

**BITCOIN, THE CONTROVERSIAL CRYPTOCURRENCY: AN INSIGHTFUL
OVERVIEW AND ITS CONTEXT IN THE PORTUGUESE MARKET**

José Miguel Nunes Amândio

Dissertation submitted as partial requirement for the conferral of
Master in Management

Supervisor:

Prof. António Freitas Miguel, ISCTE Business School, Finance Department

October 2017

Abstract

Before Bitcoin's appearance, all the payment systems had faced the requirement of being controlled by an entity, as none had shown the ability to perform in a decentralized structure. Bitcoin is also a digital currency and consequently has no intrinsic value, however it has shown an enormous price increase over the past few years, having that growth a special emphasis in the current year. Therefore, Bitcoin emerges as a disruptor in the current financial system.

This dissertation has the main objective of analysing the key concepts of Bitcoin from which the most controversial topics emerge. Then, those topics are furtherly scrutinized by developing a quantitative and qualitative research always regarding both present and future impacts of Bitcoin. The research includes statistical data from Bitcoin and other financial data providers. Additionally, and due to the lack of literature comprising the Portuguese market, a special attention is given to this country.

Despite the lack of credibility among most financial leaders which has consisted of a limitation to Bitcoin's implementation process, this cryptocurrency is a technological landmark and, so far, shows no signs of slowing down.

JEL Classification: E42, E52

Keywords: Bitcoin, Currency, Payment System, Innovation

Resumo

Antes do aparecimento da Bitcoin, todos os sistemas de pagamento enfrentavam a condição de serem controlados por uma entidade, uma vez que nenhum tinha mostrado capacidade para atuar numa estrutura descentralizada. A Bitcoin é também uma moeda digital e como tal não tem valor intrínseco, no entanto o seu preço tem tido um enorme aumento nos últimos anos, com especial ênfase no ano corrente. Deste modo, a Bitcoin surge como um disruptor do atual sistema financeiro.

Esta dissertação tem como principal objetivo a análise dos conceitos fundamentais da Bitcoin, dos quais surgem os tópicos mais controversos. Após essa fase, esses tópicos serão aprofundados através do desenvolvimento de uma pesquisa quantitativa e qualitativa, tendo sempre em consideração impactos atuais e futuros da Bitcoin. Esta pesquisa inclui dados estatísticos apresentados por intermediários da Bitcoin e outros fornecedores de dados financeiros. Adicionalmente, e devido à ausência de literatura que inclua o mercado Português, este será analisado de forma mais detalhada.

Apesar da falta de credibilidade junto dos principais líderes financeiros o que tem consistido numa limitação ao processo de implementação da Bitcoin, esta criptomoeda é um marco tecnológico e, até agora, não mostra sinais de abrandamento.

Classificação JEL: E42, E52

Palavras-chave: Bitcoin, Moeda, Sistema de Pagamento, Inovação

Thanks

To start, I would like to thank my supervisor Dr. António Freitas Miguel for introducing me to such an interesting topic and also for the enormous patience, feedback and supervision during all this process.

Secondly, I am thankful to my company EY and my colleagues for the motivation and tolerance shown towards my final objective.

I would also like to mention my girlfriend for the crucial support, enthusiasm, trust and advice. Thank you for being there.

Lastly, I want to thank my family and friends for being present in all phases of my life, never giving up on me and always believing in my success.

Table of Contents

Abstract	i
Resumo	ii
Thanks	iii
List of Figures.....	v
Section 1: Introduction.....	1
Section 2: Conceptual Framework.....	3
2.1 Conceptualisation	3
2.2 Decentralization.....	4
2.3 Blockchain	5
2.4 Mining.....	6
2.5 Wallets	8
2.6 Market.....	10
2.7 Investment	11
2.8 Valuation.....	12
2.9 Research Topics	13
Section 3: BTC in Portugal: Current Overview.....	15
3.1 ATM Locations	15
3.2 Physical Stores	17
3.3 Cryptocurrencies Legislation	19
3.4 Cryptocurrencies Taxes	22
3.5 Financial Prospects.....	23
Section 4: Key Concepts: Further Development	25
4.1 Digital Payment System Adoption	25
4.2 Blockchain Technology.....	28
4.3 Mining.....	31
4.4 Cryptocurrencies' Market	33
4.5 Most Controversial Topics.....	43
Section 5: BTC in the World: an Insightful Guide.....	44
5.1 Security/Credibility	44
5.2 Transparency	45
5.3 Technical Issues	46
Section 6: Conclusion	49
Bibliography	51

List of Figures

Figure 1: Blockchain transaction scheme	6
Figure 2: BTC's programmed supply curve	7
Figure 3: Number of wallet users worldwide from 1st Quarter 2014 to 3rd Quarter 2017.....	9
Figure 4: BTC volatility time series from September 2016 to September 2017.....	11
Figure 5: BTC investment trust valuation in 2017 (USD).....	12
Figure 6: BTC price in 2011-2017 (USD).....	13
Figure 7: Total number of BTC ATMs located in Portugal (including machine and/or teller)	16
Figure 8: Total number of BTC ATMs located in Central and Western Europe (including machine and/or teller).....	16
Figure 9: Number of BTC ATMs installed over time (including machine and/or teller).....	17
Figure 10: BTC acceptance physical store density per region in Portugal.....	18
Figure 11: BTC acceptance physical shop density in Lisbon	18
Figure 12: BTC acceptance in physical shop density in Central and Western Europe.....	19
Figure 13: BTC's legality country position	21
Figure 14: Factors enhancing use of digital payment.....	26
Figure 15: Digital payment: barriers to growth.....	26
Figure 16: Increase in volume of digital payments	27
Figure 17: BTC mining difficulty	32
Figure 18: Energy consumption by country (in terawatt hours)	32
Figure 19: BTC (USD) price 07 September to 07 October	35
Figure 20: Correlation between public attention indicators and BTC's price (USD).....	38
Figure 21: BTC's price (USD) after Mt Gox's bankruptcy.....	39
Figure 22: Total market capitalization.....	40
Figure 23: Ripple transaction's system.....	42
Figure 24: Cryptocurrency market share (June 2016 to June 2017)	47

“Bitcoin is a technological tour de force”

Bill Gates, 2014

Section 1: Introduction

History has shown that transactions are part of our society. The first settlers on earth used to do non-monetary exchange, in which every object could be either used or traded, allowing the acquisition of other goods. Many years later, some cultures adopted commodity money, that is, “objects that have value in themselves as well as value in their use as money” (O’Sullivan & Steven, 2003: 246) (e.g., gold). Over the years, transactions have involved different means and mediums of exchange, leading to the concept of money, which is theoretically considered as “any item or verifiable record that is generally accepted as payment for goods and services and repayment of debts ” (Mishkin, 2007: 8). Therefore, transactions and money are genuinely connected and as the world goes digital, developing digital money and payment systems allow simpler, easier and borderless transactions. Nowadays, digital money is exchanged using technologies such as smartphones, credit cards and the internet (via digital payment systems, which usually consist of web applications).

After the world economic crisis in the beginning of this century, many people had lost their trust in the current financial system and its institutions. Additionally, the already mentioned development of digital money and the growing trust in digital payment systems lead to Bitcoin’s appearance.

In October 2008, an unknown person or group with the pseudonymous Satoshi Nakamoto¹ published a paper describing Bitcoin’s working system, named “Bitcoin: a Peer-to-Peer Electronic Cash System”. This nine-page-paper was the entry for Bitcoin’s arrival.

In January 2009, Satoshi Nakamoto released the first version of Bitcoin software as well as the first units of bitcoins. The development of this story, will be furtherly analysed.

Regardless of all the criticism that it has taken from most financial leaders, Bitcoin emerges as a financial market phenomenon due to the incredible price increase in the current year. Its recovery from negative impacts caused by analysts occurs in short periods of time and it has been impressive. Moreover, Bitcoin appears to be not only a financial disruptor, but also a technological exciting innovation, leading to many projects regarding security system implementation.

The aim of this paper is to identify the most debatable topics of Bitcoin and accurately analysing them so that conclusions can be taken.

¹ Theories about Satoshi Nakamoto’s identity are many but, so far, they have been inconclusive.

Despite the reduced market penetration in Portugal, the absence of a study comprising domestic indicators and analysing possible impacts of Bitcoin in Portuguese society, composed a major incitement for introducing this country into the study.

The results will be important to define the viability of the present and the future of Bitcoin, concerning financial, technological and other relevant aspects of this payment method. Additionally, a particular reflexion will be given to the Portuguese market.

In order to do so, data of the most prominent influencers and the existing research papers will be collected and analysed with the support of quantitative indicators that are currently available from Bitcoin and other financial data providers.

The dissertation is organized as follows: Section 2 introduces the main concepts and the structure of Bitcoin's system; Section 3 analyses quantitative and qualitative indicators of Bitcoin's market penetration in Portugal; Section 4 provides a further development of the most significant research topics; Section 5 evaluates the most controversial topics of Bitcoin with a special emphasis on the Portuguese market; and Section 6 concludes.

Section 2: Conceptual Framework

This Section aims to introduce and conceptualise the research subject, clarify its working system and elucidate about its relevance. Due to the complexity of the topic, the Section is structured through sub-topics, in order to create a simpler rationale, allowing the fully understanding of the subject.

2.1 Conceptualisation

The following Section introduces a small number of concepts that are vital for the understanding of Bitcoin and its system.

Bitcoin (designated as BTC from this point) is both “a worldwide decentralized cryptocurrency and a digital payment system” (Brito & Castillo, 2013: 3-5). Defining concepts included in this sentence:

- Decentralized means that the system, including supply, policy decisions and litigations are publicly known and that every user of the currency has a small position when decisions have to be taken. It is often referred as a Peer-to-Peer (P2P) network, because of the application architecture, in which every participant is equally privileged and shares equivalent resources. In order to alter the system, the majority of user votes are an obligation, meaning there is a network of BTC users responsible for taking decisions about their currency. In fact, users do not directly approve or deny a change in the system, as the protocol² that runs the system cannot be changed, but they can decide to use upgraded versions of the initial program, which contain other protocols. On the contrary, in centralized banking and economic systems, Banks and the Government regulate the supply of currency by printing money units or control what interest rates to apply.
- Cryptocurrency is a digital asset formed to function as a medium of exchange, based in the concept of cryptography, which refers to “techniques for secure communication in the presence of third parties called adversaries” (Rivest and Ronald, 1990). So, cryptography is a technology that protects transactional flow and BTC’s system from robbery. Cryptocurrencies belong to the group of digital money, which basically has the same characteristics of physical money, but allows faster transactions and borderless transfer-of-ownership, as they are web based. Like traditional money, these currencies

² A set of rules used to exchange messages with other Internet points.

can be used to buy goods or services, but may also be restricted to smaller communities, such as online gaming or social network.

- BTC is also a digital payment system, because besides being a currency, it has its own system of currency exchange, in which every transaction includes a fee. This fee is calculated using Satoshis (1 Satoshi = 0, 00000001 BTC), and all fees are distributed among users' network. Fee distribution is furtherly explained in [Section 2.4](#).

The following Sections are far more specific than the previous ones, and will approach explicit characteristics of BTC's working system.

2.2 Decentralization

The already introduced paper "Bitcoin: a Peer-to-Peer Electronic Cash System" was the basis for the implementation of BTC's system. Nakamoto presents as an exclusive advantage of his system, the possibility of allowing "online payments to be sent directly from one party to another without going through a financial institution" (Nakamoto, 2008: 1), which refers to the decentralized currency. According to Hayek (1990: 30) "One of the reasons that government has maintained such a monopoly over currency is because there has never been an alternative that can offer the security of traditional money with the convenience of financial institutions that permit worldwide commerce." And Kaplanov (2012: 113) adds "That is, until the creation of bitcoins. Bitcoin is the world's first digital, private cryptocurrency that is exchanged over the Internet through the use of a peer-to-peer network. Bitcoin has no intrinsic value and there is no government, company, or independent organization upholding its value or monitoring its use."

Krugman (2013) claims that money has two characteristics: "be both a medium of exchange and a reasonably stable store of value". For Krugman, BTC fails on the second one. To justify his position, he quotes Brad DeLong (2013): "Underpinning the value of gold is that if all else fails you can use it to make pretty things. Underpinning the value of the dollar is a combination of (a) the fact that you can use them to pay your taxes to the U.S. government, and (b) that the Federal Reserve is a potential dollar sink and has promised to buy them back and extinguish them if their real value starts to sink at more than 2%/year. "Following this perspective, the fact that BTC has no intrinsic value denies it the possibility of being considered money. Thus, since dollar has financial institutions supporting its value, which is a characteristic of the already mentioned centralization, makes it possible to control maximum and minimum value boundaries, allowing a better performance of the economic system."

Plassaras (2013: 11) disagrees on Krugman's view, arguing that "when assessing a currency as a store of value, the key question is whether the currency is viewed as reliable and stable enough to operate effectively (...) After all, storing wealth in any medium that is easily susceptible to collapse or fraud is unwise." Thus, this author considers government backing to be a "double-edged sword", taking into account that "If, for example, a country is embroiled in conflict, its currency might suffer as a result. If a government decides to inflate its currency as a matter of some greater national economic policy, the wealth held by individuals in the form of currency decreases." He goes even further, stating that "electronic currencies can answer to market forces, better than the one's controlled by the Government and their interests, and the more stable the currency is, the better a store of value it becomes." Therefore, this author believes that electronic currencies can achieve a good level of stability which is directly related to becoming a better store of value and this fact will result into more investment from others.

Samuelson (1958) considers fiat money³ to be a "social contrivance", referring to the fact that money is only acceptable in society if there is the trust that every citizen will adopt it. Consequently, it is not a matter of intrinsic value, but the general acceptance of its utility. Samuelson had this rationale for fiat money, but the same paradigm applies on electronic cash, and more specifically, to BTC.

Opinions diverge about this cryptocurrency and its possibility to succeed without the supervision of financial institutions or third parties, even though achieving the required stability seems to rely on society's acceptance and adoption of BTC as money.

2.3 Blockchain

One of the main struggles of BTC has been to convince customers about money security. Over decades, "in spite of major cryptographic advances, failure to ensure double-spending⁴ prevention eventually put the viability of this new form of money (digital cash) into question" (Olleros & Zhegu, 2016). The ability to eliminate this problem is what makes BTC disruptive towards other digital payment systems.

The blockchain technology guarantees the elimination of double-spending problem. Every transaction that happens is part of a block. Once a block is processed, it is irreversible. Considering many transactions occur, and seeing each one as part of a block, a blockchain is

³ "Fiat money is a currency without intrinsic value established as money by government regulation or law." (Mankiw 2014: 220)

⁴ Double spending refers to the possibility of cash being spent twice.

created. If any block was modified, it would make all the blocks that come after it, to be changed as well, as they are part of the blockchain.

