system. It is a way of recording who owns what, who has what and who owes what to whom. For hundreds of years now there has always been the need for someone to be the central issuer, the trusted third party which could guarantee the veracity of money. Thus, so far, we've had governments controlling and issuing money, banks and financial institutions (like credit card companies) which we trust to process our transactions in a certain payment system. This is also what bitcoin is, it is essentially a way of recording transaction and value in a digital way so that everything can happen instantaneously.

But before going any further, it is important to recall the different functions and types of money that exist, how they differ and what are their characteristics, in order to compare them with cryptocurrencies and understand in which category do bitcoin or Ethereum fall into.
First and foremost, Money, to be defined as such, needs to serve several functions starting with the one of a Unit of Account. Keynes' theory of money describes unit-of-account as the numéraire standard role of money, in terms of which debts, prices and the general purchasing power are all expressed. This standard does not necessarily require a physical dimension and aims at simplifying transactions. In order to ensure the finality of payment, money serves also the function of medium of payment, which is closely related to its function of medium of exchange as all kind of exchange does involve some kind of payment in return (the opposite does not necessarily hold true). Money as a medium of exchange represents that 'thing' which everybody agrees to receive when selling something on the basis of expecting to be able to use it to buy other goods or services in the future. It allows to decrease transaction cost and facilitate its circulation into the market by possessing the features of standardization, wide acceptance, durability, divisibility in addition to have low carrying costs. Eventually, money can also perform the function of a store of value in that it is an alternative to financial assets, offering maximum liquidity and low but stable value over time. Different types of money, such as commodity money, fiat currency, scriptural money and electronic money, were implemented to fit the above functions. Commodity money which has an intrinsic value, is composed of "actual units of a particular freely-obtainable, non-monopolised commodity which happens to have been chosen for the familiar purposes of money, but the supply of which is governed – like that of any other commodity – by scarcity and cost of production" (Keynes 1930). The application of that money translated in to metal coins for the convenience of their use. But the so-called 'cash' money (Banknotes and coins) we use every day is defined as Fiat currency which is created and issued by the State, has a predetermined value and is not convertible by law into anything other than itself. Similar to this fiduciary money is the Managed

money, but the latter has a determined value in terms of an objective standard managed by the state. Subsequently, Scriptural money is defined as "deposit balances held on an account at a credit institution or a central bank" (2000/46/EC s.d.) and can be converted into fiat currency at any time, despite not having a physical dimension. Finally, Electronic money is "an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions" (ECB[1]) (E. C. ECB 2012).

At this point you may think that Cryptocurrencies are a type of electronic money, but this isn't the end of the story yet. Bitcoins and its siblings actually belong to another category of money, which is a specific type of electronic money used for transactions in the online world: Virtual currency. Although they have a lot in common, it is important to make the distinction between electronic money and virtual currencies. For instance, even if both are built on a digital basis, the former is backed by tradition currencies (US dollar, Euro, Yen…) and has a legal tender status that is regulated. It involves mainly operational risk. While on the other hand, Virtual currencies take a much wider dimension. They are completely ground-invented currencies (Litecoin, Bitcoin, Ethereum…) without a legal tender, unregulated (at the moment) and which are not backed up by a country's central back or gold reserves but by the distributed community of users of that system.

Chart 2 Types of virtual currency scheme



Source: ECB.
Note: A subscription fee may be required for Type 1.

Cryptocurrencies belong to the third type of virtual currency scheme, which allows bilateral exchanges between virtual and real money. Units of digital currencies can be purchased by credit card, PayPal or bank transfer, and be used to buy goods and services both online and in real life.

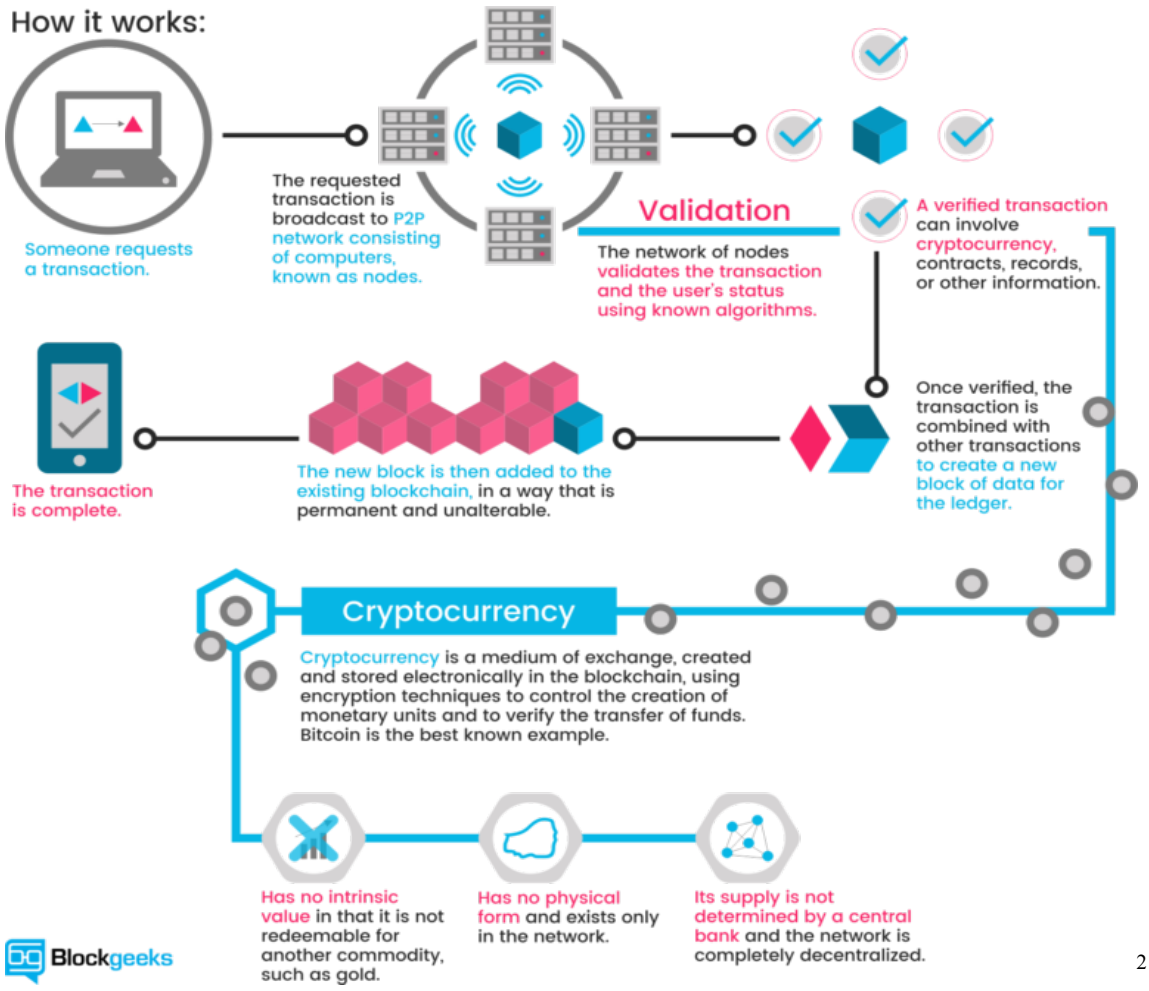
[1] ECB's definition of electronic money: https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

Cryptocurrency is digital money created from code. It can be used to send money directly to anyone in the world, cutting away the middle man and making digital currency in that sense much cheaper than fiat currencies. Digital money, through the recording of transactions on the Blockchain, ensures finite exchanges and the immediate settlement of claims. Our transactions with cryptocurrencies are unstoppable and irreversible once made, in addition to being publicly displayed for a matter of security and transparency. The design of this system is also safer since less information about the two parties involved is required. Unlike when sending a transaction through banks, cryptocurrency doesn't ask you to trust the safety of your information, it simply doesn't take it in the first place. Due to the various similarities with existing currencies, Virtual currencies can and must be recognized as such. Even though they are not yet widely accepted as medium of payment or exchange, especially in the real world, the variety of services and entities which accept them is growing at a constant fast rate. For example, nowadays bitcoin registers approximately 300,000 transactions per day, more than a 150k retail stores as well as 300 websites accepting bitcoins worldwide and 14 million wallets in use reported in 2016 by Coindesk.com.
Nevertheless, as the Founder of LiquidMoney Cryptocurrency Institute, Shireen Ramjoo, underlined: what makes this type of money different to what we are used to is that "Cryptocurrency was designed as a wealth enrichment currency as they are usually limited. Because of this, the supply and demand factor of economics come into play. As more people start using a particular cryptocurrency, the demand rises and because it is limited, the lesser they become. This in-turn allows for the price of the currency to continually rise, as long as there is a demand for it as it continues to grow. It is also viewed more as a commodity than a general currency." But we will return to that subject later on.
Although there are some similarities between virtual currencies and the ones we are used to, cryptocurrency transaction's irreversible, pseudonymous, secure, permission-less, fast and global properties make them completely unique.

1.4. How does a cryptocurrency work?

Virtual currency's functioning is very similar to the one of normal currency. Both kinds of money pretty much come down to series of verified entries in a certain database of accounts, balances and transactions. But the former is fully digitalized, meaning all the activities of issuance, storing, recording, transfer and payment happen online, virtually, in a non-finite network of computers. Thus, how can individuals acquire cryptocurrency and use it to conduct transactions? Well, while the technology supporting those currencies is based on complex encryption, their use is fairly simple. Every individual has first to set up an *electronic wallet*, next to the various

providers on the internet, which is his online currency account. Digital wallets vary according to the needs of the ones using them. They can be software-based (like an App or a computer software) or hardware (mostly USB keys) for bigger volumes of holdings and trading. It is basically just as carrying our physical leather wallet with our credit cards, IDs, receipts, but right on our phone, computer or piece of hardware. Electronic wallets allow to store one or more cryptocurrency's transactions on the Blockchain, receive and make transfer and sometimes access directly virtual currencies' trading exchange markets. The main point is that once the wallet is set up, the client will receive his public Bitcoin address, to which he can receive transactions from anyone but which differs from the private one he will be using to make payments. In addition, every wallet has its own private key which matches the public address and is very important in order to receive transfers. What happens is that when an individual sends you bitcoins or any other digital money, they are basically signing off ownership of those coins to your wallet address. Only once the Blockchain confirms that the private and public keys match, the person will be able to unlock the funds and see the balance of his digital wallet increase and be able to spend those coins. This confirmation represents the very essence of cryptocurrencies and is the central nucleus of the whole system, which is here explained in a schematic approach:



[2]

[2] Image from: https://blockgeeks.com/guides/what-is-cryptocurrency/

Thus, cryptocurrencies can be owned through transfer from another person, purchase online, trade in P2P exchange markets, Initial Coin Offering (ICO) or through mining.

- Mining

Mining is the alternative to a Government deciding when to print and issue money, which cryptocurrency do not have. It is the activity to solve complex maths problems in order to confirm the transactions carried out on the Blockchain. People then use advanced software and computer chips to solve those problems and get a certain number of units of that currency in exchange. This provides a smart way to issue money and an incentive for more people to approve transactions, hence increasing the network's safety. Miners also have to provide a 'Proof-of-work' meaning that the information (new block) was difficult (costly, time-consuming) to be made. As the popularity of cryptocurrencies rose as well as the quantity of transactions, it became difficult for individual miners to solve those maths problems. Thus, to overcome this, miners decided to combine their work in so-called mining pools which find solutions faster and each miner is rewarded based on the amount of work he or she provide. Miners are mainly involved in cryptographic *hash functions* which consist in taking an "input data (string) of any size, perform an operation on it and return output data of a fixed size" (coindesk.com). A common use of it would be to store passwords.
Mining is an important part of cryptocurrency as it helps to keep the networks fair, stable, safe and secure. (Mining 2013)

- ICOs and exchange markets

Initial coin offerings are just like Initial public offerings but with cryptocurrencies and a lot less regulations for now. The same principle applies, ICOs are a mean to perform fund raising activities, prior to the launch of a cryptocurrency, in order to attract investors looking for sky-rocking returns for their investment in the secondary market. The funds are usually raised in bitcoins, the dominant virtual currency. ICOs may offer high returns but also represent very risky investments that people blinded by fast and easy money are ready to undergo. These crowdfunding operations are a way to bypass banks' or venture capitalists' highly regulated fundraising process and raise capital, especially for young enterprises such as start-ups. It is the democratized access to investment. There are several cryptocurrency exchange markets online which may or may not require some kind of intermediation. These websites allow the buying and selling of digital currencies in exchange of traditional (fiat) or virtual currency. In other words, depending on the exchange, it either works as a stock exchange or a currency exchange.

