ISCTE Business School
Instituto Universitário de Lisboa

BITCOIN: AN ASSET OR A CURRENCY?

Francisco Santos Ferreira

Dissertation submited as partial requirement for the conferral of

Master in Management

Supervisor:

Prof. Pedro Manuel de Sousa Leite Inácio, Prof. Auxiliar, ISCTE Business School, Departamento Finanças

June 2018

Abstract

The aim of this thesis is to explore whether digital currencies such as Bitcoin can be perceived as a currency or an asset. It begins by describing different types of currencies. Functions of money are also defined, providing a comparison between bitcoin and fiat currencies. Moreover, the concept and functions of bitcoin are developed, as well as other innovations that are linked to the bitcoin software, such as blockchain and its importance for several industries in the future. Bitcoin challenges and complications are also going to be discussed. Network security, criminal activities and the importance of regulating digital currencies are the major topics regarding bitcoin challenges.
A significant part of the criticism surrounding bitcoin is due to its slow transaction processing and its volatility when comparing to fiat currencies, as well as other cryptocurrencies that may become future competitors of fiat currencies.
Due to the major challenges that were developed, bitcoin cannot be considered as a currency yet: however it fits between commodity and fiat money, which is called synthetic commodity money. As it is explained throughout this thesis bitcoin represents a unique asset class, which is able to change the way people make transactions.

Keywords: bitcoin, blockchain, synthetic commodity, cryptocurrency

JEL Classification: E42, G12

Resumo

O objetivo desta tese é compreender se as moedas digitais, tais como a Bitcoin, podem ser consideradas como uma moeda efetivamente ou meramente como um ativo. Durante este trabalho são descritos vários tipos de moeda. As funções do dinheiro são também definidas, podendo desta forma fazer uma comparação entre a bitcoin e as moedas emitidas pelos governos. O conceito e as funções da bitcoin são desenvolvidos, tal como as inovações que estão intimamente ligadas ao software desta criptomoeda. A blockchain e a sua importância nas variadas indústrias no futuro são analisadas. Os maiores desafios, bem como as complicações adjacentes à adopção desta nova forma de transaccionar bens e/ou serviços, tais como, a segurança da rede, as atividades criminais, bem como lavagem de dinheiro como os maiores problemas que a bitcoin enfrenta são alvo de escrútinio.

A maior parte dos críticos da bitcoin apontam a volatilidade e o lento processo de confirmação de transacções como os maiores problemas desta moeda digital face às moedas emitidas pelo governo.

A bitcoin ainda não poderá ser considerada como uma moeda, contudo as suas características atribuem-lhe um carácter novo, podendo ser definida como um novo grupo de ativos financeiros, chamdado de synthetic commodity money. A bitcoin representa precisamente esta inovação que permite aos consumidores alterarem por completo a forma de efetuarem transacções.

Executive Summary

Since bitcoin appeared it has evolved from a crypto-mathematical concept into an expanding economy, being adopted by millions of people and thousands of businesses worldwide. Nevertheless the huge adoptance worldwide, its classification is a major concern regarding the community.

Cryptocurrencies, such as bitcoin, use cryptography as the main source of security. Although cryptocurrencies are able to function as a medium of exchange, volatility and unpredictability of its prices forbid digital currencies to act as medium of exchange, storage of value and as a unit of account at the same time. Therefore, they do not fulfill the three functions of money.

Bitcoin is a peer-to-peer electronic cash system that differs from all the current systems due to its decentralisation: it does not rely on a third-party. Every single participant in the payment network is responsible for verifying the legitmacy of digital transactions by splitting the authority among them. Transactions are confirmed by all nodes in the network and recorded in a public ledger called blockchain. Thus, since every participant can, in principle, confirm transactions it leaves the system vulnerable to potential attacks or frauds. In order to prevent those attacks, only nodes who invest computers´processing power are able to confirm transactions by solving a cryptographic mathematical problem which solution is known as proof-of-work. This process of solving such mathematical problems is called mining and those who perform it are known as miners. Through mining new bitcoins are being generated and entering the market. Blockchain is perceived as one of the most important technological advancements in the past few years. Firstly, it was strictly used to operate cryptocurrencies however, its tremendous potential provided many other applications such as smart contracts implementation, data security or even in fields like IoT.

Bitcoin works as an asset and a currency at the same time. Besides being able to work as a medium of exchange, bitcoin lacks regulation, its still too volatile and its prices unpredictable to be considered a currency. As bitcoin falls somewhere between commodity money and fiat money it has become unique asset class that still needs to be developed.

Index

1. Introduction

In November 2008, an anonymous programmer under the pseudonym of Satoshi Nakamoto published the white paper for bitcoin, "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008). This paper presented an electronic payment protocol that included means for online transactions through a peer-to-peer digitally currency system and was able to solve the double spending problem. Internet and daily life interdependence is increasing, so as internet usage, with over 54% of the global population having internet access *(Internetworldstats.com, 2018)*.

Bitcoin is a decentralized system, meaning that is not issued by any central authority like governments, banks or any organization. Thereby, bitcoin relies on cryptographic proof-of-work that is created by network users through computational power. Since bitcoin was the first cryptocurrency, it received huge attention among media with consumers and speculators quickly adopting it. Its valuation dependes strictly on supply and demand and it can be traded against several fiat currencies, such as USD, EUR, JPY, or GBP. Furthermore, the lack of regulation and intrinsic value emphasizes the higher levels of volatility that surrounds bitcoin when comparing to those fiat currencies. Nevertheless, the usage of bitcoin as a currency has been increasing since it was introduced, becoming a mean of exchange mostly online, but also in some stores. On the 14th of Aprill 2011 bitcoin price was $1 dollar and on the 1st of January 2018 it was around $13 412, with almost 17 million bitcoins in circulation *(CoinDesk, 2018)*.

Although, several risks are involved with bitcoin, since access keys are stored in digital wallets there is the possibility of virus corrupting the data or hard drives crashes. Hence, whenever the stored bitcoins are disabled it is almost impossible to recover it. The constant demand increase shifted bitcoin researches towards legal issues, such as network security, the usage of bitcoin during illegal transactions and frauds related to the laundering of money or even evasion of tax payments.

The major purpose of this thesis is to investigate if this digital currency is able to work as a currency in a near future or if it will only be perceived as an unique asset class for investment. Therefore, this leads to the research question: Can Bitcoin function as a currency?

Thus, the author suggests that it is striclty important to first understand the concept of a currency, different types of currencies and also the functions of money. Only

afterwards, cryptocurrencies and bitcoin characteristics can be stressed out by the author.

In order to answer this research question, an in depth-understanding of bitcoin and its characteristics is required.

2. Currency

Currency is a global accepted form of money, which includes coins and paper notes. Moreover, it is issued by governments and circulates within economies. It works as a medium of exchange for goods and services, being the basis for trades. Throughout history different types of currencies had risen and its concept is still evolving.

2.1. Commodity Money

Commodity money is a form of currency that has intrinsic useful value besides from carrying out the role of an exchange medium. It is also naturally scarce and by assuming competing suppliers, this characteristic gives this type of currency a positive value in equilibrium that equals its marginal cost of production. *(Selgin, 2012)*

Gold is the most common and one of the most ancient types of commodity monies. Nevertheless it still has some limitations due to its vulnerability regarding changes in the supply of the commodity money-base schedule. Those changes may be related to technology improvements in the mining process or simply by discovering a huge easily acessed supply of gold. Those external factors will have impact on the price of gold and therefore support its volatility. Although, sometimes those changes have a positive impact since the existing commodity money leisurely decreases with the "discovery" of new onces of gold but ,on the other hand, marginal costs of the commodity increase with the development of mining processes. Therefore it is battling secular deflation *(Selgin, 2012).*

2.2. Fiat money

Fiat money is perceived as a medium of exchange that is composed of notes without any intrinsic value or bank deposits that can redeem those paper notes into specie. Economy´s acceptance is the only support that this type of currency has that guarantees those paper notes´an intrinsic value. The notes value is much higher than their marginal cost of production, therefore due to its remarkably low marginal costs when comparing to their value, it is mandatory that the supply is controlled by some authority such as

governments. Otherwise, if this type of currency were not controlled, the value of each note would reach the marginal cost of making one *(Selgin, 2012)*.

Fiat money cannot be within a competitive market: it must be controlled by a single authority and therefore be ruled under a monopoly. Governments need to control the scarcity of fiat money. The major risk regarding fiat money stems from the risk of mismanagement *(Selgin, 2012)*.

2.3. Functions of money

Money has three major functions: medium of exchange, store of value and unit of account.

As a medium of exchange, money facilitates transactions, where buyers and sellers agree upon the value of goods or services. Without money, transactions would have to be conducted as a bartering system. Bartering requires a double coincidence of wants, which means that buyers and sellers need to give something in return that fulfills the need of the other. As storage of value, it is essential that money is able to transfer value over time. Finally, as a unit of account, money allows services and goods to be measured in a standardized unit, therefore enables economic agents to make decisions regarding its choices.

3. Cryptocurrency

Cryptocurrency is a virtual or digital currency which uses cryptography as its main source of security (*Narayanan et al., 2016)*. Cryptocurrencies have unique features that differentiate them from currencies already mentioned in this study. Since they are not issued by any central authority, it renders them immunity to mismanagement or manipulations from governments and it has also an organic nature that prevents inflation *(Chiu and Koeppl, 2017)*. However, in order to function as money it is required to fulfill the three functions mentioned before: medium of exchange, store of value and unit of account.

Cryptocurrencies can serve as a medium of exchange, nevertheless its acceptance is quite relative and limited. It is possible to make transactions with cryptocurrencies, money is not the only medium of exchange available in the market. A cryptocurrency, such as bitcoin, is only valuable as the market deems it to be and therefore its value relies on the possibility of converting it into a fiat currency. Without the possibility of

converting bitcoins to any other currency its value is diminished. Thus, it is impossible to deposit bitcoins into a bank due to its characteristics, as it is going to be developed further. Theoretically bitcoin serves as a store of value, nonetheless it is impossible to affer that is a safe storage of value *(Chiu and Koeppl, 2017)*.

Volatility and unpredictability of crypto's prices determine that cryptocurrencies do not fulfill the three functions of money, because they do not act as a unit of account. According to the three functions of money, cryptocurrencies can not be categorized as money, due to its volatility and unpredictability.

4. Bitcoin

According to the bitcoin founder Satoshi Nakamoto, bitcoin can be defined as a peer-to-peer eletronic cash system that allows online payments to be sent directly from one party to another without relying on a third party, such as financial institutions *(Nakamoto, 2008).* Digital signatures are perceived as part of the solution, every bitcoin has a digital key. As per figure 1 shows, during transactions, the owner needs to digitally sign a hash of the previous transaction, the public key of the next owner and add these to the end of the coin. Afterwards, a payee needs to verify the signatures in order to check the chain of ownership and thereby validate the transaction *(Nakamoto, 2008).*

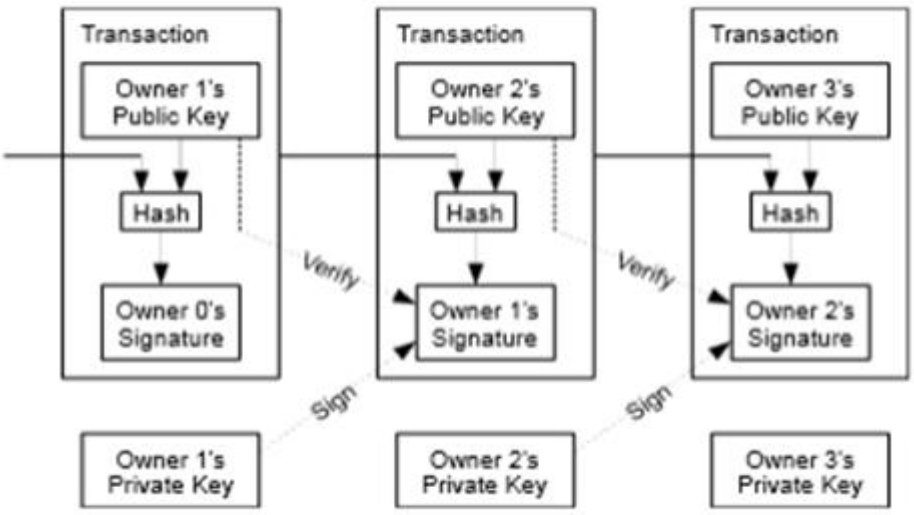


Fig 1 Transaction graph, A Peer-to-Peer Electronic Cash System (Nakamoto, 2008)

Nevertheless there is a major concern regarding bitcoin transactions, which is the **double-spending problem.** The payee that needs to verify the veracity of the signatures can not be sure that the owner of the coin did not double-spend it elsewhere. In the common money system, the solution was to introduce a trusted central authority that would check every single transaction and avoid the double-spending. If bitcoin had implemented this "solution" it would relied the fate of the coin into a third-party, because every transaction would have to go through them. However, as it was explained in this section the major purpose of bitcoin is to create a peer-to-peer decentralized cash system completely independent from banks or other institutions *(Nakamoto, 2008).*

According to Nakamoto, by using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions and by publicaly announcing all the transactions that occured to the network of participants, who can agree on the history of the order and most importantly in which order they were received, the double-spending problem can be avoided without trusting a central authority *(Nakamoto, 2008)*. Therefore, transactions would be recorded into a public ledger, called blockchain.

Bitcoin is built with the complete open-source code and fully-decentralized blockchain technology and as Nakamoto suggested in his paper, bitcoin can solve many existing critical problems of our financial model, such as the double-spending problem, security regarding the transactions, removal of banks or third-parties and provides its users' anonymity *(Nakamoto, 2008).*

4.1. Blockchain

Before blockchain creation, there was no trust between parties that none of them could make changes to the data for their own profit. There was no way to manage activities throughout internet without a centralized supervisor that was capable to ensure trustworthiness of the information and it was impossible to verify transactions without relying on a centralized authority. Blockchain uses a probabilistic approach that is capable of dealing with the validation of transactions without relying on third-parties. A network of computers increases transparency and reliability. Therefore, the ability of hackers to corrupt a distributed database with incorrect information is reduced. The only possibility to attack is when the hackers can use much more computational power than

the entire nodes that are working on the blockchain network, which is almost impossible *(Antanopoulos, 2015).*

Nakamoto argues that blockchain is a chronological database of transactions, which are recorded into blocks and that can be verified by other network users in the blockchain network. Each block has the hash of the previous one, timestamp and transactional data as shown in figure below. Whenever a block is fully completed with transactions it is generated a new one which contains some of the attributes and hashes of the previous one *(Nakamoto, 2008).*

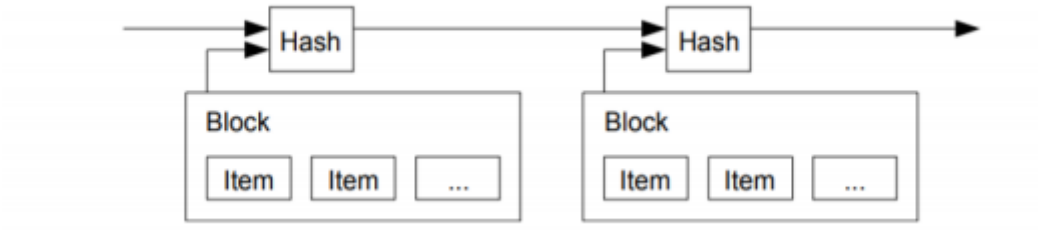


Fig 2 Structured connection of Blockchain's blocks (Nakamoto 2008, 2)

All blocks contain a hash function or a mathematical equation that can prove the integrity and non-repudiation of the information and data gathered. All members of the network have a copy of the database and computers are frequently synchronized in order to assure that every single member has the most updated and correct version.

4.1.1. Blockchain forks

Blockchain is a decentralized data structure, so blocks may arrive at different network participants not at the same time, causing nodes to have different perspectives regarding the blockchain. In order to solve this issue, nodes always attempt to extend the longest chain of blocks and the most proof-of-work representative. As long as all nodes choose the longest chain, the bitcoin network will remain consistent. Forks according to Antanoupoulos (2015) occur as temporary inconsistencies about different versions of the blockchain, whenever two blocks are competing to form the longest chain of blocks. For example, two miners were able to solve the mathematical algorithm within few seconds from each other. Since both were able to discover a solution, they intend to broadcast it to the network, so that their peers could propagate it across all participants. Therefore, each node will receive a valid block and as a result, some of them will propagate the one they received first. Let us assume that a miner in Portugal finds a

proof-of-work solution for a block "X", that is able to extend the parent block "A". On the other hand, a french miner simultaneously, who was also capable of extending block "A", finds a solution for block "Y". Nevertheless, they found two different solutions, both blocks are valid "A - X" and "A-Y". Both contain a validated solution by miners to the proof of work and both extend the same parent block "A". Moreover, it is very likely that those blocks contain the same transactions, the only difference could be in the order in which those transactions were validated. Nodes are propagating the blocks, however some peers will receive block "A-X" and others "A-Y". The network was spplited into two different versions of the blockchain. From now on, miners will extend those blockchains according to the blocks their received first. As Antanapoulos (2015) suggested forks usually are resolved with one single block and the hashing power has a fundamental role. Even if the hashing power is almost split across the two versions of blockchains that were created, it is likely that one set of miners will find a solution and propagate it faster than the other set of miners. Let us assume, that miners that were building on top of "A-Y" find a new valid block "Z", extending the chain to "A-Y-Z". Miners will immediatly propagate this new version as a valid solution. The nodes that were building on top of the "A-Y" blockchain version, will simply extend the chain one more block. Although, the nodes that chose "A-X", will perceive that two chains are currently coexisting: "A-Y-Z" and "A-X". Since, the new chain "A-Y-Z" is the longest when comparing to "A-X", nodes will understand that "A-Y-Z" is the main chain and consider the "A-X" as a secondary one. Moreover, miners that are currently working on the extention of "A-X" will stop their work because its parent "X" is no longer on the longest chain. The transactions within "X" will have to wait for processing into the next block, as that block is no longer on the main chain. The entire network participants re-converges on a single chain "A-Y-Z", therefore all miners will start working based on "Z" as the parent to extend "A-Y-Z" chain *(Antonopoulos, 2015).*

4.1.2. Hard Fork

Hard fork can be defined as a radical change from the previous version of the blockchain, which means that nodes using and running the old versions will no longer be able to use the newest version. For instance a hard fork makes previously invalid transactions valid or vice versa. Basically a fork is created into the blockchain, whereas users decide which path they want to follow, the upgraded blockchain or the old chain

they were working on. Most of the times, after a while, nodes realize the new version is better and adopt it *(Investopedia, 2018).*

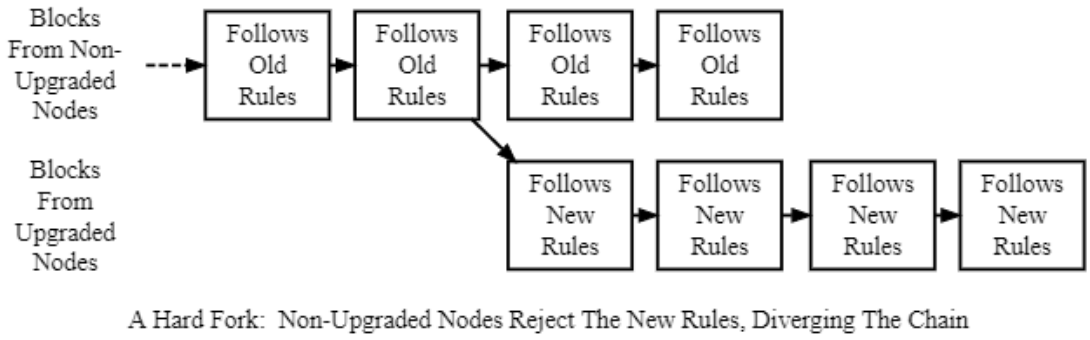


Fig 3 Hard fork, Source: Investopedia.com

Implementations of hard forks differ on its purposes. For instance, it can be implemented in order to correct important secutiry risks that were found in previous versions of the software of the cryptocurrency, to add new functionalities or to reverse transactions. By splitting the path of a blockchain, a hard fork invalidates transactions confirmed by nodes that are not using the most updated version of the protocal software *(Investopedia, 2018).*

There are successful cases of hard forks, such as Bitcoin Cash and Bitcoin Gold. Bitcoin Cash is a successful hard fork of Bitcoin Classic that happened in August 2017. The major purpose of this fork was the pressure that Bicoin was facing regarding the topic of scalability. Miners wanted to increase the size of the blocks, thus allowing more transactions to be processed. They thought that the size of the blocks was limiting the currency´s potential, nevertheless that block size limit was created in order to prevent the software from spam attacks. Several proposals were taken under consideration by nodes. Since bitcoin software does not rely on third-parties, changes require a consensus from developers and miners, which means long time processes. Nevertheless, Bitcoin Cash was a successful hard fork. Bitcoin Cash increased the block size from 1mebabyte to 8 megabytes and also removed SegWit, a code adjustment that was designed to free up block space by taking away certain parts of the transactions. The major purpose of Bitcoin Cash is slightly different from Bitcoin. Supporters of Bitcoin Cash seek faster and more transactions and they intend to compete with settled companies such as Paypal and Visa *(Investopedia, 2018).*

4.1.3. Blockchain impact and uses

Technological Implications

Nowadays, most of the technological companies´ solutions are based on centralized databases. Since Blockchain relies on the distributed network, which is completely the opposite of the technologies used, it represents not only a huge challenge but also an amazing opportunity in order to change the current path. Blockchain requires a significant amount of computational power, therefore the manufacture of hardware for miners will increase, which might lead to changes in the hardware market.