In order to make the blockchains chronologically followed, there might be conflicts when two or more transactions take place at the same time. To resolve this, instead of using a central server to process all data transactions, every user of BTC has access to all transactions ever executed in the currency. So, instead of having one database ruled by an institution, every BTC user holds transactions database and if any conflict is detected, all users can vote and decide for a fair solution. This database includes a ledger with all BTC addresses and their respective balance. BTC addresses are the common account numbers in bank accounts. Therefore, anyone can have access to the public address and the balance, and those are the only identifiers of the user, allowing the account owner to remain anonymous.

Figure 1 exemplifies how a transaction is done using the blockchain technology.

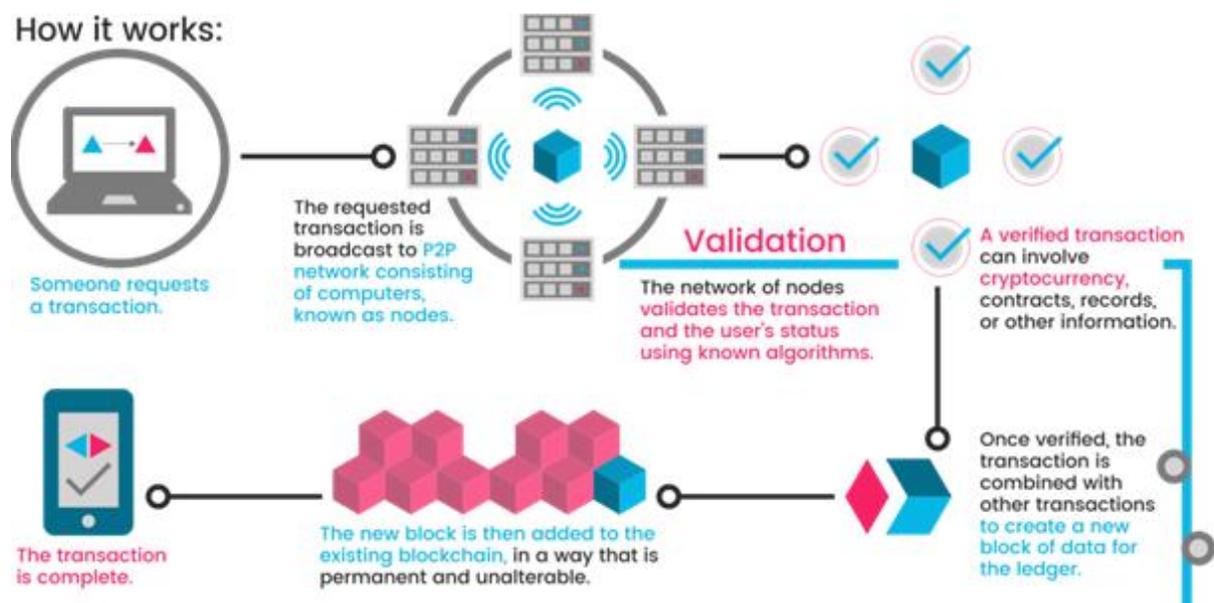


Figure 1: Blockchain transaction scheme

Source: <https://whatsthebigdata.com/2016/12/21/blockchain-and-the-iot/>

Now the question might be: What would move people to lose their time or waste their resources solving these conflicts? The next part of this thesis presents mining and the advantages of being a ruler of the blockchain.

2.4 Mining

There is a limited number of BTCs (it has a limited supply of 21 million units), but not all of them are in circulation nowadays. Figure 2 shows BTC's programmed supply curve, allowing

to confer that currently there are about 16.5 million units in the market and that BTC’s system is programmed to reach 21 million BTC’s in 2039. These numbers lead to the following conclusion:

Number of BTCs in use: 16.5 million

Number of existing BTCs: 21 million

Number of BTCs not yet in circulation: $21 - 16.5 = 4.5$ million

The process of placing BTCs into circulation is called mining.

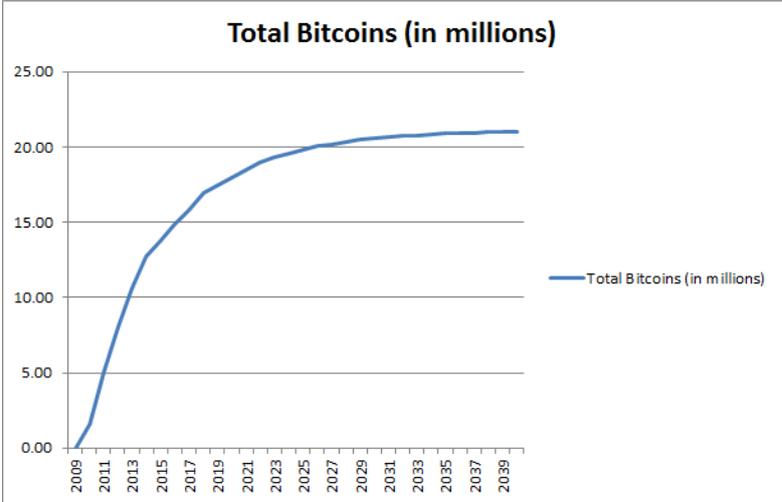


Figure 2: BTC’s programmed supply curve

Source: <http://compoundingmyinterests.com/compounding-the-blog/2013/11/11/the-rise-and-inevitable-fall-of-bitcoin-1.html>

As a mean to keep blockchain system working, while users are controlling transaction’s process, they are also playing the role of miners, by which their computers try to solve complex mathematical problems, and once they solve them, miners receive BTCs and transaction fees. This is a longstanding process, which can attract many users because of the possibility of getting rewarded, and the more miners working, the higher is the performance of the transactions system.

Mining is a rewarding scheme and therefore a source of income: “Whether a mining operation is profitable hinges on two main factors: bitcoin’s market value - which has hit record highs this year - and the price of electricity, needed to run the powerful hardware” (Chun, 2017).

The popularity of mining as a profitable activity is perfectly exemplified by Venezuela's case. Home of a hyperinflation crisis, Venezuelans find BTC as an escape from the low value of their currency. Besides, "power is so heavily subsidized that is practically free." (Chun, 2017).

As already mentioned, BTCs are a scarce resource and one day they will be all out in the market.

This fact unleashes the following question: What will happen when all BTCs have already been discovered? As most of the motivation of mining is the rewarding system, the only source of income that miners will have are the transactions fees. In the opinion of Faggart (2015), the main concern, is "whether or not transaction fees will be enough to keep miners financially afloat."

The next two Sections will introduce the requirements for doing transactions using BTCs and the decisions that must be made prior to that action.

2.5 Wallets

The first step of BTC's experience is to obtain a digital wallet. Digital wallets have the same purpose of existence as physical wallets. Both are used to carry the necessary information that enable transactions. While physical wallets contain currency, digital wallets used for BTCs store a private key which identifies the owner of the wallet and empowers it with the right to use digital money. Approving transactions can be considered the main function of the wallet, as information about the number of available BTCs is, as described in [Section 2.3](#), part of the blockchain. The private key is defined in cryptographic algorithms such that is untraceable, consequently if a user loses or forgets this information, the BTC wallet will be lost. In addition to holding a private key, wallets also include a public key which has the same function as a bank account number, making it the only identification of the owner in the network. Therefore, anyone can use the network and preserve total privacy.

Currently, there are four types of wallets: desktop, mobile, web and hardware.

Desktop wallets require installing the peer-to-peer software in the BTC foundation website: (www.bitcoin.org). After the download, the computer will act as the wallet.

Mobile wallets are designed to perform physical payments in stores, as they have near-field communication, enabling to tap the phone against a reader and pay with BTCs without having to enter any information at all. Taking into consideration that mobile devices have lower memory capabilities, they are not required to download the blockchain, and because of that, they are not considered full BTC clients.

Web-based wallets consist of storing the private keys in a computer controlled by someone else, usually ran by an organisation, which has the advantage of being accessible from anywhere, regardless of the used device, even though if not properly implemented or if the provider is not trustworthy, there is the risk of having the organisation controlling the private keys.

The last wallet type is hardware which consists of a device that stores private keys electronically, but the existing number is very limited and are still in a development phase.

The cost of setting up a wallet and being ready to use BTC is practically free, as only internet connection and power can be considered as such.

When choosing a wallet, a lot of research is recommended, as it is a dangerous step to start negotiating without a reliable place to store money.

Figure 3 shows the number of wallets variation in the last three years, accounting for a number of 15 million in the 3rd quarter of 2017, and a continuous growth during that period.

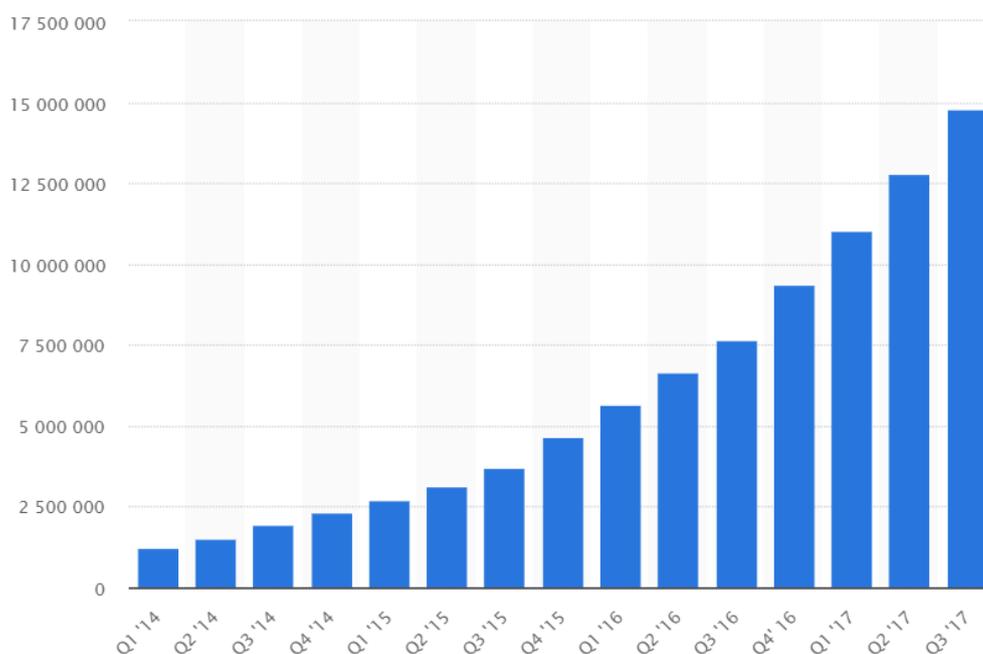


Figure 3: Number of wallet users worldwide from 1st Quarter 2014 to 3rd Quarter 2017

Source: <https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/>

The virtual place that carries BTCs has already been discussed. Following this theme, it is going to be shown where and how they can be acquired.

2.6 Market

There are three possible options to buy BTCs: the first one is a broker, the second one is an ATM, and the last option is through direct trading.

As a digital currency, BTC brokers are mostly online brokers. Once the user has a digital wallet, it can use traditional payment method, such as credit/debit card and bank transfer to transfer BTCs to its wallet. There are numerous factors to be considered when choosing an online broker:

- Exchange rate – global average price found on an Index is the most reliable source that guarantees a closer exchange rate to the current BTC's price;
- Payment method – besides the already mentioned possibilities, some brokers accept less traditional payment methods, such as paypal and paysafecard;
- Speed – since every payment method requires information verification, there are different speeds concerning BTC transfer. If urgency is necessary, the buyer should consider verification level and delivery speed of the chosen broker;
- Amount – there are buying limits for most BTC exchange. Most of them, are daily limits and favour regular basis purchasers;
- Fees - brokers charge a fee for every transaction to make their own profit; looking for the most economically viable broker is important, with special emphasis when making transactions of larger amounts of money;
- Privacy - exchanges that accept credit cards or bank transfers are required by law to collect information about users' identities. So, for privacy purposes, buying BTCs with cash is the best authorless option.
- Compliance – buying BTCs embraces private funds usage. Therefore, trustworthy is essential when choosing a broker. Most websites include information about their regulatory compliance, making less advisable trusting websites that might seem suspicious.

Another possible choice when buying BTCs is an ATM⁵.

The user introduces the money and brings the smartphone closer to the machine, allowing it to recognize the application's QR code. As any transaction requires miner's approval, this operation might take a few minutes to be concluded. ATM owner holds a tax on the transaction

⁵ ATM stands for Automated Teller Machine and consists of a machine that allows basic transactions without the intervention of a teller, such as raising money.

for its own profit. Currently, there are 1563 ATM's spread worldwide. This topic, will be furtherly developed in [Section 3.1](#).

The last available option and the most common one is direct trading, which consists of buying/providing goods or services in exchange for BTCs.

After exploring BTC's use as means of payment, another possibility will be presented, and that is acquiring this cryptocurrency as an investment.

2.7 Investment

BTC's market is often characterised as volatile. In finance, volatility is the degree of variation of a trading price series over time as measured by the standard deviation of the returns. In other words, it refers to the uncertainty or risk in the market price. This means that when facing highly volatile products, dramatic price fluctuations are expected.

BTC's volatility is exemplified in Figure 4, where 30-day volatility of BTC/USD, USD/EUR and Gold/USD are compared, using standard deviation of daily returns over a period of one year (September 2016 to September 2017).

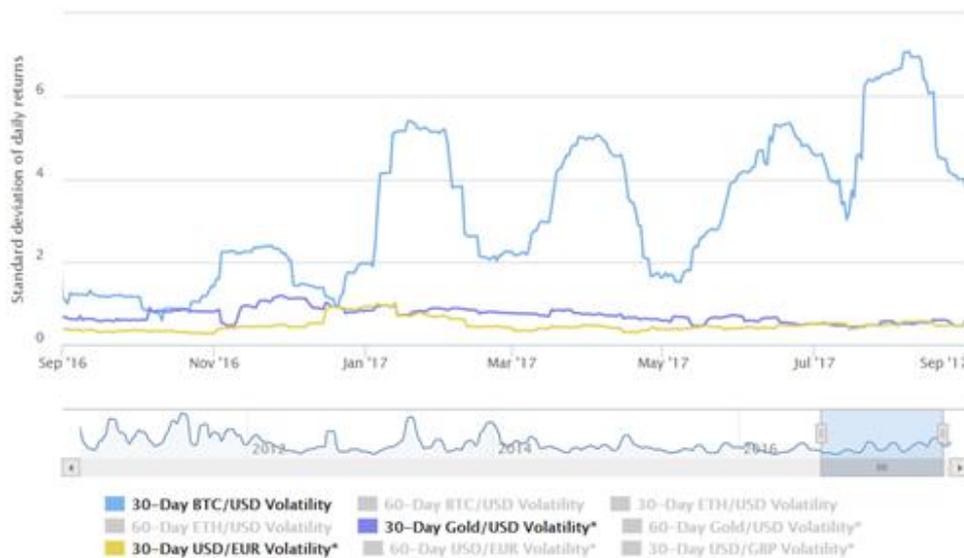


Figure 4: BTC volatility time series from September 2016 to September 2017

Source: <https://www.buybitcoinworldwide.com/volatility-index/>

While average volatility of gold for this period is around 1.2%, average for USD/EUR is lower than 1%. BTC/USD volatility for this period is close to 3%. The higher the standard deviation level, the higher is the volatility and, therefore, the increasing price fluctuations.