We distinguish among them three main types of exchanges. The first one is trading platforms which involve a 3rd party that charges a fee on each transaction for connecting buyers and sellers. These exchanges (GDAX, Kraken) are similar to traditional stoke exchanges in that buyers and sellers trade based on the current market price of cryptocurrencies Second are direct trading websites, that allow individuals from all around the world to exchange currency and each seller can set their own exchange rate. The third type are Brokers websites (like Coinbase) are similar to foreign exchange dealers, where anyone can buy cryptocurrencies at a price set by the broker. Lastly, cryptocurrency Funds are exchanges that take the form of "pools of professionally managed cryptocurrency assets which allow public buy and hold cryptocurrency via the fun. One such fund is for example GBTC."[3]

1.5. Several cryptocurrencies, with different characteristics, for what use?

There are currently more than 1000 cryptocurrencies available over the internet. It can be explained by the ease with which cryptocurrencies can be created and rapidly spread. The opportunity to raise fast and large amount of capital through ICO is also what makes new cryptocurrencies so attractive to young businesses. There exist a large variety of cryptocurrencies which serve different purposes, suit different needs and function differently. Even if the majority is based in the same technology and principle it is important to acknowledge those differences. For example, not every cryptocurrency can be considered 'decentralised' as this depends on multiple factors such as the proportion of independent and non-colluding nodes and miners, as well as the amount of hash power securing the blockchain, among others. Bitcoin is by far the most important both in terms of numbers and technology, as it was most certainly the pioneer of digital currencies. It has become de facto the standard for all the other cryptocurrencies, also called *Altcoins*, that reproduce the Bitcoin's code and create their own blockchains. Inspired by Bitcoin, these currencies present themselves as modified or improved alternatives to bitcoins. Altcoins each have their predetermined functions and characteristics but are significantly less popular and are often bought in order to form efficient and well diversified portfolios of virtual currencies. Nevertheless, they still try to differentiate themselves just as *Monero* who offers a virtual currency that makes transaction more secure and untraceable by using ring signature technology to protect privacy. Other examples of the diversity of digital currencies include the Linden Dollar, which is the virtual money used in the "Second Life" online game and managed by Linden Lab for in-game purposes.

[3] Currency Funds' definition: http://cryptocurrencyfacts.com/what-is-a-cryptocurrency-exchange/

We will review now the 5 major cryptocurrencies on the market, both in terms of popularity and size, and see how they differentiate from one another.

Bitcoin (BTC):

Started in 2009 by Satoshi Nakamoto. It is currently the most popular, widely accepted, easy to get and to use virtual currency. Bitcoin had to undergo a 'fork' at the end of July 2017, due to technical problems that were slowing the processing of transactions. After its derivative Bitcoin Cash had been set up (bigger size of blocks, solved mining issues) Bitcoin doubled its value in August.

Ethereum (ETH):

Second most popular crypto currency. Launched in 2015. It is a decentralized platform that runs smart contracts without any downtime, fraud, control or interference from a third party[4]. Ether features its own Turing-complete programming language. Attracts many developers and Businesses for running applications inside Ethereum.

Litecoin (LTC):

Started in 2011. It is considered to be the "silver of bitcoin's gold" due to its higher supply of 84 million LTC. Litecoin's open sourced global payment network is very similar to the one of Bitcoin. However, it has faster confirmation times, thanks to faster block generation, and a scrypt-based mining system.

Dash:

Also known as *Digital Cash*, is another more secured and fast altcoin. introduced in January 2014. It aims at becoming the first privacy-centric cryptographic currency with fully encrypted and anonymous transactions, to make them untraceable.[5] In contrast to most other cryptocurrencies, block rewards are being equally shared between miners and 'masternodes'.

[4] http://www.investopedia.com/terms/e/ethereum.asp
[5] https://www.cryptocompare.com/coins/dash/overview/USD

Ripple (XRP):

Released in 2012, is a complement to bitcoin. Ripple is a real-time gross settlement network that offers instant, certain and low-cost international payments. Unlike other altcoins, Ripple does not need mining which reduces the usage of computing power and minimizing network latency.[6] Ripple is the only virtual currency, here mentioned, that does not have a blockchain but instead uses a global consensus ledger.

1.6. Market facts

In order to have a deeper understanding about cryptocurrencies and their importance we will look at some market facts and statistics which will help us size this inevitable phenomenon. The focus will be mainly on the above mentioned digital currencies. What we are currently witnessing is an epic explosion of bitcoin and its alternative currencies. They are now worth more than $100 billion, six times their value at the beginning of the year. It is either the beginning of a global financial realignment or of a bubble of historic proportions. Notwithstanding their fast growth and evolution over the last decade, and even considering the unstoppable creation of new ones, the market size of virtual currencies remains relatively small compare to that of real ones. It is rather difficult to put in perspective theses new innovation with what has been in place during such a long time. Furthermore, it is difficult to provide accurate and significant indicators regarding the value of this booming market, due to the tight competition existing among cryptocurrency and to what seems to be speculative behaviours on the investors side. We will attempt to seize the virtual currency industry considering facts and numbers regarding its users & main actors as well as economic and financial data.

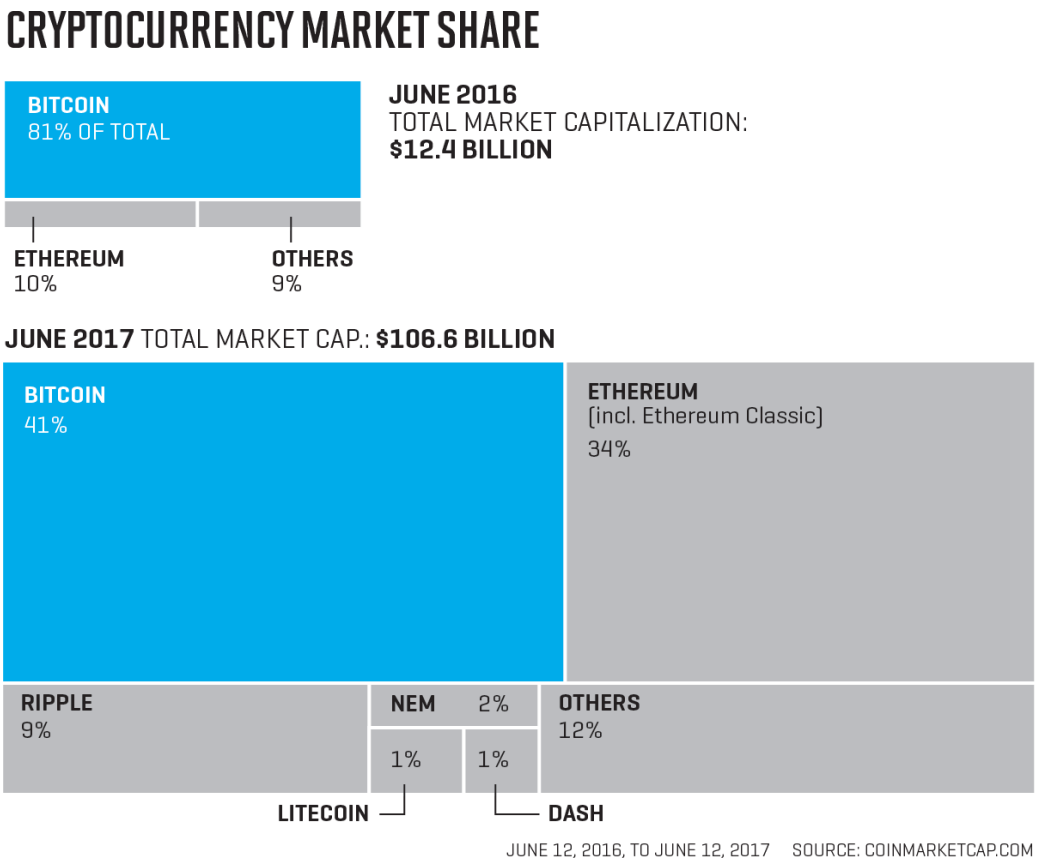
Examining the demographic repartition of cryptocurrency activity, Europe has the most number of exchanges, followed by Asia-Pacific. The Exchange sector is considered to be the biggest of the virtual currency industry, as it employs the most people. If we look at the number of bitcoin and other cryptocurrency ATMs it turns out that 94% of all publicly known ATMs are based in North America and Europe[7]. Whereas Africa, the Middle East and Latin America possess 2% of those ATMs. It gives an idea in proportion of the physical concentration of cryptocurrency activity in the world. From the growing interest for cryptocurrencies, a lot of new projects and companies have emerged to provide products and services that facilitate the use of digital currencies for

[6] http://www.investopedia.com/terms/r/ripple.asp

[7] From (Rauchs 2017) Report: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-04-20-global-cryptocurrency-benchmarking-study.pdf

mainstream users and build the infrastructure for applications running on top of public or private blockchains. Today, the number of people employed full-time in the cryptocurrency industry is estimated at 2000 employees in 2017 (Rauchs 2017).

Cryptocurrencies are following unprecedented trends of growth, and different indicators help determining what they really weight in our financial sector. Starting with the one of their Market capitalization: there is a reason why Bitcoin stands as the best-know cryptocurrency on the market and this is reflected in its $62,028,307,522 Market Capitalization[8]. This number puts Bitcoin way on top of the overall ranking, as it accounts for more than the double of Ethereum's $26,428,762,997 Market Capitalization, which is the second highest ranked digital currency, followed by Bitcoin Cash ($6,977,309,109 Market Cap).



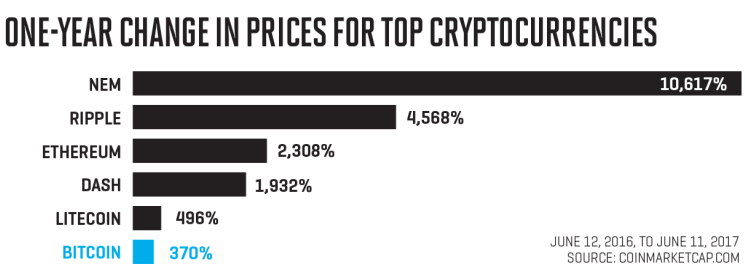
Referring to the above chart, we can observe that the total market capitalization has known an astonishing 760% increase, on a one year basis, as of June 2017 (Eha 2017).

While this statistic indicates how cryptocurrency popularity and use strongly spread last year, another information about the market share might be worth the analysis.

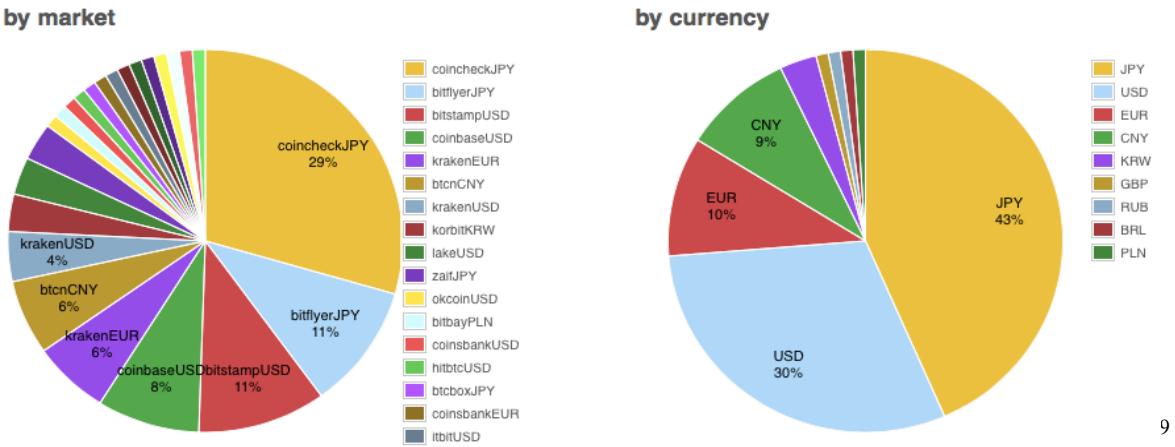
[8] All figures are taken from https://coinmarketcap.com/ on the 23rd of September 2017.

Bitcoin's market share has indeed decreased from 81% to 41% due to the rise of investments in other cryptocurrencies because of their technical or return possibilities.

