Gabinete de Estratégia e Estudos

Tema Económico

Economic Study

67

Maio de 2019

Cryptocurrencies: Advantages and Risks of Digital Money

Gabriel Osório de Barros

Gabinete de Estratégia e Estudos do Ministério da Economia
Office for Strategy and Studies of the Ministry of Economy
Rua da Prata, n.º 8 – 1149-057 Lisboa – Portugal
www.gee.gov.pt
ISSN (online): 1647-6204

Cryptocurrencies:
Advantages and Risks of Digital Money

Gabriel Osório de Barros[1]

Abstract

In 2018, in "The Economics of Cybersecurity" and "Cybersecurity in Portugal" (Barros, 2018a and 2018b), ransomware was identified as one of the main risks associated with the Cyberspace. However, according to Microsoft (2019), more recent studies indicate a decline in ransomware attacks, with attackers targeting their activity to attacks with cryptocurrency mining.

Considering this new perspective, which attributes to Cryptocurrencies not only a set of opportunities but also a set of risks, this study identifies the main advantages and the main risks associated to the Cryptocurrencies.

If, on the positive side, the speed of transaction, the reduced cost, the privacy or the permanent availability of the system are highlighted, on the other hand, concerns are identified regarding the volatility, the reduced supply of goods and services that accept crypto-currencies as payment, the high energy cost and environmental threats, the potential criminal attacks, money laundering and the funding of criminal activity.

JEL Classification: E42, O33

Keywords: Cryptocurrencies

Note: This article is the sole responsibility of the authors and does not necessarily reflect the positions of GEE or the Portuguese Ministry of Economy

[1] Office for Strategy and Studies, Ministry of Economy, gabriel.barros@gee.min-economia.pt

Contents

1. Introduction 1
2. History of Cryptocurrencies 2
3. Credibility of cryptocurrencies in the early years 4
4. "Old money" and the Cryptocurrencies 6
5. Bitcoin revolution 7
6. Blockchain 9
6.1 Decentralization 9
6.2 Anonymity / Pseudonymity 9
6.3 Immutability 10
7. Externalities of the Blockchain 11
8. Practical use 13
8.1 Buying online 14
8.2 Buying at a local merchant 16
9. Volatility 18
10. Investment with Cryptocurrencies 21
10.1 Investment in projects through Initial Coin Offering 21
10.2 Investment vs speculation 22
11. Lack of regulation 23
11.1 Risks for consumers 23
11.2 Income and Taxes 24
11.3 Money laundering and financing of terrorist activities 24
12. Energy consumption and environmental impact 25
13. Attacks 28
13.1 Double Spend Attack or 51% Attack 28
13.2 Distributed Denial-of-Service 28
13.3 Sybil Attack 29
13.4 Forking 29
13.5 Malicious cryptocurrency miners 29
14. Final Remarks 30
References 31

1. Introduction

Initially, human beings exchanged goods. Whenever someone had a good that someone else needed and there was a good that was wanted in return, the exchange was made. But the exchange could also be done for an unwanted good as long as this could later be exchanged with someone who needed it, thus opening the range of people involved. It also emerges the hypothesis that someone does not currently have a good for exchange but remain in debt until they achieve the desired good, thus giving rise to credit. The introduction of money has facilitated this process.

The movement of money has evolved over time, thanks to various forms of transaction - currency, banking transactions, credit cards, etc. The increasing digitalization of society and a certain liberal perspective of society led to the emergence of electronic money. The history of virtual currency is full of examples that have not survived and some are only academic proposals. Others, on the other hand, have even been implemented and currently exist.

There is, however, an increasing interest in this type of digital money, in particular based on cryptography, with entities creating their own crypto-currencies or creating technology that facilitates cryptocurrency reporting and compliance. On the other hand, the creation of Bitcoin (Nakamoto, 2008) was also the driving force behind blockchain technology, which has increased externalities in diverse fields.