High volatility products favour short-term traders. Seeking for changes that occur second-to-second, minute-to-minute, and considering recent upward path that BTC has taken, which will be approached in the next Section, the chances of profitability are increased.

More conservative traders with a buy-and-hold strategy, which basically consists of buying a financial product and holding it for an extended period, can also benefit from BTC because of the already mentioned price increasing in the last years.

Another possibility when pursuing investment prospects is through investment funds.

In 2015, the Bitcoin Investment Trust (BIT) was launched as a publicly traded ETF (Exchange-Traded Fund)⁶. The objective of this ETF is to invest solely in BTCs and be an option for users that are afraid of direct investing in this cryptocurrency. Figure 5 shows the price variation in 2017.



Figure 5: BTC investment trust valuation in 2017 (USD)

Source: <https://www.bloomberg.com/quote/GBTC:US>

The average return of the ETF was 636%, recording a minimum value of 86 USD and a maximum of 1.064,95 USD during this period.

Now, it becomes pertinent to reveal what makes this topic of an increasing relevance.

2.8 Valuation

Why is it pertinent to study this theme?

In 2010 (one year after its launch), BTCs were getting traded for 0.003 cent USD/unit, seven years later, one unit of BTC is worth approximately 5.670 USD. This phenomenon has captured

⁶ ETF is a marketable security that tracks an index, a commodity, bonds, or a basket of assets like an index fund.

the attention of most financial leaders and a consensus about the future of this cryptocurrency has not been reached.

Nobel-Prize winner Warren Buffet (2014), said that BTC is a “mirage”, arguing that it has “no intrinsic value”. Even though he considered BTC to be an “effective method of transmitting money”, he compared that same purpose to the use of a check, concluding that checks are not worth a lot of money and for that same reason neither are BTCs. Despite his statement, the price of BTC has not left a growing path.

Figure 6 exhibits the price increase of BTC from 2011, back when the currency was worth close to nothing, to 2017 when it reached its higher ever value.

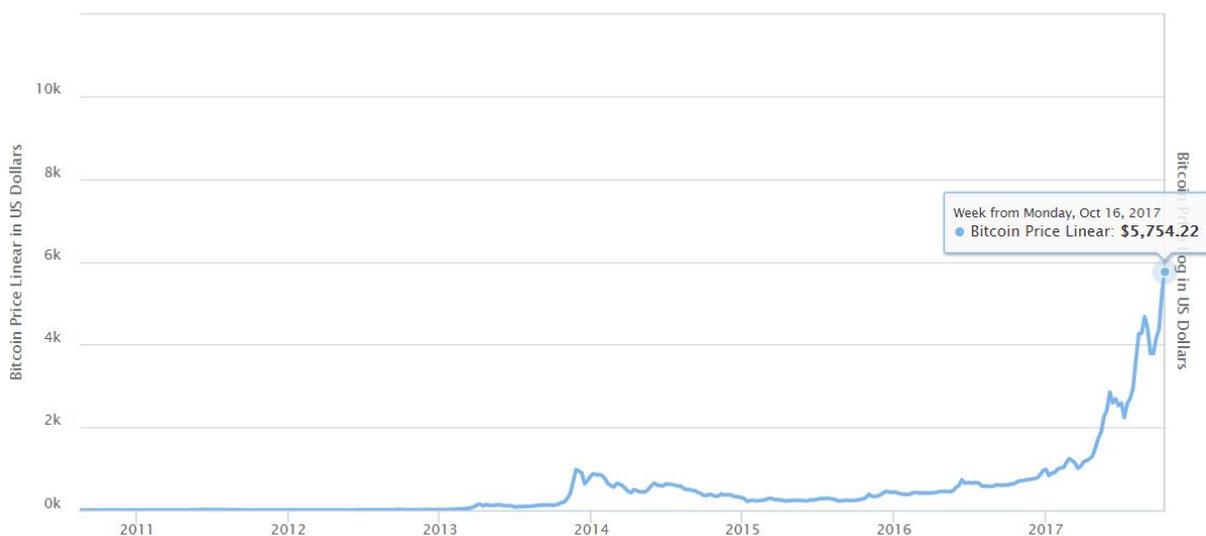


Figure 6: BTC price in 2011-2017 (USD)

Source: <https://www.coindesk.com/price/>

BTC basics have already been stated. Further Sections will approach specificities of the already mentioned concepts and the applications that derive from them.

2.9 Research Topics

Given the existing literature and considering the concepts that are the basis for BTC’s system and that have been previously introduced, the following topics will be furtherly analysed:

- ATM/Physical stores distribution
- Cryptocurrencies legislation/taxes
- Digital payment system adoption
- Blockchain technology

- Mining activity
- Cryptocurrencies market

After achieving a deep knowledge about these topics, most controversial themes will arise and create the main issues that this thesis will try to address.

Section 3: BTC in Portugal: Current Overview

While the first part of this thesis mainly focused on analysing the most important aspects of BTC's system, this Section presents an overview on BTC's current Portuguese market penetration. The objective is to provide an insightful overview about what has already been implemented and what can be done in the future, considering potential opportunities and threats.

Firstly, statistical data will be presented, namely touchpoints between the consumer and BTC. Secondly, the approach will consist of analysing current legislation, with a main concern on taxes. Lastly, a few topics with considerable relevance for the Portuguese economic system will be examined.

All these topics will be scrutinised in a comparison with the rest of the world.

3.1 ATM Locations

We start by looking at ATM's distribution.⁷ October 2014 marks the launch of the first BTC ATM located in Portugal whose purpose was to exchange local currency (Euros) for BTCs and its reciprocal.

The chosen location was Saldanha Residence, near the cinema located in that shopping center, as its technological characteristics were believed to be ideal to give ATM the necessary exposure. That is, rather than being an optimal location for trading exchange, the objective of this ATM was to create media and social impact. The company responsible for this machine declared the success of this operation, even though the ATM was posteriorly closed.

Figure 7 shows the current available BTC ATMs in Portugal. The only ATM active is located in Funchal, Madeira.

⁷ The concept of ATM was already introduced in the previous Section.

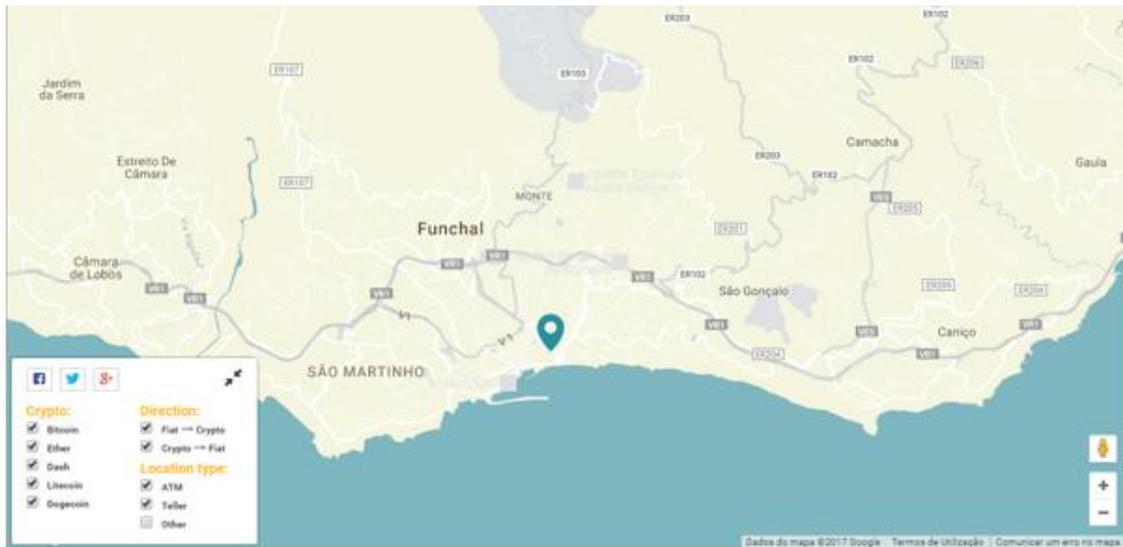


Figure 7: Total number of BTC ATMs located in Portugal (including machine and/or teller)

Source: <https://coinatmradar.com/city/541/bitcoin-atm-funchal>

Figure 8 provides an overview on the number of BTC ATMs in Central and Western Europe.



Figure 8: Total number of BTC ATMs located in Central and Western Europe (including machine and/or teller)

Source: <https://coinatmradar.com/>

Spain has about 40 ATMs at this moment, and the European leading country is England with 86. Despite the size of the country, Switzerland (28 ATMs) proof that it is not a matter of area dimension, but technological will. The same premise can be applied for France or Germany, but in a backward sentence, as they have few or none machines.

Figure 9 shows the increasing number of BTC ATMs worldwide. 2017 price boom was escorted by a huge growth in machine numbers. While 2014 ended with about 300 machines, nowadays, the total number is close to 1600.



Figure 9: Number of BTC ATMs installed over time (including machine and/or teller)

Source: <https://coinatmradar.com/charts/#by-country>

United States is the leading country with 989 locations, followed by Canada with 234. The top five closes with three European countries, the two already mentioned (England and Spain) and Austria.

From the exposed information, we can see that in Portugal, ATMs are scarce and the BTC market is much less developed when compared to other countries.

3.2 Physical Stores

We move to analyse the existence and distribution of physical stores accepting BTC as a payment method.

The reason that explains online shops exclusion from this study is that exclusively Portuguese online stores are not representative in Portuguese total market. Even though physical stores do not represent all commerce, as e-commerce is not included, and also taking into account that BTC might be headed to this second type of market, the possibility of using BTCs in every transaction that is made induces consumer orientation towards its use.

Figure 10 shows BTC acceptance in Portugal. Lisbon represents the highest density region, but there are a few spots all over the country.

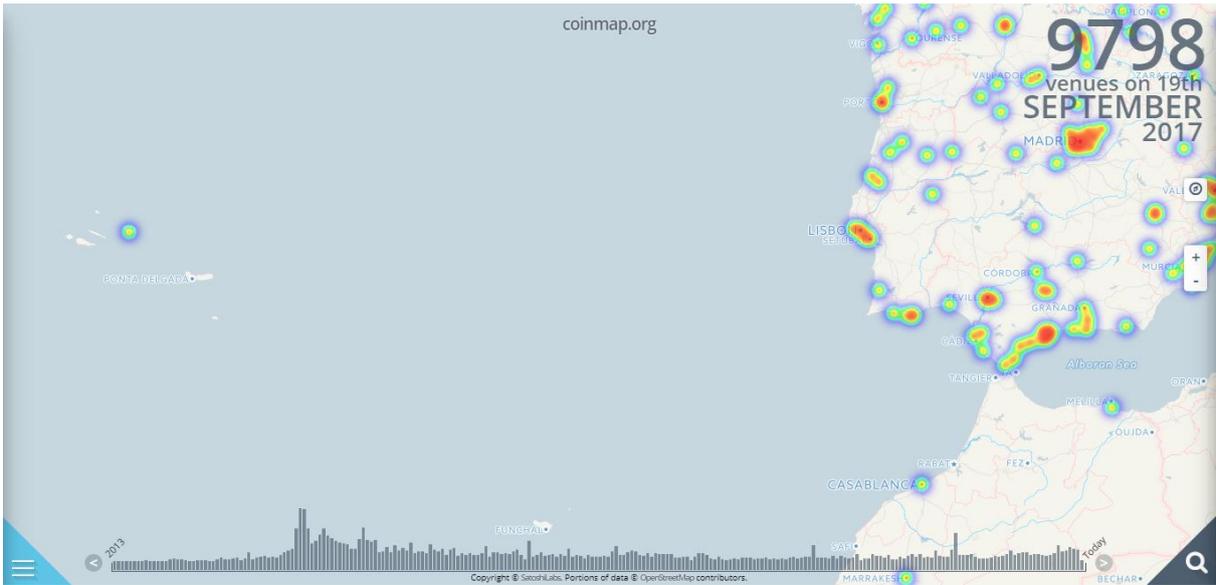


Figure 10: BTC acceptance physical store density per region in Portugal

Source: <https://coinmap.org/#/world/37.43997405/-15.35888672/6>

A closer zoom allows to find the exact location of the shops, in Figure 11. The total number of shops in Lisbon is 20 (including suburbs) and it includes dental clinics, lawyers, hotels, bars and a few other businesses.

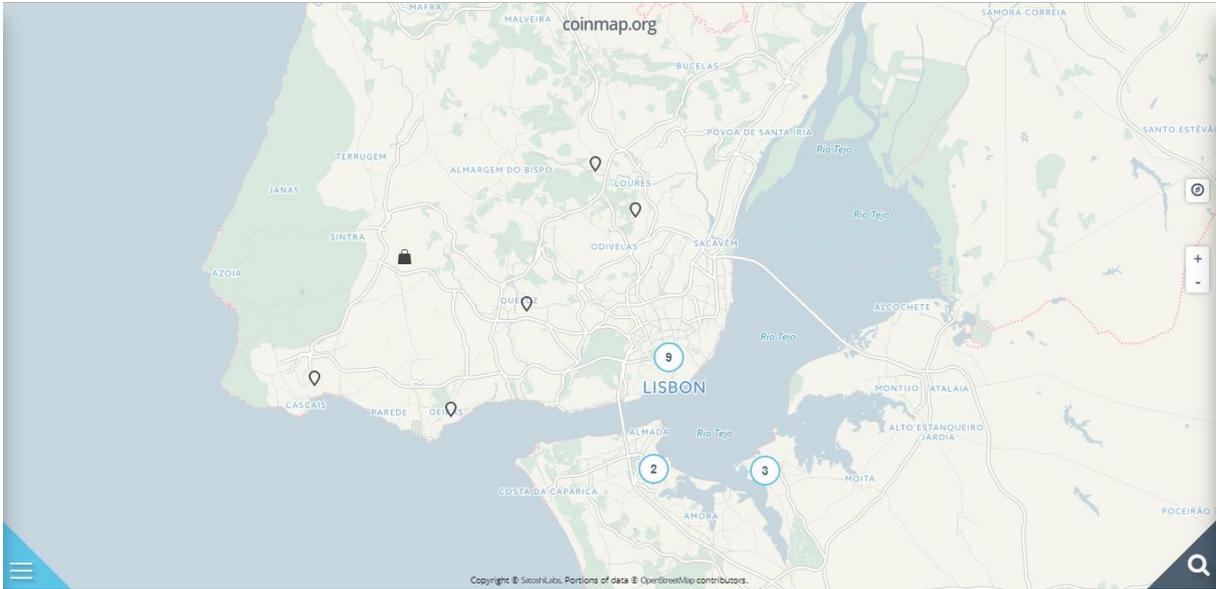


Figure 11: BTC acceptance physical shop density in Lisbon

Source: <https://coinmap.org/#/map/38.76265034/-9.18663025/11>

Once again, the comparison has to be made. Madrid has over 90 physical stores accepting BTC as a payment method. The countries that show higher density are England, the Netherlands, and

some Central Europe countries such as Austria, Czech Republic and Switzerland. This distribution can be observed in Figure 12.