As the attached table displays it, evidence suggests that altcoins are starting to catch up, even though bitcoin's price have kept increasing exponentially, certain altcoins's prices simply soared even faster.



As of today, the price of a unit of NEM and Ripple cryptocurrency is worth respectively $0.221139 and $0.176873. These amounts might seem ridiculous compared to the prices of Bitcoin ($3771.79) and Ethereum ($280.80) but they actually increased at a higher growth rate. Emerging and well performing virtual currencies are slowly taking down Bitcoin's monopoly. This latest trend reminds of the saying "the stronger entrants will get stronger and the weaker entrants will get weaker". Data on Coindesk revealed that, last year, Ethereum surged past his rival in terms of daily trading volume and raised its value by 3500%. This performance appears even bigger when put it perspective with the one of traditional assets such Palladium, Nasdaq and S&P 500, which grew respectively by 25%, 15% and 9%. With an increasingly more balanced market, we could say that a kind of crypto-pluralism is taking hold. Whereas trading volumes of cryptocurrencies across the top exchanges are more evenly distributed following increased regulation of Chinese exchanges in early 2017, the processing of transaction appears to be surprisingly low. This problem initiated Bitcoin's fork, as the currency was facing a very high demand and old Blocks were able to support only 7 transactions per second while circuits like Visa and MasterCard can execute thousands of them in the same amount of time.



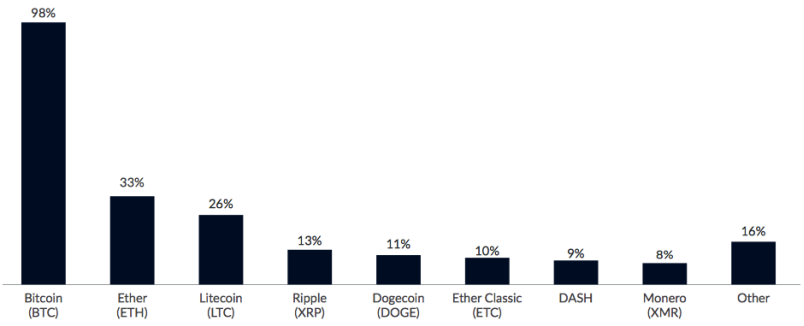
[9]

[9] Exchange volume distribution, based on the last 30 days: https://bitcoincharts.com/charts/volumepie/

Overall, a handful of large exchanges and four national currencies (USD, EUR, JPY and CNY) dominate global cryptocurrency trading volumes. It is striking to observe that the dominant online Exchange platforms of 3 years ago, such as Bitstamp and Bitfinex, lost a significant part of their market share or even disappeared. That can be explained by Exchanges not able to cope with the increasing amount of regulations and by the down-pace of USD-BTC trading versus the JPY-BTC. Taking into account the above figures as well as the recent strong expansion of cryptocurrencies, many well-established entities decided to invest in virtual money. Giants like Goldman Sachs, Visa, Nasdaq, JP Morgan and the New York Stock Exchange have all invested in Bitcoin's and its underlying technology.

Concerning the use of cryptocurrencies from a client point of view, the most common applications of cryptocurrencies are divided among the following categories: speculative digital asset / investment, medium of exchange, payment rail and other non-monetary use cases. The number of cryptocurrency users is complex to estimate as it is rather difficult to know precisely how many wallets a single person owns on average Data obtained from collective study participants (Rauchs 2017) suggests that the number of active wallets, which has significantly grown, ranges from 7.5% to 30.9% of the total number of wallets (i.e. between 5.8 million and 11.5 million in 2017). Although the term 'active' is not very clear as can be interpreted in many different ways, this shows that the majority of cryptocurrencies' users act as long-term holders and are involved in very few transactional activities. Analytics revealed also that Mobile Wallet Apps were the most widely offered format to hold virtual currency, perhaps because of their easy carrying mode.

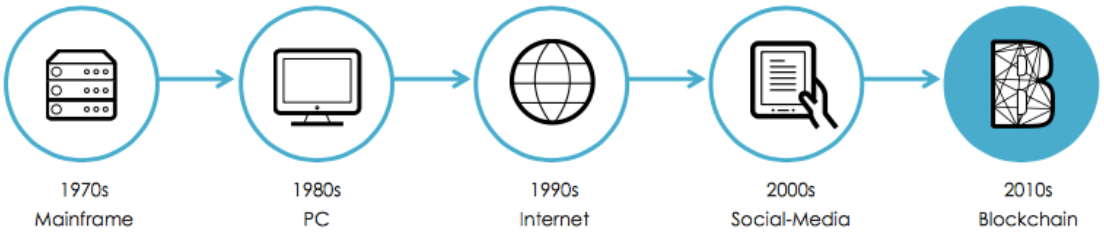
Percentage of wallets supporting the listed currencies (Rauchs 2017):



Moreover, while the vast majority of wallets, payment companies and participating exchanges support bitcoins, 39% of electronic wallets providers offer the ability for users to store more than one crypto currency in the same wallet. Ethereum, litecoin and dogecoin are the most widely supported cryptocurrencies after bitcoin. Statistics form (Rauchs 2017) show that overall, the majority of wallet providers based in Europe and Asia-Pacific are satisfied with the existing regulatory environment, but that the ones of North America are divided in how they perceive existing regulations.

2. Breaking-Down the Blockchain

Although the Blockchain can be a very powerful tool for significant volumes of transactions in terms security, disclosure and rapidity, the complexity of its system of operation is worth a deep and accurate explanation. Using cryptography as the pillar of its recording process, the Blockchain introduces a whole new way of managing worldwide exchanges and interactions, through its unique book alike recording system.



10

2.1. Block I: Decentralization giving the heart beat

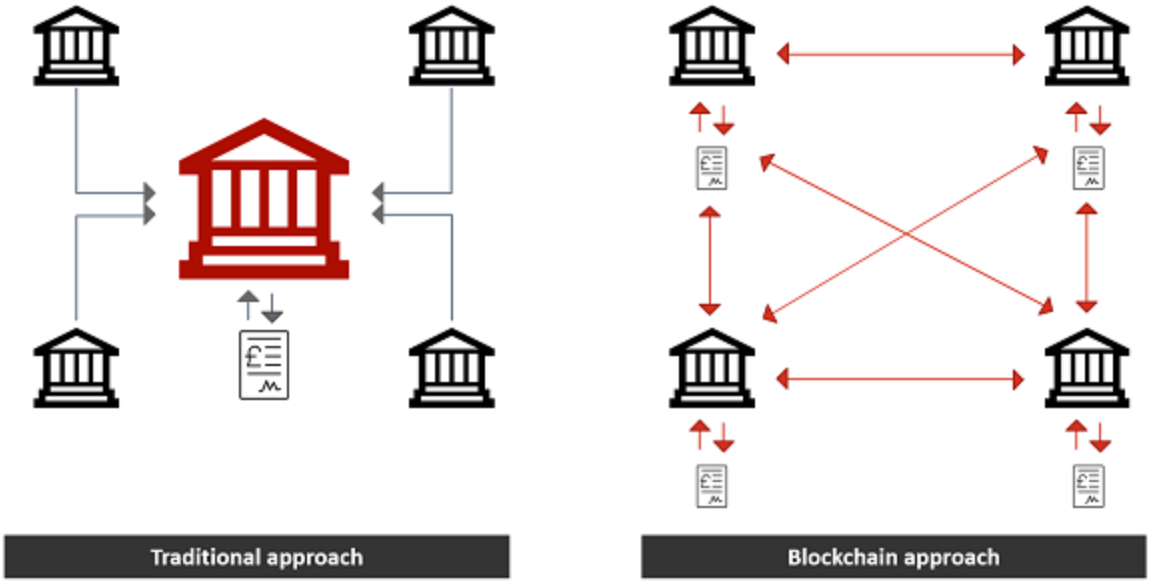
Even though everyone heard about it and considering *The Economist* defines it as "The trust Machine which will revolutionize the world", no one really knows what the Blockchain is and how it works. In order to understand its utility, we must familiarize with the functioning of exchanges on the Internet, that is the double spending problem. When sending an email or a document, we are actually sending a copy of it, which in a sense is great for fair sharing of information. But when it comes to money, financial assets, intellectual property and vote, finite transactions are a must. Double-spending is a problem unique to crypto currencies as digital information, unlike physical currencies, can be reproduced relatively easily. With digital currency, there is the risk that the digital units be copied in order to send it to another party while at the same time keeping the original. The digital token will end up being spent twice. Thus, how is the Blockchain allowing finite exchanges to happen on the Internet?

Starting from its definition, a Blockchain is a public distributed ledger held by a wide and non-finite Peer-2-Peer network of computers. It is a technology of storage and transmission of information, working without a central authority, in a transparent and safe manner. Private Blockchains do exist also, where access and use are limited to a certain number of users. A Blockchain can be seen as a constantly updated registry of assets, intellectual property and transactions available by anyone at any time. This immutable and perfectly traceable virtual database, which is fully protected by the use of secured cryptographic keys, compresses

10 Blockchain as an historic evolution, source: http://irishtechnews.ie/bitcoin-and-blockchain-the-difference-and-what-does-their-future-hold/

information such as titles of ownership, amount, type and location of transactions in Blocks following each other's, just as pages of a book would. When exchanging value, individuals must validate the whole present Block of transactions, which makes recording issues impossible as they would immediately result as a visible mistake to miners and the whole network. Hence, through this unique system of recording transactions, based on the concept of validation (algorithm of consensus), the Blockchain is more than a simple book-record, it is an extremely powerful tool in terms of transparency, efficiency and security.

The Blockchain is repeatedly said to be a decentralized distributed platform. Decentralized because the information can come from literally from anywhere. Every user can make a transaction and an entry wherever he might be, without the need for any kind of authorization or control from a third party. The information is than instantly made visible for all the past and present users of the infinitely extendable network. That is what makes the Blockchain distributed, it is the direct links and interactions that are created within the Network. The current payment systems require third-party intermediation that often charge high fees, but machine-to-machine payment using the Bitcoin protocol allows for direct payment between individuals as well as support micropayments.



Freedom of transaction and public access to its records on a Peer-to-Peer platform, instead of a server-based one, represent the strength points of the Blockchain. This system of governance of exchanges benefits from both its distributed computing infrastructure and its common protocol, which make nearly impossible to create fraudulent transactions.

[11] Image source: https://openwt.com/en/trends/blockchain

2.2. Block II: Process of virtual value creation

As an extension of its definition, a blockchain constitutes a database which contains the historic of all exchanges carried out by its users since its creation. To ensure the validity of the chain, this database is secured and distributed, meaning it is shared by all its different users. Any Blockchain runs necessarily with a programmable currency or unit of 'token' that can possibly represent anything. The transactions of the network's users are grouped by blocs. Then, each bloc is validated by the nodes of the network, the miners, according to the techniques upon which the Blockchain depends. In bitcoin's blockchain for example this technique is called "Proof-of-work" and consists in solving complex algorithmic problems. Once the transactions have been confirmed and the bloc has been validated, the latter is timestamped and tied to the previous Block, hence creating the so-called *Blockchain*. All the written transactions in this last block are now perfectly visible by both the receiver as well as the whole network. The confirmation of blocks creates an immediate transfer of ownership as, at this point, transactions are certified and cannot be disputed. This process may take a certain amount of time, depending on the Blockchain concerned. We expect 10 minutes for bitcoin and 15 seconds for Ethereum (BlockchainFrance 2016)[12].