Regarding industries of Blockchain applications there are some changes that can be implemented. Moreover, the blockchain adaptation will promote transparency, elimination of third-parties and also workflow optimization. It is possile that optimization technological changes may occur in several workflow processes such as supply chain and manufacturing. Therefore, the majority of the devices required on those processes would become useless for companies, so they might be used for mining, sold or even upgraded.

Social and Political Implications

Blockchain technology could solve some problems, such as poor social institutions work, censorship in social media, and lack of acess to the education in third-world countries or developing countries. Governments´ mismanagement and lack of tools are the major political features that can benefit from the blockchain technology. There are several countries whereas the trustworthiness on the election tool is broken, therefore the implementation of this technology would increase confidence among elections. Moreover, a blockchain-based system of election is able to provide results much more accurately and eliminate the administrative methods to manipulate the results. Not only blockchain technology could help solving the problems mentioned before, but it could also start transforming and empowering services that already exist. For instance, Uber and Airbnb are based on networked integrity principle, which establishes trust between two parties withouth a central authority or middleman. With the usage of blockchain, there are plenty of opportunities to create much more platforms for several areas such as private healthcare and education. All those new services would be supported by a

technology structure and publicly opened for all users in order to modify, rate or review it.

Economy sharing has become very popular, as mentioned above carsharing and flatsharing services are disrupting the hotel and taxi industries. Nevertheless, all those new services lack security and capability of predefining conditions. Moreover, blockchain is able to solve those problems and upgrade the existing service. Entrepreneurs could also benefit from blockchain, since barriers to establish new businesses could be simplified. Initial Coin Offerings facilitate crowdfunding, with minimum or no documents required. Furthermore, blockchain could provide the announcement of information without censorship, therefore ensuring freedom of speech. Tor private browsing environment represents one of the advantages of blockchain: a secure, transparent and trusted source of all type of information. Governments may feel threatened by blockchain technology usage, nevertheless it provides equality and freedom worldwide.

Corruption could be fought with the usage of blockchain technology, since the political management tools become transparent and more importantly traceable. Estonia is a perfect example of an established blockchain projet. National health, judicial, security and commercial systems are all integrated in the blockchain technology *(CTGA, 2017)***.** Estonians are able to vote, manage their tax forms, access the different public services and even apply for social compensations virtually. Thus, Estonia become the first state to provide a digital identity worldwide, so it can be issued to every person and gives access to the countries e-services. Anyone by using the e-Residency of Estonia can start a business and manage it remotely there. Thus, Estonia by empowering blockchain technology solutions can change completely the perspective of the business market *(CTGA, 2017.)*

Economic implications

There are major risks and challenges that global economy needs to face. Transparency and nature of investments, lack of new markets that enhance the development of the economy and insecure capital accounting represent some of those risks that prevent an economic growth *(Spence, 2016).* Blockchain is able to manage those obstacles and therefore boost economy growth. Economic implications caused by the implementation

of blockchain can be spllited in two stages: Use cases of the technology in finance and overall consequences by its implementation into the different set of industries.

Tapscott (2016) suggested that there are six major reasons that support the idea that blockchain technology will enhance finance monopolies and develop the industry: trustworthiness, cost, transaction speed, risk management, value innovation and open source structure *(Tapscott, 2016).*

With the usage of blockchain, any financial intermediary is irrelevant in order to assure the identity and trust between two parties. The public ledger records transactions history, rates based on reviews and other additional options support the trustworthiness of connections between two parties.

According to Belinky, Rennick and Veitch (2015), if blockchain was implemented by financial institutions they could save up to 20 billion USD by simply decreasing infrastructure costs related to cross-border-payments. Moreover, withouth changing significantly their business model and by reducing their costs, banks would become much more competitive, therefore could offer private and public clients better opportunities, which include, higher amount of services, new markets and also opportunities to invest in developing economies. Thus, would be a benefic measure for all parties involved (*Tapscott, 2016).*

Bitcoin blockchain software validates transactions within 10 minutes as it was shown before in this paper. On the other hand, trades on stock exchanges or money transfers between users need three days to be validated and processed. Thus, the implementation of a public ledger can signifcantly boost the economy by freeing up capital with faster transactions validations *(Tapscott, 2016).*

The adoption of Blockchain enables some financial risks to be smoother. Settlement risk, risk of failing the deal and systemic risk are examples of counterparty trust risks that can be eliminated by the Blockchain. Moreover, accounts are able to find all the transactions at any time and analyse the operations that occured. Therefore, blockchain brings integrity and non-repudiation of transactions *(Tapscott, 2016).*

Blockchain contains an open code, which enables several projets similar to the bitcoin, known as altcoins. Those projets can be used for different purposes and industries,

therefore blockchain represents an innovative iniciative for several areas *(Tapscott, 2016).*

Nowadays, financial instutions rely on technologies, therefore any changes have a major impact on those companies, which may require developments regarding their business model. Blockchain open source basis provides continuously development, evolvment, test and improvement of the system whenever the consensus in the network is achieved *(Tapscott, 2016).*

According to a Deloitte's study there are 5 major blockchain use cases that are able to transform the financial sector: speeding up and simplifying cross-border payments, implementation of smart contracts, share trading, online identity management and loyalty and rewards *(Deloitte, 2018).*

Smart contracts are one of the most important applications regarding blockchain technology, corresponding to effective programmes which are loaded into, and sit alongside traditional transactions within a blockchain, that are able to automatically execute the predertermined terms of a contract when trigger events occured. For example, a digital confirmation occures if certain price or volume conditions are met. The key feature of smart contracts is the decentralized system that doesn´t rely on any intermediary (*Deloitte, 2018*).

Blockchain has potential to disrupt several financial services. Accenture estimated that global investment banking industry has $30 billion cost base and the implementation of the blockchain technology could save financial institutions up to 70% in reporting costs, 50% in compliance and on-boarding costs and 30% on infrastructure costs. Finally, it would reduce opex for the world´s 10 largest investment banks by $8-12 billions (*Accenture, 2018*).

Financial services areas are very sensitive and sudden changes compound a huge risk, thus one error can lead to major consequences, and intense regulatory oversight requires extreme caution. Therefore, other areas such as consumer products and manufacturing whereas there are more room to experiments, already begun implementing blockchain solutions in 2017. According to a study developed by Deloitte and as per figure shows, 58% of the consumer products and manufacturing senior exectuvies that were interviewed confirmed they were deploying blockchain solutions in 2017, 53% executives of life sciences and healthcare said they would deploy blockchain solutions in 2017, compared to 36% of executives in the financial services. (*Deloitte, 2018*)

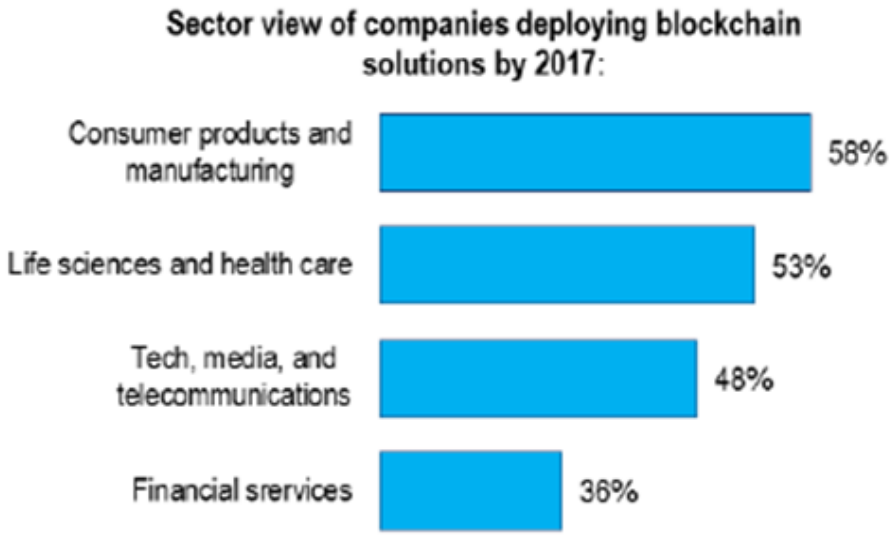


Chart 1 Not just about the financial services, Source: BI Inteligence, Credit Suisse Research

Non-financial applications - Provenance

Provenance is one non-financial company that aims to solve supply-chain challenges by adopting blockchain technology. According to Deloitte, around 200 retailers and producers in the food and drinks industry already use Provenance´s application services in order to track the origins and movements of their products. Product information can easily be checked, that information cannot be changed or even more certifications added without validation from the nodes. Thus, retail costumers are able to scan products in stores and then obtain all the necessary details regarding the producer, methods of production and quality of the product. Provenance is still working towards an open traceability protocol, in order to guarantee that every consumer can track the provenance of every product available *(Deloitte, 2018).*

Blockchain technology has several characteristics that emphasize the possibility of disrupting some industries mechanisms, such as: highly secure transactional platform, low cost, fast, risk minimization, innovation of value, attestation and enhances the possibility of reducing capital requirements *(Deloitte, 2018).*

4.1.4. Obstacles for blockchain:

Blockchain, alongside with bitcoin, is not immune from hype and therefore some concerns and challenges will have to be surpassed in order to widespread production and implementation.

There is a huge trade-off between security and cost. A blockchain can either be expensive and secure or cheap and comparatively risky. Security comes at prices not dissimilar from the transaction costs charged in legacy systems.
Blockchain solutions rely on multiple nodes, therefore critical mass is essential. Nevertheless, some threats come along the way such as the fragmentation of platforms or even institutional or social inertia to change or agree on a new platform. Furthermore, a single open-source platform would be required in order to achieve critical mass.
The constant interest on this new technology brings more nodes to the software, therefore hackable entry points of blockchains increase (*Credit Suisse, 2018*).

4.2. Mining

Antonopoulos (2015) argued that mining is the process by which new bitcoins are added into the money supply. Moreover, it is also strictly important to remain the bitcoin system secure against fraudulent transactions or double-spending transactions *(Antanopoulos, 2015).*

Miners play an essential role in all cryptocurrencies systems, not only bitcoin. They are responsible for gathering unconfirmed transactions into new blocks and group them into the blockchain. Therefore, miners provide the necessary computing power to guarantee a blockchain by computing several numbers of hashes in order to discover a valid block. Whenever a miner adds a new block into the public ledger, he generates a reward for himself and makes it harder for an hacker to reorganise the ledger and spend the already confirmed transactions *(Hileman and Rauchs, 2017).*

Miners receive two different types of rewards in order to perform their job: new bitcoins with each new added block and also a transaction fee from all the transactions that were included in the mined block. In order to earn this reward, miners compete with each other to solve a mathematical problem based on cryptography. The solution of this mathemathical problem is called proof-of-work. It is included in the new mined block, so that it acts as a proof that the miner was able to solve the problem and spent significant computing effort to perform it *(Antanopoulos, 2015).* Nakamoto (2008) believed that this competition to solve the proof-of-work algorithm and earn rewards by record transactions into the blockchain was the basis for bitcoin's security model.

Miners with this procedure feel incentivized not only to win rewards but also to make the security of the blockchain immune to hackers' attacks.

Mining is the process of new coins generation and the associated rewards are designed to constantly be lower, just like mining for precious metals such as gold or silver. Central Banks issue money by printing bank notes and bitcoin´s supply money is created through mining. As mentioned before the reward is designed to decrease proportionally over time. The amount of bitcoins a miner is able to create whenever he mines a block decreases approximately every four years or 210 000 blocks. When bitcoin was created, 50 new bitcoin's were issued per block, it halved to 25 Bitcoins per block in November 2012 and to 12,5 in 2016**.** In 2140, based on this formula, all bitcoins will have been issued and after that no more bitcoins can be created *(Antanopoulos, 2015).*

Transaction fees are also important for miners. Every transaction may include a "bonus", this is a surplus between the inputs and outputs. So miners are more motivated to mine that block and validate the transactions, because if they are able to solve the mathematical problem then they will remain with the diference - transaction fee. Nowadays, transaction fees represent only 0,5% of a miner's income, nevertheless after 2140 when no more bitcoins are going to be created, all the miners earnings will be under transaction fees.

The major purpose of mining is not the reward that miners receive or the generation of new bitcoins. Mining is the major process of the decentralised system, whereas transactions are validated and added to the blockchain. Mining assures the security of the bitcoin system and enables a wide network consensus without trusting on a central authority *(Antanopoulos, 2015).* Rewards are an incentive scheme that alligns miners job with the security of the network. This symbiosis is fundamental to the bitcoin network system *(Nakamoto, 2008).*

4.3. Transactions

Antanopoulos suggests that transactions are data structures that are able to encode the transfer of value between users in the bitcoin system. Transactions represent the most important process of bitcoin system, therefore, everything is designed to ensure that it can be performed, propagated, validated and also added to the blockchain.

A transaction lifecycle has 4 major steps:

- Creation; Origination of a transaction. Transactions can be created by anyone online or offline, even if the person creating it is not entitled to sign it. For example, someone responsible for the payments at a company can create a bitcoin transaction and then have the CEO signing it digitally, so that the signature is valid.

- Signature; Transaction is signed, with one or more signatures, which means that the funds referenced by the transaction were authorized to be spent. The transaction is valid whenever it was correctly formed and signed. After its validation a transaction contains all the necessary information to execute the transfer of funds.

- Broadcasting and Propagation; Afterwards, the transaction is broadcasted into the bitcoin network, whereas nodes validate and propagate it in order to reach every participant in the community.

At this stage, transactions are already signed. Moreover, transactions do not contain any confidential information, such as private keys or credentials, so it is possible to broadcast it using any network transport that suits the sender. According to Antanopoulos (2015), the major issue is to reach a bitcoin node that is able to propagate the transaction into the bitcoin network.

After the broadcasting stage, the transaction needs to be validated by the node who received it. That node will propagate it to other nodes if the transaction is considered valid. On the other hand, the originator of the transaction will receive an automatic success message in case of validation and a rejection message if the transaction is considered invalid. As Nakamoto suggested the bitcoin network is a peer-to-peer network which means that each node is connected to others that were discovered throughout the peer-to-peer protocol *(Nakamoto, 2008)*. Therefore, the entire network forms a tremendous structure making all nodes equal peers. A transaction is propagated from each node to the peers that the participant is connected to. Moreover, with this process within a few seconds a valid transaction is able to exponentially be propagated through the network untill all nodes received it.

Nakamoto explains that the bitcoin network was designed to propagate those transactions to all participants in a resilient and most efficient possible manner. The major goal was to resist from the attacks of hackers. Therefore, to prevent those attacks,

every node will independently validate all the transactions before propagating it into the network *(Nakamoto, 2008).*

- Verification; the last step of a transaction lifecycle is the verification. Transaction is verified through miners and included or not on the blockchain.

After completing its lifecycle a transaction is recorded on the blockchain and represents a permanent part of the ledger. The funds that were allocated to a new owner by the transaction can start the transaction lifecycle all over again, which means that the funds can be spent in a new transaction.

4.3.1. Transaction Fees

Nakamoto argued that by imposing a transaction fee, which would serve as an incentive to fight malfunction transactions or any kind of abuse of the network but also as an incentive to include transactions into the next block *(Nakamoto, 2008)*. As it was stated before miners are the ones responsible for the record of the transactions and therefore those who can collect those fees.

Antanopoulos explains that fees are calculated according to the size of the transaction in kilobytes, not based on the value of the transaction. Transaction fees impact the processing priority, so that a transaction with fees is likely to be mined and validated first. On the other hand, a transaction with insufficient or no fees at all may be postponed and validated later on *(Antanopoulos, 2015)*. Transactions fees are not mandatory, it simply encourages miners to prioritize the transactions they are going to mine first. Throughout the years, the way fees are calculated has evolved. Firstly, they were fixed and constant, but this has been gradually changing over time. The fee structure is influenced by market forces and based on transaction volume and network capability.

4.4. Deflationary money

Bitcoin supply cap is around 21 Millions coins and its diminishing issuance creates a fixed supply that is inflation resistant. Fiat currencies can be printed by a central bank whenever they decide in infinite numbers, however bitcoin can not. Therefore, Bitcoin tend to be deflationary. Deflation is the phenomenon that drives up the value of a currency due to mismatches in supply and demand. It may be seen as the opposite of inflation, whereas price deflation represents the more purchasing power that money has over time *(Antanopoulos, 2015).*

According to Antonopoulos many economists defend that a deflationary economy is a tragedy that should be avoided. In periods of deflation, consumers tend to stop spending their money, instead they hoard it hoping that prices continue to decrease. Nevertheless, bitcoin experts suggest that deflation is not as bad as it seems and it might be beneficial for the cryptocurrency. Deflation in bitcoin is caused by a constrained supply, consumers know there is a supply cap, and therefore they hoard their coins because they expect to be rewarded in the future with the increase of value of the coin *(Antanopoulos, 2015).*

4.5. Bitcoin major challenges

4.5.1. Network Security

Bitcoin is not an abstract reference to value, therefore one of the major challenges that bitcoin network faces represents its security. Possession is essential, since users need keys to unlock bitcoins, otherwise it becomes worthless and users can not do anything with their own money. In case of theft, or accidentally transfering the wrong amount to someone else the end user has no recourse, which means it is almost impossible to get it back.

Although, Bitcoin network has capabilities that cash and bank accounts do not have to prevent the issues mentioned above. A bitcoin wallet, which contains the keys, can be backed up, it can be stored in plural copies or even printed on paper for hard-copy backup. Bitcoin stands out from the remaining currencies due to this capability of backing up your own bitcoins in order to prevent the attacks from hackers.