This document tries to synthesize the history of the cryptocurrencies, with particular emphasis on Bitcoin, which commemorates 10 years in 2019, in view of its relevance, and identifies the main advantages and risks associated with their use.

2. History of Cryptocurrencies

At the base of the cryptocurrencies, from the outset, there is a concern associated with liberalism, according to which State intervention should be as little as possible. On the other hand, the emergence in the 1990s of Cypherpunks[2] and Crypto-anarchists[3] movements that considered essential to guarantee privacy in transactions by using cryptography and having less participation of the State had great impact in the creation of cryptocurrencies.

Concerns about how to deal with the movement of money through cryptography led to the initial studies, of which the works of Chaum (1985, 1988) stand out. The concern for privacy[4] is central in these studies and Chaum focus on the creation of "unconditionally untraceable electronic money" (Chaum et al., 1988).

However, unlike physical money, this type of solution presents difficulties because it is necessary to avoid creating multiple copies of electronic money (in physical currencies it is much more difficult to create exact copies).

Dwork and Naor (1992) presented a computational technique to control, in general, access to shared resources and also aiming to combat junk emails. In 1997, Back (2002) proposed a similar function to what he called HashCash[5].

In 1998, Wei Dai wrote a proposal on B-Money[6], although he did not continue with his study. In 2008, Satoshi Nakamoto sent an email to Wei Dai in which he referred his interest in the study published on the B-Money page and said he would release a paper that turned the idea into a "complete working system"[7]. Two months later, Nakamoto (2008)[8] published the white paper on Bitcoin, with the design and motivation for the creation of a currency that is not controlled by any entity, based on Cryptography.

The white paper thus laid the foundations for an open, accessible, non-centralized currency independent of financial intermediaries (the network acts as a substitute for banks) and where user privacy is guaranteed. The same document also laid the foundations of Blockchain technology.

With Bitcoin, anyone with a computer and internet connection can join the network. Minting and distribution of bitcoins are carried out through mining[9], in a process that aims to be decentralized.

---

2 https://www.activism.net/cypherpunk/manifesto.html

3 https://www.activism.net/cypherpunk/crypto-anarchy.html

4 "The use of credit cards today is an act of faith on the p a t of all concerned. Each party is vulnerable to fraud by the others, and the cardholder in particular has no protection against surveillance." Chaum et al., 1988

5 "Hashcash used the cryptographic hash function SHA-1 (Secure Hash Algorithm 1) to create a stamp that would help in verifying to the recipient that the email was not spam"

6 http://www.weidai.com/bmoney.txt

7 https://www.gwern.net/docs/bitcoin/2008-nakamoto

8 To this day, Nakamoto's identity remains unknown.

9 "The records are grouped and stored in blocks. Each block contains a timestamp and a link to a previous block so that the blocks are chained together, thus the name blockchain. The blocks are mined in sequence, and once recorded, the data cannot be altered retroactively. A complete record of transactions can be found on the main chain. Each block on the chain is linked to the previous one and can be traced all the way back to the very first block, which is called the genesis block. However, there are also blocks that are not part of the main chain, called detached or orphaned blocks. They can occur when more than one miner produces blocks at similar times, or they can be caused by attackers' attempt to reverse transactions. When separate blocks are validated concurrently, the algorithm will help maintain the main chain by selecting the block with the highest value." (Lee, 2018)

In 2009 the Bitcoin source code was launched and the Bitcoin network started with the mining of the first bitcoins.

Bitcoin is considered to be the first successful crypto-currency, being the largest, most used and best known. Subsequently, many other crypto-currencies were created (known as altcoins - alternative coins) that also use the Blockchain technology, standing out in terms of market cap, besides Bitcoin (Nakamoto, 2008), Ethereum (Buterin, 2014) and Ripple (Schwartz et al., 2018).

The top 5 cryptocurrencies have currently a market value of around 100 billion USD.