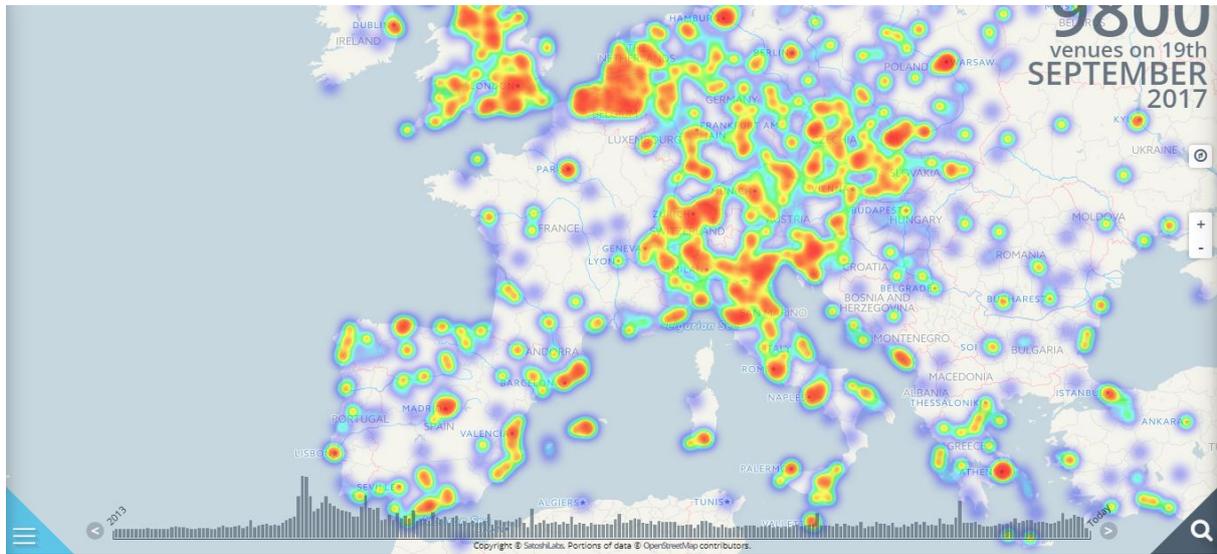


Figure 12: BTC acceptance in physical shop density in Central and Western Europe

Source: <https://coinmap.org/#/world/45.73685955/4.52636719/5>

Overall, Portugal shows undergrowth facing other countries.

3.3 Cryptocurrencies Legislation

As an European Union (EU) member, Portugal has to comply with its legislation.

In October 2015, the Court of Justice of the EU stated that exchange of traditional currencies for BTCs is exempt from Value-Added Tax (VAT). According to judges, the tax should not be charged because BTCs should be treated as means of payment and that is why the EU has not passed specific legislation relative to BTC as a currency. However, paying for goods or services requires both VAT and income tax. Regarding taxing profit from those transactions, European Central Bank (ECB) considered that existing rules do not apply to BTCs as it does not involve traditional financial actors. However, current rules can be extended to include BTCs and related companies.

As for ECB, it categorizes BTC as a convertible decentralized virtual currency.

Summarising, currency exchanging transactions are exempt from VAT, although the profit can be taxed if the country decides to. About transactions made using BTCs to pay for goods or services, both VAT and income tax must be applied. EU and ECB have different views on

BTC's classification, as the first one, only treats it as means of payment and the other sees it as a virtual currency.

Both these entities have shown concern on the possible use of BTC for money laundering and terrorism. In 2016, the European Parliament approved a proposal to set up a task force to monitor virtual currencies to combat the already mentioned threats.

In October 2012, ECB released a paper named: "Virtual currency schemes" (ECB, 2012). In this paper, BTC is given as an example of a virtual currency scheme. The main issues regarding BTC use are the transparency of the system, lack of legal status and security.

After looking at the European scenario, attention will be given to some important examples at a global scale.

In April 2017, Japan officially recognized BTC as currency, along the lines of other fiat currencies. This privilege led to the implementation of additional regulation, already applied to banks and financial institutions. BTC will have to comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements and will be scrutinized by annual audits:

- AML – policies that allow the authorities to easily detect money laundering schemes;
- KYC – identification of customers who open accounts, keep transaction records and notify the authorities when a suspicious transaction is recognized.

After BTC legalization in April, Japan has been focused on developing better strategies to track down possible threats. Following this movement, Australia has decided to join Japan and prepare its own legislation for digital currencies. Many Asian countries have taken an official position regarding BTC's use, most of them allowing it and only expressing their concerns on illegal activity such as money laundering. There are also a few countries who are said to be preparing legislation on this subject. Two countries have decided to ban BTCs: Bangladesh and Kyrgyzstan.

North American countries have different views: Canada classified BTC just as intangible, and regulates its use under anti-money laundering and counter-terrorist financing laws. United States of America classified BTC as a commodity, just like gold or petroleum.

Most African countries have not passed any official information regarding a possible legislation towards its legality or prohibition.

Central and Southern American countries followed African's trend, with two exceptions: Ecuador and Bolivia. Both countries banned the use of BTCs.

Lastly, most European countries have been permitting the use of BTCs, even though most of them express aversion to the risks of the cryptocurrency not being controlled or regulated by an entity. Iceland is the exception, as this country has decided to ban the use of this currency for any purposes.

Figure 13 shows each country's position about BTC's legality.



Figure 13: BTC's legality country position

Source: <http://bitlegal.io/>

While North America and Europe adopt a more permissive posture, Asian countries and Russia are more contentious. African and Central and South American countries position is still unknown, as they have not made any political exposure. Even though it is not represented, Australia follows Asian posture.

Overall, most developed countries seem to be aware of BTC's existence and have taken actions towards regulating its use. Portugal, as an EU member, must obey to this organisation's rules. However, as it still misses specific legislation on this subject, and also considering that other members have already taken an official position, Portugal can define rules to judge BTC's transactions.

3.4 Cryptocurrencies Taxes

In April 2017, a journalist from a national newspaper⁸ made an attempt to understand if BTCs were taxed in Portugal. He called several members of Finances Ministry and the answer, even though it took a little long, was a no. This answer is the opposite from the one given by the AT (Autoridade Tributária).

AT bases its answer as they categorise BTC's income as profit distribution and therefore, they should be classified as capital gain for tax purposes. This profit distribution implies an entity, and AT classifies it as non-resident (foreign entity).

A few months later, the Ministry issued a statement, agreeing with AT and reporting that if consumers who work with BTCs make it a professional and/or business activity out of it, they should be taxed.

Given the increasing need, Banco de Portugal (BP) issued a statement declaring the insecurity of using BTCs, mainly due to the lack of supervision from any official entity (BP, 2013). However, it recognizes a possible future necessity of monitoring the phenomenon of virtual currencies.

In order to compare Portugal to other countries, two European countries will be examined: Germany and the UK. The first one, considers BTC as a type of private money and taxes 25% of capital gains, only if those happen within one year after the receipt of BTC. If this situation does not happen, the cryptocurrency gains will fall into the category of non-taxable. UK treats BTC as a foreign currency, and tax rules applying to currency gains and losses are used for BTCs, however there are exceptions to the primary rule, as all cases are based in their own individual facts and circumstances.

Summarising, in Portugal there is a lack of specific legislation, as the current one does not include BTCs. Though, efforts have been made to tax the cryptocurrency in Portugal. Nevertheless, agreement over taxing is not clear. Overall, it is clear that the EU countries' profit from BTC's transactions can be taxed even if not included in the existing European law. However, this is not mandatory, as it is an extension from existing rules. Despite EU's statement over BTC's taxes, they have not passed specific legislation on this theme. Many European countries took official positions on this matter, either encouraging BTC's use or disallowing it.

⁸ Mariana Adam from Jornal de Negócios carried this investigation and published the article: "Bitcoins are not legal however they may have to pay taxes" on 23th June 2017

This said, the lack of legislation can be imputed to the Government's absence of action. Regarding tax issues, Portugal seems to have adopted the idea of taxing these transactions. The Portuguese AT classifies these as foreign capital gains.

3.5 Financial Prospects

Tourism

In December 2015, a small island off the shore of Madeira, commonly known as Principality of Ponta da Formosa and whose independence has been under disputation, declared BTC as its national currency (Dotson, 2015). While this event might go unnoticed for most of the Portuguese population, especially due to the lack of credibility that this Principality owns, this currency adoption can be considered a market strategy in two ways: first, because of the press cover around the world, willing to get to know this pioneer country, and second as a tourist attraction, who are curious about this odd law implementation.

Another example of an impactful story was Felix Weis, a pro-BTC who wanted to show that it was possible to travel around the world exclusively using BTCs. He settled a few rules for himself, such as prohibiting the use of banks and local currency, except for BTCs exchanging, and he started an eighteen months journey. He visited countries like Cuba, Switzerland or Australia, at least one in each continent. He did not go to Portugal.

As a significantly growing practice, tourism plays a main role in the Portuguese economy. Everything that can be a tourist attracter should be implemented and all the events that could be a potential exclusion factor should be avoided. Implementing BTC as a main currency is unthinkable, but creating the necessary environment for its settlement in the commerce and supporting companies and initiatives that advertise this type of digital money, would show compromise in creating infrastructures and public knowledge regarding a successful market penetration. Being a leader, in this case, could be another key appealing factor that boosts country visits. So, instead of just following other countries and their practices, the integration method could come from Portugal's Government.

Financial System

In the last few years, the Portuguese financial system has suffered huge losses. Banks went into bankruptcy and only Government help allowed some others to survive, namely Banco Espírito Santo (BES) or Novo Banco (NB). Even though existing laws protect bank deposits up until a money limit, the same does not happen with bank shares. Therefore, not only bank deposits

higher than the stipulated level, but also shareholders lost their money when banks were closed. The described events lead to a growing distrust in the current financial system of the country. BTC could be seen as an alternative, because it avoids financial institutions. However, there are few information sources and little literature as well, which combined with the lack of investment in cryptocurrencies from local businesses (as already mentioned during this Section) does not provide enough support for BTC's market penetration in Portugal.

BTC's impact in media and social media, considering media as all information provided by journalism and social media as consumer discussion using digital technologies is not significant. In Portugal, media coverage on this subject has been focused in the financial aspect of BTC, namely the incredible price increase over the last years. There are not many social information sources, a few blogs, some social media pages and a few discussion forums.

Missing social media attendance is the result of the lack of interest or knowledge from the population. Being digital market an increasing force that drives consumer behaviour, it is of utmost importance to encourage discussion on this subject. Once the Government starts giving attention to this subject for legislation purposes, it is expected an increase on public awareness.

Section 4: Key Concepts: Further Development

The following Section aims to present a further development of the key concepts of BTC, which were defined in [Section 2](#). In accordance to this thesis' purpose, the chapter goal is to identify the most debatable topics concerning BTC.

4.1 Digital Payment System Adoption

“Cash had a pretty good run for 4,000 years or so. These days, though, notes and coins increasingly seem déclassé: They're dirty and dangerous, unwieldy and expensive, antiquated and so very analog” (Bloomberg, 2016).

In an increasingly technological society, the use of physical money is becoming obsolete.

Sweden is considered the European leading country in a cashless society adoption. “According to central bank the Riksbank⁹, cash transactions made up barely 2% of the value of all payments made in Sweden last year” (Henley, 2017).

In November 2016, the Government of India announced a demonetization scheme, consisting of removing 86% of its currency from circulation. The government claimed that the action was taken in order to crack down on the use of illicit and counterfeit cash to fund illegal activity and terrorism, as “corruption and black market is a big hindrance in removing poverty” (Singh, 2016). The implementation process has been slow, but “even the vegetable vendors on the streets have opened up Paytm¹⁰ accounts and they have a machine outside their shop where someone can scan the bar code and make the payment” (Shepard, 2016).

A recent inquiry conducted by KMPG India in 2017 (after the demonization adoption) about digital payments lead to the conclusion that 88% of the inquiries prefer a cashless payment and 48% of the respondents were already using this sort of transaction in 75% of their payments. Also the most important factors that are enhancing the use of digital payment are, as shown in [Figure 14](#): ease of doing payments and tracking of all payments.

⁹ Sweden's Central Bank.

¹⁰ Paytm is an Indian electronic payment and e-commerce brand based out of Delhi NCR, India.

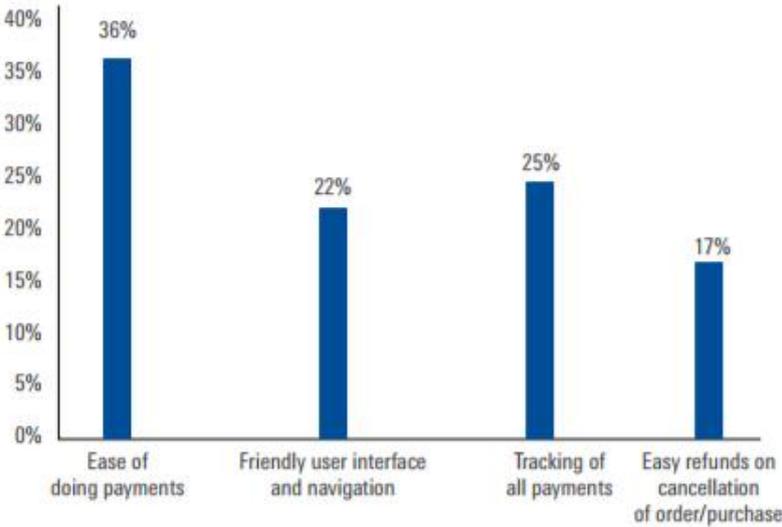


Figure 14: Factors enhancing use of digital payment

Source:https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analysing_the_cyber_landscape.pdf

The same study concluded that the two major causes that act as barriers to adoption are cybersecurity and awareness. Cybersecurity comprises not only security concerns, but also the absence of a strong ecosystem for cashless payments. Figure 15 illustrates this scenario.