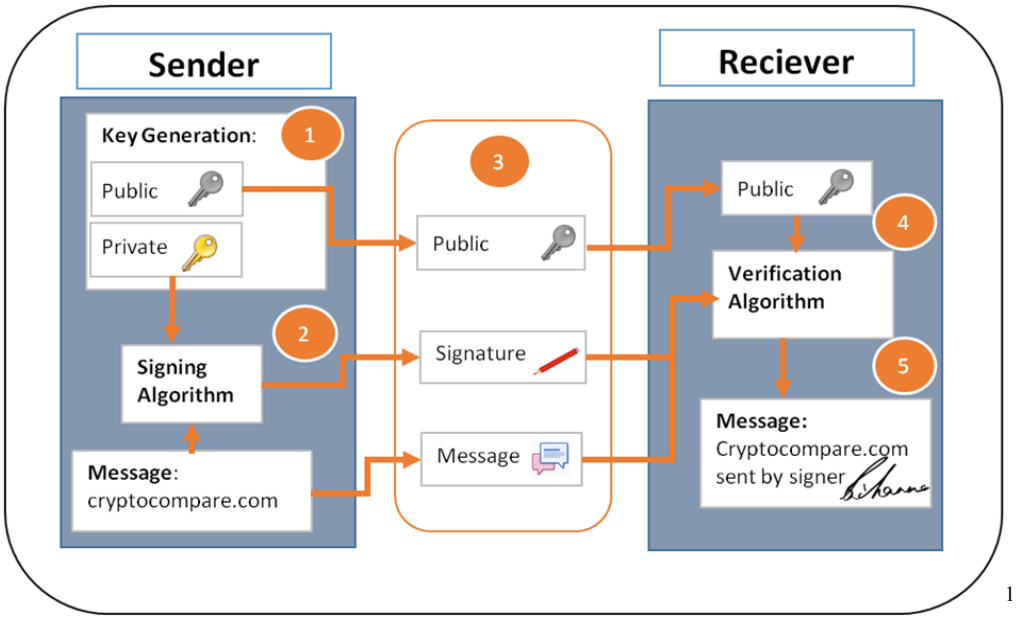
From an economic stand point, a Blockchain is based on a circular economy chain: The work done generates value which in return offers tokens as earnings. That currency can subsequently be spent inside the marketplace, that the Blockchain represents, making an additional transaction or outside the market place in exchange of another cryptocurrency or fiat money (Mougayar 2016). The value that this system permits to create, resides in the work that is done to verify transactions and legitimate the use of the currency. When the validator nodes of the network receive the proposed block, they start working to validate it through a repetitive process which requires the consensus from a majority of the network. Validation techniques other than bitcoin's "Proof-of-work" include Ripple's "Distributed consensus" and Ethereum's "Proof-of-stake". The collective and maintained agreement of the network on the content of the digital ledger is really the key to the blockchain's operations. Bitcoin's most common blockchain let miners compete to add the next set of transaction (block) by racing to solve extremely difficult cryptographic puzzles consisting of a mathematical function called *hash*. The first miner who achieve it receives 12.5 newly issued BTC per block (Castor 2017). Unfortunately, this iterating task is computationally expensive as it requires a lot of energy. It is the reason why the vast majority of mining firms are located in areas of the world where climate is relatively cold and electricity is cheap, like Island. The above issues have caused problems to bitcoin in the past by delaying the time of transactions and may suggest

[12] Data from: https://blockchainfrance.net

that the Proof-of-work consensus algorithm is not the most efficient one for big volumes of transactions.

2.3. Block III: Cryptography as a pillar (virtual signature)

In virtual currencies' public blockchains the trade-off between the full disclosure of all transactions and the protection of private data is a bit counter-intuitive, but is solved with cryptography. Users' information in the database of cryptocurrencies are processed through the mechanisms of Blockchains which are strongly based on the encryption of data. Paradoxically, the cryptography of blockchains is fundamental for transaction authentication purposes. As said previously, a digital currency consists of a network of peers and every peer has access to the record of the complete history of all transactions and hence of the balance of every account. Typically, a transaction file says: "User A gives X to User B" which are defined by their public address. The exchange is *signed* by both users' private keys which are uniquely related to their respective public address (key). Only after being signed and confirmed, a transaction is then broadcasted in the network, sent from one peer to every other peer. Transactions are represented by binary codes which are then verified by script execution. This is basic P2P technology. Of course, the 'signature' has a digital format as it is computed by computer, we generally talk about *virtual signatures*.



[13]

Private keys are assigned whenever a person opens an account on a digital wallet with a public address to which it is tied. But it is impossible to trace back a private key from its public address. Thanks to numerical signatures, users can validate the message containing the timestamped

[13] Example of an encrypted transaction on the blockchain, with digital signature, from: https://www.cryptocompare.com/wallets/guides/how-do-digital-signatures-in-bitcoin-work/

information about the transaction. Those signatures are the irrefutable proof that these specific users have exchanged value on the blockchain. In other words, the system does not relate to persons but to but to private keys for ensuring the veracity of transactions. Because only the single users involved in the transaction can prove they possess the private key through their pubic address, certifying that the message was emitted by that specific person and preventing the modification of the message. The algorithm in charge of the virtual signatures is called ECDSA (Elliptic Curve Digital Signature) and was invented by Scott Vanstone in 1992. It is considered safe since it insures the impossibility to pass from the public key to the private one by using keys of 256 bits (for bitcoin) called "discrete logarithm" and that have close to zero probability to be cracked. Naturally, all keys' operations are carried out automatically by electronic wallets without the need for the user to program them (Delahaye 2016).

Another major component of virtual currencies' cryptography is *hashing.* Bitcoin's hashing function (SHA-256) is used for many steps of the protocol. It is involved in the creation and identification of public addresses. But primarily, it is used to tie the different blocks of the open registry and thus ensure its continuity. Hashing plays also an important in the system of issuance of bitcoins, because minor's probability is directly and proportionally bound to his power of calculation. Overall, a hash of a transaction is "a double hash of the binary format of the transaction. Algorithm SHA-256 is applied twice, for historical reasons, and to increase safety" (Pares 2016).

2.4. Block IV: Redefining models of trusts

With everything being recorded in the Blockchain open ledger which is monitored and updated in a collective, consensus-based system, there is no need any more for a central authority that would act as a repository for all the information. This is what eliminates the fees, the inefficiencies and ultimately the potential corruption and risk that come with centralizing information in that way. What it does is it takes that trusted third party function and it automates it. It puts it online, in an open ledger which everybody can see that cannot be shut down, so that every unit of currency is accounted for and you know that you are not getting a counterfeit one.

Cryptocurrencies seduce because they are easily transferable, anonymous and do not require the involvement of a middle-man (a credit card company, PayPal or a bank) if you want to transfer value online. With virtual currencies, you are directly sending the value to another person and the

Blockchain network performs the function another third party would before. What they really do is putting control back in the hands to whom this value belongs.

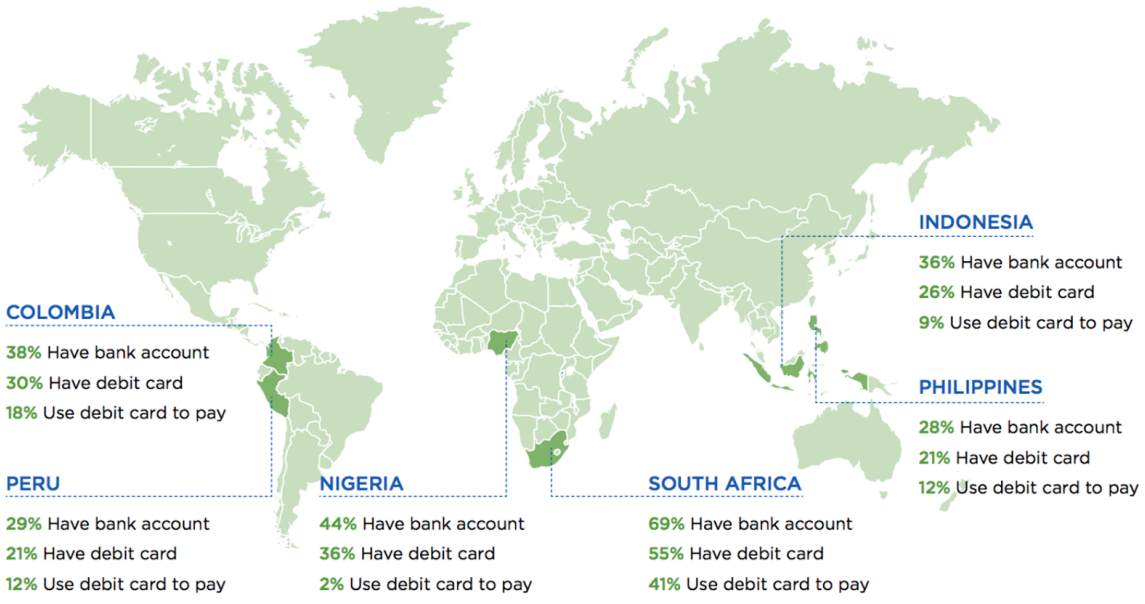
From a policy perspective, this system implies that the money supply is controlled by computers. This means that the burden of trust and security was transferred from humans to technology. Unlike any other ledger, the Blockchain does not have a physical location nor a physical server which can be turned off, and that makes it simply un-hackable. Every single transaction, once recorded on the Blockchain is permanent and cannot be altered or changed so that everybody can read it. However, the identities of the people are encrypted, the *wallets* are encrypted, so we cannot know who is spending the money but we know the history and tracks of any unit transferred. This makes the activities of the network completely transparent and traceable. Centralized intermediation has been replaced with decentralized and continuous interaction of computers. All these elements might suggest that now people feel safer with an algorithm than a separate entity, for the management of their private information. The blockchain technology is mainly being used only for cryptocurrencies purposes but it opens the door to a whole new world. Many other applications of the Blockchain are going to be extremely helpful and some have already proven their efficiency. Such applications include the management of value registry, ecosystem and of the web. The future of intermediation seems to gravitate more than ever towards a distributed and digitalized system. The disruptive and promising technology of the Blockchain could transform the very basic pillars our society by strongly influencing the functioning of our economy, governance and Businesses. It could lead us to rethink the concepts of trade, ownership and trust, especially in the financial sector.

3. Towards a new economy

Many scholars still think that cryptocurrencies are an ephemeral trend, due to their lack of regulation, their potential illicit and dangerous use or because of the large amount of speculation they are surrounded with. One thing is for sure, they will not suddenly die. That is because no entity nor authority is actually owning, controlling and managing virtual currencies. They are fuelled by the power of internet and their peers, which eventually cannot be turned off. An increasing number of people instead, argue that cryptocurrencies will embrace our common future and its applications will serve the interests of our society as a whole, leading us on the road of technological progress. We will examine the major challenges of what is already called the biggest evolution of the century after the one of the Internet.

3.1 Addressing the entire world, integrating emerging countries

Bitcoin is often said to be the invention which will revolutionize the banking system. But what is disturbing about this statement is that it omits to take into consideration the 39% of the world population, mostly in developing countries, that does not have access to a bank account (according to the OECD). The following map displays some key figures about the situation in 2015:



	HAVE A BANK ACCOUNT	HAVE A DEBIT CARD	USE DEBIT CARD TO PAY
WORLD	61%	40%	23%
LOW & MIDDLE INCOME COUNTRIES	53%	31%	14%

[14]

[14] Source: Small Merchants, Big opportunity; World Bank Financial inclusion database 2015.

What it shows is that our banking system is currently putting aside a significant part of our worldwide population, perhaps the one which happens to be the most in need. But the lack of political and financial stability in those country certainly make their development long and very costly. But with the large development of cellular and internet networks, some countries have been eager to find alternatives. In Kenya for example, people have adopted a system of payment that is suited their needs, through their mobile phones. This mobile payment system uses phone credit as a money of exchange and proves once more that the concepts of money as a medium of exchange are rapidly changing. It seems inevitable that money, already virtual, will only become more so as we shift into a digital economy.

Bitcoin and cryptocurrencies have the potential to "bring billions of people from the emerging markets into a modern, integrated, digitalized and globalized economy" (Paul Vigna 2015). In Afghanistan, where women powers and independence are very limited, bitcoin is starting to be used in several e-commerce websites and also as way to pay-out salary. Because women do not have the right to own a bank account without the authorization of their husbands, some employers are currently paying out women salary in bitcoins. In other countries where financial infrastructure is limited, cryptocurrencies have the potential to create a safe place to store capital, send and receive money around the world without exchange rates and fees. Bitcoins represent a valuable alternative to Wester Union to send funds abroad as it eliminates all the physical inconveniences and costs associated with the later. Moreover, the fact that Mongolia, with a population of less than 3 million people, has four times more bitcoin users than the United States shows us that the population of some emerging countries feels indeed very concerned about this new technology and the potential benefits of adopting digital currencies. Meanwhile, the number of Businesses related to crypto-values continues to rise in developing countries as well as ever more Exchange marketplaces which are opening in countries such as China, India and Vietnam. It is currently a win-win situation for both providers and users.

3.2 The view of central authorities and the ECB

The level of decentralization cryptocurrency advertises for, does not gains everybody's agreement. Governments are worried about the social and political question that arise, regarding the current hierarchical system of authority. The tax collection issue causes a real problem if the majority of people start using digital currencies instead of fiat currency and bank accounts. The potential risk that people start using them to carry out illegal activities such as drug dealing, financing terrorist plans and laundering money represent indeed a threat. China and some countries' authorities have already taken action in order to limit exchanges of cryptocurrencies.