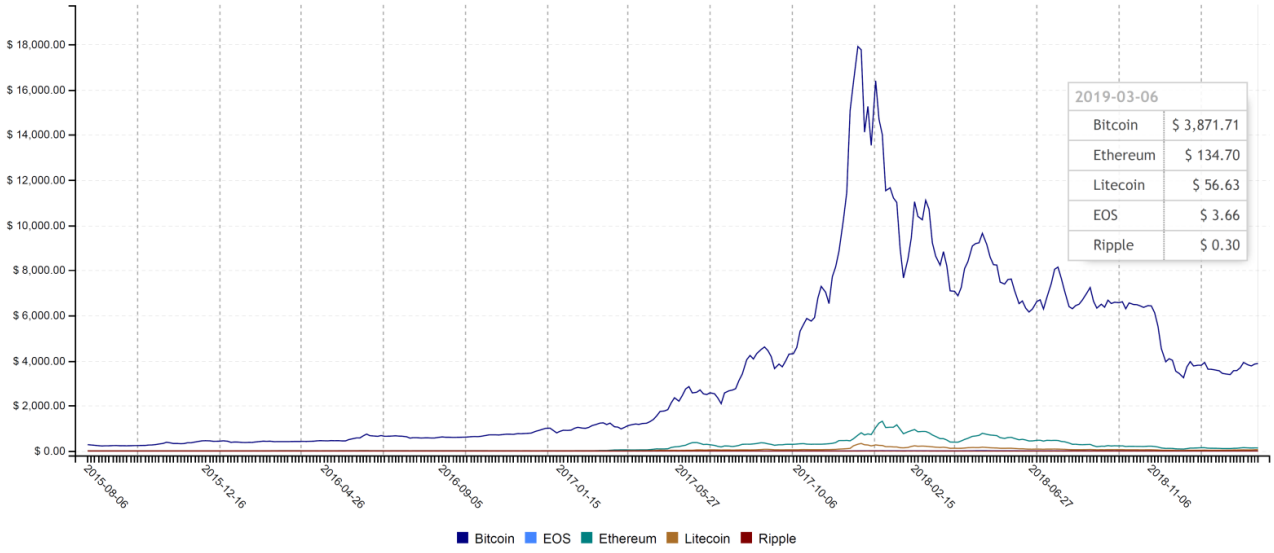
Table 1 – Main Crypto-currencies - above 3 billion USD market value

#	Name	Symbol	Market Cap (USD)
1	Bitcoin	BTC	$69 233 443 342
2	Ethereum	ETH	$14 580 929 102
3	Ripple	XRP	$12 944 164 605
4	Litecoin	LTC	$3 471 465 656
5	EOS	EOS	$3 410 910 431

Source: https://coinmarketcap.com (March 8, 2019)

The graph below shows the evolution of the price, in USD, of these currencies since August 2015.

Graph 1 – Evolution of the quotation of the main Crypto-currencies (in USD)



Source: https://www.cryptocurrencychart.com/chart/BTC.ETH.XRP.EOS.LTC/price/USD/linear/2015-08-06/2019-03-09 (March 9, 2019)