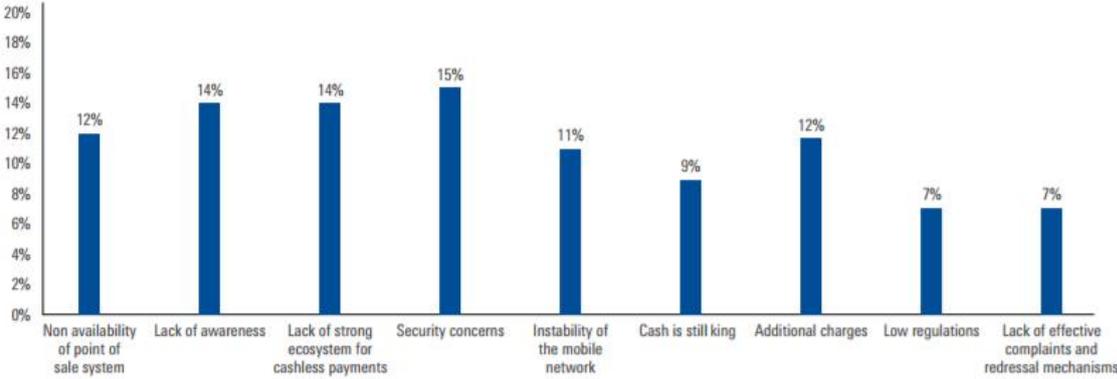


Figure 15: Digital payment: barriers to growth

Source:https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analysing_the_cyber_landscape.pdf

Another conclusion from this study was that the increase in volume of digital payments was mainly in digital wallets. Figure 16 illustrates this situation.

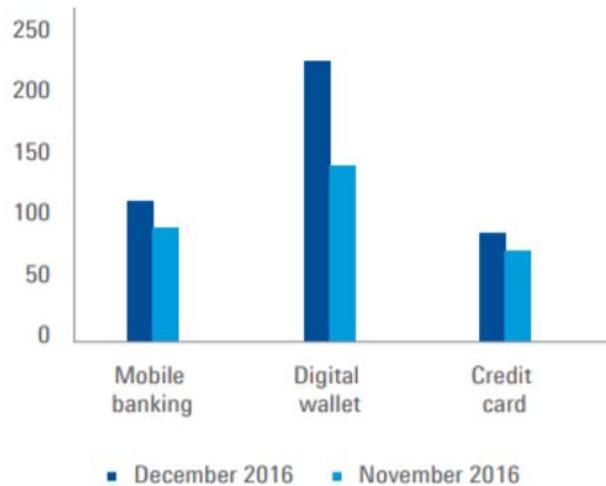


Figure 16: Increase in volume of digital payments

Source:https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analysing_the_cyber_landscape.pdf

Despite security issues, many countries already reflect signs of moving towards a cashless society, either by citizen's adoption or by law enforcement.

The benefits of adopting digital cash include better tracking financing routes and therefore, controlling illegal activities. Also, being able to record every transaction, allowing to apply appropriate monetary policies, such as tax deduction. Moreover, it allows simpler, easier and borderless transactions, as already mentioned in [Section 1](#). However, transaction tracking also concern privacy issues, "as in a digital-only economy, governments and banks could take control of your financial life; with a flick of a switch, they could leave you without a penny. Networks can fail. You could lose your mobile phone. And everybody could be vulnerable to a cyberattack¹¹ or power outage, which is why the U.S. government encourages citizens to keep some cash on hand for emergencies" (Sivabalan, 2017).

As shown, society is moving towards digital payment system's adoption, however, BTC adds something different, which is decentralization. For that reason, the user's privacy is kept, but since no entity controls the system, other fears arise. Additionally, there's the security of the system which is guaranteed, in BTC's case by the blockchain technology.

A Wonglimpiyarat (2016: 8) study considered that BTC was target of slow-adoption from the market, being the main reasons for the slow rate, the wallets being vulnerable to theft and loss and the lack of Government support which impacts on the adoption of central banks. Therefore,

¹¹ This topic will be deeply analysed in the next Section.

the study indicated that BTC's payment infrastructure needed improvement in order to fulfill the security requisites. Though, this study also concluded that there seems to be a trajectory in today's payment system, moving from a cash-based economy towards a less cash society, based on the development of digital money, specifically BTC.

Another study (Tasca, 2015: 78) focused on understanding the future development of digital currencies, having concluded that in the upcoming digital era characterized by a cashless and a massively connected society utilizing high frequency transnational transactions, currencies need to fulfill one need, which is reduce market frictions, allowing its users to make efficient expenditure decisions. In order to satisfy this requirement, the study proposed a multi-currency wallet, with instant conversion between the supported currencies, permitting users to spend different digital currencies in the same transaction.

A cashless society is said to be the future of money, but that does not necessarily mean abolishing the use of fiat currencies. In order to do so, society would have to trust the payment system, allowing the absence of third-party control, and that implies additional improvements in the systems.

4.2 Blockchain Technology

Like previously mentioned in [Section 2.3](#), blockchain is what is really disruptive about BTC, as this technology allows network decentralization. The applications for this technology are many. In this Section, the most significant will be examined.

Digital Identity

In 2013, Target Corporation, one of the biggest retailers in the United States of America, suffered a cyberattack, allowing the access to 41 million customer identities, including full names, phone numbers, email addresses, payment card numbers and credit card verification codes. This event resulted in a loss of 18,5 million dollars for this company, which included compensating clients who suffered losses and a multistate settlement as a penalty for not following all the required security rules (McCoy, 2017).

Another more recent example, had Deloitte as a target. In September 2017, the global accountancy firm, was hit by a cyberattack, compromising the data of a small number of clients. The company decided to mobilize a team of experts in this matter, which would review the system and find possible breaches. Having the duty of protecting financial information about their client partners, Deloitte could have potentially damaged its image (Hopkins, 2017).

“Lloyd’s of London has warned that a serious cyberattack could cost the global economy more than \$120bn – as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy” (Kollewe, 2017). Lloyds Bank, the second oldest in the United Kingdom, published a 56-page report on this subject, two months after a cyberattack that harmed National Health Service hospitals in the United Kingdom.

According to Blockchain Technologies Website: “Blockchain offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner. Blockchain-based authentication systems are based on identity verification using digital signatures based on public key cryptography. In blockchain identity authentication, the only check performed is if the transaction was signed by the correct private key. It is assumed that whoever has access to the private key is the owner and the exact identity of the owner is deemed irrelevant.”

MIT also found usage for this technology. “The app is called Blockcerts Wallet, and it enables students to quickly and easily get a verifiable, tamper-proof version of their diploma that they can share with employers, schools, family, and friends. To ensure the security of the diploma, the pilot utilizes the same blockchain technology that powers the digital currency Bitcoin.” (Durant, 2017). Summarising, it is a pilot project of the MIT that provides their students electronic diplomas that they can share with their contacts, and the security is enabled by using the blockchain technology.

Since the future is digital information, numerous other data sources could be mentioned and in which the blockchain could be applied, allowing a secure manner to carry vital information:

- IDs
- Passports
- Wedding certificates
- Birthday certificates
- Financial Authority Service ID’s

Cloud Storage

Cloud storage is a model of data storage in which the digital data is stored in servers, hosted by a company. Many big companies have models like this, namely Apple, Microsoft, Amazon or mail hosts. Currently, cloud storage services are centralized.

Company centralized hosting means that users must place trust in a single storage provider. The company controls the data and not only it can become accessible if cyberattacks happen, as already scrutinized in the previous topic, but also concern privacy issues (Rosic, 2016).

In a recent interview, Apple's Senior Vice President of Software Engineering Craig Federighi, spoke about differential privacy (Greenberg, 2017). This term refers to being able to learn as much as possible about a group, while learning as little as possible about the individual. The purpose of his intervention, was to emphasize that even though Apple focuses on developing its products based on customer's demands and that means having to collect information about individuals, all the gathered data is treated as a group, which is after translated into market needs. Consequently, individual information is not separately analyzed, and users should not be worried about having personal information inspected. Though, a blockchain storage provider would avoid this risk, as already explained in the previous topic.

Storj¹², an online startup storage provider, is currently beta-testing cloud storage using a blockchain powered network. The method that is being developed is to encrypt user's data and send it to a network of other users, being able to easily track it. Additionally, customers can rent out their excess storage capacity, creating new marketplaces. The system is similar to BTC's, as users can get rewarded by lending their computer while conceding privacy to the received information.

Digital Voting

A number of digital voting systems are currently in use in countries around the world. In 2005, Estonia was the first country having electronic voting and since then this nation has developed an e-voting system and has allowed it in the preceding elections. However, an Estonian municipal elections report in 2013, which was performed by a designated team, "observed election officials downloading key software over insecure internet connections, typing PINs and passwords in view of cameras, and preparing election software on insecure PCs" (Arthur, 2014). Norway also attempted to perform digital elections, but cancelled its trial of e-voting systems, because of citizens' fear regarding their votes becoming public, not being able to perform real elections using online system.

The main advantage of adopting such a system is allowing geographically remote citizens to vote through the internet. Moreover, it could increase the effectiveness of the system, as

¹² <https://storj.io/>

fraudulent votes would more easily be controlled and the system could also block common errors such as multiple candidates picking or no candidates at all. In addition, younger generations as technological adopters, would have an extra motivation to perform their citizen's rights.

A Barnes, Brake and Perry (2016: 13) paper proposed a solution to solve most of the digital voting problematics, basing their model in the blockchain technology. The idea is to make progress of the anonymity that this system allows, ensuring privacy is kept. In addition, security is assured by the regular use of the blockchain, by creating a powerful network of computer nodes, which would require an immense computer power to hack the system.

Overall, the blockchain technology seems to be a key driver of digital privacy and anti-hacking systems. As such, the importance of this technology and the potential it has to change many industries and aspects of our society is enormous. Tough, most of these applications are still underdeveloped. Still, several efforts have been made by important companies such as Tesla or IBM in order to provide services based on this technology. Market acceptance and development will rule blockchain's implementation as a leading force in many areas, but it seems like blockchain is here to stay.

4.3 Mining

In [Section 2.4](#) mining was introduced as a rewarding system for users that control the transaction's process. Mining rewards are paid to the miner who discovers a solution to the mathematical problem first, and the probability that a participant will be the one to discover the solution is equal to the portion of the total mining power on the network (Tulic, 2017). Consequently, participants with a lower power percentage, have a lower probability of discovering the next BTC. Moreover, mining competition has increased in the past few years due to the higher number of miners joining the network encouraged by the increasing BTC price, and the system is programmed to increase the level of mathematical problem complexity as the supply runs out.¹³ Every 2016 blocks that are mined, or approximately every two weeks, the difficulty of finding new BTCs is augmented. Figure 17 demonstrates the increasing difficulty over time.

¹³ Regarding the limited supply of 21 million BTC mentioned in [Section 2.4](#).

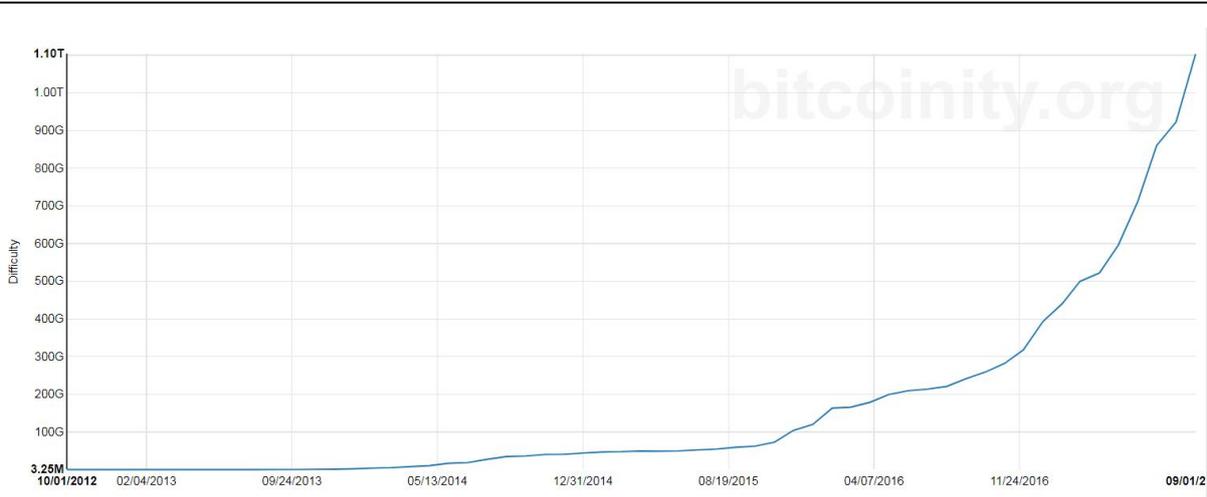


Figure 17: BTC mining difficulty

Source: <https://data.bitcoinity.org/bitcoin/difficulty/5y?t=1>

More demanding mining is associated with two computer costs: electricity and hardware (Coppock, 2017). The impacts of such are the devastation of midrange and high-end GPUs¹⁴ and increasing power consumption. The first fact lead to the appearance of companies dedicated to the production of mining equipment, namely powerful graphic cards, which were previously mainly used for video games. Concerning power consumption, cryptocurrencies has already surpassed the energy spent by some nations. Figure 18 shows that Bitcoin power consumption is already ahead of countries such as Nigeria, Oman or Bahrain, reaching a position in the top 70's.