Centralized models, such as bank institutions or payments network like Paypal, rely on access control and evaluate their users by trying to keep bad actors out of their database. Thus, these type of institutions need to be very careful, because anyone with access to the identifier can steal their funds over and over again. Moreover, if a hacker gains access, current transactions can be compromised and even worse, when data from a customer is compromised, the customer is exposed to identity theft. Thus, it is necessary to take actions in order to prevent fraudulent use of his account. Bitcoin software is completely different, since it does not reveal any private information such as the identity and more importantly it does not allow additional payments or transaction. A bitcoin transaction only authorizes a certain amount to be transfered to a specific recipient that cannot be changed. Unlike the other institutions Bitcoin does not need to

be encrypted, in fact bitcoins transactions are broadcasted throughout a public channel as it was explained before in this paper.

Since Bitcoin is a decentralized security model, end-users have a tremendous power in their hands. Moreover, with that power comes responsability in order to maintain the privacy of the keys. One major concern rergarding Bitcoin software is that it is too developed for those who are not familiriarized with technologies. For the majority of users keeping their keys safe is very complicated. So, bitcoin decentralized software system needs to assure that mass compromise users are able to do it or create a simplified model of securing keys, in order to attract even more people and increase confidence regarding transactions between users. Otherwise, people with lack of knowledge will fell insecure because they are not able to secure their keys and most importantly hackers will continue to attack.

Mt Gox

Bitcoin depends on a decentralized model and transactions among users are validated by miners as it was presented before. In order to maintain the security it is essential to keep up with the security model provided by bitcoin. Otherwise, disastrous cases such as Mt Gox can happen.

Mt Gox, an exchange based in Japan, once was the largest Bitcoin Exchange in the World. It was created in 2010 by a programmer Jed McCaleb, who a year after sold it to a French Developer called Mark Karpéles. Mt Gox was an exchange that concentrated most of their users funds in a single wallet, with the majority of the keys stored into a single server. This type of design is not alligned with the Bitcoin core system, because it removes control from users and centralizes it to a single server that contains all of the users keys *(Blokonomi, 2017).*

The increased interest in Bitcoin, as the price of the the coin was increasing a lot turned Mt Gox into the largest Bitcoin Exchange in the world. It ws holding around 80% of all Bitcoin trades. Nevertheless, mismanegement policies and concentration of the users´ keys on a single server were the major concerns regarding the company. It was vulnerable to an attack, which eventually happened on 2014. Mt Gox sttoped all withdrawls from their users after the attack and some weeks later suspended all trading.

As a result of this attack 850,000 Bitcoins vanished, which at that time was equivalent to 460 Millions USD *(Blokonomi, 2017)*.

Norry (2017) states that it could happen again, because there are loads of exchanges operating, some more reputable than others. Exchanges enable trading of cryptocurrencies, although in order to save your coins those are not the best options, because wallets were created to do so. Exchanges are fundamental for Bitcoin, without it people would not be able to trade. Moreover, the current increase in the number of exchanges allows the hackers to exploit failures in some of them and extract value from their attacks. Users should use exchanges to trade and wallets to save their coins.

Bitcoin often offers a secure and untraceable method of transaction, making it a perfect environment for those who seek their financial activities to remain hidden. In May 2017 occured a massive attack, called the WannaCry ransomware attack, which completely froze hundreds of thousands of computers all over the world, including UK´s National Health Service system. Attackers demanded users who wish to have their computers back to pay $300 worth of bitcoin to specific wallets. Moreover, earlier 2018, it was reported that several websites harbored malicious malware code that was being used to mine bitcoin. Visitors' of those websites were running a code that behaves like malware and the website was using processing resources to mine cryptocurrencies without users´ permission. The potential of cryptocurrencies is certainly alligned with its problems *(Credit Suisse, 2018)*.

4.5.2. Criminal Activities

Criminal activities such as mondey laudering and illicit transactions represent one important challenge that bitcoin needs to face. Its anonymity provides an easy access for those who seek trafficking illegal goods and services *(Brito and Castillo, 2013)*. For example, the author suggests the case of the infamous black-market "Silk Road". Silk Road is one of the most useful examples to sustain the Brito and Castillo claim.

Silk Road started its operations in February 2011 and can be defined as an online anonymous marketplace. Moreover, Silk Road provided the necessary infrastructures for their users to transact anonymously online, it was like Amazon Marketplace or eBay *(Christin, 2012)*. Nevertheless the major purpose of Silk Road was guaranteeing the anonymity of buyers and sellers. During his studies, Christin concluded that 4,5% of all traded bitcoin were exchanged through Silk Road. Also, regarding those transactions it

was suggested that around 36% were related to drugs and the report also stated that Silk Road was selling almost $1,5 millions / month worth of black market (Christin, 2012). Bitcoin's association with Silk Road damaged its reputation and increased confidence over those who related illicit activities with the cryptocurrency system.

Another challenge that is related with criminal activities is money laundering. Besides being a very theoretical claim, bitcoin has particular characteristics that enhance the possibility of laundering money in order to traffic illegal goods or even financing terrorism *(Brito and Castillo, 2013).* A possible example of comparison is Liberty Reserve. Liberty Reserve was a private centralized digital currency service, which was shutdown due to money laundering charges *(BBC News, 2013).*

Both concepts are based on digital currencies but there are significant differences among them. As the author mentioned Liberty Reserve was a centralized currency owned by a private company with the purpose of facilitating transactions that were not transparent *(Brito and Castillo, 2013).* Bitcoin, as it was explained in this study, is completely different. Nevertheless, those charges of Liberty Reserve tarnished bitcoin´s reputation, since digital currencies and anonymous transactions were a completely new topic. Transactions, as it was suggested in section of this paper, are recorded in a public ledger and acessible at any time by law enforcement. Therefore, it is much riskier for money launderers to use a decentralized system like bitcoin rather than Liberty Reserve. Moreover, bitcoin exchanges according to FinCEN regulations as it is going to be developed further in this work, have to comply with anti-money laundering rules *(Sparshott, 2013).*

The cooperation between bitcoin exchanges and the usage of blockchain to collect information relying its customers makes bitcoin community less atractive to those illicit activities. The theoretical association between bitcoin and money laundering damages and dimishes the cryptocurrency perception among those who are not aware of digital currencies processes and methods *(Brito and Castillo, 2013).* On the other hand, cash has been for many years the vehicle for those criminal activities that the author exploited above. However, regulators and policymakers are not considering banning it. The downsides of bitcoin concerning criminal activities are exactly the same as those that fiat currencies face *(Brito and Castillo, 2013).*

4.5.3. Consensus Attack

Bitcoin network system is secured by miners, computers that are processing network transactions and recording all validated ones in the blockchain. Nevertheless, pottencial attacks may occur. Whenever an organisation is able to control the majority of the hashrate power or mining power in the network system then they have the ability to perform a consensus attack or 51% attack *(Learncryptography.com, n.d).* However, 51% of control does not give attackers full power over the system. The farther back in the blockchain transactions are, the more difficult and secured they are against possible attacks. Furthermore, it is important to mention that hackers are not able to issue new coins with the control of the network, except those that are received as reward for validating transactions. Consensus attacks do not affect the security regarding keys, it cannot steal cryptocoins, spend them without signatures or change transactions that occured or even ownership records. Those attacks can affect the most recent blocks, cause disruptions on the creation of future block and reduce confidence over the community. Attackers by colluding to attack the network have the ability to mine most of the blocks and cause deliberate forks in the ledger, double spend transactions or prevent some transactions to occur (*Antonopoulos, 2015).*

In order to attack the network it is not necessary to have more than 50% control. It is possible to attempt attacks with less control, however chances of success are very low due to the security processes of the network. The 51% level almost guarantees that the attack is going to succeed. Those attacks are essentially a war for the next block to be mined in which those who have more computacional power are more likely to take advantage. Theoretically it is possible to perform a 51% attack due to the characteristics of the network: free and open. If someone or an organisation has enough hashrate or mining power, which would cost a huge amount of money as it is going to be discussed further in this work, there is no central authority that can stop the hackers from attacking the system. The constant increase of hashing power turned bitcoin secure against single miners attacks. However, the centralization of computacional power due to mining pools has significantly increased the risk of those attacks. Miners are able to collaborate to form mining pools, which means that they group and share their hashing power increasing the chances of sucessfully mining a block. In case of success they split the profits among them. As it was mentioned, for a single miner it is impossible to perform

a consensus attack, although the constant increase of mining pools increases the risk of those attacks *(Antonoupolos, 2015).*

4.5.4. Energy Consumption

The Bitcoin Energy Consumption Index, presented in chart 2, shows the continuosly increase regarding the energy consumption. This index was created in order to provide insights regarding the constant growth and most importantly to raise awareness on the unsustainability of this usage.

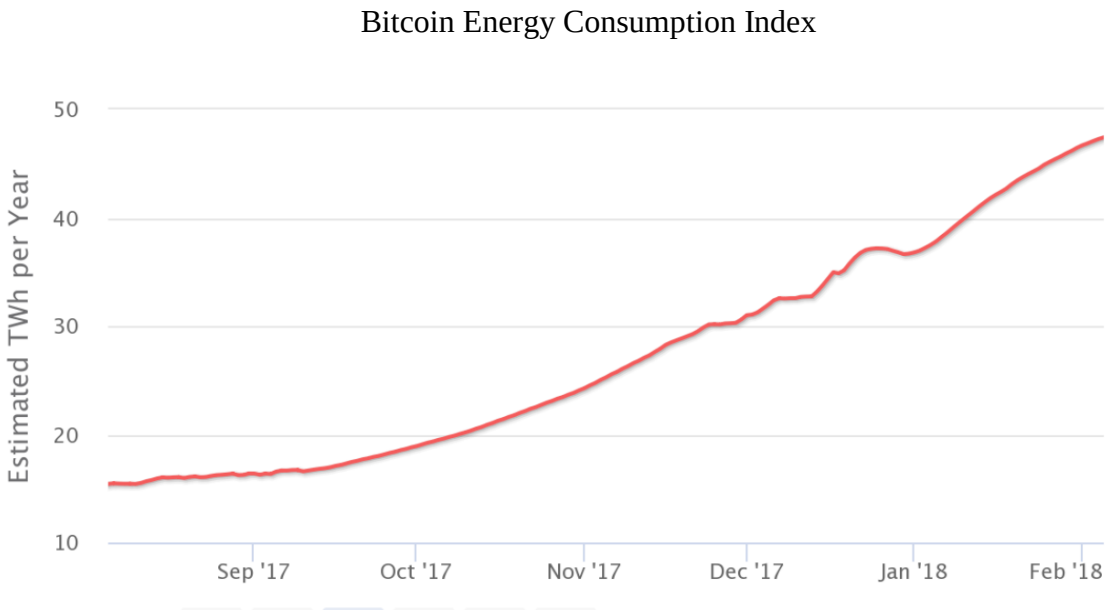


Chart 2 Bitcoin Energy Consumption Index. Source:digiconomist.net

The mining system that was implemented by Satoshi Nakamoto incentivizes loads of people to start mining, since it can be a very good source of revenue. As it was explained before in this section, it is almost impossible for a single miner to validate and record a transaction into the public ledger. Nowadays, there are thousands of powerful machines working towards the same goal, the so-called mining pools. Therefore, it is required a huge investment in order to be profitable in the mining sector. Moreover, as it is possible to verify through chart 3, bitcoin network is currently consuming more energy than several countries such as Peru, Singapore and Iraq.

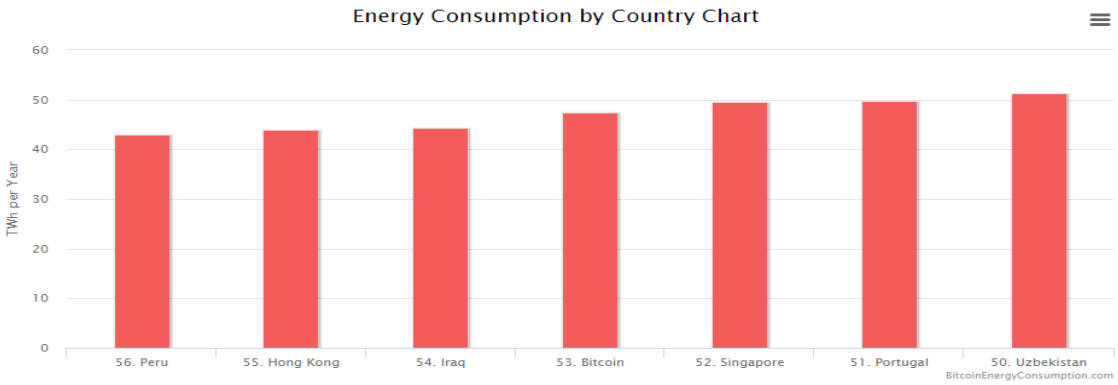


Chart 3 Energy consumption by country, Source: Digiconomist.net

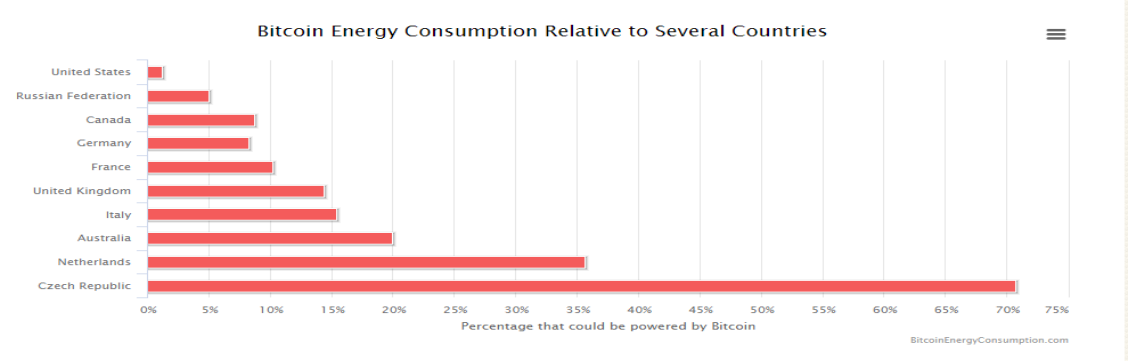


Chart 4 Energy consumption relative to countries, Source: Digiconomist.net

The mining game is quite simple. As it was developed previously in section 4.2, the miner that successfully solves the mathematical algorithm is currently rewarded with 12,5 bitcoins plus all the transaction fees. This is a winner takes it all game, where the prize is guaranteed to be paid every 10 minutes. Therefore, assuming that the price of bitcoin is going to increase and reach the values that the community seeks, miners will want to invest more on eletricity so that they can win the final prize. Burning more eletricity, will increase their odds of getting the reward. However, this constant energy consumption usage is quite dangerous. The network users are already consuming more energy than entire countries, so major concerns such as global warming should be addressed *(Digiconomist, 2018)*.

5. Regulation

Bitcoin has had a tremendous growth over the past 10 years as it was explained throughout this paper. Therefore, some agents are concerned about the future of the

cryptocurrency and look towards a path of regulation. *(Federal Bureau of Investigation, 2012, p.4).* In April 2012, The Federal Bureau of Investigation, also known as FBI, published an assessment, whereas it was revealed the concerns and challenges regarding Bitcoin development. The anonymous nature of the system incentivizes illicity activities and makes it harder for law enforcement agencies to detect those suspicious activities, since there are no central authorities controlling the platform. *(Federal Bureau of Investigation, 2012, p.4)*

Bitcoin's decentralization is a novelty which emcompasses some risks, like money laundering, stealing and drug dealing. FBI emphazises that this decentralization turns the system a riskier market for manipulation using malware and botnets. *(Federal Bureau of Investigation, 2012, p. 5)* Besides bitcoin being different from other electronic systems, the major differences relie on anonymity and the dependence of a third-party authority *(Federal Bureau of Investigation, 2012, p. 5).* Furthermore, Bitcoin as a decentralized system makes it harder to implement regulatory guidelines for its users. FBI on his report states that it is almost impossible for the Bitcoin community to fight money laundering. Moreover, as long as the cryptocurrency can be converted into real money, hackers and attackers will keep on with their work. *(Federal Bureau of Investigation, 2012, p. 10).*

As the author is trying to suggest in this paper, Bitcoin has not yet been defined by law, it is a technological achievement which is changing several industries. Current regulations and laws are not prepared for technological advances like this, therefore regulation becomes more difficult. Nevertheless, in order to prevent illicity activities such as drug trades through dark markets, as it was shown in section regarding Silk Road, it is necessary to implement a certain type of regulation. It is a huge challenge to regulate Bitcoin so that it remains useful for its participants. *(Brito & Castillo, 2013, p. 38).*

5.1. Regulation across the world

Bitcoin´s technology is censorship-resistant, it permits the processing of transactions that were previously restrained by intermediaries or that were not allowed by law. Given this feature of the technology and that the first application of the bitcoin system has been money transfers and simple payments, it is normal that the first regulatory activities regarding bitcoin have focused on money transmissions *(McKenna, 2017).*

5.1.1. United States

FinCEN

The Treasury Department´s Financial Crimes Enforcement Network, also known as FinCEN, issued the first rules regarding bitcoin in March of 2013. According to those rules, bitcoin exchangers and other related companies are qualified as money transmitters under the Bank Secrecy Act.30. Therefore, all those businesses are required to be registred with FinCEN as money services businesses in every state in which they do their business. Moreover, it is mandatory to comply with customer rules, anti-money laudering programs and file suspicious activity reports. (FinCEN, 2013)

FinCEN started to clarify the applicability of its regulations to specific business cases, whereas each case is different and rules may act differently. (FinCEN, 2014). According to FinCEN, a virtual currency operates like a fiat currency in some environments, nevertheless it does not have all the attributes of a currency, such as EUR or USD (FinCEN, 2014). Moreover, FinCEN also defines a convertible virtual currency as a substitute for real currencies or a currency which has an equivalent value in real currencies. As mentioned previously in this paper, companies that intend to transmit convertible virtual currencies or exchange those virtual currencies into fiat currencies are those who fall under FinCEN regulation (FinCEN, 2014). Therefore, miners and bitcoin traders that trade for their own investment purposes are not going to be regulated by FinCEN rules (FinCEN, 2014). This policy taken by FinCEN tends to suggest that transactions that occur inside Bitcoin economy, this means transactions that are not convertible to fiat currenices, are unique and should not be considered for regulation purposes.

Securities Exchange Comission:

SEC has not registered any ICO or approved any exchange-traded products holding digital currencies or any asset related to cryptocurrencies for trading or listing. Moreover, SEC on July, 2017 issued a paper about ICO's, whereas it was suggested that it can be "fair and lawful investment opportunities", nevertheless it can be used for illicit activities and improperly (SEC, 2017). SEC already issued three enformecent actions against ICO's, one halt and two alleged frauds (SEC Gov, 2017)

Commodity Futures Trading Comission

Commodity Futures Trading Comission declared Bitcoin as a commodity. Therefore, any fraud or manipulation is under the authority of the CTFC, regarding the cryptocurrency commodity futures or trading in interstate commerce. Bitcoin futures were launched due to the authorization of the CTFC. CME and CBOE are the exchanges where it is possible to trade the first future contracts regarding Bitcoin.

Commodity Futures Trading Comission classified bitcoin as intangible exempt commodities, because it can be owned and consumed in the sense of being spent elsewhere or traded.