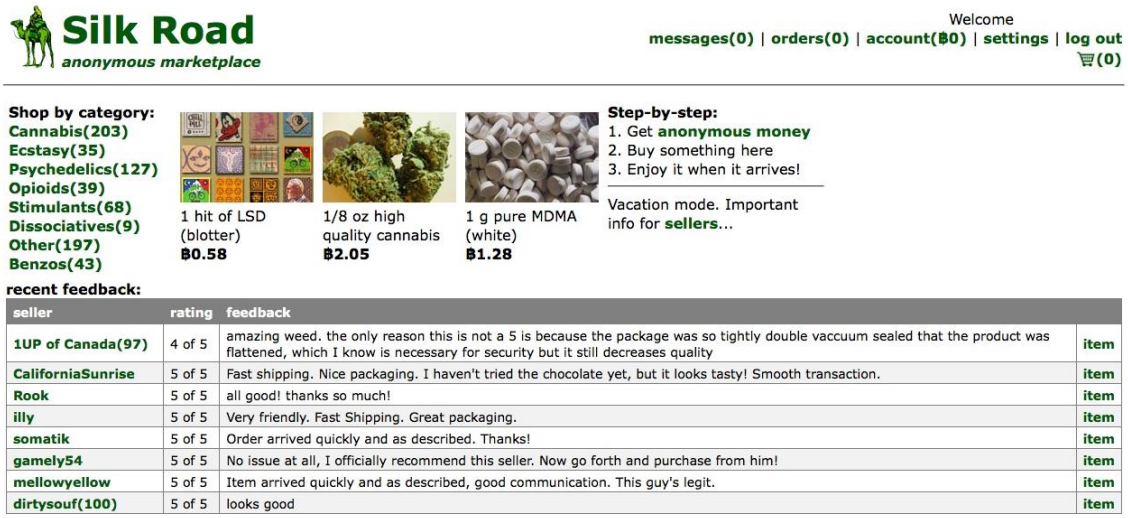
With the proliferation of Bitcoin, other platforms that allow the commercialization of bitcoins without the need to join the Bitcoin network have emerged, namely Coinbase, Bitpay, blockchain.info, and others have not been successful and which will be discussed later in the section in which are analysed the risks of cryptocurrencies.

3. Credibility of cryptocurrencies in the early years

The beginning of Bitcoin was marked, at an early stage, by two great scandals.

One of these situations regards the Silk Road case. The website was launched in February 2011, becoming the largest anonymous online market in the world, known for its large collection of illicit drugs, reaching some 960,000 registered users (Pagliery, 2013).

Image 1 – Screenshot from the Silk Road Website



Source: https://silkroaddrugs.org/

The website operated through Darknet, which used the Tor network, and transactions were paid in Bitcoin, ensuring the anonymity of buyers and sellers. By August 2012, it was estimated that annual site sales would reach 22 million USD (Greenberg, 2012).

In October 2013, the FBI closed the site and arrested[10] the alleged site owner, Ross William Ulbricht.

Shortly after, in 2014, Bitcoin was again associated with a police case, that of Mt. Gox. Mt. Gox was a Bitcoin trading platform launched in 2010 that in 2013 operated about 70% of all Bitcoin transactions (Frunza, 2015).

[10] https://web.archive.org/web/20140220003018/https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf

Image 2 – Screenshot from the Mt. Gox Website

Source: https://xbt.net/

In February 2014, Mt. Gox suspended transactions, closed the website and filed for bankruptcy protection from creditors (Abram et al., 2014), and in April of the same year began the winding-up proceedings (Mochizuki et al., 2014).

Mt. Gox then stated that bitcoins worth approximately 450 million USD were missing and probably had been stolen (Abram et al., 2014).

4. "Old money" and the Cryptocurrencies

Money is used in exchanges, for example to pay for goods and services, to purchase other currencies or for financial transactions, and is generally materialized in the form of banknotes and coins.

Usually, the following characteristics are attributed to money:

- It is a common denomination of value, allowing the comparison of the value of different goods and services;
- It is a means of payment;
- It is divisible into subunits;
- It is portable, allowing easy transportation;
- It is widely accepted;
- It has a relatively stable value;
- It is a reserve of value, allowing to make savings;
- It is controlled by the central banks of the countries.