In the case of China, the government authorities just started shutting down a significant number of cryptocurrency exchanges, forcing them to cease any kind of activity and immediately notify their users of their closure. It also decided to ban all funding activities that are carried out through ICOs. The government decided to take these radical actions as it was concerned about the risk that consumers were subject to by entering this highly speculative market, since the collapse of the Mt. Gox Exchange in December 2013. The rapid growth of cryptocurrencies urged Chinese regulation to come, also to limit the threat of illegal flows that could spring from the use of digital tokens by the population. In September 2017, when the Chinese government made public his action plan, bitcoin's price dropped by 30% in just five days, following the introduction of these regulations. Some even more extreme measures have been taken by governments to limit cryptocurrency-related activities in their countries. Venezuela which is currently facing a huge crisis, with record inflation drowning its citizens in poverty, made Bitcoin mining liable to imprisonment. People who decide to mine cryptocurrencies, in order to have an alternative sound and predictable source of income to support the basic needs of their families, are now facing the threat of going to prison. The Venezuelan government saw in bitcoin a threat to its already weak currency and thus decided to arrest people 'contributing to its growth' as the ultimate solution to a non-existing problem.

National and Central Banks are also against the use of virtual currencies, as they are direct substitutes to the services Banks. They are also a way to get around the traditional financial intermediation system and could put out of business many financial institutions in the payment and investing sectors. The Bank of America and Chase already took some provisions by forcing their clients who were making too many bitcoin purchases, to close their bank accounts. Investment banks seem to have widen their horizon as they were found recently investing in cryptocurrencies. Overall most of the well-established players in the financial sector seem not to welcome bitcoin and its alternatives. And just as anything slipping their supervision, regulation came and will keep coming. The first one was introduced on August 8, 2015 by the New York State Department of Financial Services (NYSDFS). "BitLicense" was the term used to describe the first attempt to create a business license for virtual currency activities. Although a bit harsh and misleading at some point, BitLicense regulation allowed to close many unsound companies that were supposedly destined to fail. Two years after its introduction, the number of consulting companies giving advices for compliance to the BitLicense have surged, as very few firms managed to obtain it. The European Central Bank on its side, declared that "Virtual currencies do not fit the economic or legal definition of money or currency" in the second Virtual currency scheme (VCS) report of 2015 (ECB 2015). Introducing a new definition from a Central Bank perspective, the ECB questioned the integrity of VCS through their low level of acceptance among

the general public, which limits its function of medium of exchange, in economics terms. Furthermore, the ECB argued that from a legal point of view, virtual currencies by not having a legal tender status (like scriptural and electronic money) can be considered a medium of payment *by choice* but certainly not *by law* since they are used or accepted enough when exchanging value in transactions. More recently, in accordance with its plan to combat money laundering and terrorist financing through cryptocurrency, the European Parliament and the council of the European Union have introduced a new legislation aiming at identifying suspicious activities and anonymous users profile. The directive was amended on the 6th of June 2016 and is currently in its implementation phases. The ECB expects only 'Know Your Customer' (KYC) approved Virtual currencies to be authorised to operate within the European framework, requiring some significant disclosure from Exchanges and wallet providers. In contrast, we acknowledge an increasing number of new cryptocurrencies with strengthen privacy. The latest decisions of the Central Banks raise concerns about the viability of these virtual currencies' companies which will have to comply in order keep operating within the European Union (4AMLD 2016).

Regulation on cryptocurrency is undeniably necessary to a certain extent, even though it goes against the ground principle of virtual currencies which are created to be decentralized and free of any kind of intervention from a 3rd party in managing direct exchanges. (Virtual Currencies and Beyond: Initial Considerations 2016)

3.3 Potential downsides

Governments seem to have a lot to worry about when it comes to cryptocurrency. Indeed, before becoming a popular tool to exchange value as well as a business opportunity, digital money was involved in some illicit activities as it was a way to avoid authorities' supervision.

Cindy Williamson, a certified anti-money-laundering specialist with the National White-Collar Crime Center (NW3C), summarized the situation by saying that "many within the law enforcement community are concerned about the frightening levels of technology that criminals have at their fingertips." (Cindy Williamson 2013). Because some virtual currencies can be freely exchanged without being traced and protect the parties' identity, they offer a real opportunity for money laundering activities. Cryptocurrencies open doors to a lot of possibilities for criminals, from storing illicit revenues in bitcoins, to buying other illegal goods on the Deep web – the hidden part of the internet that cannot be indexed by normal search engines such as Google. Although virtual currencies becoming a money of exchange on the Deep (dark) Web can be a bad thing, it is also an additional tool for experts to conduct future fraud investigations, giving them little more information about those transactions. Combined with technology, digital currency is the key for

analysts to monitor money-laundering by identifying unusual patterns within the transfer and flow of illegal money into the supply of legal money.

Perhaps one of the most self-explanatory examples of the use of cryptocurrency in online illegal transactions, it the case of Silk Road web platform. Silk road was an illegal marketplace, on the Dark web, for the buying and selling of the worst of humanity. It gave access to goods and services such as drugs, fire arms, fake ID documents, child pornographic content and even the hiring of assassins. Silk road made $1.2 billion revenues in its two years of existence, before being shut down on October the 2nd 2013 by the United States' authorities. Its creator Ross William Ulbricht was charged with Money laundering and narcotics trafficking and took maximum penalty for his crimes. U.S. authorities sent a strong message to anyone attempting to conduct illegal activities with cryptocurrencies, but also showed their interest in bitcoin as the decision was made to keep part of Ulbricht's revenues and sell in an auction the remaining. Since this event, the U.S. kept their strict and uncompromising line of law enforcement towards cryptocurrency-related illegal activities. Another example might be the one of *BitInstant*, the former bitcoin Exchange based in New York City. It provided a faster way to converter traditional funds into bitcoin. Charlie Shrem, the founder of BitInstant, was arrested because only one of his clients was using bitcoin for money laundering on the Deep. Despite Shrem's attention to how his customers were moving funds, he was judged as he may have been aware of the activities of Robert Faiella, the underlying subject. Charlie Shrem was eventually charged with alleged money laundering, and was sentenced in December 2015 to two years of prison.

Cryptocurrencies' exponential growth and promising returns have raised the question of their resemblance with Ponzi schemes. According to Investopedia, "a Ponzi scheme is a fraudulent investing scam promising high rates of return with little risk to investors. The Ponzi scheme generates returns for older investors by acquiring new investors". Whereas most of cryptocurrencies have proved not to be one since there is no central operator or pyramidal structure which will control the flows of money, OneCoin has been found to be a scam. It has adopted a scheme where investors become the perpetrators as well as victims, with scammed funds moving through a payment processor in Germany (Morris 2017). Many authorities, including the Indian and German one, are investigating on the case and have already seize a significant amount of OneCoin funds.

Nonetheless, the biggest concern among all entities and people remain the unpredictable fluctuations of prices cryptocurrencies are subject to, especially bitcoin. Though it is clear that the overall enthusiasm and controversy about this currency attracted many sorts of speculations, the future of bitcoin as an investment still remains shady.

II. THE RISK OF BITCOIN AS A FINANCIAL ASSET: A COMPARATIVE ANALYSIS WITH S&P500 CLASS ASSETS

Among all cryptocurrencies, the most advanced and well known by the general public is surely bitcoin. Whereas a few years ago, bitcoin was mentioned during work intervals at the office, it has now become a serious subject which is not to be dismissed and constantly analysed, especially in the financial sector. The pioneer of cryptocurrency nowadays attracts the attention of investment banks, venture capitalists and other investors, due to its unique characteristics. Mostly seen as an alternative investment opportunity, the enormous returns and instability of bitcoin made medias and financial peers call for a dangerous 'speculative asset' currently engaged in huge a bubble. But it is unclear whether bitcoin is able to behave and follow the pattern of a normal financial asset or if its unprecedented variations are linked to a new form of asset. This study will attempt to define what kind of asset is bitcoin by examining in the first instance its features as well as its functioning, and then confront the results of a comparative financial analysis of bitcoin against the S&P 500 index funds.

1. Defining Bitcoin as a financial asset

1.1 Liquid currency or investment opportunity?

Going back to the initial definition given by Satoshi Nakamoto, bitcoin was first introduced as a "Peer-to-Peer electronic cash system". Hybrid between fiat currency and commodity currency, bitcoin is independent of any government or monetary authority and does not have an intrinsic value. It appears that the primary purposes its creator seem to have intend in his paper introducing this innovative technology, was to invent a system of payment as well as medium of exchange that could compete with fiat money by sharing its features of liquidity and convenience to settle claims or payments. However, the exponential growth of bitcoin prices during the last two years made bankers and all kinds of investors to forget about its 'currency' side and focus the investment opportunity it represents. As previously stated, the amount of 'dormant' wallets, the ones not running frequent transactions in bitcoin once acquired, is significantly prevailing over the ones considered 'active'. This may suggest that people are trying to hold bitcoin as a store of value, expecting it to appreciate over time. Evidence shows that different uses of bitcoin are made according to the people using it. Hence it is worth categorizing users based on what are their approach toward this digital currency. A study from the SWIFT Institute ran several analyses in

order to address this issue (Dirk G. Baur 2015). The study categorized the types of users based on their lifetime activity up to the balance date, examining the 'sending of bitcoin' which refers to the transfer of bitcoin to another user (for fiat currency or goods/services) as well as the 'receiving of bitcoin' for transactions perceived from another user. Baur's paper identified four main categories: Active investors, Passive investors, Currency users, Testers, Miners and Hybrid users, all of which are classified according to the following table:

Total Balances (millions)												
Balance Year End	2011				2012				2013			
User Types	Bitcoin	USD Value	% Share	No. Of Users	Bitcoin	USD Value	% Share	No. Of Users	Bitcoin	USD Value	% Share	No. Of Users
Active Investor	0.29	1.38	3.64	18,940	0.28	3.73	2.62	82,621	0.52	376.11	4.27	1,035,596
Passive Investor	1.66	7.84	20.63	32,996	2.46	32.96	23.16	86,304	3.64	2,630.26	29.86	319,988
Hybrid	2.78	13.11	34.49	425,347	4.39	58.82	41.34	1,529,848	5.43	3,928.32	44.59	4,044,719
Currency User	0.41	1.94	5.10	31,780	0.74	9.89	6.95	116,986	0.27	198.19	2.25	464,397
Miner	2.76	13.02	34.23	93,304	2.58	34.58	24.30	119,010	2.17	1,568.60	17.81	135,187
Tester	0.15	0.73	1.91	118,338	0.17	2.31	1.63	256,072	0.15	107.65	1.22	722,451
Total	8.05	38.02	100	720,705	10.62	142.29	100	2,190,841	12.18	8,809.13	100	6,722,338

This other table reports the wallets' characteristics of the various users' types according to transaction data from the Bitcoin public ledger. Panel A displays individuals' bitcoin balances, Panel B their number of bitcoin trades and Panel C the different transaction sizes.

Panel A. Bitcoin Balances in USD of User Types

	2011			2012			2013		
User Type	Mean	Std	N Users	Mean	Std	N Users	Mean	Std	N Users
Active Investor	71.15	5,649.96	20,217	45.09	2,799.94	84,375	374.54	40,849.14	1,039,517
Receive Only Investor	225.34	4,673.96	39,784	377.30	9,324.76	93,843	8,073.60	370,268.33	329,730
Hybrid	32.99	1,875.10	469,466	40.23	2,229.50	1596,202	998.02	72,828.99	4,118,031
Currency User	77.22	1,074.72	34,560	97.56	3,115.00	121,494	473.23	58,460.70	473,089
Tester	60.42	114.41	156,678	91.62	249.88	294,927	1,868.71	8,608.79	761,971

Panel B. Number of Bitcoin Trades by User Types

	2011			2012			2013		
User Type	Mean	Std	N Users	Mean	Std	N Users	Mean	Std	N Users
Active Investor	3.90	39.08	20,217	2.98	6.61	84,375	3.29	18.91	1,039,517
Receive Only Investor	10.07	30.45	39,784	12.98	57.60	93,843	11.12	39.79	329,730
Hybrid	3.27	70.70	469,466	7.03	2,941.21	1,596,202	9.38	4,593.90	4,118,031
Currency User	38.55	112.83	34,560	68.41	557.22	121,494	43.27	387.85	473,089
Tester	1.00	0.00	156,678	1.00	0.00	294,927	1.00	0.00	761,971

Panel C. Transaction Size by User Types

	2011			2012			2013		
User Type	Mean	Std	N Users	Mean	Std	N Users	Mean	Std	N Users
Active Investor	16,202.06	10,4261.97	20,217	8,741.47	54,424.90	84,375	18,120.06	156,325.10	1,039,517
Receive Only Investor	97.97	3,303.67	39,784	53.21	993.54	93,843	759.31	36,687.30	329,730
Hybrid	232.36	1,885.73	469,466	242.47	1,197.28	159,6202	672.33	33,865.47	4,118,031
Currency User	60.01	149.68	34,560	78.20	174.53	121,494	130.14	388.84	473,089
Tester	4.02	24.80	156,678	3.53	16.56	29,4927	7.55	38.87	761,971

[15]

[15] Baur, Dirk G. and Hong, Kihoon and Lee, Adrian D., Bitcoin: Medium of Exchange or Speculative Assets?