Furthermore, there is one reason that supports this classification of bitcoin as an intangible exempt commodity. Bitcoins are similar to precious metals due to its limitation in supply and capability of being phisically delivered. Moreover, bitcoin can be perceived as a capital good because they can be used to produce other goods or services such as digital assets and contracts *(Bloomberg.com, 2014).*

Internal Revenue Service

Regarding tax purposes, according to IRS bitcoins must be treated as property. Furthermore, a capital gain or loss should be recorded as if an exchange involving property occured and it should be treated as inventory if it is held for resale. Finally, if bitcoins are used as a medium of exchange, than it should be treated like a currency and must be converted at its fair market value verified on a certified exchange *(IRS Gov, 2014).*

5.1.2. China

China financial institutions and third-parties payment providers were banned from exchanging virtual currencies. People´s Bank of China also warned banks from working aside with virtual currencies based businesses, although its use remains legal it is now required for exchanges to be registered within the appropriate authorities. Moreover, China´s Governement is planning to shut down Bitcoin miners. According to Hsu, bitcoin mining is estimated to consume the equivalent electricity to three nuclear reactors' production levels *(Forbes, 2018).* Nevertheless, the move from the Government is not only based on the electricity consumption. Risks of the cryptocurrencies, which regulators associate with malicious acts such as frauds and

money laudering are the major concern for the Chinese Government. Therefore, on last September China banned all companies and individuals from raising funds through Initial Coin Offerings, relating ICO's with illegal activities.

According to Hileman and Rauchs China represents the country with most mining facilities and uses the highest power of all countries *(Hileman and Rauchs, 2017)*. Mining facilities are based on three key factors: low-cost eletricity, fast internet connections and mining equipment must be kept from overheating in order to optimize the process. Therefore, the dismissal of bitcoin mining companies in China could lead to a price decrease. If the Chinese Government force miners to give up their operations, then they will move elsewhere and relocate their mining operations in regions whereas those key factors mentioned above are found. Moreover, by decreasing the supply of Bitcoin its price may be reduced, but only in a short-term perception. Thus, this decision taken by the Chinese Government may have a short-term impact, however, it will have minimal effect on the supply of the cryptocurrency in a long-term perspective *(CCN, 2018)*.

5.1.3. Portugal

Bank of Portugal warned consumers about the risks of virtual currencies and do not want to regulate Bitcoin. According to Helder Rosalino, a director at Portugal´s Central Bank, bitcoin cannot be considered a currency. For Rosalino, a currency needs to be associated itself with the idea of store of value as shown before in this paper (Section..) and also have the ability to be used as credit. Nevertheless, Rosalino recognizes the potential of the Blockchain technology but also considers it purely speculation. Furthermore, due to its limited supply and volatility the Bank of Portugal director assures it is mandatory to the central bank to train and protect consumers from the risks associated to those problems *(CCN, 2017)*.

Portugal Government seeks to tax bitcoin users, despite the lack of regulations. Autoridade Tributária, an organism that is part of the Ministry of Finance, consider that bitcoin earnings are distribution of profits, therefore bitcoiners should declare their earnings as long as those earnings represent a professional or business activity *(Jornaldenegocios.pt, 2017)*.

6. Bitcoin - Asset classification

According to Investopedia *"an asset is a resource with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit (Investopedia, 2018)".*

Greer argues that an asset can be divided into three categories: capital assets, consumable assets and store of value assets and also emphasizes the difficulty of classification between those categories, giving the example of gold which can be perceived as a consumable but also as store value asset *(Greer, 1997).*

According to Greer studies, the three categories derives from fundamental economic features and the correlation of their returns, as shown in Table 4:

	CAPITAL ASSETS "Ongoing source of something of value...valued on the basis of net present value of its expected returns."	CONSUMABLE/ TRANSFORMABLE ASSETS "You can consume it. You can transform it into another asset. It has economic value. But it does not yield an ongoing stream of value."	STORE OF VALUE ASSETS "Cannot be consumed; nor can it generate income. Nevertheless, it has value; it is a store of value asset."
EQUITIES	X		
BONDS	X		
INCOME-PRODUCING REAL ESTATE	X		
PHYSICAL COMMODITIES (e.g., grains or energy products)		X	
PRECIOUS METALS (e.g., Gold)		X	X
CURRENCY			X
FINE ART			X

Table 1 Categorization of traditional asset classes by their superclass. Source: "What is an asset class anyway?" Robert J.Greer 1997, The journal of Portfolio Management

Bitcoin valuation is around $185 billions *(Coinmarketcap, 2018),* nevertheless its classification confuses the majority of the expertises around the globe. The Commodity Futures Trading Comission classificates Bitcoin as a commodity, the Internal Revenue Service assures it is property. On the other hand, the U.S Securities Exchange Comission does not have a general classification, approaches Bitcoin on a case-by-case basis *(McKenna, 2017).*

Based on Greer´s study (1997), ARK Invest and Coinbase defined four characteristics that help defining traditional asset classes: investability, politico-economic features, correlation of returns or price independence and risk reward profile. An asset class needs to be significantly investable, providing enough liquidity and opportunities for investors. Moreover, it is considerable important that it has a different politico-economic profile that arises from its governance, basis of value and use cases. Furthermore, assets should exhibit low correlation regarding returns, their market value must change independently of other assets in the market. All those characteristics mentioned before, should guarantee a differentiated risk-reward profile, which can be described as volatility associated or absolute returns *(ARK Invest and Coinbase, 2017).*

6.1. Investability

ARK Invest and Coinbase define investability as opportunities for investors to invest in an asset which has enough liquidity. Investors are able to evaluate the liquidity of bitcoin, through bitcoin exchange traded volumes *(ARK Invest and Coinbase, 2017).* As shown in figure below, from February 2016 until January 2018 there was a huge growth regarding transactions volume. Transactions averaged $1.5 billions in 2016 and around $2 billions in 2017, which represents a 33,33% increase.

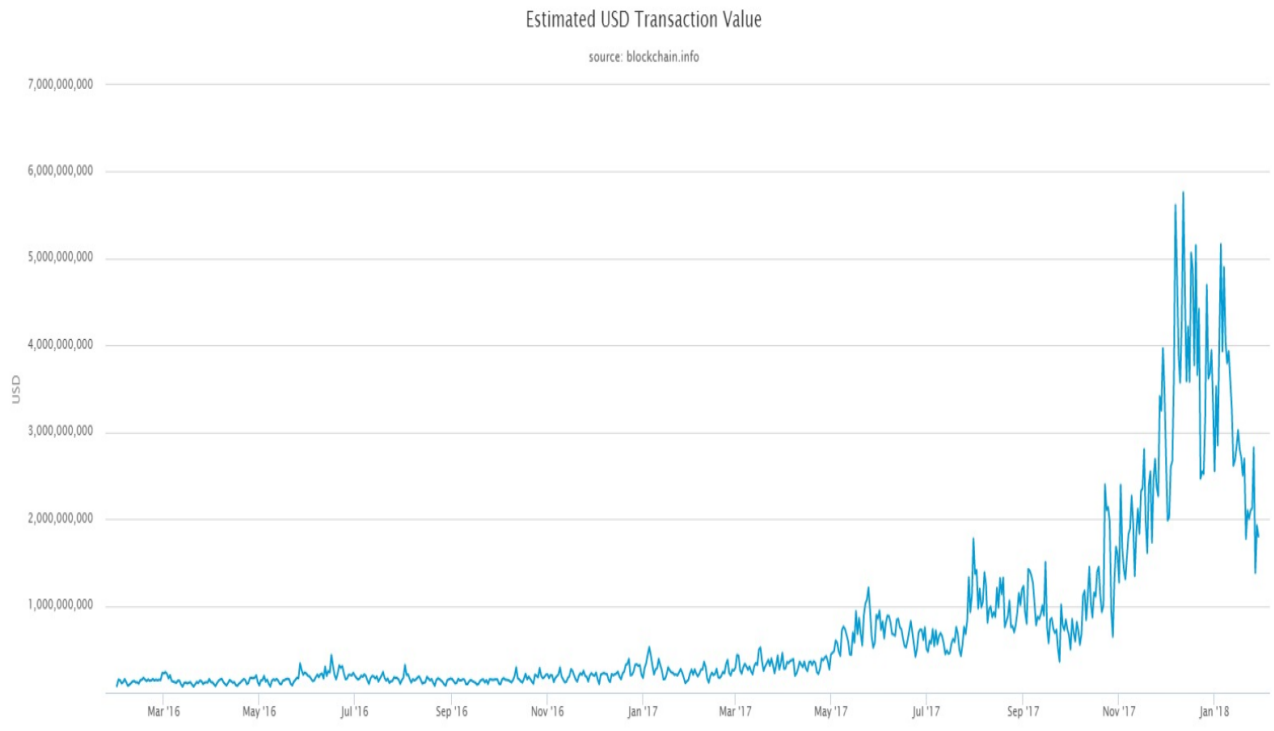


Chart 5 Bitcoin transaction volume in USD, Source: Blockchain.info

Nevertheless, from October 2016 till the end of 2017 there has not been a proportional explosion in transactional volume when comparing to bitcoin´s value. As per figure shows, the number of daily transactions has remained constant. On the other hand, bitcoin´s value has amazingly increased (*Credit Suisse, 2018*).

Trading, which is oriented to a short-term perspective, represents only half of the investability possibilites,. Many investors are retail holders, as per figure shows, they invest with a different perspective in comparison with traders, they are long-term oriented and seek rises in bitcoin valuation.

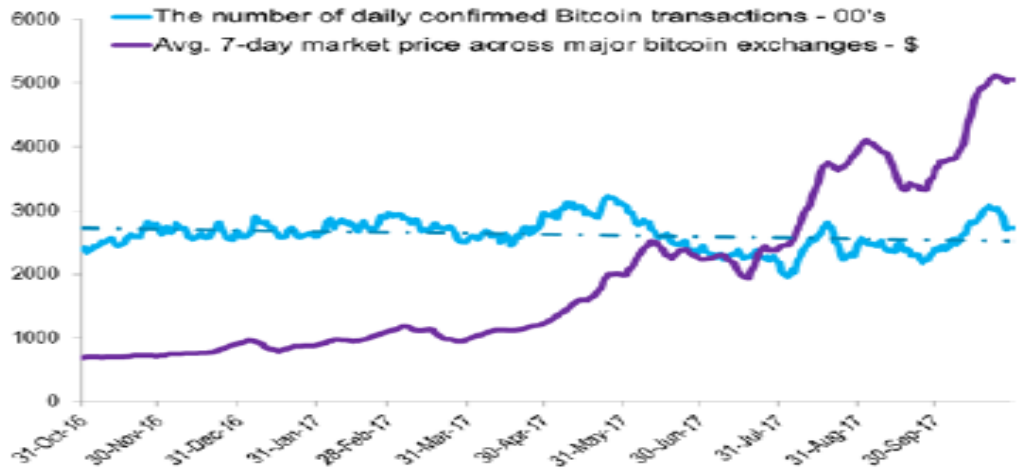


Chart 6 Daily transaction volume vs Bitcoin Value in $, Source: Credit Suisse Paper

From 2012 to 2016, as per graph 7, users on Coinbase were using it mainly as an investment, this means as long-term investors. Coinbase is the securest exchange and according to ARK Invest and Coinbase study, in the beginning of 2017 it stored over a billion dollars of bitcoin *(ARK Invest and Coinbase, 2017)*. Assuming that transactors and investors hold almost the same amount of bitcoins, between 50% - 60% of bitcoin worldwide is strictly storage of value. Bitcoin was originally designed as an online payment system, whereas transactions could be sent directly from one party to another, without relying on third-parties. Nevertheless, its tremendous success and the rise in value undermine the utility of bitcoin as a medium of exchange, because it is worth to hold it instead of making transactions with it. The intrinsic characteristics of the bitcoin, especially the supply cap and protection from inflation increased the perception among investors that bitcoin can be seen as a storage of value, just like gold *(ARK Invest and Coinbase, 2017).*

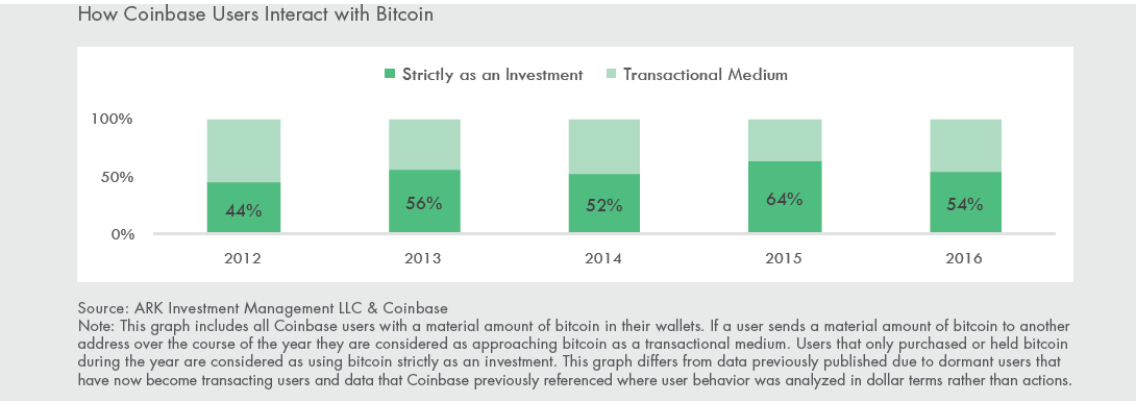


Chart 7 Coinbase Users Interaction with Bitcoin, Source: ARK Investment Management LLC & Coinbase

Moreover, according to ARK Invest and Coinbase study, more than 10 million people around the world currently own bitcoins *(ARK Invest and Coinbase, 2017).* Assuming a world population of 7,5 billions at the time of the study, bitcoin market has penetrated around 0,14% of the global population (*Worldmeters.info, 2018*). It is quite impressive the potential of cryptocurrencies, the number of holders is able to expand significantly and provide a positive impact over the investability within this unique asset class.

Centralisation is a key aspect in order to examine bitcoin´s investability. According to a Credit Suisse estimation, 4% of all bitcoin addresses hold 97% of all bitcoin (*Credit Suisse, 2018).* The concentration of wealth surrounds a small group of addresses. Key players can have massive influence on the market, however, each address represents more than one individual. Bitcoin wallets and exchanges which hold currency for enormous number of people often have just one address for specific groups *(Credit Suisse, 2018).* Therefore, the author tends to suggest an illustrative rather than an actual analysis.

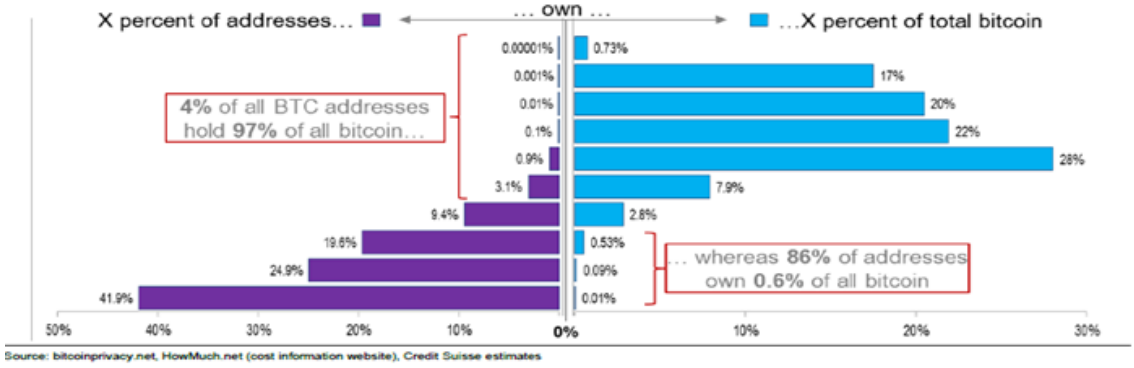


Chart 8 Bitcoin holders percentage, Source: bitcoinprivacy.net, Howmuch.net (cost information website), Credit Suisse estimates

Bitcoin is not the most liquid asset in circulation, nonetheless it is quite impressive the developments of the industry over the past years. Investors have the opportunity and tools to drive billions of dollars in daily liquidity.

6.2. Politico-Economic

Other major characterist of an asset class is driven by its politico-economic profile, based on its basis of value, use cases and governance.

6.2.1. Basis of Value

Bitcoins value proposition relies in basic economics: scarcity, utility, supply and demand. Just like gold, bitcoin is scarce. There is a supply cap of 21 million bitcoins and as per figure shows, there are almost 17,5 million in circulation. Moreover, bitcoin has utility, it can be used as a mean of exchange, it can facilitate transactions of all kinds. This tends to suggest that as more infrastructures is built around bitcoin and more developments are made on its technology, demand and price of the cryptocurrency will increase.

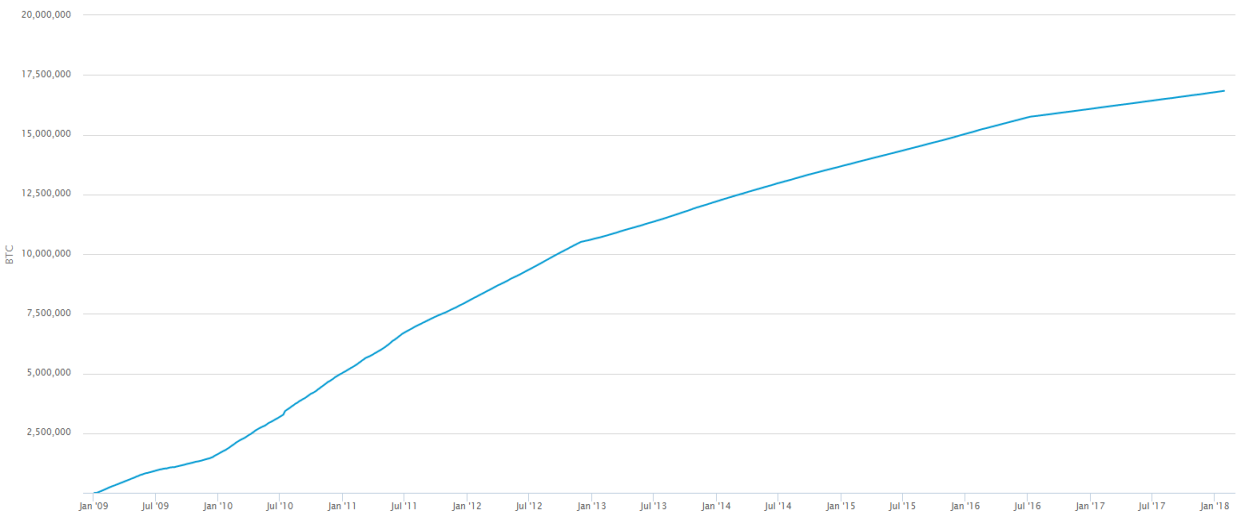


Chart 9 Bitcoins in circulation at the end of January 2018, Source: Blockchain.info

6.2.2. Governance

As it was shown previously in this paper bitcoin´s basis of value is unique, but on the other hand, its governance is quite different, it can be seen as a game changer. Bitcoin transactions do not rely on a third-party, such as banks. As the author explained previoulsy, through a decentralized and open network, all nodes are able to verify and validate transactions. Unlike fiat currencies, which are governed by monetary policies that can lead to supply shocks, bitcoin has its own characteristics that provide inflation resistance and a fixed number of coins available in the market.