Let's look at what is common and what distinguishes Cryptocurrencies:

- As a unit of measure, they allow, like traditional money, the comparison of the value of different goods and services, although the volatility may prevent comparison at different times;
- Like traditional physical money, it is a means of payment;
- Since they exist as a global currencies, their value is the same anywhere in the world and no exchange rate is required (except in exchange for other currencies), facilitating international trade;
- They are also divisible, like traditional currencies, into sub-units, but, unlike traditional currencies, it allows dividing up to 8 decimal places (the smallest portion being called Santoshi);
- Its portability is even greater than the physical money, being necessary only to have the keys for access;
- However, its acceptance is not generalized and there is still a limited set of entities that accept it, although the number of people and companies that accept them as means of payment is growing (as referred later);
- As for value stability, Cryptocurrencies have shown great instability, generally justified by the fact that it is still an emerging technology at an early stage, and does not currently have stability similar to that of traditional money;
- Exactly because of the volatility issue and because the Cryptocurrencies have no intrinsic value, it is questionable that they can be considered a reserve of value[11];
- In the case of Cryptocurrencies, for the very reasons that justified its creation, there is no control by central banks and no supervision.

Throughout the present work, these issues will be analysed in more depth.

[11] This is also true for "normal" money, especially for currencies of countries that are exposed to hyperinflation.

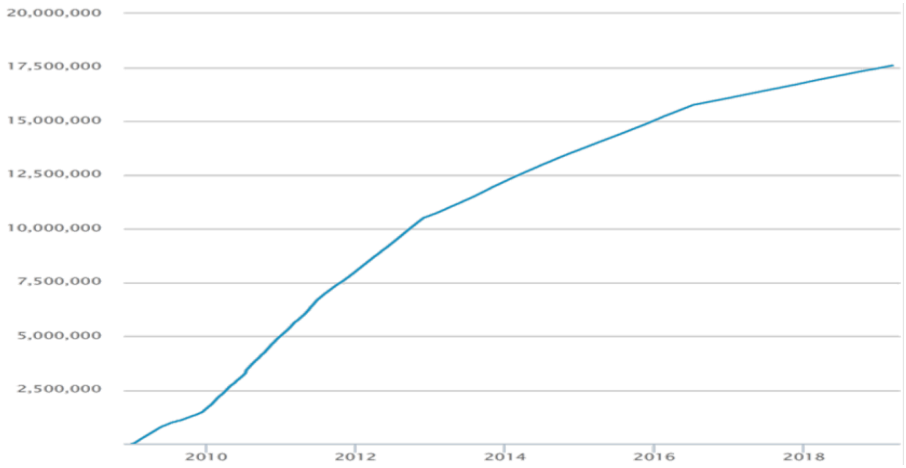
5. Bitcoin revolution

As previously referred, the cryptocurrencies are a form of digital payment, in many aspects with characteristics similar to traditional money (notes and coins), which uses encryption in its operation and which is increasingly used in the economy.

Among the cryptocurrencies, it is necessary to emphasize the role of the Bitcoins as the first and most used cryptocurrency.

Since its inception, 10 years ago, the number of Bitcoins in circulation has already exceeded 17.5 million coins.

Graph 2 - Bitcoins in circulation[12]



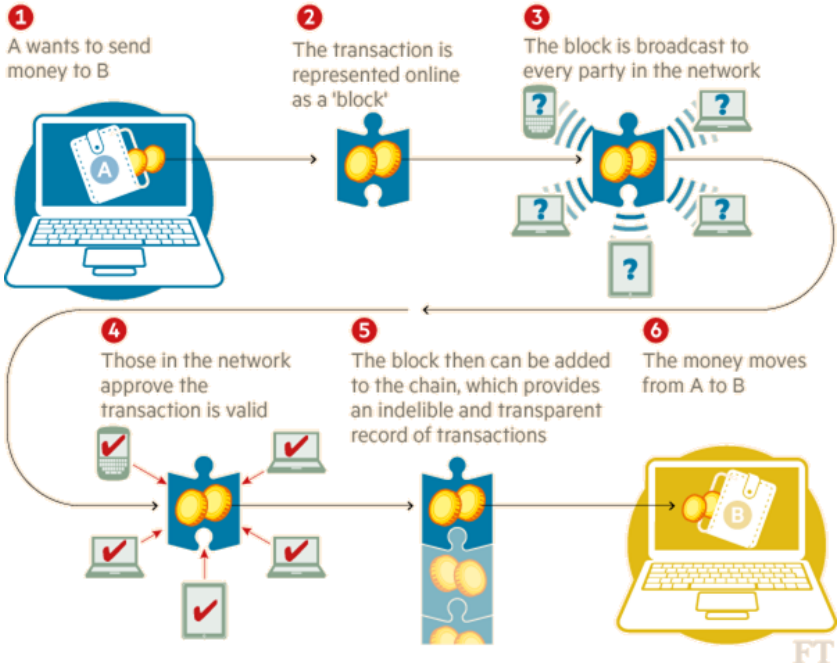
Source: https://www.blockchain.com/en/charts/total-bitcoins