The data shows that more than a third of bitcoin in circulation during this period was held by the *investor* category of users, closely followed by the one of *passive investors* which receive bitcoins but never send them to others. In addition, few users are observed using bitcoins in recurrent transactions, most certainly because of its limited acceptance in our global economy. This issue was recently addressed by bitcoin's healthiest investor, which decided in July 2017 to proceed to Fork in the Blockchain due to the delay in transactions causing poor liquidity conditions. The decision was made to create a new currency, bitcoin cash (BCH), alleged to the original one, in order to have one dedicated to liquid and fast transactions and the other more to keep holding its store of value function. the All these elements bring us to conclude that bitcoins are being used more as an investment than as a medium of exchange.

1.2 A complex currency with basic factors of variations

The price fluctuations in the bitcoin spot rate observed on bitcoin Exchanges are driven by many factors. When it comes to Satoshi Nakamoto's currency, the term price is not to be mistaken with the term value. The former is the monetary cost of a bitcoin, whereas the latter is associated with bitcoin's perceived benefits and usefulness by its users. For now, bitcoin prices are expressed as an exchange rate in terms of another currency. The one we will employ is the bitcoin-to-dollar one, which is written as BTC/USD. Before going into the reasons of this currency's volatility, it is important to understand what is the basis of its variations. Taking bitcoin as a class asset, many scholars claim some similarities with Gold. In fact, both are known to be finite resources, as by design, there are 21 million bitcoin that will be created according to its underlying algorithmic release function. Currently, there are already more than 16.5 million bitcoins in circulation (Data from Blockchain.info on the 30/09/17). Therefore, bitcoin works under the concept of scarcity: the more people are buying it, the less of the resource is available, it becomes rare, the more its value and hence its price will rise. Of course, new bitcoins will always be issued through mining activity, but the proportion is so small it is insignificant.

The increasing demand linked with the decelerating of the 'coinbase' explain why the price of bitcoin has gone up in an exponential manner. Most of well informed investors adopt a long-term strategy with this regard, expecting bitcoin price to gradually increase over time. However, fix supply and scarcity may not be enough to reduce bitcoin's variations to such a simplistic model. It is true that bitcoin will not be affected by interest rates, government action plans or even the price of oil, unlike other assets and currencies. But history have shown correlation between bitcoin's prices and events related directly or indirectly to it. Whether it is Microsoft accepting bitcoins in 2014, Donald Trump's election in 2016, or the SEC denying bitcoin ETF applications

in 2017, they all resulted in a change in the behaviour of bitcoin users regarding the buying or selling, thus its wide changes in price (Figure 1, Appendix).

The reasons of bitcoin's volatility are still difficult to measure as, unlike in traditional markets, there is not a general accepted volatility index such the Chicago Board Options Exchange (CBOE). This might be due to the young stage of bitcoin which, however, has shown incredible volatility in relatively short periods of time. In his article about bitcoin's volatility, Jonathan Todd Barker attempted to give the following elements of answer regarding this issue (Barker 2017). He obviously highlighted the geopolitical events and statements that affected bitcoin's rate of adoption. But he also advertised the fact that the variance of bitcoin's perceived store of value compared to fiat currencies and decisions of large holders, have both a significant effect on bitcoin's price. In addition to regulation and tax treatment, its increasing acceptance as a method for Foreign Direct Investments (FDI) in countries with high inflation as well as the higher returns it may offer compared to local debt instruments, result in faster and higher adoption rate.

1.3 Characteristics of a financial asset: a comparison with Bitcoin

The nature of bitcoin fluctuations seems to be closely linked with the investors behaviours. They seem, indeed, to have made of bitcoin a new financial tool on which to speculate in order to get higher returns. But investors treating bitcoin as a normal financial asset does not necessarily determines it as such. We will address the differences and similarities bitcoin has with a financial asset by taking, step by step, a descriptive list of financial assets characteristics and compare them with bitcoin (What are the characteristics of financial assets? 2015).

- Moneyness & liquidity

Financial assets are related to money, due to the relative ease with which they can be converted into cash. As the perceived benefits from holding an asset are really perceived when their transformed in cash, this conversion needs to be done within a specific time and determinable value. Some financial assets are defined as not liquid because the process of converting them into cash takes too long. Some others are regarded as near-money because they are highly liquid in terms of the ease with which they can be traded for cash. On this point, bitcoin perfectly match since it is always readily convertible into cash at any given time and even does it faster than normal assets, making it in a sense more liquid than Treasury bills for example.

Bitcoin's moneyess differs from classic assets as it does not incur transaction cost which most of the time decrease the face value of a financial asset.

- Divisibility & denomination

The denomination of financial assets depends on the face value decided by corporate organizations and institutions which are willing to raise funds. This face value is usually denominated in government currency. In the case of bitcoin, denomination depends on the currency employed in its trade with fiat currency, the most common one being BTC/USD.
The term divisibility represents for both bitcoin and financial assets, the minimum amount of money an asset can be bought or liquidated. The only difference being that one bitcoin is divisible down to 8 decimal places, making its supposedly constant supply significantly larger.

- Reversibility

Financial asset's reversibility consists in minimizing the risk and costs of assets not readily convertible into cash. One example may be a tight 'bid-ask' spread. Several market agents, such as Brokers, exists to ensure the well-functioning of markets and flows of money. With bitcoin, these costs are much lower since there is no need for a middle man. Transactions are carried out instantly, Peer-to-Peer, through electronic channels and recorded on the Blockchain. The insignificant cost associated with the moving of funds is the mining fee, taken by the users of the network who approve the transaction and ensure the viability of the network. The variability of the price of a financial asset states that the fluctuations of a financial asset reflect the probability of market maker possible gains or loose in the bargain. The concept is that higher variability in Exchanges is associated with more uncertainty. This is especially true in the case of bitcoin which can see its prices go up or down by 20% in just a few days. For both kind of assets, the thickness of the market is defined by the frequency and volume of transactions.

- Cash Flow & Maturity

Designates the coupon payments that an investor will receive from holding a financial asset. This cash distribution is mostly expressed in terms of dividends on shares or coupon yields. They are the frequent source of return (usually annual) for the holder of an asset, in addition to the price at which he or she could sell it. Financial assets also have a certain maturity period that consists in the final payment date of a financial instrument. Here bitcoin differs completely as it has no maturity or intermediate payments. The unique Cash Flow which is perceived is the price at which

a certain amount of bitcoin is sold, in exchange for fiat money or another cryptocurrency. Cash Flows are seen as an obligation from the company, which may not be able to pay-out in the case of bankruptcy. Bankruptcy status does not exist in bitcoin since there is no institution owning it. This can be dramatic for investors that are facing the risk of losing all without being backed-up. The absence of Cash Flow from holding bitcoin might be the biggest difference with financial assets.

- Convertibility

This characteristic refers to the ability of financial asset to converted into another class of asset which will still be used by the underlying institution to raise funds for its activities. Since bitcoin does not run any Initial Coin Offering (ICO) we cannot say that investing in this particular digital currency is helping to finance corporate operations. However, many wallet providers, Exchanges and online platforms allow the conversion of bitcoin into other cryptocurrencies which have their own interest rates. Indeed, bitcoin is the primary medium of exchange for other virtual currencies, before bank transfer and fiat currency.

- Predictable returns

The prediction of returns can be more or less accurate depending on the riskiness of the underlying asset. Nevertheless, investors are most of the time well-aware of the percentage of interests that are attached to certain financial assets before staking their funds on them. For example, the returns of shares are mostly determinable and available as information for investors. Other financial assets such as government securities (T-Bills) have basically predetermined and certain returns, as government cannot default. For less predictable asset's returns some ratios and tools exists to give close estimates. On the contrary, predictable returns absolutely do not exist in bitcoin. As previously explained, the over-enthusiasm over the digital asset and its high responsiveness to external events resulting in unexpected behaviour from its investors, make unpredictable its prices so as its expected returns. With bitcoin, ratios and formulas may not be enough for predictions. Analysts should rather focus in attempting to predict the behaviour of bitcoin's investors. According to a recent IMF report, bitcoin prices have been extremely volatile over the past several years and more volatile than any other key currencies and assets (See figure 2, Appendix).
Last but not least, financial assets' returns are subject to tax status as they are taxable earnings, whereas there is not legislation which has been enforced to this regard for bitcoins, yet.

2. A quantitative analysis

2.1 S&P500 as an investing reference

The S&P 500 index fund is one of the most well-known stock index in the world. It is perhaps the most common index for the US stock and is seen as a worldwide leading indicator of equities and of the performance of the large market capitalization as it comprises the leading industries of the US economy. The 'large cap' companies the S&P 500 considers are companies with over 10 billion dollars of market capitalization (Investopedia.com). Stocks from these companies are chosen based on their market size and/or outstanding liquidity. S&P 500 stocks are characterised by the ease with which they can be bought, sold and converted into cash, without affecting its market price. The index also reflects the risk and returns associated with those companies.

S&P 500 was chosen as an element of comparison for the study as it is recognized as a market indicator. It also has some common features with bitcoin, such as the aim for liquidity, that makes it an interesting reference.

This study will not attempt to define which of bitcoin or S&P 500 is a better investment opportunity, but rather compare the behaviour and variation of these two distinct assets.

2.2 What historical values tell us

Taking a line chart of prices and returns of both BTC/USD and S&P500 assets in percentages, over a 3 years' time period, we will examine and compare their respective evolutions.

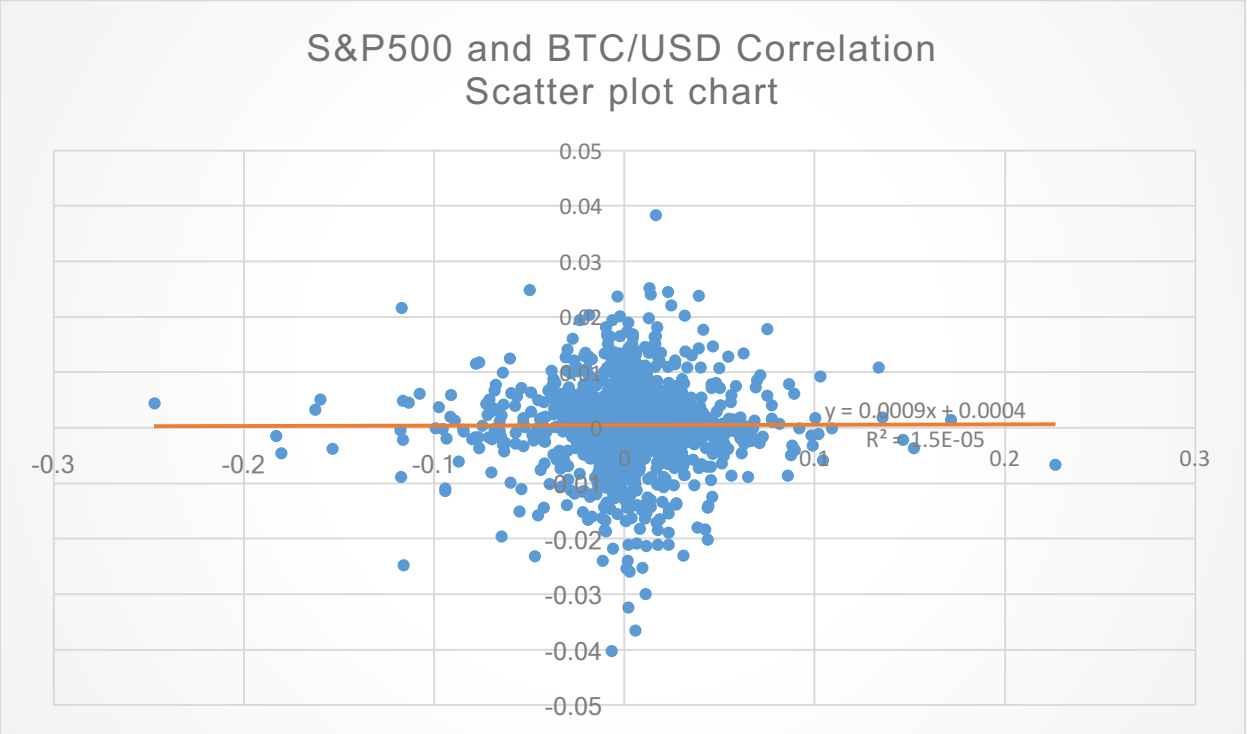
On the joint graph which illustrates data from finance.yahoo.com, we can observe that S&P 500 returns stood around 20.04% since 2015. Its stock returns have grown at a slow but constant rate, following almost a linear pattern. In logarithmic terms, its prices have arisen from $1,839.024 to $2,517.2 during this time interval. In 2016 S&P 500 return was 12.25%. Overall, it appears that S&P 500's stock performed quite well.