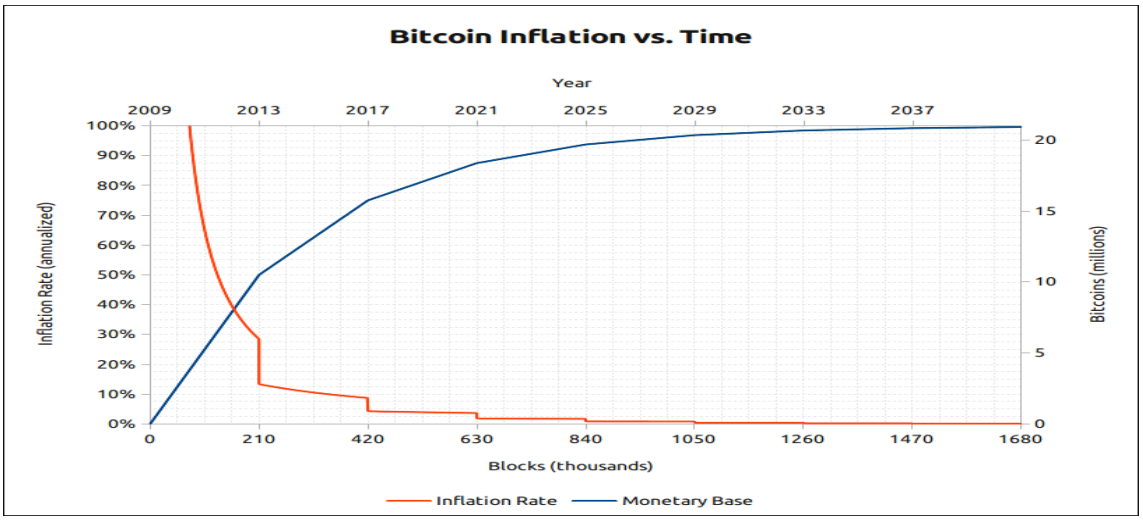


Chart 10 Bitcoin inflation resistance

As ARK Invest and Coinbase witnessed no asset has evolved so quickly as bitcoin did. Furthermore, no asset has followed a predictable supply trajectory as bitcoin is following, it has evolved from a concept to a billion dollar business in 10 years *(ARK Invest and Coinbase, 2017)*.

6.2.3. Use Cases

Bitcoin´s applications have tremendous potential. Since it was invented, investors and entrepreneurs in several industries across the world have come to understand the impact and implications of this development.

As it is going to be further developed in this paper, blockchain technology can have a positive impact in several industries. As a platform it can be used to develop smart contracts, automated governance for markets. Moreover, as a system of record it can enhance digital identity, tokenization, inter-organization data management, audit trails.

6.3. Correlations of returns:

Since bitcoin has unique politico-economic characteristics, its price is going to be affected by different market forces, thus it is expected that bitcoin´s price will behave differently when comparing to other assets.

According to Bernstein, correlation is a standardized that measures the relationship between two different assets in the same market conditions *(Bernstein, 2018)*. It ranges from +1 to -1, therefore if two assets are perfectly correlated at "+1", then when one asset increases 5% the other will also up by 5%. On the other hand, if they are

negatively correlated at "-1", whenever one asset decreases by 5%, the other will also be down by the same 5**%** *(ARK Invest and Coinbase, 2017)***.**

As per table 2, assets that are perfectly correlated, the least diversification they are able to provide and therefore no risk reduction is possible. On the other hand, negatively correlated assets provide a more diversified portfolio and risks can be substantially reduced. Assets that have zero correlation are not tied in their market behavior, which ARK Invest and Coinbase suggested was fundamental to consider bitcoin as a completely novelty asset *(ARK Invest and Coinbase, 2017).*

CORRELATION COEFFICIENT	EFFECTS OF DIVERSIFICATION ON RISK
+1.0	NO RISK REDUCTION IS POSSIBLE
+0.5	MODERATE RISK REDUCTION IS POSSIBLE
0	CONSIDERABLE RISK REDUCTION IS POSSIBLE
-0.5	MOST RISK CAN BE ELIMINATED
-1.0	ALL RISK CAN BE ELIMINATED

Table 2 Correlation Coefficient and effects of diversification on risk, Source: A Random Walk Down Wall Street, Burton G. Malkiel, 2015.

ARK Invest and Coinbase performed a study, whereas they calculated the one year rolling correlation between the various assets from 2011 to 2016. As per table, bitcoin is consistently the only asset that maintains low correlations with the others. Moreover, the maximum correlation, which includes positive or negative, that bitcoin performed was near the minimum correlation that any pair of assets displayed with each other *(ARK Invest and Coinbase, 2017).*

Furthermore, as Bernstein suggested diversification among assets with low correlation is fundamental in order to pursuit long-term profitability. Thus, poor performance regarding one investment can be easily offset by better performance in another asset. Therefore extreme losses in a portfolio with low correlated assets may be reduced *(Bernstein, 2018).*

	S&P 500	US Bonds	Bitcoin	Gold	US Real Estate	Oil	Emerging Market Currencies
S&P 500		-0.67	0.35	0.48	0.87	0.73	0.83
US Bonds	-0.67		0.28	0.53	0.59	-0.52	0.57
Bitcoin	0.35	0.28		-0.51	-0.39	-0.37	0.27
Gold	0.48	0.53	-0.51		0.45	0.52	0.62
US Real Estate	0.87	0.59	-0.39	0.45		0.63	0.74
Oil	0.73	-0.52	-0.37	0.52	0.63		0.63
Emerging Market Currencies	0.83	0.57	0.27	0.62	0.74	0.63	

Low correlation (-0.4 to 0.4) in green, Mid correlation (absolute value 0.4 to 0.666) in white, High correlation (absolute value > 0.666) in red
Numbers in the table were chosen based on the maximum "absolute value" one-year rolling correlation that paired assets displayed since 2011

Chart 11 Correlation table between different assets. Source: ARK Investment Management LLC & Coinbase, data sourced from Bloomberg & Coindesk BPI

6.4. Risk Reward Profiles

In this section, a comparison between the risk in the form of volatility and reward in the form of absolute returns is going to be established. Sharpe ratio measures returns per unit of risk taken, when comparing risk and reward in the forms mentioned above. (*Investopedia, 2018*).

6.4.1. Volatility

Volatility regarding bitcoin´s price is clear since it was founded, as chart 12 shows.

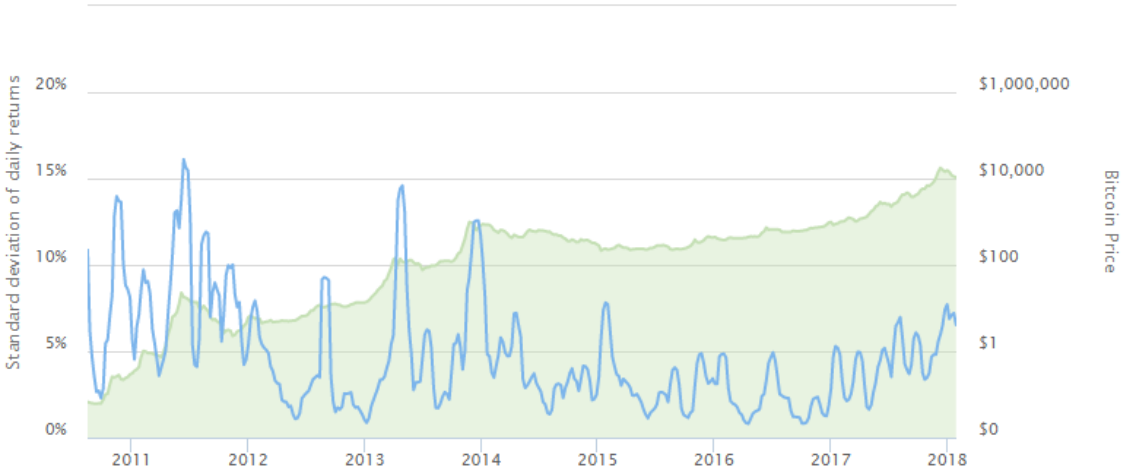


Chart 12 Bitcoin Price and Volatility over time, Source: https://www.buybitcoinworldwide.com/volatility-index/

According to ARK Invest and Coinbase, investors tend to measure volatility via the standard deviation of daily returns as it was considered in figure (*ARK Invest and Coinbase, 2017).* Bitcoin price has had dramatic swings, nevertheless it is possible to understand that since its creation the volatility has been decreasing. As figure shows, standard deviations of daily returns ranged mostly between 2,5% - 7,5 % a day, which is quite impressive when comparing to the previous years.

Chart 13 Bitcoin Volatility Index in 2017, Source: - https://www.buybitcoinworldwide.com/volatility-index/

Although Bitcoin´s volatility has been considerably decreasing, it is still the most volatile asset class, as shown in graph 14. However, it is possible that it may not remain the most volatile one for long, since its volatility is decreasing over the years.

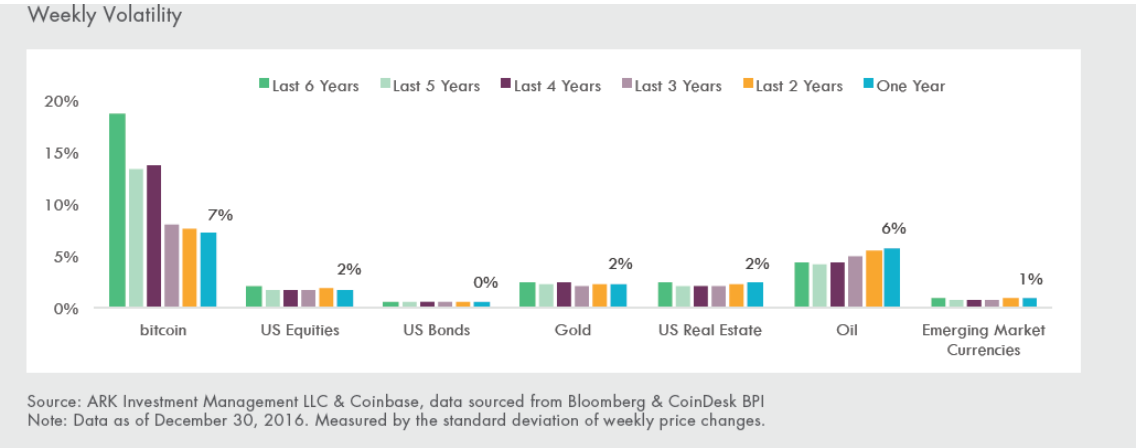


Chart 14 Bitcoin weekly volatility over the last 6 years. Source: ARK Investment Management LLC & Coinbase, data sourced from Bloomberg & Coindesk BPI

6.4.2. Absolute Returns

Since its creation, bitcoin provided incredible returns to its investors, above and clearly beyond every asset available on the market. As per chart 15 illustrates, bitcoin provided a 212% compound annual return on invesment since Facebook was launched public on 2012.

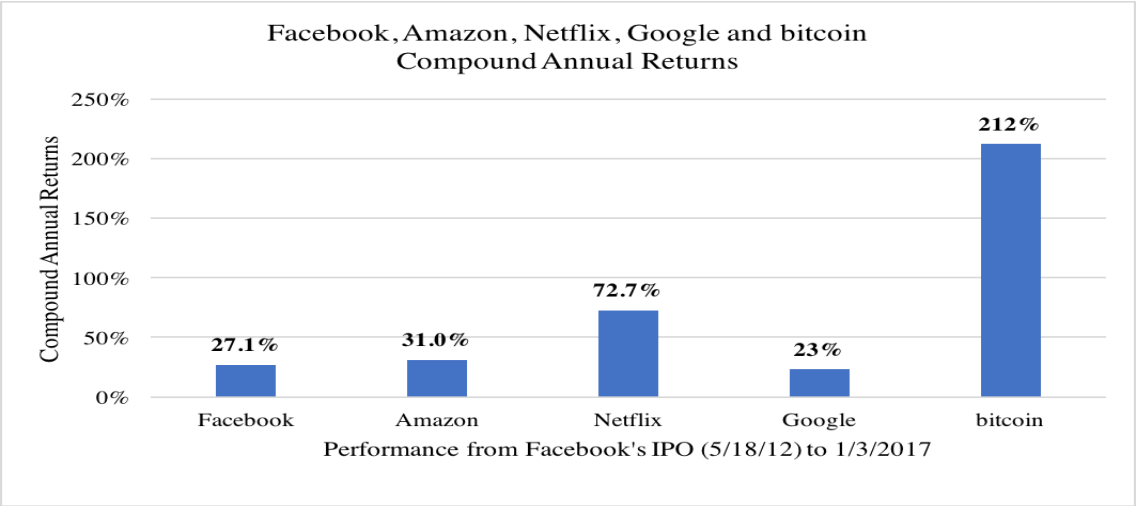


Chart 15 Bitcoin versus Facebook Annual compound returns, Source: bitcoinist.com

Comparing bitcoin´s returns with the other major asset classes, if an investor had invested $10,000 in bitcoin back in 2011, it would worth at the end of 2016 nearly $2,3 million and at the end of 2017 (price on 31 Dec) an incredible $138,604 millions.

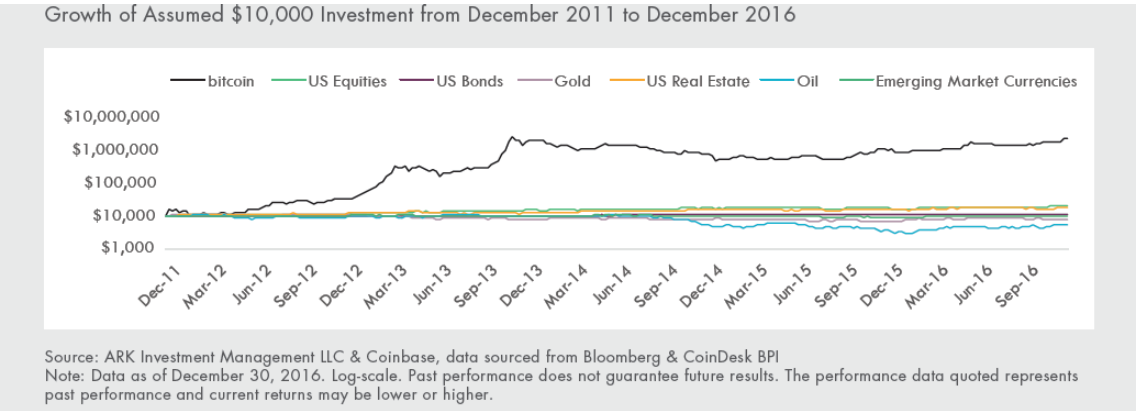


Chart 16 Growth of assumed $10,000 investment from 2011 to 2017 in different assets, Source: ARK Investment Management LLC & Coinbase, data sourced from Bloomberg & Coindesk BPI

Modern portolio theory indicates that neither volatility nor absolute returns are complete enough in order to define a good investment. Thus, an investor needs to adjust absolute returns for the amount of volatility, or risk, so that it calculates the adjusted returns *(Elton et al., 2014)*.

Sharpe ratio is the best measure and can be defined as the average return in excess of the risk-free rate per unit of total risk or volatility of the asset. Assets with higher values regarding Sharpe ratio are those who compensate better their investors for the risk they are taking *(Investopedia, 2018)*. As per graph 17, bitcoin Sharpe ratio has been superior

regarding the other asset classes. Besides its volatility, bitcoin returns have compensated and therefore outperforming the competition in what concerns profitability.

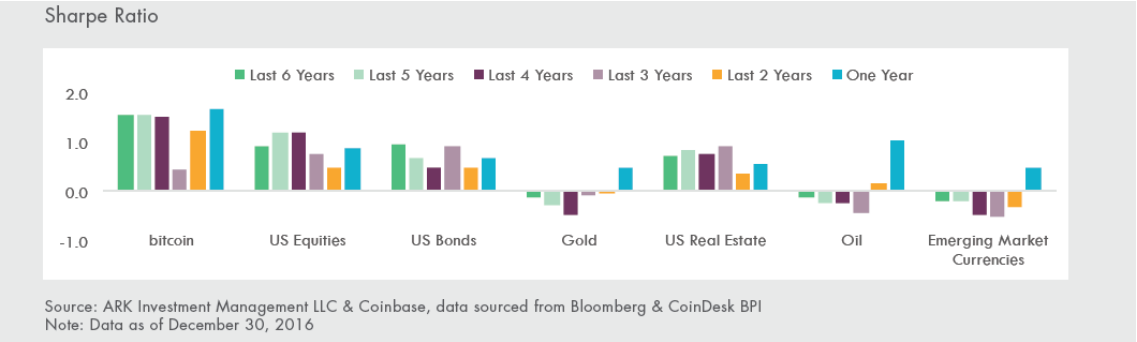


Chart 17 Sharpe ratio , Source: ARK Investment Management LLC & Coinbase, data sourced from Bloomberg & Coindesk BPI

7. Bitcoin Classification

Money is usually described as a unit of account, medium of exchange and also as a store of value. Bitcoin can be used in the same way as traditional money and there is one major characteristic that turns this digital currency even closer to traditional money rather than fiat currencies. Bitcoin is counterfeit-proof by design, on the other hand, traditional money can be faked *(Medium, 2017).* Nevertheless, all parties need to declare it as money. Bitcoin needs political approval in order to have the status of a currency. Nowadays, money in the sense of currency relies on third-parties such as banks or governments, even though most people accepted bitcoin as money, it cannot be considered a currency, unless governments approve it as so *(Medium, 2017).*

The constant volatility around bitcoin, the wild swings, both up and down in value make it a speculative asset rather than a more plausible currency. Besides the approval of governments, there are several concerns that bitcoin needs to improve in order to be considered as an actual currency: unstabilitity of its value and the slow transaction processing.

One of the major features of a currency is its stable store of value. According to Forbes the role of an investor in a developing country is risky enough. Moreover, if the risk is compounded by uncertainty over the value of the currency from which future income streams flow, there will be even more risk-taking**.** Bitcoin is still too volatile to be perceived as a currency *(Forbes India, 2015).* The author suggests Zimbabwe´s example in order to understand the impact of volatility.

7.1. Are Cryptocurrencies able to solve Zimbabwe´s hyperinflation problem?

Zimbabwe government decided to adopt US Dollars when hyperinflation had driven the local currency into a near bottomless grave. Currently, Zimbabwe is slowly running out of US Dollars. The major economic concerns of the country are as follows:

- Zimbabwe´s Governement spends more money than it can collect and finance the remaining difference by forcing local banks to buy treasury bonds from them.

- Since Zimbabwe adopted US Dollars, banks are forced to lend US Dollars to the Zimbabwean Government. Therefore, this tends to suggest that it is necessary to analyse the Balance of Payments of the country.

- On the BoP front, Zimbabwe spends more on imports than Exports. Extra needed was being covered by inward foreign loans;

The collapse of the country occured when the commodity cycle turned and Zimbabwe started to win less money from their mining exports. Currencies of Zimbabwe´s neighbours weakened, therefore Zimbabwean manufacturing companies become less competitive. In those countries, the diaspora might have been sending the same amount of locally-denominated money to Zimbabwe, nevertheless it become significantly less in US Dollar terms. A drought also occured and exports become lower than expected. Zimbabwe was facing a hyperinflation issue and erratic government policies meant that foreign loans dried up. Since Zimbabwe adopted the US Dollar as its major currency, it is possible to compare the differences among wages between a south african and Zimbabwean miner according to the following table:

Year/Monthly wage in $	Zimbabwe	South Africa
2012	1,430 USD	770 USD
2017	1,430 USD	1,430 USD

Table 3 Comparison between Zimbabwean and South African wages in $ between 2012 and 2017, Source: Own drawing

Zimbabwean productive industries found themselves unable to compete with the flood of cheap imports, higher costs regarding extractions rendered their mining shafts unprofitable and foreign investors prefered to invest their money elsewhere, where inputs were cheaper, like South Africa. All these actions tend to suggest that if Zimbabwe had had its own currency, then it would have weakened alongside their

neighbours´currencies and the country would be more competitive than it is with US Dollars. Zimbabwe´s Government was the major issue, their policies ruined the country. For example, regarding the wages a good measuere was to slash the wages and attract investors to their mining shafts. Nevertheless, Zimbabwe law forbids slashes on wages.