Although Bitcoin distinguishes itself from banks, since it guarantees the confidentiality of users, it intends to have bank-like functions: ensuring that only the owner of an account can access it, keeping a record of transactions and allowing users to manage their accounts.

The reliability associated with Bitcoin is connected to how users' identities are guaranteed, each of which manages their public and private keys to send and receive money. On the one hand, public keys are used to transfer funds and private keys are randomly generated allowing to prove ownership of the public keys. On the other hand, to carry out a transaction it is necessary to ensure that funds are available and there can be no other transaction to move the same funds using an Unspent Transaction Output (UTXO). This ensures that the already-expended outputs will not be re-expended and that acts as input to a new transaction. Bitcoin stores the transactions in blocks built from its previous blocks and in this way form the blockchain.

[12] The total number of bitcoins that have already been mined, i.e., the current supply of bitcoins on the network.

Image 3 – Blockchain transaction



Source: Financial Times

(https://assets.weforum.org/wp-content/uploads/2015/12/151103-blockchain-bitcoin-technology-banking-fintech-FT.png)

6. Blockchain

As mentioned earlier, Blockchain came to revolutionize the cryptocurrencies and is currently the basis of existing electronic currencies. Blockchain is the key data structure that records transactions of cryptocurrencies in so-called blocks, where new transactions are recorded as new blocks that join to existing ones (each block is connected to a previous block) and each time a transaction is logged is very difficult to reverse.

The trust given to the Blockchain results from its transparency (the information is public) and its independency (it does not depend on any entity). The operation of Blockchain seeks to prevent the counterfeiting of coins, avoiding the reversal of transactions.

Blockchain and the main current cryptocurrencies are based on 3 essential principles that will be mentioned below and from which results the reliability that is currently generally attributed to it: Decentralization, Pseudonymity and Immutability.

6.1 Decentralization

For a transaction to take place, it is necessary to verify a consensus through the so-called proof-of-work that, in the absence of a central authority, limits the voting power of each user, seeking to restrict the voting capacity of malicious entities.

The process occurs through a peer validation in which the user who intends to carry out the transaction sends the request to the entire network and in which everyone can validate the transaction and in which only after received a majority of votes the transaction is accepted.

In this way, the decision occurs in a decentralized way. This process allows identifying discrepancies between different versions of the database, facilitating consistency among all members of the network.

6.2 Anonymity / Pseudonymity

As mentioned earlier, the identity of the users is one of the specific characteristics of the cryptocurrencies. In fact, one of the benefits of using it is that it allows for anonymity which is not possible with traditional banks. Traditionally, banking information was associated with the identity of the customer. In the cryptocurrencies, it is particularly difficult to establish this connection. For this reason, since it is not necessary to provide information about the buyer, the risk of identity theft in online payments is avoided.

As with traditional money, the use of cryptocurrencies always requires some form of authentication in order to prevent others from transacting with money that does not belong to them by associating the money with its owner. On the other hand, it is also necessary to keep track of transactions so that undue access can be identified and prevent malicious activity in the future. Finally, it is essential to maintain the integrity of the information, preventing the manipulation of the transactions carried out through false authentication, copying of the identity or adulteration of its contents.