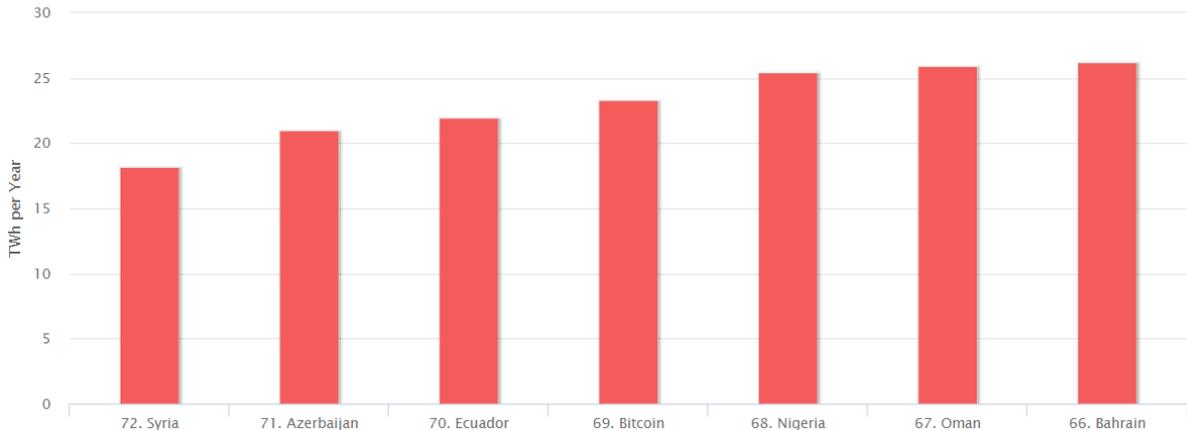


Figure 18: Energy consumption by country (in terawatt hours)

¹⁴ A Graphics Processing Unit (GPU) is commonly known as the chip of a graphics card.

Source: <https://digiconomist.net/bitcoin-energy-consumption>

Since mining is an investment in hardware and consists of a cost in electricity, in order to make this a viable activity as a miner alone could stay long periods without finding BTC's, mining pools are formed. These, consist of a group of miners working together and sharing their achievements. Currently, there are many mining pools, being China the top country, as it accounts for four of the top five groups. The other one is BitFury, a producer of mining hardware and chips, with three data centers in Georgia (Freeman, 2017). "In August 2017, a company co-owned by Russian President Vladimir Putin's internet ombudsman Dmitry Marinichev reportedly plans on raising as much as \$100 million in order to help Russian entrepreneurs challenge China's bitcoin mining supremacy". Challenging China's leadership in this market, Marinichev claims that "Russia has the potential to reach up to 30 percent share in global cryptocurrency mining in the future" (Memoria, 2017).

While the race for the cryptocurrency persists, there will be several interested parties in the continuing of BTC's appreciation. Though, this activity will not last forever, at least considering this scenario. As mentioned before in [Section 2.4](#), once the supply limit is reached, the profit will only comprise transaction fees.

4.4 Cryptocurrencies' Market

Recent Events and Forecasts

Two major events have negatively affected BTC in 2017: ICO ban in China and JPMorgan statement over BTC (Imbert, 2017).

ICO stands for Initial Coin Offering and it refers to fund raising for a new cryptocurrency venture in the market. In an ICO campaign, a percentage of the cryptocurrency is sold to initial backers of the project in exchange for other currencies (Marshall, 2017).

The process starts with a startup firm plan creation. This phase, consists of explaining what the project is about, what needs the project is addressing, the amount of funds that are necessary, project time extension and how many virtual tokens the pioneers will keep for themselves. If the project meets its initial requirements within the specified timeframe, the money raised is used to complete the new scheme, otherwise it is returned to the early investors.

The rationale of this process is very similar to crowdfunding, just instead of getting a participation in the company or a rewarding gift, investors keep tokens for themselves, hoping to have contributed for a successful plan, and, therefore, having a return on their investments.

An example of a fruitful plan is Ethereum. Currently the second most valuable cryptocurrency, it started with an ICO. This BTC alternative will be furtherly explained in this Section.

Unfortunately, some of these campaigns are fraudulent, and since there is no regulation on them, funds that are lost due to fake initiatives may never be recovered.

In September 2017, the Bank of China “said initial coin offerings are illegal and asked all related fundraising activity to be halted immediately” (Chen and Lee, 2017).

Following the China ICO ban, regulators instructed domestic BTC exchange platforms to voluntarily shut down their operations. One of those platforms, the Shanghai-based BTCC was the oldest platform still running processes, holding a record of 2.305 days of activity. This fact becomes interest to prove that most platforms have a short living period, as they are either scams, replaced by other competitors or shut down by local Governments.

The second event troubling BTC was performed by JP Morgan’s president Jamie Dimon. CEO of America’s biggest bank, he classified BTC as a “fraud” and that only “If you were in Venezuela or Ecuador or North Korea or a bunch of parts like that, or if you were a drug dealer, a murderer, stuff like that, you are better off doing it in bitcoin than US dollars” (Monaghan, 2017). Dimon also referred to this case as being worse than tulip bulbs in 1600s, which was considered the first speculative bubble in the history. Back then, people were trading tulip bulbs as a luxury item and without asset intrinsic value. As an example, at its peak, a single tulip bulb was sold for ten times the annual income of a skilled craftsworker. Dimon’s conclusion was that BTC will eventually blow up as it is just a speculative bubble.

Following this statement, John McAfee, known for his anti-virus software company McAfee, and currently member of MFT Capital Investments, a firm focused on BTC mining, argued that in order to create a BTC, his company spent around 1.000 USD per coin¹⁵. He also compared this to USDs creation cost, as it only costs the paper used. He concluded: “Sure it will rise and fall as all new technologies are. But at the same time, it is certainly not a fraud (Lewis, 2017).

Both these events occurred at the same time in the year, leading to a decrease in BTC’s value in the market. Figure 19 shows their impact.

¹⁵ Referring to the mining costs: electricity and GPU



Figure 19: BTC (USD) price 07 September to 07 October

Source: <https://www.coindesk.com/price/>

In the middle of September, BTC's price dropped to around 3.000 USD, after starting the month with a price estimated over 4.500 USD. Following China's positioning on BTC's, the majority of China's trading volumes moved to Japan and South Korea. Additionally, in the same month, Japan officially authorized 11 cryptocurrencies exchanges. As a result, the market absorbed part of the impact and recovered BTC price to above 4.000 USD. Moreover, BTC's transactions in China did not cease, they just moved to close neighbour countries or started being performed using other platforms, other than the one's already controlled by the Government with strict implemented policies and with shut down orders. Furthermore, as a decentralized currency, authorities cannot control citizen's involvement in those transactions, unless they implement the already mentioned in the previous [Section 3.3](#) KYC and AML policies in all platforms.

China's ban over cryptocurrency's exchange is probably "temporary" as suggested by Xinhua, the official news agency of the Chinese government. BTC should be back online once rigorous laws are released (Applancer, 2017).

Most recent negative influences have already been analysed. While countries are still developing financial structures to either avoid or embrace BTC's use, some are taking part in the technological and financial benefits of this cryptocurrency. Therefore, some positive impacts will be presented.

The Russian Central Bank is contemplating the creation of a national cryptocurrency named "cryptoruble". The designation comes from the obvious association with Russian's national currency, the ruble. While being sceptical about BTC, the Government sees many benefits from

the adoption of a national cryptocurrency. Olga Skorobogatova, Deputy Governor of the Central Bank said: “the creation (...) stimulates the growth of non-cash payments and electronic payments, including, possibly, cross-border payments” (Helms, 2017). Essentially, it is a mean of “avoiding cash”. She added that “it is becoming more convenient for all users to pay for goods and services through electronic wallets, and the digital currency can play the role of a catalyst for using it for payments in a broader sense.” Furthermore, the Central Bank will focus on educating Russians about cryptocurrencies by paying more attention to existing literature on the subject, avoiding basic mistakes from the population. Russian First Deputy Prime Minister Igor Shuvalov emphasized that the implementation of this strategy should occur between 2017 and 2023 and that this is a step into strengthening Russian’s economy. Both the Government and the Russian Central Bank prepared the proposed plan.

The highlight of this proposal is the creation of something that could benefit the population in general, in an attempt to exclude what might be considered problematic regarding cryptocurrencies. It must be considered that Russian Central Bank has repeatedly spoken against the legalization of cryptocurrencies such as BTC. Recently, the bank’s governor Elvira Nabiullina said that legalization “is "actually a loss of control over the money flows from abroad (Helms, 2017).

Estonia, home of digital voting, has also been considering the launch of their own cryptocurrency: “estcoin”. The idea is to issue its own virtual currency with the help of Ethereum founder Vitalik Buterin, who has proposed an ICO for that purpose. Alongside this initiative, the Estonian Government has also started a project called e-residency, which consists of a “digital ID for non-Estonians that offers access to services like banking, payment processing and taxation”. The Governments’ expectation is to create a “borderless digital nation” (Browne, 2017).

Cristine Lagarde, head of the International Monetary Fund (IMF) also sees a path ahead of cryptocurrencies. Lagarde shared an optimistic vision about their future, claiming that “citizens may one day prefer virtual currencies.” The examples given to support her point of view were countries with weak institutions or unstable currencies. Instead of adopting the currency of another country, the adoption of a virtual currency is a possibility. Venezuela’s case was already stated in [Section 2.4](#), and even though it is far more associated with mining activities, only the use of BTC allowed this opportunity. Lagarde also considers that in remote regions, holding virtual currencies could be far easier than obtaining paper bills (Hackett, 2017).

Besides her positivity, IMF's boss only sees this scenario happening in a few years. For now, the market is still too unstable and not enough transparent. However, "issuance could be fully transparent, governed by a credible, pre-defined rule, an algorithm that can be monitored...or even a "smart rule" that might reflect changing macroeconomic circumstances." This statement clearly sustains the idea that Lagarde thinks that with proper recognition and treatment of political and financial institutions, virtual currencies can be part of the future.

Countries where a decentralized service economy is taking off are also part of Lagarde's vision. Small amount transactions in different coins have many complexities attached. Paying high exchange fees, payment delays, central registration or intermediary to check identities and accounts. Once people can rely on cryptocurrencies, they can solve this problem.

She also argues that "the best response by central bankers is to continue running effective monetary policy, while being open to fresh ideas and new demands, as economies evolve." (Hackett, 2017). Concluding, she sees cryptocurrencies appearance as an opportunity of monetary development if the society is able to adopt and adapt to the new demands it represents.

Price Prevision

Regarding price, it was already shown, in [Section 2.8](#), its increase over the years. However, this Section aims to analyse what are the predictions for the future.

BTC price dynamics has been a controversial topic since its creation. Garcia, Tessone, Mavrodiev and Perony (2014: 12) find that BTC's price fluctuation is largely related to public attention. The study comprised indicators such as search volume in Google engine, number of tweets, number of BTC client downloads and new BTC users, all of them in a comparison with BTC price in USD. The findings were that there is a correlation between all those indicators and price fluctuation. Also, the tested items were categorised as being image of public attention. Figure 20 illustrates the described logic. Moreover, growing popularity is a cyclical event, which means that "more interest encourages the purchase of bitcoins by individual users, driving the prices up, which eventually feeds back on the search volumes."

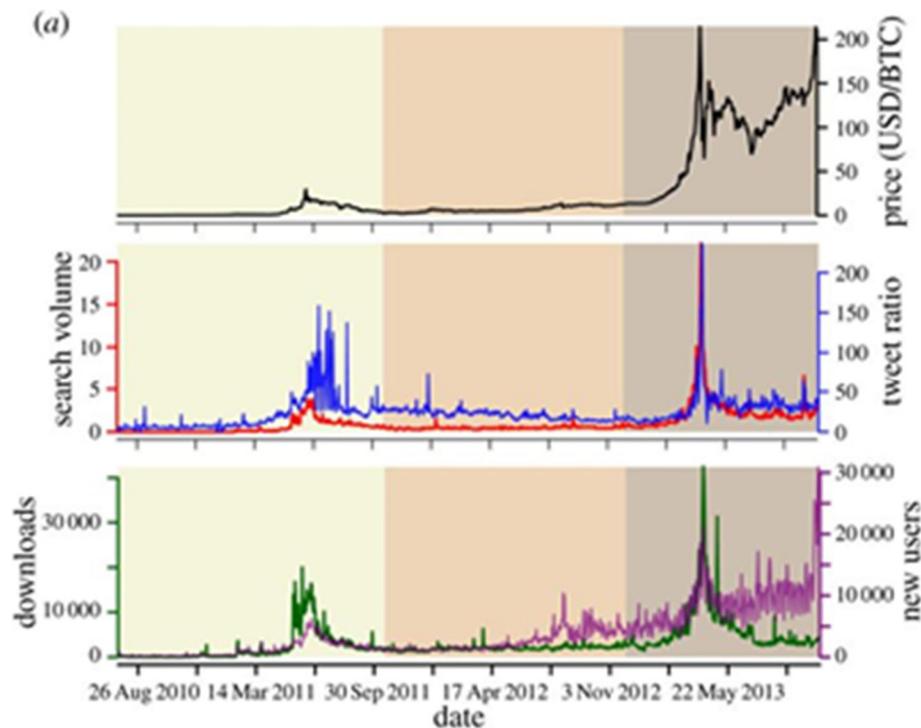


Figure 20: Correlation between public attention indicators and BTC's price (USD)

Source: <http://rsif.royalsocietypublishing.org/content/11/99/20140623>

Being popularity a cyclical phenomenon, BTC's success would be dependent on social media impact, market acceptance and a growing number of subscribers. Garcia *et al.* (2014: 12) also find that there are several price decreases related to distrustful events that had lately tormented BTC's raising. Cyberattacks were already discussed, but one that has not yet been mentioned, Mt. Gox's case lead to a several decrease in BTC's price in 2014. At that time, Mt. Gox was considered the biggest BTC exchange provider and was permanently closed after getting pillaged for a few days, losing 850 thousand BTC's of their customers, in an estimated value of 450 million USD's at that time. During that period, BTC's price dropped to nearly half of its value, in a period shorter than 15 days. Figure 21 illustrates the described price fluctuation.



Figure 21: BTC's price (USD) after Mt Gox's bankruptcy

Source: <https://www.extremetech.com/internet/177283-bitcoin-value-plummets-as-mt-gox-disappears-with-375-million-in-coins>

Kristoufek (2013: 2) also studied the mentioned correlation between public attendance and BTC's price, and added as information source Wikipedia, apart from the already used in the previous research Google. The conclusion of this study backed the idea of a bi-directional relationship, as "not only do the search queries influence the prices but also the prices influence the search queries." This connection forms an "environment suitable for a quite frequent emergence of a bubble behaviour" (Kristoufek, 2013: 5). When prices are high, the increase interest pushes price even further to the top, while the opposite rationale also applies, leading to deeper price decreases.

Public attendance is also related to consumer/merchant adoption, institutional tolerance, media cover and geo-political factors. These can be considered the main price-drivers of cryptocurrencies.