Cryptocurrencies demand increased a lot in Zimbabwe. But could it be the solution to the hyperinflation problem? Taking on the Wages Example between South Africa and Zimbabwe:

As table shows 4, in 2017 Zimbabweans would be earning 600x more than South African if they implemented bitcoin as major currency. Bitcoin can be a useful asset for Zimbabweans in terms of store of value. Nevertheless it is completely unnafordable as a currency. It is still too volatile and in an emerging country like this its strictly necessary to have a stabilized government and currency. There are several issues on emerging countries such as Zimbabwe, cryptocurrencies may help people having an easy way to access markets and financial services, and nevertheless it is still dificult to replace a fiat currency for bitcoin.

Year / Monthy Wage in BTC	Zimbabwe	South Africa
2012	119 Btc	119 Btc
2017	119 Btc	0,19 Btc

Table 4 Comparison between Zimbabwean and South African wages in bitcoin between 2012 and 2017, Source: Own drawing

In developed countries happens the same, investors require a stable currency, because they expect a stream of future earnings to earn back their investment plus some profit. The volatility that is currently associated to cryptocurrencies, means that investors cannot accurately predict their future earnings. Therefore, the uncertainty associated makes investments less valuable, so investors are not willing to invest more *(Forbes, 2017).*

Bitcoin can improve developing countries, by facilitating access to basic financial services. This is a measure to prevent world's poorest countries isolation regarding financial trades and commerce. Almost 64% people living in emerging or developing countries lack access to basic financial services, such as credit, savings and insurances. Thus, the lack of access due to higher costs for tradicional financial institutions led people in those countries to seek other solutions, such as mobile banking services *(Brito*

and Castillo, 2016). Developing countries such as Kenya, Tanzania, and Afghanistan adopted a closed-system mobile payment known as M-Pesa.
M-Pesa is a form of electronic money that allows consumers to use their mobile phone, besides that it helps unbanked people to have access to financial services at significant lower costs because it is not necessary physical infrastructures *(CNBC Africa, 2017).* According to a study from Sun and Jack, the increased access to mobile phone reduced poverty in Kenya, especially among females *(Suri and Jack, 2016).* Therefore, bitcoin as an open-system payment service can augment the mobile banking services in those countries. People would have access to financial services with no costs on a global scale. The intrinsic characteristics of bitcoin allow those countries to freely transact with others, because there is no manipulation on the supply of coins, there is no central authority that forbides or prevent transaction to occur. People who desire alternatives to their country´s devalued currencies and/or limited access to captal markets have a great opportunity with the bitcoin system. Moreover, bitcoin provides privacy which is very important to individuals in oppressive or emergent countries *(Brito and Castillo, 2016).*
The other major concern mentioned above is the transaction processing. As it was developed, transactions are very complex in bitcoin network. In order to be validated and recorded in the public ledger it takes about 10 minutes. Thus, the dynamic regarding transactions processes that were set by Satoshi Nakamoto had the intention to slow the transaction down time, so that it could be able to prevent hackers to obtain advantage. Moreover, bitcoin fees are measured in Satoshi's per byte of data that is transmitted. Since Satoshi represents a fraction of a bitcoin, if the price goes up then the fee will also increase. Therefore, in day to day purchases it is quite difficult to use bitcoin as a medium of exchange. Besides the 10 minutes wait to confirm your transactions, you will also be charged for a fixed fee that is proportionally to bitcoin´s price.

Given these drawbacks regarding the transaction processing and volatility on its value, the perception of Bitcoin as a currency is still far. Investors speculate on its value or use it to shield transactions from others. In order to be a currency, bitcoin needs to have a stable value. Nowadays, it is a commodity asset that one trades in hopes that its value will rise and therefore yield some profits. Speculation helps to add market liquidity and to determine the value of assets, there is nothing wrong with speculators *(Forbes, 2017).* Kevin O´Leary considered Bitcoin one of the most sucessful assets on the planet

because it is perceived as global speculation. According to Mlyin CNBC bitcoin unlike a currency, which is used to assign and exchange value, has inherent value based on what people are willing to pay for it *(Montag, 2017).* Bitcoin offers advantages over assets such as gold, because it was designed to be a payment system, it is portable and divisable as mentioned before. Although, there are still few companies, stores, marketplaces that accept Bitcoin as a medium of exchange when comparing it to fiat currencies *(LaVere, 2017).*

Perception that bitcoin community has over the future of the cryptocurrency is relevant to take under consideration. Thus, if the community wants Bitcoin to perform as a currency then it is important to develop the transactional processing and allow transactions to be validated much faster. It is also required to pressure companies to accept bitcoin as a medium of exchange. On the other hand, if the community perceives and wants bitcoin to be seen as an asset, then the major goal it is to increase awareness and market capitalization *(LaVere, 2017).*

The strenght of bitcoin is its ability to work as both asset and money. Due to its scarcity, the value of bitcoin is expected to continue to grow. As Wences Casares mentioned Bitcoin will behave as an asset until it reaches market saturation. Whenever, the market reaches the 21 M cap supply, prices will stabilize and payment services will be much easier, allowing bitcoin to work as a currency *(LaVere, 2017).*

As Selgin proposed, bitcoin falls somewhere between commodity money and fiat money, a category called synthetic commodity money. It does not require a central authority to create macroeconomic stability by being adjustable *(Selgin, 2012).* As it was developed by the author, bitcoin acts as both a currency and an asset. Its classification is quite dubious, nevertheless it cannot be considered a currency due to the lack of regulation, volatility and also transaction processing. It is a unique asset class, which meets the bar of investability and stands out from the other asset classes in terms of price independence, risk reward and politico-economic profile characteristics. The constant development of bitcoin´s open source software will enhance the differentiation that this asset class has regarding the others. According to ARK and Coinbase study, bitcoin is the first of its kind and represents a unique asset class *(ARK Invest and Coinbase, 2017).*

8. Methodology

The autor suggests that the research in this dissertation is built upon a deductive approach, therefore existing researches, industry reports and theories are used to examine the topic that is being studied.

In the first part, quantitative research follows a form of a survey aimed at bitcoin community. Based on results previously obtained from literature review, several questions were prepared in order to better understanding the perception around bitcoin and its future. Afterwards, in order to have a deeper insight into the topic a qualitative research in form of interviews was conducted. The intervieews are experts in the industry, people that have influence and ability to provide their opinion regarding the topic being discussed. With this approach, it is possible to have a more objective perspective around bitcoin and its characteristics.

Data Collection

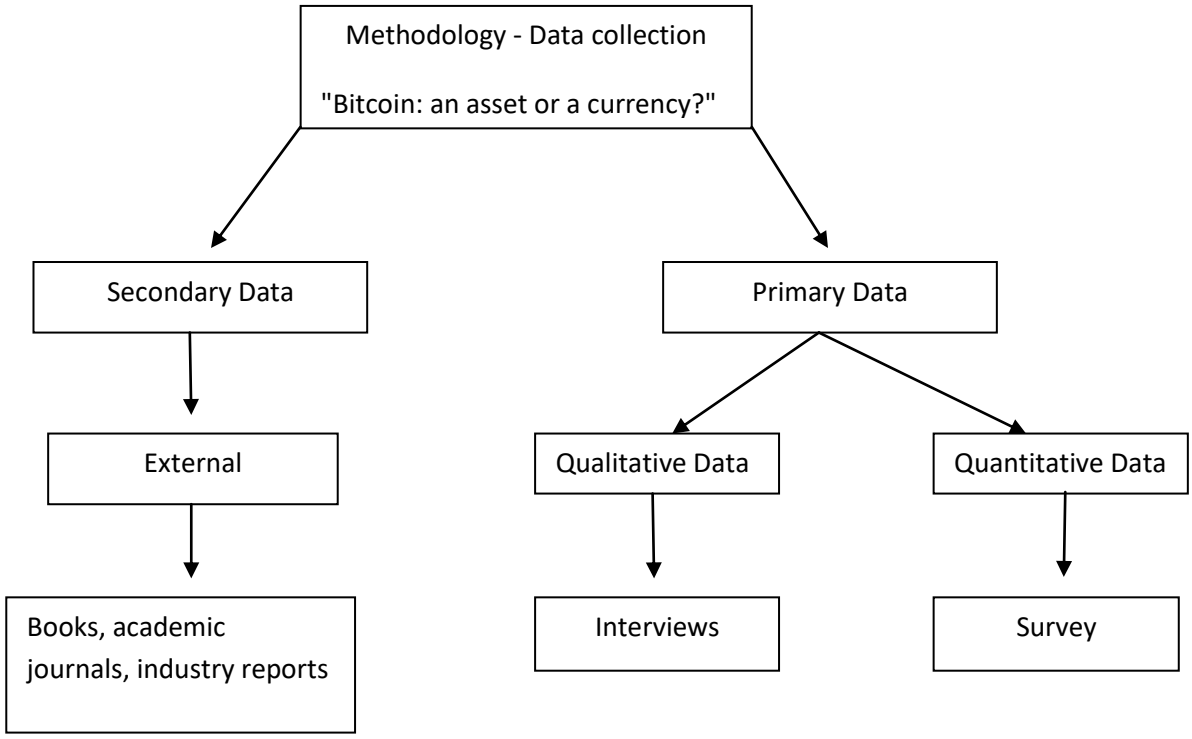


Fig 4 Summary of the data collection, Source: own drawing

8.1. Survey Analysis

8.1.1. Objectives

A survey was conducted in order to facilitate the process of making some assumptions about bitcoin classification *(Appendix A)* . The survey for this thesis was conducted among 110 adults worldwide, during March 2018. It is important to state that the price of bitcoin decreased a lot during that month, therefore it might had influenced some of the answers by the respondents.

The report covers a wide range of opinions regarding bitcoin. About 40 people that filled out the questionnaire are programmers and developers of a consultancy firm called InnoWave Technologies. Moreover, 50 responses were extracted from Bitcoin network groups, which mean that those people understand the concept and try to keep up as much as possible with the latest news and informations about the cryptocurrency market. Finally, the remaining 20 answers were provided by other Masters in Management students worldwide. The author tried to reach a different audience, so that the results were unbiased. The sample is quite small, nevertheless the author suggests that the majority of the people that filled the questionnaire are aware of the cryptocurrency market and understand about the blockchain technology.

The author suggests that a survey analysis might be helpfull in order to easily classificate bitcoin and better understand the perception about cryptocurrency market among the population.

8.1.2. Key Findings

Firstly, it was important to understand the perception of the inquiries about bitcoin. Thus, question *"Have you ever heard of bitcoin?"* was strictly important in order to affer the relantionship between respondents and the topic analysed. Since the sample was chosen in order to have the most addequate and accurate results it was expected that the majority of the inquiries had heard of bitcoin.

90% of the respondents have heard of bitcoin. According to Chen et al, a hot topic can be defined as a topic that appears frequently in different platforms over a certain period of time. It is classified as hot based on two factors: the frequency that it appears in a document and also the number of documents that cointain those terms. There is a life cycle of birth, growth and maturity *(Chen, Luesukprasert and Chou, 2007).* The author tends to suggest that bitcoin is a hot topic and its concept is still evolving and growing

over the media, newspapers, TV broadcasts. The table shown below, that was extracted from Google Trends illustrates the popularization of bitcoin regarding searches on the web. Interest over time has been increasing, nevertheless the huge drop that occured in the beginning of 2018 that may be associated to the price reduction of the cryptocurrency.

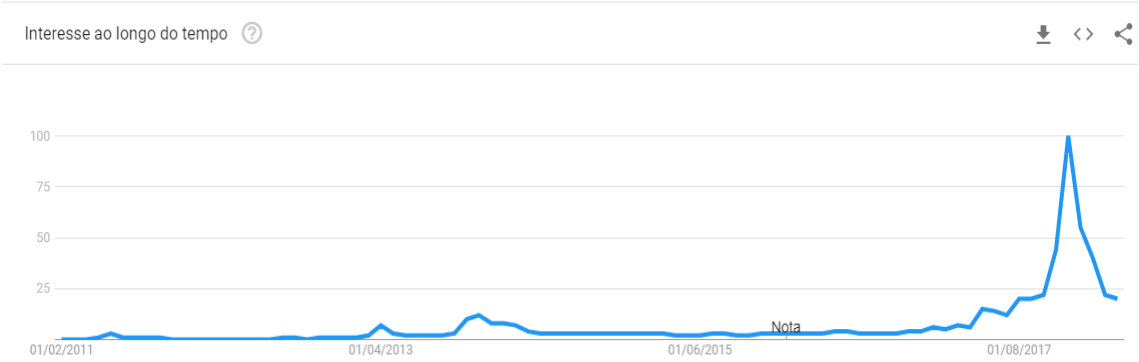


Chart 18 Bitcoin interest over time, Source: Google trends

Furthermore, around 31% of the inquiries have invested in bitcoin. Besides its popularization, these results can emphasize the uncertainty that is associated to the concept of cryptocurrencies, people are relutant to invest their money in a concept that is still evolving and that is not defined yet.

From the 34 respondents that invested in bitcoin, the majority did it because they believe that bitcoin is a disruptive technology, for trading purposes or even as a storage of value. It is quite interesting that only 8% of those who invested did it for transactions purposes. These results show that investors believe that bitcoin is a new concept that can change some business models. Blockchain has a tremendous potential, almost 55% of the respondents believe that bitcoin is a disruptive technology. Of course there is a linkage between this belief regarding bitcoin as a disruption of the current business models and its prices. Therefore, 60% of the respondents invested for trading purposes, because they believe that bitcoin prices will continue to rise.

Moreover, only 24% of the investors have sold some or all of their bitcoins. These results support the idea that bitcoin concept is still growing. As it was concluded before in this survey analysis, the majority of the respondents that invested in bitcoin did it for

trading purposes. Nevertheless, only 24% of them have sold their bitcoin. These numbers show that for those investors bitcoin still didn´t reach the potential that it is able to reach in a long-term perspetive. Therefore, 76% of the inquiries that invested in bitcoin still hold their coins, because as mentioned above they believe it is a disruptive technology or a storage of value.

Since 76% of the inquiries still hold their bitcoin, it was important to understand at what prices respondents were willing to sell their bitcoin. As mentioned before, this survey took place during March 2018. Since prices of bitcoin faced a constant decrease during the period of conduction of the survey, probably inquiries were influenced by those events. Around 36% of them assured they were able to sell their bitcoin between $1,000 and $10,000. These results may be influenced by the constant price decreases that bitcoin has faced during 2018. Furthermore, those results also show the fear and uncertainty that surrounds bitcoin community. Investors are relutant regarding bitcoin future, therefore they are willing to sell their investment right away. Around 34% are willing to sell between $10,000 and $50,000. It supports the idea that a great percentage of bitcoin investors invested due to their belief regarding future price increases. The remaining 30% indicated that they were willing to sell their coins only for prices above $50,000.

The results show the uncertainty regarding bitcoin prices. However, majority of the respondents, around 64% of the inquiries are willing to sell their bitcoin for prices above the $10K, which supports the belief that bitcoin has potential to continue to grow in the future.

Although, there are several cryptocurrencies that have different features when compared to bitcoin that have great potential to succeed, not only as a possible currency but also as investment purposes the major focus of this study relies on bitcoin. Besides the great competition that bitcoin faces, around 63% of the respondents invested only in bitcoin, which emphasizes the confidence that the majority of the investors have in the major cryptocurrency regarding market capitalisation. Nevertheless, 37% it is a relevant number that suggests investors are seeking alternatives and looking into other cryptocurrencies. According to Hileman and Rauchs although bitcoin remains the dominat cryptocurrency regarding market capitalisation, other cryptocurrencies are surging into bitcoin´s market share *(Hileman and Rauchs, 2017).* Bitcoin market

capitalisation accounted for 86% of the total cryptocurrency market in March 2015, however it has dropped to 80% in March 2016, to 72% in March 2017 and to an incredible 40% in March 2018 *(Coinmarketcap.com, 2018)*.

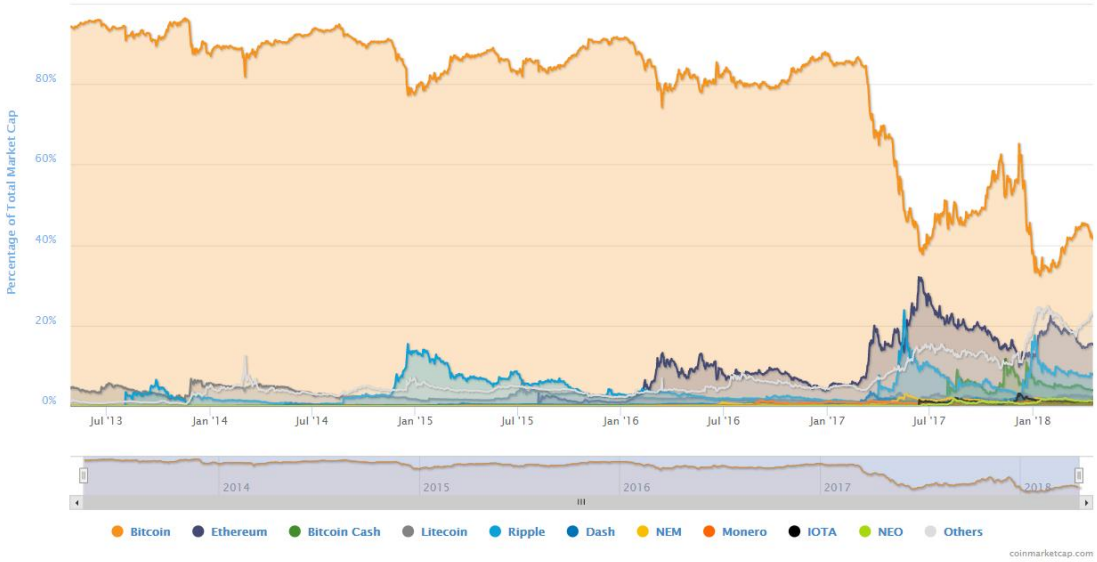


Chart 19 Cryptocurrencies market capitalisation, Source: Coinmarketcap.com

The results shown in the previous chart can be supported by the results extracted from the question *" In 10 years do you believe that Bitcoin will be the largest cryptocurrency regarding market capitalization?"*, whereas 60% of the respondents believe that bitcoin will no longer be the largest cryptocurrency regarding market capitalization. The constant growth regarding bitcoin competitors' such as Ethereum, Ripple and Litecoin suggest that one of them will problably surpass bitcoin regarding market capitalization in the upcoming years.

Moreover, 45,5% of the respondents believe bitcoin is a macroeconomic tool hedge against monetary policy. On the other hand, 28,2% don´t know the answer and the remaining 26,4% believe bitcoin is not a threat to the current monetary policies. Once again, uncertainty surrounds respondents. Almost 50% of the inquiries believe in the power of bitcoin as a disruptive technology to have an influence against current monetary policies. Although, more than 50% expect or are not sure about the future of the cryptocurrency when relating it with the current monetary policies.