On the other hand, bitcoin's pattern of growth is radically different. Over the same time period, bitcoin's price, and hence return, have increased by 1,687.95%. In logarithmic term, from the 9th of February 2015 where the value of a bitcoin was $235, it has skyrocket up to date where a bitcoin is worth $4,201.68. Besides the huge difference in returns these two class assets have offered, what in striking is the deepness of bitcoin's price fluctuations. Just in 2017, BTC/USD have surged by more than four times its value, bypassing S&P 500's index price. By taking a closer look, we acknowledge the fact that bitcoin's percentage of growth was fluctuating very close to the one of S&P500 stocks until October 2015. After that, the digital asset accelerated its percentage growth but following a strict and steady line. It reached 235.47% in December 2016, which was already huge considering the 20% of S&P 500. Bitcoin price rises and so had its value, which is said to have appreciated, with respect to the US Dollar in this case. From a currency point of view, this means that bitcoin can purchase more goods and services than before. Form an asset perspective, this means that the price at which a holder can sell bitcoin for fiat currency or another cryptocurrency rises and so does his expected return. But from January 2017 on, bitcoin percentage return started taking a whole other path with much wider fluctuations. Indeed, its expansion may be associated with that of a *boom*. Huge returns were also followed by big losses, which makes many investing specialist speak about a bubble. In just a month, from June to July 2017, bitcoin price depressed from nearly $3,000 to $1,908. Then it has subsequently surged back to today's level of above $4,000. (See figure 3, Appendix).

2.3 Analysis' results summary

Historical data from S&P500 index and Bitcoin-to-USdollar was taken respectively from finance.yahoo.com and coindesk.com. The time frame chosen is 5 years, from October the 1st 2012 to September the 29th 2017, as it is at this point that bitcoin started to register significant activity. Simple individual and cross analysis of the two asset types was made in order to bring further elements of comparison. The following numbers displayed are the result of statistics and regression, carried out on Excel sheets.

Obs: 1258	S&P 500		BTC/USD
Mean price	$1,976.81		$805.07
Max. Price	$2519.36		$4950.72
Min. Price	$1353.33		$10.17
Average daily Return	0.04%		0.17%
Variance	5.88434E-05		0.001204709
Standard deviation	0.77%		3.47%
Beta	1		0.0008
Autocorrelation	-1.4%		-0.6%
Covariance		1.04001E-06	
Correlation coeff.		0.39	



2.4 Observations and Interpretations

Before looking at the data, it is important to acknowledge some institutional differences between the US stock market and bitcoin exchange. The S&P 500 being used as a reference for the market, it functions under specific rules of the US marketplace. For example, trading times in S&P 500 are divided in two periods during the day, the *pit* and the *globex* hours. Both follow a very strict plan of opening and closing hours, excluding (or not) non-holiday weekends. This is the first distinction that strikes when managing the data, as bitcoin is, on the other side, completely decentralized and its exchanges work continuously, 24 hours a day and 7 days a week.
Bitcoin also admits all investors independently of the weight of their purse, whereas S&P 500 requires a minimal capital to invest in the 'safest and best performing stocks'. Eventually, bitcoin trading happens most of the time without 3rd parties and buying and selling activities can be carried out at any time and by anyone.

Several information ca be drawn from the above numbers. Starting with the average price of these assets, we can observe that S&P 500's mean price accounts for more than the double of bitcoin's average price. This reflects the nascent nature of bitcoin which surged lately and too fast. Even if the by choosing a smaller time interval, this average could have been much higher, the data period was chosen on purpose of a certain length in order to have a better understanding of bitcoin historical prices and trends. Bitcoin is in a too early stage to have found its balance yet. On the other hand, S&P 500 index seems to represent a lot sounder investment than bitcoin, especially when looking at the difference between the maximum and minimum close prices. Again, US stocks appear to maintain a reasonable interval throughout this period, but bitcoin out bounds them both in terms of minimum and maximum price. The spread between $4950.72 and $10.17 is worse than one would expect. It might suggest that bitcoin is subject to non-negligible fluctuations in its price and hence make future revenues even more uncertain for investors which could make 20% in a day and lose 30% on the following one.
Overall, a fair point for bitcoin as a digital asset is its average daily return of 0.17% compared to the 0.04% for S&P500. However, this value to be replaced in context. Bitcoin exponential price expansion was concentrated only in the last two years and its pattern of growth has been extremely irregular. Therefore, this value should not be taken as granted when it comes to returns.
It is because risk and returns is all that matters for investors, it is worth examining the standard deviation of the two assets, which can be a good measure of volatility as it indicates the level of dispersion of future returns. The higher is the standard deviation, the more risk is associated with the stock since realized returns can be very different from expected ones. In this case indeed, the

standard deviation of bitcoin (3.47%) was found to be significantly higher compared to that of S&P 500 index funds (0.77%).

The Beta is also an alternative way of estimating the potential volatility of a financial asset. Mostly used in the Capital Asset Pricing Model (CAPM) to estimate the systematic risk, meaning the market risk, the Beta tells the investor how a stock reacts to changes in the market portfolio. In this case it is interesting analysing the bitcoin's beta against the one of the S&P 500 index, as the latter is equal to 1 by definition since the index is used as a proxy for the market. Bitcoin's 0.0008 beta is the results of two different methods of analysis which ended by confirming this value. After having calculated the periodical daily returns (Rbtc and Rs&p), the variance and covariance of the two assets, the normal Beta formula was used in order to calculated the one of BTC/USD:

$$\beta = \frac{Cov(Rbtc, Rs\&p)}{Var(Rs\&p)}$$

The second method employed to calculate the Beta of BTC/USD returns, was to run a regression on Excel, taking bitcoin's historical returns as the dependent variable and the S&P500 funds' returns as the independent variable (the Beta result is shown in the orange rectangle):

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0.003967917
R Square	1.57444E-05
Adjusted R Square	-0.000781056
Standard Error	0.007673987
Observations	1257

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	1.16364E-06	1.16364E-06	0.019759493	0.888233421
Residual	1255	0.073907045	5.88901E-05		
Total	1256	0.073908208			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	0.000441948	0.000216707	2.039379381	0.041621288	1.67998E-05	0.000867096	1.67998E-05	0.000867096
X Variable 1	0.000876965	0.0062387	0.140568462	0.888233421	-0.011362467	0.013116396	-0.011362467	0.013116396

The reason why the analysis was made twice, is that such neutral Beta (basically 0) is unusual for what should be considered as a financial asset. It indicates that bitcoin price changes are absolutely unrelated to any swings or variation in the market's stocks. This classifies once more, bitcoin as a unique type of asset which follows trends and rules outside of the financial sector.

In order to have a comprehensive analysis, it was also important to estimate and compare the Autocorrelation coefficients of bitcoin's and S&P 500 stocks' historical returns. Calculations accounting for the 1258 observations gave a -1.4% Autocorrelation coefficient for the S&P 500 index and a -0.6% one for BTC/USD. Although both coefficient came out as negative and small, signifying very little correlation between historical returns and future ones, bitcoin's one is certainly closer to 0% than the US stock market. The negative component advertises for decreasing future returns when the present ones are rising, but again, the coefficients are too small to make such statement. Instead, what can be deducted is that, based on historical values, bitcoin's returns are less predictable than S&P 500 ones. Moreover, addressing the issue of bitcoin's recent exponential growth compared to its previous period of stagnation, the same autocorrelation coefficient was calculated on a one year basis, from 2016 to 2017. Last year was bitcoin's breaking record growth and its autocorrelation coefficient was -4% as an element of comparison. This suggests that bitcoin is currently facing increasing volatility, with bubble alike expansions that are usually followed by unexpected drops.

Finally, the correlation coefficient shows little or no interaction between the two asset classes. Although 0.39% is still a positive correlation, it is too small to assess that bitcoin and S&P 500 move in relation to each other. The above Scatter plot shows a very concentrated data which doesn't seem to adopt a trend. Because the correlation coefficient is close to 0, it is said that the two assets have weak form of correlation. The trend line attempting to show a kind of correlation is flatter than anything else. This justifies the miscellaneous scatter plot that came out of the analysis. These elements have shown us how big returns do not necessarily imply the presence of a good investment opportunity. Bitcoin remains a technology in its early stage and it is imperative that it achieves to stabilized in order to be considered as a real asset. The riskiness of its returns may only bring further speculation and short-term positioning from investors. Perhaps the huge capital inflows as well as the exaggerated amount of trade and speculation bitcoin has been subject to, made this cryptocurrency move away from its original function of currency and purpose of a "Peer-to-Peer electronic cash system". One thing is for sure, people are not making the best out of bitcoin, yet.