Knowing what supports this speculative market, lead to many studies trying to predict BTC's price, but none of them could determine the price boost in 2017. Though, Saxo Bank performed one close approach. The Danish bank, in December 2016, forecasted a triple market value of BTC, going from 700 USD to 2.100 USD in 2017. Even though that was not the case as the price almost reached 5.000 USD, multiplying by 7 the registered value in 2016, Saxo Bank was able to predict a major boost in this market, even if the forecast also advised consumers to monitor banking system's tolerance and Russia and China acceptance, as both could pose possible threats to the prevision.

Overall, BTC has become one of the hottest topics in the financial markets and every day a new financial-world heavyweight adds another opinion. Although BTC's awareness is supposed to increase over time regarding the enlarged media coverage, there are negative opinions concerning BTC's future, and many consider it to be a speculative bubble, able to explode and leave no trail.

BTC alternatives

After BTC's success, many other cryptocurrencies have appeared in the market, each of them with minor differences from each other and also fulfilling different needs. Currently, there are more than a thousand cryptocurrencies according to Coin Market Cap website in a total market cap of over 150 billion USD. Figure 22 shows the total market capitalization (including all the existing cryptocurrencies) since 2013.



Figure 22: Total market capitalization

Source: <https://coinmarketcap.com/charts/>

Throughout all the presented study, cryptocurrencies have been mentioned, but only BTC, as the main player in this market, has been properly approached. In the past few years, hundreds of new cryptocurrencies have appeared, and as some reach the spotlight, it seems like there is a trend to keep developing and improving BTC's initial technologies and apply them to new cryptocurrencies.

One of the main struggles that BTC has faced, is the length of time of a transaction, which is approximately 10 minutes. Litecoin (LTC) is a faster alternative to the original one. Currently, it has a market cap close to 2 billion USD, at an average unit cost of approximately 53 USD and a circulating supply of approximately 53 million units, which can ultimately reach 84 million total supply. The average time of a transaction using Litecoins is 2.5 minutes, making it 4 times faster than BTC.

Created by a former Google engineer Charles Lee, Litecoin's technology structure is much more demanding than BTC's structure, so that it can carry faster transactions. The advantages of having faster transactions are not only relying on time-consuming, but also in a higher volume of transactions in a shorter period and in better prevention of the already mentioned double-spending problem in case of a cyberattack attempt. Additionally, due to the higher market cap, which is about 4 times higher than the total of BTCs that can be mined, once the demand increases, there will be a larger supply to face it. Furthermore, mining is also part of this cryptocurrency and it is a faster task. Because of that, transaction fees are considerably lower, and that is why Litecoin is often preferred for performing smaller amount transactions (Coindesk, 2014).

The second most valuable cryptocurrency in the market is Ethereum. Apart from the use of the blockchain technology, this cryptocurrency adds something further to BTC, which are the smart contracts: "applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. These enable developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk."¹⁶ Starting with a basic function, user A could set a payment in a certain period of time to user B. Once the terms are agreed from both parties, that transaction would take place without the intervention of any of the users and the blockchain would take care of the legitimacy of the operation. The applications for this technology are many. A paper from the Chamber of Digital Commerce allied with Deloitte published in 2016, referred 12 businesses that could benefit from smart contracts. One of them is the insurance industry. The current problem with this business is that insurance companies take too long to take decisions due to the required large degree of human interaction, which ends up in a lot of administrative costs. Setting agreement on thresholds and conditions under which smart contracts would intervene, would force the events to happen without any human intervention. (Smart Contracts Alliance, 2016: 34). This example perfectly describes the use that can be given to most of the industries, which is cost and time saving through reduced human interaction and a secure manner to perform stipulated terms.

The ability to create irrefutable transactions, has been under observation by the main assurance companies. In charge of guaranteeing the correct execution of financial activities and taking

¹⁶ <https://ethereum.org/>

into consideration that accounting records are performed by the audited firms, the possibility of having a technology that can avoid errors or fraudulent behaviors could change the way this business is done. “Smith (2017: 3) concluded that “from an audit perspective, it is a great opportunity to start embracing the evolving concept of real-time, or continuous, auditing””. Though, the same paper claims that the first step of the implementation process is “an exhaustive assessment of the underlying cryptography, key management and security around the blockchain engine “

Another cryptocurrency in the top 5 of market capitalization is the Ripple. This currency does not share the same common characteristics of most cryptocurrencies, as Ripple is not decentralized. The purpose of existence of this cryptocurrency is to provide a transaction’s system for the Banking institutions. Figure 23 shows how transactions work in this system.

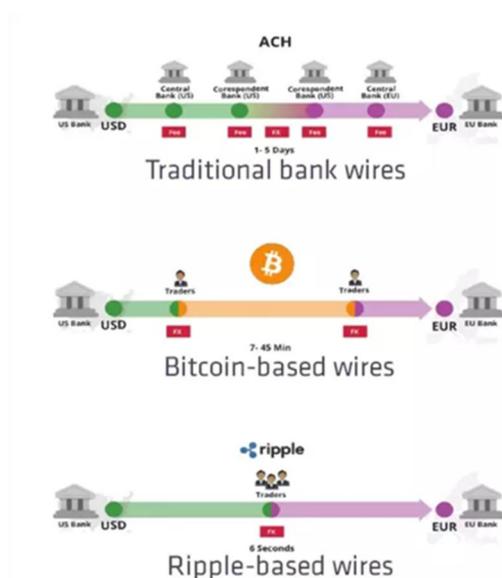


Figure 23: Ripple transaction’s system

Source: <https://www.quora.com/How-is-Ripple-different-from-bitcoin>

The reason for the allocation of this cryptocurrency to Banks is that transaction’s confirmation only takes about 6 seconds and allows cross-border transactions. Therefore, due to the usual costs and time expenditure of transnational transactions, Ripple was created to address the need of having “businesses sending more than \$155 trillion of cross-border payments annually”, according to Ripple Official Website¹⁷.

¹⁷ <https://ripple.com/use-cases/banks/>

4.5 Most Controversial Topics

The purpose of this thesis was the finding of debatable topics of BTC and accurately analyse them. After having furtherly developed the key concepts of BTC, and taking into account all the previous research, the following points will be considered for this analysis:

- Security/Credibility
- Transparency
- Technical Issues

Section 5: BTC in the World: an Insightful Guide

After having analysed the past, the present and the most predictable future of BTC, and having also examined the current BTC implementation status in Portugal, this last Section aims to approach the most prominent topics of BTC, with a special emphasis on Portugal. The topics that will be approached were already mentioned in [Section 4.5](#).

5.1 Security/Credibility

In [Section 2.2](#) decentralization was discussed and while opinions diverged about BTC's value, there was the consensus that security and credibility of any currency is deeply connected to the stability of its value. Cryptocurrencies in particular, also depend on user's belief that the system can protect their financial assets, as shown in [Section 4.1](#).

Concerning the first topic, BTC has not achieved price stability in the market, and exhibits high volatility across short periods of time like previously mentioned in [Section 2.7](#). Additionally, while fiat currencies can use an adjustable supply to stabilise the price, BTC's supply is limited and only increases through mining activities¹⁸. Moreover, public attention seems to be the only known driver of BTC's price, which ends in higher volatility, as shown in [Section 4.4](#).

“Eventually, attracting more people into the network will allow to decrease speculation behaviour and stabilize price” (Albrecht, 2013). Financial market leader's backup would also strengthen BTC's position and even though opinion makers have shown interest in this market due to its fruitful rise, some have doubted about its future success, which was stated in [Section 4.4](#).

A recent study conducted by Cambridge University (Hileman and Rauchs, 2017) revealed various aspects of BTC World such as total numbers of wallets, ATM dispersion or number of providers, but was unable to conclude on how many users exist, having invoked two main reasons: firstly, some individuals own multiple wallets or exchange accounts leading to multiple times counting. Secondly, some users use centralized wallets that pool funds together, which is particularly used in mining corporations¹⁹. However, a report from the Boston Federal Reserve estimates that 0,87% of United States of America consumers have owned cryptocurrency in 2015, which accounts for 2,8 million, solely in that country. Also, Coinbase and ARK Invest, two BTC focused innovation companies, reported an estimation of 10 million users in 2016 (Torpey, 2017). Despite facing the double counting problem, in [Section 2.5](#) it was shown that

¹⁸ Stated in [Section 2.4](#).

¹⁹ Stated in [Section 4.3](#).

currently there are about 15 million wallets and the number has increased in the last three years. While the number of users follow a growing path, in [Section 4.1](#) it were analysed the reasons that keep consumers away from mass consumption, being trust in the system a main issue.

The second topic relies on the functional system created to make BTC work. Blockchain, as the main technology that drives transaction's completeness, has showed to be an enthusiastic achievement, and many companies including financial institutions are already working on security systems based on decentralized systems that are quite similar, which was furtherly explained in [Section 4.2](#). There is a difference between trusting system capabilities and exchange or wallet providers, and as the first one seems quite reliable, problems concerning BTC disappearance such as Mt. Gox case are associated with dishonest providers (Khaliq, 2017). Therefore, it is not about regulating BTC's system, but institutionalise rules for BTC market related providers.

Overall it is clear that in a decentralized system, agents must be regulated in order to create trust among consumers. Given Portugal's current lack of national physical providers as shown over [Section 3](#), the Government must monitor web applications used, to protect their citizens from getting misled and follow Russia's example as stated in [Section 4.4](#), which implies educating its citizens by paying attention to the existing literature. Another deduction that can be made is that BTC's success is deeply connected to achieving stability in the market and that will only happen if people embrace its use.

5.2 Transparency

This term refers to BTC association with money laundering and as a mean to fund illegal activities, such as drugs or terrorists. This connection is based on two aspects: first, the system allows anonymity, as BTC's protocol does not require customer identification, and second as a decentralized currency, there is no financial or any type of entity controlling and authenticating transactions. ECB (2012) referred to BTC as a virtual currency scheme and mainly focused on transparency issues regarding the BTC system. This topic was developed in [Section 3.3](#).

A recent and controversial case was "Panama Papers", which can perfectly describe the problems of fiscal fraud and how anonymity can aid criminals through the use of offshores as a mean to make money untraceable. As already mentioned in [Section 3.3](#), many countries have taken official positions regarding developing and implementing policies that act over cryptocurrency transactions, having some countries taken more extreme positions and

forbidden its use. Japan, one of the most powerful BTC adopters, has been proactive on this subject, creating strict AML and KYC laws.

It is clear that the critical point here is that one thing is buying BTCs through an exchange, and another is peer-to-peer connection. While in the first case, AML and KYC laws perfectly apply and the buyer has to provide information about himself when registering, making the only threat having all suppliers properly licensed, it is much more complicated to monitor the second case, as the transfers are totally anonymous. Florida, United States of America, has decided to pass money-laundering charges against unlicensed BTC users that perform transactions. As a result, all types of unlicensed transactions became a crime. Additionally, some detentions have been made in that state, as there are many undercover federal agents seeking for criminals. The fear of being controlled is also a barrier to illegal activities (Parker, 2017).

Portugal, as an EU member must act in accordance with its regulation. However, in the absence of such and following what other countries have already pursued, the Government should create mechanisms to control peer-to-peer transactions and avoid criminal activity in its territory.

5.3 Technical Issues

Section 4.4 presented three of BTC's major competitors: Ethereum which can be considered its biggest rival, Litecoin which was presented as a faster alternative and Ripple which has the main purpose of addressing borderless transactions. However, nowadays there are thousands of cryptocurrencies, each of them with their own characteristics and different needs to address. BTC's protocol can be changed and adapted to new market demands, but it suffers from the evil of most technological product problems which is facing followers (Mohr, Sengupta and Slater, 2009: 53) and that is explicit in the cryptocurrency market share, which is exposed in the Figure 24 below. While in June 2016 BTC had a total market capitalization of 81%, one year later it has fallen below 50%. During this period, Ethereum has increased its market capitalization, while some other cryptocurrencies are also gaining market share. Despite the fearless competition, one conclusion can be taken: the total market capitalization has massively increased.

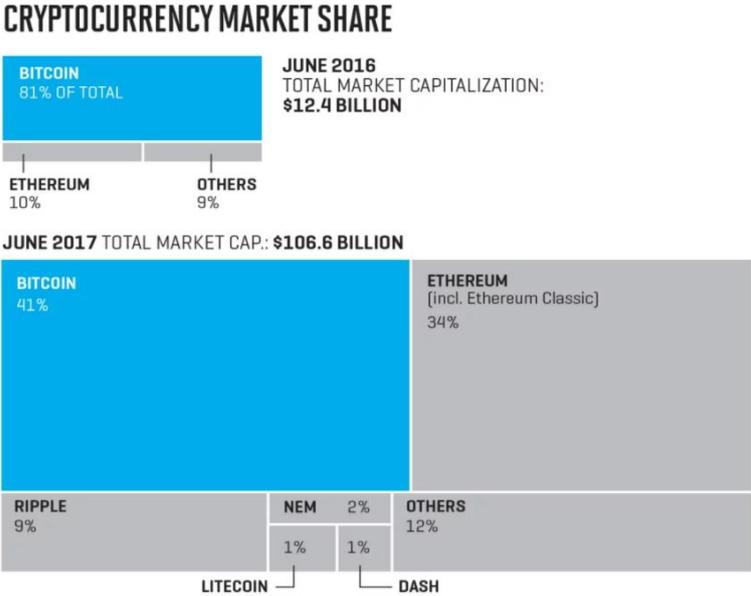


Figure 24: Cryptocurrency market share (June 2016 to June 2017)

Source: <http://fortune.com/2017/06/26/bitcoin-blockchain-cryptocurrency-market>

The new cryptocurrencies find in BTC’s weaknesses their entry into the market. Two main issues have been highlighted: transaction’s slowness and increasing hardware demand for mining activities. The first problem lead to the appearance of cryptocurrencies with a more powerful structure, namely Litecoin. However, BTC users have been working on a proposal called SegWit2x. The idea is to increase the network’s block size, allowing a faster and higher number of transactions, which will result in a more demanding system and therefore, higher transaction’ costs as more mining power is required (Hertig, 2017). If SegWit2x is accepted, mining activities will become even more demanding. The second topic boosted the arrival of mining companies, as formerly stated in Section 4.3. The only danger regarding powerful companies taking control is the 51% attack, which refers to the possibility of an entity having the majority of the hardware that supports the blockchain, allowing it to commit fraud (Khaliq, 2017). Though, the power required to perform such an action is difficult to obtain.

Another event that recently happened was the split of BTC into two divisions: BTC and BTC Cash. While BTC remains the same, BTC Cash is focused on global acceptance of cryptocurrencies, which implies a higher number of daily transfers. Whereas the old version allows 250.000 transactions per day, the new one is capable of around 2 million. Still, the market recognition of the new version was not as expected and the old version remains as the market leader.