As developed before regulation is one of the most important issues that need to be addressed. 44% of the respondents believe that increased regulation and oversight by several governments could be benefic. Hence, there is a trade-off between the purpose

of bitcoin´s community and its regulation, because with an increased regulation and oversight by governments bitcoin would not be a peer-to-peer electronic system and would rely on a third-party. That was not the purpose of the creation and it is an issue that needs to be solved, so that bitcoin can become more sustainable and less volatile.

Finally, around 53% of the respondents believe that bitcoin is not able to become a currency such as US Dollar or Euro. Those results are quite impressive, it shows the potential that respondents recognize regarding bitcoin, because 47% believe that bitcoin will be able to become a currency. Those who do not believe, stated that competition from other cryptocurrencies, volatility and transaction processing are probably the major reasons that will prevent bitcoin from becoming a currency accepted worldwide such as Euro or Dollar.

It was previously mentioned in this survey analysis that only 8% of the respondents that invested in bitcoin did it for transaction purposes. However, 47% of the respondents believe that bitcoin is able to become a currency. Those results are quite inconsistent and tend to emphasize the confusion that surrounds bitcoin community. In a short-term perspetive, bitcoin users seek profit by performing several trades or simply keep their coins so that in a long-term perspetive they get rewarded for that. Bitcoin holders currently do not perform as many transactions as they want because bitcoin is still not accepted worldwide and its volatility is influencing its usage.

8.2 Interviews

This section develops an overview of the industry by analysing interviews conducted with Portuguese stakeholders. The two major themes in the discussion were the general perception towards bitcoin and its future outlook. All interviews were previously prepared, guided with a set of questions that aimed to a better understanding of the bitcoin categorization and its future usage. The interviews were also conducted with different actors, from different areas, so that a broader escope of information is gathered.

8.2.1. Interviewes

The interviews were conducted between April and May 2018. All interviews were conducted in Portuguese and afterwards transcribed to English by using records. Moreover, all transcripts were previously checked and approved by each interviewee. Table below contains a list of all the interviewes and their current position.

Interviewee(s)	Organisation	Position	Appendix
Hélder Reis	Presidência da República	Consultor da Casa Civil da Presidência da República	B
Eduardo Rodrigues	REN	Senior Cybersecurity Analyst	C
José Galamba de Oliveira	Associação Portuguesa de Seguradores	President of APS	D

Table 5 Interviewes, Source: Own Drawing.

8.3. Bitcoin Perception

Generally, Bitcoin was met with a lot of interest by all interviewees. Nevertheless, there are some differences regarding their attitude towards it. Eduardo Rodrigues, Senior Cybersecurity at REN, confessed that he studied the phenomenon and even decided to invest, because he truly believes in the blockchain potential. Despite recognizing the potential that the technology has, Reis believes that bitcoin only comparison with a normal currency is that it might be used as a mean of exchange. Therefore, all the other functions of money that were developed in chapter , are not fulfilled. On the other hand, José Galamba de Oliveira, President at APS, believes that bitcoin has the potential to make transactions more autonomous and secure, but also to compete with the current international financial system that **according to him is "loosing trustworthiness among the consumers".**

Another important topic that was addresed, represented the classification of bitcoin.Among the interviewees, all of them stated that bitcoin cannot be defined as a currency yet. According to Galamba de Oliveira, bitcoin is positioned as a speculative financial asset. However, in a long-term perspective, Oliveira recognizes that if bitcoin is able to solve the volatility and regulation issues it might be considered a currency. Furthemore, Eduardo Rodrigues, believe that not only bitcoin, but all cryptocurrencies have still a long way to go before they are fully adopted by people. According to Rodrigues, the banking system is based on the same principles for decades and is quite relutant on adopting disruptive technologies on their procedures. Nevertheless,

Rodrigues states that Revolut and Monzo, digital banks, may have a crucial role in order to make bitcoin a widely accepted method of payment. Helder Reis, argues that bitcoin classification depends on the international community and its regulation. However, an interesting argument was presented by Reis. He stated that the international community, especially in Europe, has been trying to reduce foreign exchange risk as much as possible, by creating the unique currency, Euro. Therefore the acceptance of bitcoin as a currency might be seen as a significant risk and against its principles.

In what concerns regulation, all interviewees confessed that regulating bitcoin would increase confidence among consumers, but also increase the number of people that uses it. Despite being pro regulation, Eduardo Rodrigues as an investor of bitcoin, indicated that regulation could be beneficial as long as it does not strangle technology.

Although the results of the survey shown that around 45% of the inquirees believed that bitcoin is a macroeconomic tool against monetary policy, all the interviewees pointed some characteristics that prevent bitcoin from becoming a real threat to the monetary policy. Eduardo Rodrigues mentioned that cryptos might be a viable way to the banking system and he understands why countries and regulators are wary of the phenomenon, nevertheless the adoption of the blockchain and bitcoin are already in the mature phasis, therefore according to Rodrigues bitcoin is not a real threat against the current monetary policy. On the other hand, Galamba de Oliveira argues that bitcoin is too volatile and Helder Reis states that bitcoin characteristics do not fulfill the functions of money as mentioned before. Thus, bitcoin cannot be seen as an instrument of monetary policy.

Helder Reis works directly with the President of Portugal and therefore also with the Portuguese government stated that the techonology "has a lot of good things". Besides recognizing the benefits of the technology, Reis also concluded that intermediares are not necessary a problem. It all depends on the transaction costs and the safety that the intermediary is able to guarantee or not. So smart contracts might be benefical, but the current procedures are very effective in several industries according to Reis and changes are not necessary in all those fields. A more excited account was given by José Galamba de Oliveira, President of Portuguese Association of Insurances, who enhanced the tremendous opportunities that bitcoin technology may have in different industries and business models. According to Oliveira, blockchain technology might link transparent

and secure business models with organisations, consumers, employees and authorities without relying on an intermediary. He also stated that it might enhance the grownage of the Internet of Things. According to Rodrigues, there are some issues that need to be adressed such as Data Privacy, especially after the implementation of the General Data Protection Regulation, although the opportunities that blockchain technology provides are very important.

8.4. Future Outlook

Regarding the future outlook of bitcoin and its comparison to gold, there were some differences regarding the opinion of our interviewees. Galamba de Oliveira and Reis believe that the future of the cryptocurrency is kind of unknown, nevertheless it all depends on its usage as a mean of exchange. Its virtual concept gives bitcoin a speculative nature since it does not evolve as a real asset. So its survival will rely on its acceptance as a mean of exchange. On the other hand, Rodrigues explains that there are cryptocurrencies with more potential rather than bitcoin, such as Ethereum. Nevertheless, the Cybersecurity analyst believes that bitcoin is "too big to fail" and it will remain the biggest cryptocurrency in the upcoming years.

Finally, all interviewees stated that bitcoin could and will not be compared to gold. Reis explains that gold is a tangible asset with special characteristics that guarantees its value. Moreover, he asserts that bitcoin is far from representing all those functions performed by gold, the mainly speculative nature of bitcoin will undermine its value. Rodrigues confirms that some comparisons could be taken, but explain that people are very attached to the idea of having some real asset rather than digital, therefore the idea of bitcoin becoming a storage of value such as gold is very very unlikely, because both have completely different characteristics.

9. Conclusion

This section concludes the thesis by summarizing the main findings and giving suggestions for alternative researches regarding bitcoin.

Bitcoin is a new and innovative system that differs from everything that has existed before. Peer-to-peer eletronic cash system is playing a important role regarding the virtual currency systems. Some comparisons with money are made, thereby it is

important to delineate some differences in order to better understand the concept. The preliminaries differences arisen rely on the decentralisation and anonymousity of bitcoin. Bitcoin functions as money, anyway it lacks in stability and durability of its value. Moreover, it is possible to find international overview of the legal framework regarding bitcoin community. As developed in this thesis, the lack of regulation attracted many fraudulent cases such as Mt Gox. A deeper analysis of bitcoin is given by US regulation and to the declaration of the Internal Revenue Service of the US Governement that defined bitcoin as a form of money, which needs to be treated as an asset. Furthermore, it is required to be taxed as income on the basis of fair market value as of the date of the specific activity.

Bitcoin market is relatively young, therefore loads of changes are taking place within it. Throughout the years bitcoin has been rapidly growing in terms of market capitalization due to its decentralization and virtual usage. However, bitcoin has been traditionally associated with high levels of risk because there is no authority regulating the community and there is no intrinsic value supporting it. Therefore, it is more susceptible to speculation and eventually bubbles. It is a disruptive technology that still requires a clear and unanymous classification. Nevertheless, as it was developed through this thesis the increased popularity surrounding bitcoin turned bitcoin into a synthetic commodity asset, because it not only works as a currency but also as an asset. Despite the difficulties regarding its classification, bitcoin behavior can be associated to a unique asset class. Furthermore, bitcoin trade volume has been growing exponentially since its introduction and price volatility has been declining steadily over the past few years, which supports the idea that bitcoin behaves as a new asset class.

Blockchain was initially designed as the technology behind bitcoin, nevertheless it has opened other avenues across the internet. Blockchain is a digital ledger that records not only financial transactions but virtually everything that has value. One of the most important feature of this technology regards its security and incorruptibility of information. Blockchain network is based on a state of consensus, therefore it seeks transparency and it is very difficult to be corrupted. Although, it is possible to corrupt blockchain network, by using huge amounts of computing power, hackers are able to have access and change data cointained in the ledger.

Blockchain could be a very successful tool for many industries sectors in a near future. Transparency could help companies saving millions in resources by optimizing their systems. Plenty of economic opportunities emerged with the introduction of the blockchain, **such as initial coin offerings for crowdfunding the projects** and the reduced barriers for entrepreneurs by simplyfing their access to resources. The technology has a huge potential depending on the area of its implementation, it could solve several obstacles that industries are facing nowadays and evolve the major core processes.

Throughout the analysis of the survey and interviews that were implemented, it is possible to make some assumptions. Bitcoin is certainly not a currency yet, as Helder Reis mentioned it does not fulfill the functions of money. Nevertheless, its potential might change monetary policy. Many doubts surround the bitcoin network and it is important that regulation comes into the sector, so that consumers feel confident to use bitcoin not only as a mean of exchange but also as an investment. Probably with increased regulation, volatility will steadily continue to decrease and potentially reach values in which the cryptocurrency could be used as a currency. Nevertheless, bitcoin and its features are not prepared to work as a currency right away. It is required plenty of time, regulation and acceptance by consumers. Actually, nowadays, bitcoin is perceived as a new type of asset, as mentioned before and stated by Selgin bitcoin could be classified as synthetic commodity money.

Suggestions

Synthetic commodity money concept is quite interesting and there is very few researches regarding the topic. The author suggests that further analysis of syntethic commodity money is necessary because the constant growth of cryptocurrencies will surely require a much deeper analysis about this fourth group of monies (commodity, fiat and coase durables are already exploited).

10. References

Accenture, (2017). ***Banking on blockchain: A value analysis for investment banks.*** [online] Available at:https://www.accenture.com/usen/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf [Accessed 11 Feb. 2018]

Adam Hayes, C. (2018). ***Hard Fork***. [online] Investopedia. Available at: https://www.investopedia.com/terms/h/hard-fork.asp [Accessed 5 Apr. 2018].

Adam Hayes, C. (2018). ***Sharpe Ratio***. [online] Investopedia. Available at: https://www.investopedia.com/terms/s/sharperatio.asp [Accessed 9 Mar. 2018].

Antonopoulos, A. (2015). Mastering Bitcoin. Sebastopol, CA: O'Reilly Media Inc.

BBC News. (2013). ***Raids take digital cash firm offline***. [online] Available at: http://www.bbc.com/news/technology-22680297 [Accessed 5 Mar. 2018].

Belinky, M., Rennick, E. & Veitch, A. 2015. ***The Fintech 2.0 Paper: Rebooting Financial Services***. [online] Available at: http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf. [Accessed 12 February 2018]

Blockonomi. (2017). ***The History of the Mt Gox Hack: Bitcoin's Biggest Heist.*** [online] Available at: https://blockonomi.com/mt-gox-hack/ [Accessed 5 Feb. 2018].

Bloomberg.com. (2014). ***Bitcoin 2.0 Shows Technology Evolving Beyond Use as Money.*** [online] Available at: https://www.bloomberg.com/news/articles/2014-03-28/bitcoin-2-0-shows-technology-evolving-beyond-use-as-money [Accessed 6 Feb. 2018].

Brito, J. and Castillo, A. (2013). ***Bitcoin: A primer for policymakers***. Arlington: Mercatus Center, pp.20-22.

Brito, J. and Castillo, A. (2016). ***Bitcoin***. Arlington, Virginia: Mercatus Center, George Mason University.

CCN. (2018***). China's Crackdown on Mining Could Lead to Bitcoin Price Surge***. [online] Available at: https://www.ccn.com/low-supply-chinas-crackdown-mining-lead-bitcoin-price-surge/ [Accessed 6 Apr. 2018].

CCN. (2017). ***Portugal's Central Bank Governor: "Bitcoin Isn't a Currency"***. [online] Available at: https://www.ccn.com/portugals-central-bank-director-bitcoin-isnt-currency/ [Accessed 6 Apr. 2018].

Centre for technology & Global Affairs, CTGA. (2017). ***Blockchains for governmental services: design principles, applications, and case studies.*** University of Oxford [online] Available at: https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickellosluganovic.pdf [Accessed 17 Mar.2018]

Chiu, J. and Koeppl, T. (2017). ***The Economics of Cryptocurrencies Bitcoin and Beyond***. SSRN Electronic Journal.

Christin, Nicolas ***"Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace,"*** Carnegie Mellon CyLab Technical Reports: CMU-CyLab-12-018, July 30, 2012 (updated November 28, 2012), http://www .cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf.

CNBC Africa. (2017). ***M-pesa has completely transformed Kenya's economy, this is how...*** - CNBC Africa. [online] Available at: https://www.cnbcafrica.com/news/east-africa/2017/01/04/mpesa-economic-impact-on-kenya/ [Accessed 7 Feb. 2018].

Coindesk.com. (2018). ***Bitcoin Price Index - Real-time Bitcoin Price Charts***. [online] CoinDesk. Available at: https://www.coindesk.com/price/ [Accessed 8 Apr. 2018].

Coinmarketcap.com. (2018*). **Cryptocurrency Market Capitalizations*** | CoinMarketCap. [online] Available at: https://coinmarketcap.com/ [Accessed 10 Jan. 2018].

Credit Suisse, (2018). ***Blockchain 2.0***. [online] Available at: https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&sourceid=csplusresearchcp&document_id=1080109971&serialid=pTkp8RFIoVyHegdqM8EllLNi1z%2Fk8mInqoBSQ5KDZG4%3D [Accessed 12 Feb. 2018]

Deloitte, (2016). ***Blockchain Enigma. Paradox Opportunity***. [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf [Accessed 14 Feb. 2018]

Digiconomist. (2018). ***Bitcoin Energy Consumption Index*** - Digiconomist. [online] Available at: https://digiconomist.net/bitcoin-energy-consumption [Accessed 6 Mar. 2018].

Elton, E., Gruber, M., Brown, S. and Goetzmann, W. (2014). ***Modern portfolio theory and investment analysis.*** 9th ed. John Wiley & Sons.

FinCEN. (2013, March 18). ***FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities.*** Retrieved from Financial Crimes Enforcement Network: http://www.fincen.gov/news_room/nr/pdf/20130318.pdf

FinCEN. (2014, January 30). ***Application of FinCEN's Regulations to Virtual Currency Mining Operations.*** Retrieved from Financial Crimes Enforcement network: http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf

Federal Bureau of Investigation. (2012). ***Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.*** Washington, D.C: Federal Bureau of Investigation.

Forbes.com. (2017). ***Bitcoin is not an asset.*** Forbes Welcome. [online] Available at: https://www.forbes.com/sites/jeffreydorfman/2017/05/17/bitcoin-is-an-asset-not-a-currency/#27dcd35a2e5b [Accessed 7 Feb. 2018].

Forbes.com. (2018). ***China's Shutdown Of Bitcoin Miners Isn't Just About Electricity***. [online] Available at: https://www.forbes.com/sites/sarahsu/2018/01/15/chinas-

shutdown-of-bitcoin-miners-isnt-just-about-electricity/#51e0a9b0369b [Accessed 6 Apr. 2018].

Forbes India. (2015). ***Steve Forbes: Elephant in the room-money*** | Forbes India. [online] Available at: http://www.forbesindia.com/article/column/steve-forbes-elephant-in-the-roommoney/40573/1 [Accessed 7 Feb. 2018].

Greer, R. (1997). ***What is an Asset Class, Anyway?.*** The Journal of Portfolio Management, 23(2), pp.86-91.

Hileman, G. and Rauchs, M. (2017). 2017 ***Global Cryptocurrency Benchmarking Study.*** SSRN Electronic Journal.

Internetworldstats.com. (2018). ***World Internet Users Statistics and 2018 World Population Stats.*** [online] Available at: https://www.internetworldstats.com/stats.htm [Accessed 8 Feb. 2018]

Investopedia. (2018). ***Asset***. [online] Available at: https://www.investopedia.com/terms/a/asset.asp [Accessed 1 Mar. 2018].

Irs.gov. (2014***). IRS Virtual Currency Guidance***. [online] Available at: https://www.irs.gov/pub/irs-drop/n-14-21.pdf [Accessed 6 Feb. 2018].

Jornaldenegocios.pt. (2017). ***Trabalha com Bitcoins? Tem de pagar impostos.*** [online] Available at: http://www.jornaldenegocios.pt/mercados/detalhe/bitcoins-nao-sao-legais-mas-podem-ter-de-pagar-impostos [Accessed 6 Apr. 2018].

LaVere, M. (2017). ***Ongoing Debate: Is Bitcoin Money or an Asset Class?*** | Oracle Times. [online] Oracletimes.com. Available at: https://oracletimes.com/ongoing-debate-is-bitcoin-money-or-an-asset-class/ [Accessed 7 Feb. 2018].

Learncryptography.com. (n.d.). ***Learn Cryptography - 51% Attack***. [online] Available at: https://learncryptography.com/cryptocurrency/51-attack [Accessed 5 Apr. 2018].

McKenna, F. (2017). ***Here's how the U.S. and the world regulate bitcoin and other cryptocurrencies.*** [online] MarketWatch. Available at: https://www.marketwatch.com/story/heres-how-the-us-and-the-world-are-regulating-bitcoin-and-cryptocurrency-2017-12-18 [Accessed 1 Mar. 2018].

Medium. (2017). ***Is Bitcoin money or a commodity?*** – Marko Kovic – Medium. [online] Available at: https://medium.com/@marko_kovic/is-bitcoin-money-or-a-commodity-c1a1bc5bfb39?) [Accessed 7 Feb. 2018].

Montag, A. (2017). ***Kevin O'Leary explains one big thing people don't understand about bitcoin (but need to)***. [online] CNBC. Available at: https://www.cnbc.com/2017/12/07/kevin-oleary-bitcoin-is-an-asset-not-a-currency.html [Accessed 7 Feb. 2018].

Nakamoto, S. (2008). ***Bitcoin: A Peer-to-Peer Electronic Cash System***. [online] Available at: https://bitcoin.org/bitcoin.pdf [Accessed 20 Jan. 2018]

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016***). Bitcoin and cryptocurrency technologies: A comprehensive introduction***. Princeton and Oxford: Princeton University Press, pp.14-17.

Selgin, G. (2012). ***Quasi-Commodity Money***. SSRN Electronic Journal.

Sec.gov. (2017). ***Statement on Cryptocurrencies and Initial Coin Offerings***. [online] Available at: https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 [Accessed 6 Feb. 2018].