III. CONCLUSIONS

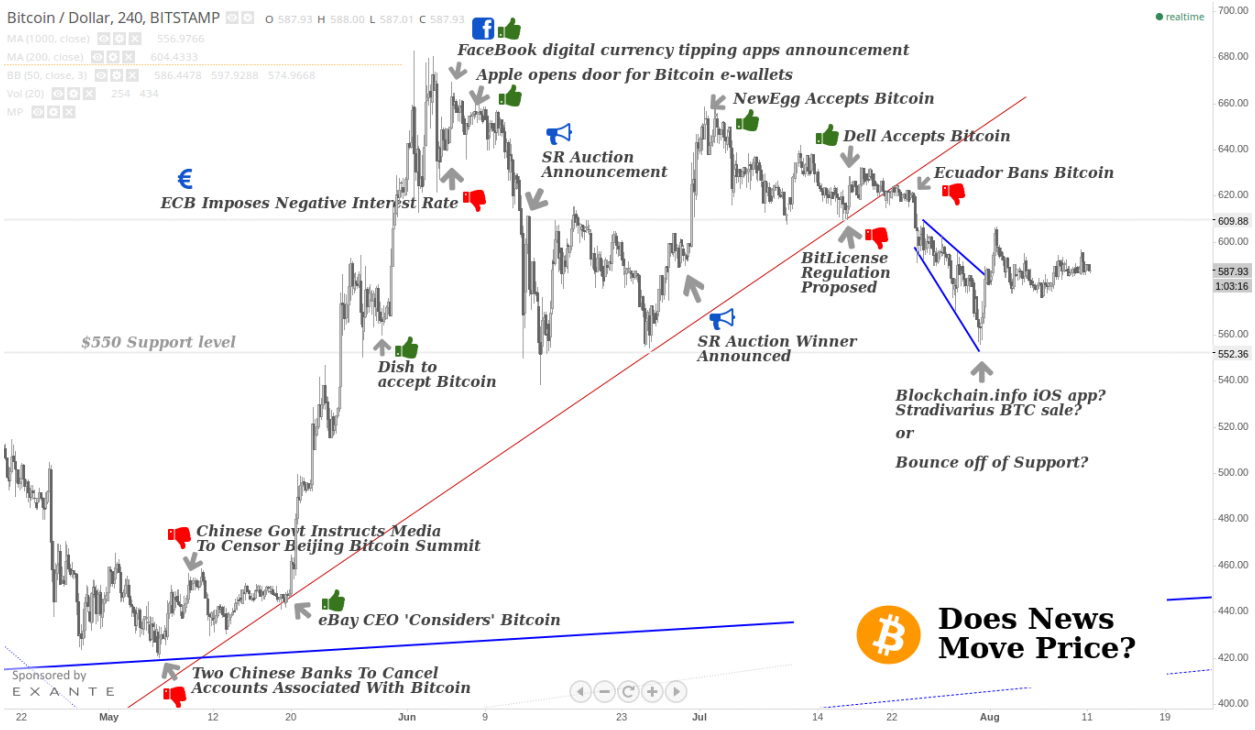
Innovation is a historical process. Cryptocurrency is certainly one of the biggest invention of the 21st century. One which led us to rethink the way we conduct exchanges, that gives an extension to what money really is and questions our most well-established entities and systems on which we relied upon until now. Cryptocurrency not only offers an alternative when it comes to intermediation, ownership and trust, but it also opens a whole new world of opportunities with ever more technological progress. Digital currencies are complex virtual schemes that for the first time allow for the creation and transfer of virtual value, based on algorithms and mathematic functions instead of relying on human services. This redefines models of trust in a globalized world which will only keep expanding its boundaries. Cryptocurrencies are also inclusive, since they have the potential to make the worldwide population of unbanked, enter an efficient and decentralized financial system. It is an opportunity for the population of emerging countries to carry out what seem to us normal payment and exchange activities, without suffering the consequences of ineffective decisions from governments and financial institutions, or unattainable transaction costs. The rising adoption of cryptocurrencies attracts many investors and entrepreneurs who are eager to start new businesses based on the underlying distributed ledger: the Blockchain protocol. The Blockchain technology market is expected to be worth $7.74 Billion by 2024. Payment acceptance of bitcoin is expanding everywhere in the world, both in physical and online locations. Government and Financial institutions fell threatened and are concerned about the fraudulent uses of cryptocurrency. The anonymity and very restricted control they have upon these currencies, which in addition are created on a quasi-daily basis, raise authorities' concerns about the role it may play in terrorist attacks, tax evasion, drug dealing and in the underground economy. Even if an increasing amount of regulations are emerging, some of the regulatory institutions are willing to work in hand with this technology in order to integrate it at its best in our society. Regulatory responses should adapt to the rapidly changing landscape of virtual currencies. The long-term position of regulation regarding digital currency will focus on the financial soundness of virtual intermediaries, such as exchanges, wallet and coin providers, as well as developing standards and best practices. Although born as an alternative medium of exchange and payment, cryptocurrencies such as bitcoin and ethereum are currently being used for investment purposes. The basic factors of variation of bitcoin, which are similar to the ones of Gold, attracted many investors also from the banking sector to speculate on the rollercoaster alike volatility of bitcoin.

Even though bitcoin does share some common features with S&P 500's financial assets, it still has some significant differences which makes it more of a unique digital asset. Its extreme liquidity and moneyness are not being used to their full potential, as counter balanced by unpredictable fluctuations which make it not a good store of value. Exchanges of bitcoin do work as normal stock exchanges, organized as direct decentralized platforms with efficient price discovery, and without any kind of intermediation. Transactions are approved and made irrefutable by miners, once encrypted on the blockchain, which ensure the continuous viability of the network and its interactions. Unlike traditional financial assets, Bitcoins do not offer a revenue stream of cash flow, the only revenue perceived is when selling it in exchange of fiat currency or other cryptocurrencies. Additional classical elements of financial instruments, such as maturity, do not apply to bitcoins. However, bitcoin offers unprecedented divisibility, has a predetermined denomination, good rate of reversibility and convertibility, just as financial assets.
Evidence from quantitative analysis and regression show, that bitcoin undergoes significantly higher and wider fluctuation than US model stocks, but incredible returns possibilities. It is still unclear if bitcoin is in a bubble, as the different patterns of growth and nature of investment do not seem to reflect any of what we know so far. Bitcoin's biggest risk appears to come from its own volatility and not from the market one, to which it is completely uncorrelated.

Overall, bitcoin may be an acceptable investment depending on individuals risk aversion. But new trading mechanisms and estimates will have to be introduced in order to better understand this digital asset class. Due to the early stage of this technology, we do not seize the exact potential of such currency, but we know it will definitely fit into our globalized world. Only the time will tell us how this exiting digital currency, asset, technology or simply revolution is going to be accepted and integrated in our modern society.

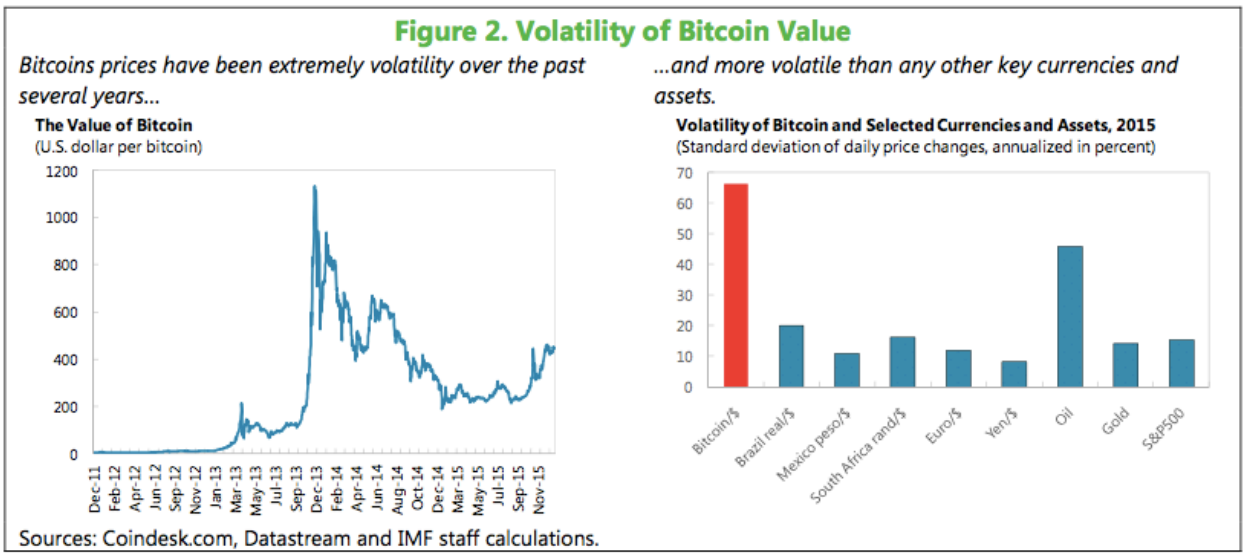
IV. APPENDIX

- Figure 1: Historical news linked with bitcoin's price fluctuations



Source: https://www.cryptocoinsnews.com/affects-bitcoin-price/

- Figure 2:



(Virtual Currencies and Beyond: Initial Considerations 2016)

- Figure 3: Average USD market price across major bitcoin exchanges.

Source: blockchain.info (Accessed on the 30/09/17)

- Figure 4: S&P 500 index funds' result analysis summary

GSPC	Periodical daily returns	lag1	Mean closing price	Variance	SD	Autocorrelation	Average daily return
	0.09%		1,976.81	5.88E-05	0.77%	-1.4%	0.04%
	0.36%	0.09%			Beta		
	0.71%	0.36%			0.017674193		
	-0.03%	0.71%					
	-0.35%	-0.03%	Min	Max		Correlation	Covariance
	-0.99%	-0.35%	1353.33	2519.36		0.39%	1.04E-06

...

- Figure 5: Bitcoin-to-USdollar result analysis summary

BTC/USD	Periodical daily returns	lag1	Mean closing price	Variance	SD	Autocorrelation	Average daily return
	-1.77%		805.07	0.001204709	3.47%		0.17%
	0.51%	-1.77%			Beta	-0.60%	
	2.70%	0.51%			0.000863287		
	-8.47%	2.70%				-4%	in 1 year period
	-0.76%	-8.47%	Min	Max			Random walk.
...	-5.98%	-0.76%	10.17	4950.72			

V. SITOGRAPHY

- Cryptocurrencies' instant prices: https://www.cryptocompare.com
- http://www.marketwatch.com
- Bitcoin charts: https://bitcoincharts.com/charts/mtgoxUSD#rg730zm1g10zm2g25zv
- Altcoins: http://altcoins.com
- Additional charts: https://blockchain.info
- Blockchain solutions: https://blockchainfrance.net
- Definitions: https://blockgeeks.com | http://www.investopedia.com
- Bitcoin price chart with historic events: https://99bitcoins.com/price-chart-history/
- Statistics: https://coin.dance/stats#bitcoinChart
- https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/
- Data: https://finance.yahoo.com/quote/%5EGSPC/history?p=%5EGSPC
- Characteristics of financial assets: http://bankersoftomorrow.blogspot.fr/2015/06/what-are-characteristics-of-financial.html

VI. BIBLIOGRAPHY

2000/46/EC, Directive. n.d. *ELECTRONIC MONEY DIRECTIVE, DIRECTIVE 2000/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Directive 2000/46/EC, EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION.

4AMLD, European Commission -. 2016. *DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC.* EU Directive, Strasbourg: European commission.

Barker, Jonathan Todd. 2017. "Why is Bitcoin's value so volatile ." *Investopedia.* 16 May. Accessed September 29, 2017. http://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp.

2016. *Banking on Bitcoin.* Directed by Christofer Cannucciari. Performed by Banking on Bitcoin.

BlockchainFrance. 2016. *La Blockchain décryptée, les clefs d'une révolution.* Paris: netexplo.

Castor, Amy. 2017. "A (short) Guide to Blockchain Consensus Protocols." *Coindesk.* 4 March. Accessed September 24, 2017. https://www.coindesk.com/short-guide-blockchain-consensus-protocols/.

Cindy Williamson, Jason Vazquez, Katherine Sagona-Stophel, Thomson Reuters. 2013. *Technology in the fight against money laundering in the new digital currency age.* White Paper, Toronto: Thomson Reuters.

Delahaye, Jean-Paul. 2016. "Les monnaies cryptographiques et les systèmes à Blockchain." *http://inference-review.com/article/les-monnaies-cryptographiques-et-les-systemes-a-blockchain* 3-5.

Dirk G. Baur, KiHoon Hong, Adrian D. Lee. 2015. *Bitcoin: Medium of Exchange or Speculative Assets?* Paper, UWA Business School, Hongik University College of Business, University of Technology Sydney, Hambourg: SWIFT Institute.

Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes. 2016. *Virtual Currencies and Beyond: Initial Considerations.* Staff Discussion Note, IMF.

ECB. 2015. *Virtual currency schemes - a further analysis.* Report, Frankfurt: ECB.

ECB, European Central Bank. 2012. *Virtual currency schemes.* Report, Frankfurt: ECB.

Eha, Brian Patrick. 2017. "Can Bitcoin's First Felon Help Make Cryptocurrency a Trillion-Dollar Market?" *Fortune.*

Mining, BTC. 2013. *Bitcoinmining.com.* 5th January. Accessed september 2nd, 2017. https://www.bitcoinmining.com.

Morris, David Z. 2017. "The Rise of Cryptocurrency Ponzi Schemes." *The Atlantic* 1.

Mougayar, William. 2016. *The Theory of a Blockchain Circular Economy and the Future of Work.* 02 January. Accessed September 24, 2017. http://startupmanagement.org/2016/08/02/the-theory-of-a-blockchain-circular-economy-and-the-future-of-work/.

Nakamoto, Satoshi. 2009. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Paper, /: https://bitcoin.org/bitcoin.pdf.

Nicola Cetorelli, Benjamin H. Mandel, and Lindsay Mollineaux. n.d. *The evolution of Banks and Financial intermediation.* Research paper, New York: Newyorkfed.org.

Pares, Pascal. 2016. *An introduction to the Bitcoin system.* 02 april. Accessed September 20, 2017. https://pascalpares.gitbooks.io/implementation-of-the-bitcoin-system/content/1-transaction-2-hash.html.

Paul Vigna, Michael J.Casey. 2015. *The age of crypto currency.* Picador.

Rauchs, Dr Garrick Hileman & Michel. 2017. *Global Cryptocurrency Benchmarking Study.* Study, Cambridge: University of Cambridge, 50.

Yusuf, Malik Abolaji. 2015. "What are the characteristics of financial assets?" *Bankers of tomorrow.* Wednesday June. Accessed September 28, 2017. http://bankersoftomorrow.blogspot.fr/2015/06/what-are-characteristics-of-financial.html.