Summing up, as a technological force, cryptocurrencies are still in a development phase, and as it happens with most innovative products, there seems to be room for further improvement. The upgrading progress combined with the reliability recognition from experts will define most of the cryptocurrencies' future.

Section 6: Conclusion

This dissertation presents Bitcoin and explores its characteristics and main functionalities, with the purpose of finding and inspecting the most debatable aspects concerning its use. Conceptualising this topic required exploring the blockchain technology, the mining activity and the market segment of cryptocurrencies, which includes wallet types, suppliers, investment options and valuation.

The Portuguese market current overview was discussed, considering relevant aspects of Bitcoin's implementation and which were introduced in the previous Section, such as ATM locations, number of physical shops accepting the cryptocurrency and institutional legislation, including tax control. All these indicators were analysed in a comparison with the rest of the World. Even though the Portuguese market has not massively adopted this cryptocurrency, there are positive economic impacts associated with Bitcoin's use, and in order to fully exploit them, some actions must be taken by the financial regulators.

Further development of key concepts provided information regarding the blockchain technology being a fundamental driver of digital privacy and anti-hacking systems, having the potential to change an increasingly digital World. Mining, as a profitable activity, has turned into a dispute of pools who desperately chase the next token.

Despite the discovery that Bitcoin's applications are many, in order to meet the initial expectations, this paper focused on perceiving the most controversial aspects of this cryptocurrency. The following topics were considered: security/credibility, transparency and technical issues. These topics were closely inspected allowing us to conclude that Bitcoin has been a resilient force in the market, but in order to achieve the required stability that is cursing its success, more people will have to embrace its use. Thus, despite being a decentralized currency, some stages of Bitcoin are provided by suppliers, that need to be controlled so that people can entirely trust the system and adopt it.

Another crucial point for Bitcoin's implementation is associated to illegal activities. While some countries have been adopting strict policies regarding user's identification, as transaction tracking is deemed impossible due to the decentralization, there is a deficiency in efficiently controlling the system, and as such, financial regulators must act towards accomplishing a capable solution.

Finally, as a technological force, Bitcoin's system is still in a development phase and some features need to be updated in order to meet the increasing market needs. This fact, combined with the price increase in the current year, has led to the appearance of market competitors.

Regarding future work, Bitcoin has been in a rapid increase throughout this last year, but as its development go beyond the expectations, theories concerning its future are constantly changing. Therefore, as time goes by, most studies get outdated and a similar structured paper to this one that is performed within one year shall come with different results. Hence, updating the developments of Bitcoin will consist of a very important and interesting subject for future research.

Another possibility is one of the introduced topics, which consists of the existence of alternative cryptocurrencies, being Ethereum the most noteworthy. As such, either analysing the functional structure of this digital currency or comparing it with the already studied Bitcoin are natural extensions of this work.

Bibliography

Albrecht, Radoslav; Bitcoin Volatility– The 4 Perspectives, Bitcoin Magazine, <https://bitcoinmagazine.com/articles/bitcoin-volatility-analysis-1377627247/>, posted on 27th August 2013.

Arthur, Charles; Estonian E-voting shouldn't be used in European elections, say security experts, <https://www.theguardian.com/technology/2014/may/12/estonian-e-voting-security-warning-european-elections-research>, posted on 12th May 2014.

Banco de Portugal; Esclarecimento do Banco de Portugal sobre Bitcoin, <https://www.bportugal.pt/comunicado/esclarecimento-do-banco-de-portugal-sobre-bitcoin>, posted on 22nd November 2013.

Barnes, A., Brake, C. and Perry, T. 2017. *Digital voting with the use of blockchain technology*. Working paper of Team Plymouth Pioneers, Plymouth University, United Kingdom.

Bitcoin taxation in the developed countries, NoMoreTax article, <http://www.nomoretax.eu/bitcoin-taxation-developed-countries/> accessed on 2nd October 2017.

Blockchain Technology for Digital Identities, <http://www.blockchaintechnologies.com/blockchain-identity>, accessed on 6th October 2017.

Brito, J. & Castillo, A. 2013. *Bitcoin: A primer for policymakers*. Mercatus Center: George Mason University.

Browne, Ryan; Estonia Wants to Launch its Own Government-backed Cryptocurrency Called “Estcoin”, CNBC Website, <https://www.cnbc.com/2017/08/23/estonia-cryptocurrency-called-estcoin.html>, posted on 23rd August 2017.

Chen, Lulu and Lee, Justina; Bitcoin Tumbles as PBOC Declares Initial Coin Offerings Illegal, Bloomberg Technology, <https://www.bloomberg.com/news/articles/2017-09-04/china-central-bank-says-initial-coin-offerings-are-illegal> posted on 4th September 2017.

China Will Likely Resume Cryptocurrency Trading by Licensing Bitcoin Exchanges, Applancer Blockchain, <https://www.applancer.co/blog/china-will-likely-resume-cryptocurrency-trading-by-licensing-bitcoin-exchanges>, posted on 7th October 2017.

Chun, R. 2017. Big in Venezuela: Bitcoin Mining. *The Atlantic*, 320: 26-26.

DeLong, Brad; Watching Bitcoin, Dogecoin, etc, Washington Center for Equitable Growth, <http://equitablegrowth.org/equitablog/watching-bitcoin-dogecoin-etc/> posted on 28th December 2013.

Dotson, Kit; A Tiny Island Off the Coast of Portugal Just Became the First Country with Bitcoin as its Official Currency, <https://siliconangle.com/blog/2015/12/15/a-tiny-island-off-the-coast-of-portugal-just-became-the-first-country-with-bitcoin-as-its-official-currency/>, posted on 15th December 2015.

Durant, Elizabeth; Digital Diploma Debuts at MIT, MIT news, <http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017> posted on 17th October 2017.

European Central Bank; Virtual Currency Schemes, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, published on October 2012.

Faggart, Evan; What Happens to Bitcoin Miners When all Coins are Mined? <https://news.bitcoin.com/what-happens-bitcoin-miners-all-coins-mined/>, posted on 15th August, 2015.

Freeman, Nikita; 10 Best and Biggest Bitcoin Mining Pools Comparison 2017, <https://medium.com/@NikitaFreeman1ap/10-best-and-biggest-bitcoin-mining-pools-comparison-2017-cb4ef322eb4>, posted on 13rd June 2017.

Garcia, D., Tessone, C., Mavrodiev, P. & Perony, N. 2014. The digital traces of bubbles: Feedback cycles between socio-economic signals in the Bitcoin economy. *Journal of the Royal Society Interface*, (11).

Gates, Bill; “Fox Business”. Fox News. Fox. 6th May 2013. Television.

Greenberg, Andy; Apple’s ‘Differential Privacy’ Is About Collecting Your Data—But Not Your Data, <https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/>, posted on 13th June 2017.

Hackett, Robert; IMF Head: Cryptocurrency Could Be the Future. Really, Fortune, <http://fortune.com/2017/10/02/bitcoin-ethereum-cryptocurrency-imf-christine-lagarde/>, posted on 2nd October 2017.

Hayek, F. A. 1990. *Denationalisation of money - The argument refined: An argument refined: An analysis of the theory and practice of concurrent currencies*. London: The Institute of Economic Affairs.

Helms, Kevin; Russia’s Central Bank Pushes for National Cryptocurrency, <https://news.bitcoin.com/russias-central-bank-pushes-for-national-cryptocurrency/>, posted on 6th October 2017.

Henley, John; Sweden Leads the Race to Become Cashless Society, The Guardian, <https://www.theguardian.com/business/2016/jun/04/sweden-cashless-society-cards-phone-apps-leading-europe>, posted on 4th June 2016.

Hertig, Alyssa; Explainer: What Is SegWit2x and What Does It Mean for Bitcoin? <https://www.coindesk.com/explainer-what-is-segwit2x-and-what-does-it-mean-for-bitcoin>, posted on 12th July 2017.

Hileman, G. and Rauchs, M. 2017. *Global cryptocurrency benchmarking study*. Academic research paper, University of Cambridge, United Kingdom.

Hopkins, Nick; Deloitte Hit by Cyber-attack Revealing Clients’ Secret Emails, <https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails>, posted on 25th September 2017.

How to Store Your Bitcoins, CoinDesk Inc, <https://www.coindesk.com/information/how-to-store-your-bitcoins/>, last updated 19th October 2015.

Imbert, Fred; JPMorgan CEO Jamie Dimon Says Bitcoin is a 'Fraud' That Will Eventually Blow Up, CNBC, <https://www.cnbc.com/2017/09/12/jpmorgan-ceo-jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-third-quarter.html>, published on 12th September 2017.

Kaplanov, N. 2012. *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*. Temple University Legal Studies Research Paper.

Khaliq, A.; The good, the bad and the ugly of Bitcoin security, Hongkiat article, <https://www.hongkiat.com/blog/bitcoin-security/> accessed on 5th October 2017.

Kim, T.; Bitcoin Up Sevenfold Since Warren Buffett Warned Digital Currency Was a 'Mirage', CNBC Investing article, <https://www.cnbc.com/2017/09/07/bitcoin-up-sevenfold-since-warren-buffett-warned-digital-currency-was-a-mirage.html>, published on 7th September 2017.

KPMG; Digital Payments- Analysing the Cyber Landscape, https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analysing_the_cyber_landscape.pdf, posted on April 2017.

Kollewe, Julia; Lloyd's Says Cyber-attack Could Cost \$120bn, Same as Hurricane Katrina, <https://www.theguardian.com/business/2017/jul/17/lloyds-says-cyber-attack-could-cost-120bn-same-as-hurricane-katrina>, posted on 17th July 2017.

Kristoufek, L. BitCoin Meets Google Trends and Wikipedia: Quantifying the Relationship Between Phenomena Of The Internet Era, Scientific Reports, <http://www.readcube.com/articles/10.1038/srep03415> published on 4th December 2003.

Mankiw, G. 2014. *Principles of Economics*. Cengage Learning 7th Edition.

Marshall, Andrew; ICO Explained, The CoinTelegraph, <https://cointelegraph.com/explained/ico-explained> posted on 7th March 2017.

McCoy, Kevin; Target To Pay \$18.5M For 2013 Data Breach That Affected 41 Million Consumers, <https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932>, posted on 23th March 2017.

Memoria, Francisco; Putin's Advisor \$100 Million ICO for Bitcoin Mining Farm in Russia, <https://www.cryptocoinsnews.com/putins-advisor-seeks-100-million-through-ico-to-invest-in-bitcoin-mining-infrastructure/>, posted on 29th August 2017.

Mishkin, F. S.; 2007. *The Economics of Money, Banking, and Financial Markets*. Boston: Addison Wesley.

Mohr, J., Sengupta, S., & Slater, S. 2009. *Marketing of high-technology products and innovations*. Upper Saddle River, NJ: Pearson Prentice Hall.

Monaghan, Angela; Bitcoin Is a Fraud That Will Blow Up, Says JP Morgan Boss, The Guardian, <https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers>, posted on 13th September 2017.

Nakamoto, Satoshi; Bitcoin: A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf> accessed on 6th October 2017.

Olleros, F. X. & Zhegu, M. 2016 *Research Handbook on Digital Transformations*. Cheltenham: Elgar.

O'Sullivan, A.; Steven, M. S. 2003. *Economics: Principles in action*. New Jersey: Pearson Prentice Hall.

Parker, Luke; Florida Passes Law Making Crimes With Bitcoin Money Laundering, Brave Newcoin article, <https://bravenewcoin.com/news/florida-passes-law-making-crimes-with-bitcoin-money-laundering-2/>, posted on 9th May 2017.

Paul Krugman; Bitcoin is Evil, The Opinion Pages- Conscience of a Liberal, <https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?mcubz=3> posted on 28th December 2013.

Plassaras, N. 2013. Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. *Chicago Journal of International Law*, 14: 1-26.

Raposa, Keneth; What China Ban? Cryptocurrency Market Cap Rebounding, Forbes, <https://www.forbes.com/sites/kenrapoza/2017/09/28/china-ico-ban-bitcoin-crypto-currency-market-cap-returns/#45164f0a6c21>, posted on 28th September 2017.

Rivest, Ronald L. 1990. Cryptography. In J. Van Leeuwen (Ed.), *Handbook of Theoretical Computer Science*, Vol. 1. New York: Elsevier.

Rosic, Ameer; 5 Blockchain Applications That Are Shaping Your Future, Huffpost Blog, https://www.huffingtonpost.com/ameer-rosic/-5-blockchain-applications_b_13279010.html, posted on 28th November 2016.

Schuh, S. and Shy, O. 2016. *U.S. Consumers' Adoption and Use of Bitcoin and Other Virtual Currencies*. Working paper, MIT Sloan School of Management, Cambridge.

Singh, Shruti; Here Is What PM Modi Said About The New Rs 500, Rs 2000 Notes And Black Money, India Today Article, <http://indiatoday.intoday.in/story/live-pm-narendra-modi-addresses-nation/1/805755.html> posted on 8th November 2016.

Sivabalan, Srinivasan; Going Cashless? Bad for Tax Cheats, Privacy, Poor, Bloomberg Businessweek, <https://www.bloomberg.com/news/articles/2017-07-17/going-cashless-bad-for-tax-cheats-privacy-poor-quicktake-q-a>, posted on 17th July 2017.

Smith, A. 2017. Creating assurance in blockchain. *ISACA Journal*, 2: 1-3.

Szabo, N. 2016. *Smart contracts: 12 use cases for business & beyond- A technology, legal and regulatory introduction*. Paper prepared by Smart Contracts Alliance in collaboration with Deloitte, an industry initiative of the Chamber of Digital Commerce, Washington, D.C.

Tasca, P. 2015. *Digital currencies: Principles, trends, opportunities and risks*. Working Paper, Deutsche Bundesbank, Frankfurt am Main and ECUREX Research, Zurich.

The Editors; Bring On the Cashless Future, Bloomberg View, <https://www.bloomberg.com/view/articles/2016-01-31/bring-on-the-cashless-future>, posted on 31st January 2016.

Torpey, K.; Report Estimates There are More Than 10 Million Bitcoin Holders Worldwide, CoinJournal article, <https://coinjournal.net/report-estimates-10-million-bitcoin-holders-worldwide>, posted on 11th January 2017.

Tulic, Admir; What is Bitcoin Mining? A Step-by-Step Guide, <https://captainaltcoin.com/bitcoin-mining/>, posted on 10th August 2017.

What is The Difference Between Litecoin and Bitcoin?

<https://www.coindesk.com/information/comparing-litecoin-bitcoin/>, last updated on 2nd April 2014.

Wilmoth, Josiah; Drunk the Crypto Kool-Aid? Get Ready for Bitcoin Vodka, <https://www.cryptocoinsnews.com/>, posted on 29th October 2017.