Sparshott, J. (2013**). Bitcoin Exchange Makes Apparent Move to Play by U.S. Money-*Laundering* Rules.** [online] WSJ. Available at: https://www.wsj.com/articles/SB10001424127887323873904578574000957464468 [Accessed 5 Mar. 2018].

Suri, T. and Jack, W. (2016). ***The long-run poverty and gender impacts of mobile money.*** Science, 354(6317), pp.1288-1292.

Tapscott, D. & Tapscott, A. 2016. ***The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World***. ISBN 978-0-670-06997-2.

Worldometers.info. (2018). ***World Population by Year*** - Worldometers. [online] Available at: http://www.worldometers.info/world-population/world-population-by-year/ [Accessed 2 Mar. 2018].

11. Apendix

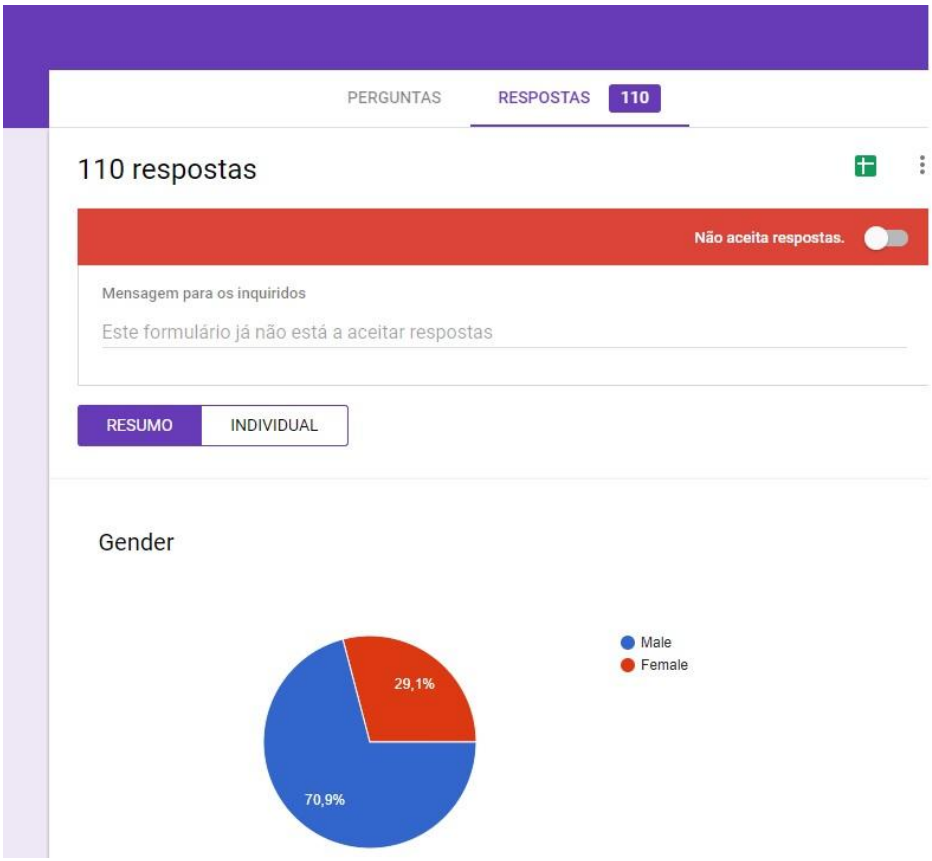
Appendix A - Survey

Appendix B - Helder Reis, Presidência da República, interview transcript

Appendix C - Eduardo Rodrigues, REN, interview transcript

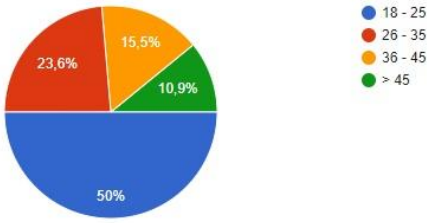
Appendix D - José Galamba de Oliveira, Associação Portuguesa de Seguradoras, interview transcript

Appendix A - Survey

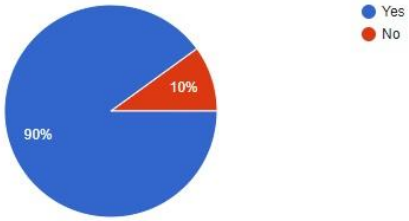


PERGUNTAS RESPOSTAS 110

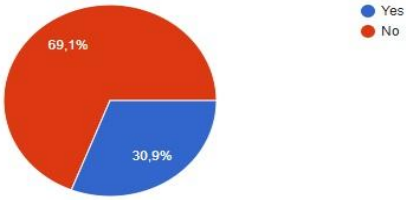
Age



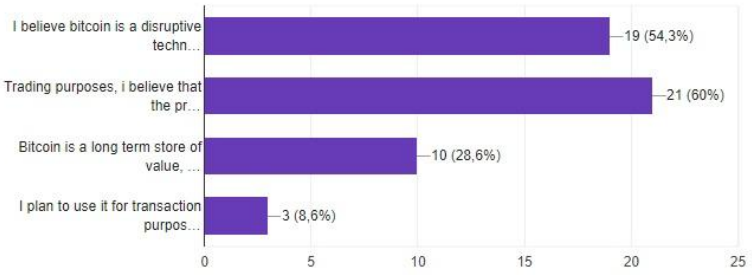
Have you ever heard of Bitcoin?



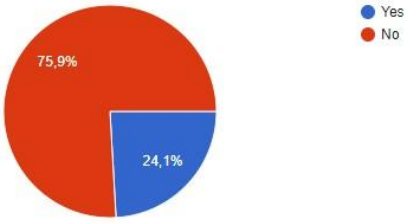
Have you invested in Bitcoin?



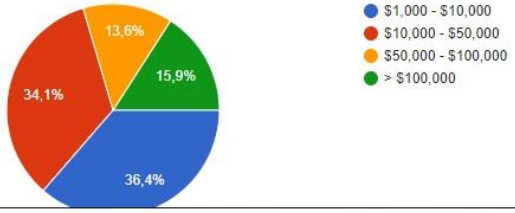
If you answered "Yes" in the previous question, please choose the option that explains the reason why you invested.



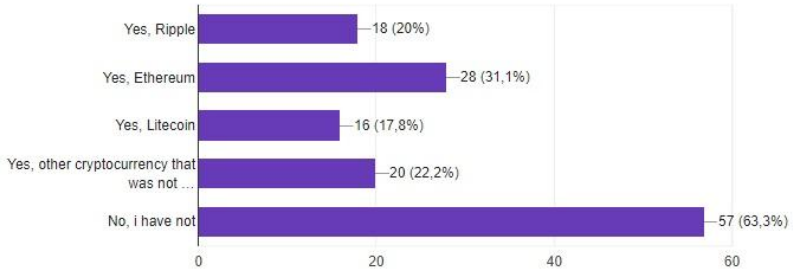
Have you sold any of your Bitcoin?



At what price are you willing to sell your bitcoins?

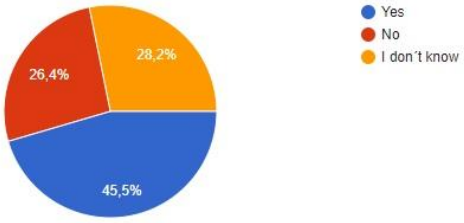


Have you invested in other cryptocurrencies besides bitcoin? Note: Please select all that apply.



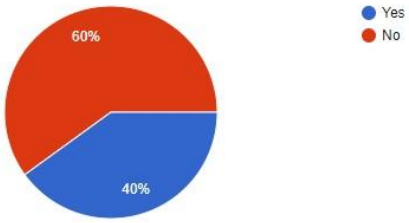
PERGUNTAS RESPOSTAS 110

Do you see Bitcoin as a macroeconomic tool hedge as against monetary policy?



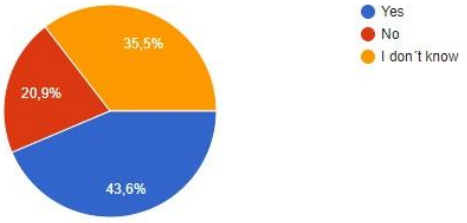
PERGUNTAS RESPOSTAS 110

In 10 years do you believe that Bitcoin will be the largest cryptocurrency regarding market capitalization?



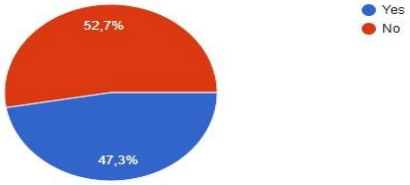
PERGUNTAS RESPOSTAS 110

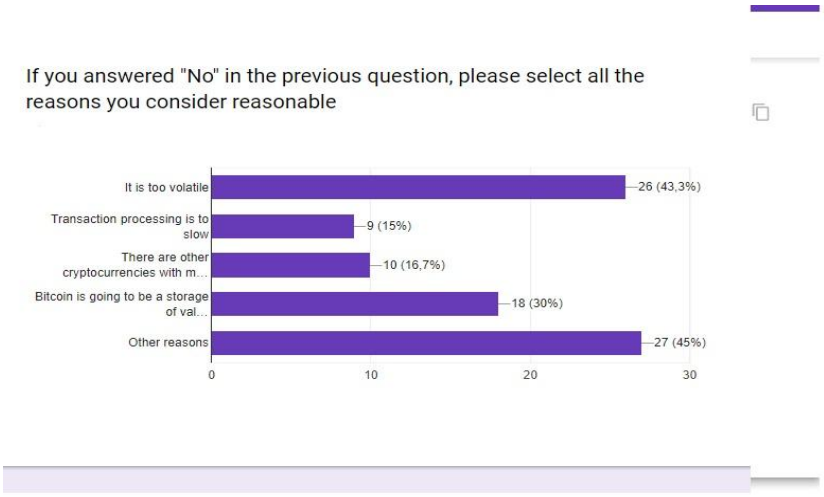
Do you believe that increased regulation and oversight by several governments would be benefic for bitcoin?



PERGUNTAS RESPOSTAS 110

Do you think bitcoin is able to become a currency, such as US Dollar or Euro?





Appendix B - Helder Reis, Presidência da República, interview transcript

Name and position: Helder Reis, Consultor da Casa Civil da Presidência da República

Date: 24.04.2018

Interviewer: Francisco Santos Ferreira

FF: What do you think of the Bitcoin phenomenon and what is your general attitude toward it?

HR: *Due to its novelty, bitcoin phenomenon has generated a huge confusion among consumers. People went crazy about it, because it changed the perception of money completely. I do not have bitcoin and i do not accept bitcoin as mean of payment, nevertheless i agree that the only similarity that it has with a normal currency is its usage as a mean of exchange.*

FF: So bitcoin is certainly not officially a currency and it is very difficult to categorize. Do you think that a new category needs to be defined? Could it be considered a virtual commodity? What is the likelihood that it will become a more widely accepted method of payment?

HR: *In my opinion it all depends on the international community and the regulation that they will apply to the cryptocurrency sector. The evolution tends to suggest that the major purpose it is to decrease the uncertainty that cryptos are facing nowadays. Between countries the cambial risk reduction is essential. European Union decided to create a unique currency in order to reduce as maximum as possible that risk. So, the characteristics of bitcoin and its volatility makes it difficult to be accepted as a mean of exchange due to the enormous risk associated.*

FF: How do you see the comparison to gold from your point of view? Do you see more similarities or differences?

HR: *I do not see any comparison between bitcoin and gold. Gold can be classified as a tangible asset with specific characteristics that undermine its value. On the other hand, bitcoin is far from representing those functions, they do not represent anything besides a speculative will from their investors. Therefore the value of bitcoin is determined by that will that surrounds all the investors. Its prices increased a lot because investors thought it would be a tremendous success and started to invest without even knowing what was going on. Thus, some "crisis" have already been faced and it is important to affer that bitcoin is resisting to the several crisis and is still operating and looking for improvements.*

FF: In terms of regulation, do you think that it is mandatory to regulate bitcoin in order to increase confidence among users? Would regulation benefit bitcoin network?

HR: *Yes it will be necessary to regulate bitcoin in order to increase confidence among users and raise the potential entrants in the market.*

FF: Some countries such as China banned bitcoin. Do you see Bitcoin as a macroeconomic tool hedge as against monetary policy?

HR: *Nowadays i do not consider bitcoin as an instrument against monetary policies, since bitcoin due to its characteristics are not normal currencies, they do not respect the functions of money. Therefore, it is not even an instrument of monetary policy.*

FF: When we look at the technology, some consider it revolutionary. For example with the blockchain technology it is possible to transfer ownership and make other contracts without intermediaries (smart contracts). Do you see this more as a threat or as an opportunity?

HR: *Of course i understand there is a huge opportunity regarding blockchain technology. But it is important to enhance that sometimes it is not necessary to change the way business models are operating. There are several areas working perfectly that are studying the implementation of the blockchain technology and that is not necessary a good thing. It all depends on the cost of the transaction and the safety of the procedures associated to those intermediaries. Business models becoming more autonomous might be benefic, nevertheless sometimes intermediares play an essential role that could not be changed.*

FF: If we look five years forward, do you think Bitcoin will become a case study of a new bubble or will it survive?

HR: *Looking into the future and thinking about bitcoin is a very hard task. It all depends on the dynamic usage of bitcoin as a possible mean of payment. Naturally, its virtual concept gives bitcoin a speculative nature since it does not have an implicit evolution of a real asset. Thus, its survival will depend on the acceptance of the worldwide community of bitcoin as a mean of payment. However, in order to occur that acceptance, volatility will have to be reduced as maximum as possible. Major doubts arise whenever we look into bitcoin as a reserve of value or storage of value, since its volatility is still tremendously high, which compounds a huge risk for investors.*

Appendix C - Eduardo Rodrigues, REN, interview transcript

Name and position: Eduardo Rodrigues, Senior Cybersecurity Analyst at REN

Date: 06-05-2018

Interviewer: Francisco Santos Ferreira

FF: What do you think of the Bitcoin phenomenon and what is your general attitude toward it?

ER: *The phenomenon and adoption has been driven by the coin's massive price increase, future potential gains but also lack of knowledge on how to invest and on the underlying technology. In my case, as an IT graduate I've studied the technology and its potential for a while and decided to finally invest in November 2017.*

FF: So bitcoin is certainly not officially a currency and it is very difficult to categorize. Do you think that a new category needs to be defined? Could it be considered a virtual commodity? What is the likelihood that it will become a more widely accepted method of payment?

ER: *Despite of the popularity boom I think bitcoin (and other cryptocurrencies) still has a long way to go in order to be fully adopted by people but also by the banking system which has been stuck in the same principles for decades. It is also important to note that the baking system isn't famous for being fast paced on adopting technology, Fintechs such as Revolut and Monzo may play a big role on making bitcoin a widely accepted method.*

FF: How do you see the comparison to gold from your point of view? Do you see more similarities or differences?

ER: *Some comparisons can be drawn but I think that people are still very attached to the idea of having something real rather than digital.*

FF: In terms of regulation, do you think that it is mandatory to regulate bitcoin in order to increase confidence among users? Would regulation benefit bitcoin network?

ER: *Hard to tell. I am pro regulation as long as it doesn't strangle technology.*

FF: Some countries such as China banned bitcoin. Do you see Bitcoin as a macroeconomic tool hedge as against monetary policy?

ER: *Cryptocurrencies were thought out to be a viable alternative to the banking system and I can see why countries and regulators may be wary of it. However, I think that we already got past that and full adoption of the blockchain and bitcoin is coming in the next 1 or 2 years.*

FF: When we look at the technology, some consider it revolutionary. For example with the blockchain technology it is possible to transfer ownership and make other contracts without ntermediaries (smart contracts). Do you see this more as a threat or as an opportunity?

ER: *I see it as an opportunity, mainly on the autonomy side. Agreements can be made with no need to rely on a lawyer or a government official and that can be very beneficial. There are still some things to tackle such as Data Privacy, especially after the implementation of the General Data Protection Regulation.*

FF: If we look five years forward, do you think Bitcoin will become a case study of a new bubble or will it survive?

ER: *Hard to tell. There are other cryptocurrencies with a clearer future such as Ethereum (which has a lot of potential) but I feel like bitcoin is one of those 'too big to fail' cases and it will always be regarded as the biggest cryptocurrency.*

Appendix D - José Galamba de Oliveira, Associação Portuguesa de Seguradoras, interview transcript

Name and position:

José Galamba de Oliveira/Presidente da APS (Associação Portuguesa de Seguradores)

Date: 20 de Abril de 2018

Interviewer: Francisco Santos Ferreira

FF: What do you think of the Bitcoin phenomenon and what is your general attitude toward it?

JGO*: In my opinion bitcoin phenomenon derives from the huge interest among our society surrounding disruptive technologies that are able to compete with the current business models in a cheaper and more efficient way. Bitcoin supporters believe that the cryptocurrency is able to guarantee more autonomy and confidence regarding financial transactions, because the current financial system is losing trustworthiness among the consumers.*

FF: So bitcoin is certainly not officially a currency and it is very difficult to categorize. Do you think that a new category needs to be defined? Could it be considered a virtual commodity? What is the likelihood that it will become a more widely accepted method of payment?

JGO*: It is certainly not a currency. Nowadays bitcoin can be classified as a speculative financial asset. Nevertheless, i believe that in a long-term perspetive it classificiation might change. If bitcoin is able to have more stable values,therefore its volatility diminished and also increased*

regulation by international authorities i strongly agree that it might become a way of making payments accepted worldwide and consequently become a currency.

FF: How do you see the comparison to gold from your point of view? Do you see more similarities or differences?

***JGO**: At the moment i cannot see any comparison between gold and bitcoin due to the lack of maturity surrounding bitcoin phenomenon.*

FF: In terms of regulation, do you think that it is mandatory to regulate bitcoin in order to increase confidence among users? Would regulation benefit bitcoin network?

***JGO**: I believe that sooner or later we will see new rules and regulation coming in this sector. If bitcoin community wants to take the cryptocurrency sector to another level, then it is stricly important to ask for regulation processes. It will only benefit consumers, because whenever bitcoin is considered legal and regulated much more consumers will feel free to invest in this area and therefore start using it. I truly believe that regulation is beneficial for bitcoin and all the other cryptocurrencies.*

FF: Some countries such as China banned bitcoin. Do you see Bitcoin as a macroeconomic tool hedge as against monetary policy?

***JGO**: Nowadays i don´t believe bitcoin is a macroeconomic tool agains the current monetary policies. The levels of volatility that we face at the moment do not allow bitcoin to even be compared to a normal currency.*

FF: When we look at the technology, some consider it revolutionary. For example with the blockchain technology it is possible to transfer ownership and make other contracts without intermediaries (smart contracts). Do you see this more as a threat or as an opportunity?

***JGO**: Blockchain technology for me is the key success factor that surrounds bitcoin network system. There are plenty of opportunities to transform current industries and its business models, just by adopting this type of technology. It is possible to make a linkage between transparent and secure business models with diferent types of organisations, employees and authorities without relying on a third-party. Moreover, the impact that it might have on Internet of Things is incredibly positive. It is possible to conclude that big organisations are looking into blockchain technology, almost every multinational organisations have departments looking for the advantages of blockchain implementation.*

FF: If we look five years forward, do you think Bitcoin will become a case study of a new bubble or will it survive?

***JGO**: In my opinion i believe bitcoin will survive as a mean of exchange. Whenever it reaches a more mature state, speculators will stop using it and internaut "geeks" will use it as a mean of payment.*