In this way, as in a signature, the identity of each person is guaranteed through the existence of a public key to receive the crypto-coins and a private key that is extremely difficult to obtain by any other person and which has to be kept confidential. In this way, the private key gives access to the public key in order to prove the property. From the private key is automatically generated the public key that guarantees the identity and whose probability of repetition between two different users is extremely reduced. This combination guarantees the identity of the user and that allows the owner to transact the crypto-coins, replacing the existence of a central authority that traditionally would guarantee the unique identity of each user.

Although it is difficult to identify the user, some authors argue that it is not impossible to associate users' virtual identity with their real identity (Narayanan et al., 2016) and that anyone who knows the identity of a user in any transaction can get information about other transactions made with the same pseudonym/address (Böhme, 2015) - hence the name pseudonymity.

6.3 Immutability

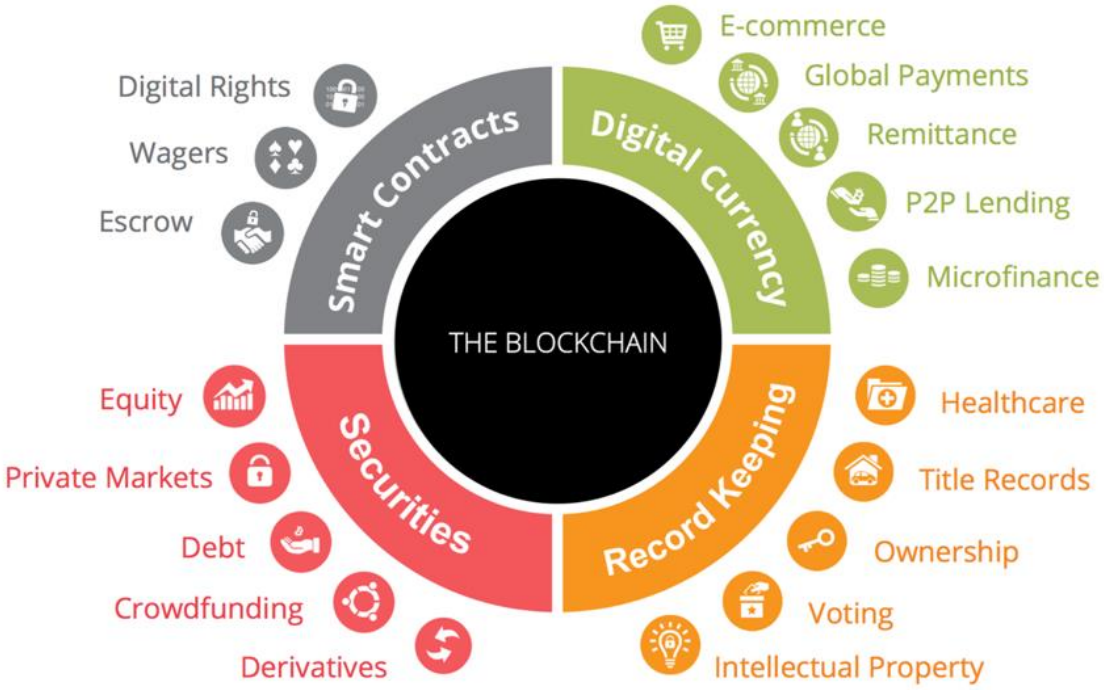
As previously referred, decentralization seeks to replace a role that is usually played by a central entity. This decentralization presupposes the dissemination of a copy of all transactions by all participants in the network.

This decentralization allows the immutability of information since it is very difficult to subsequently reverse a decision because this would imply changing the information of all the users.

7. Externalities of the Blockchain

While Blockchain has emerged as the basic technology solution for the cryptocurrencies, the technology has been adapted to enable new applications in areas such as energy, industry and finance.

Image 4 – Blockchain Potential Application and Disruption



Source: Equinix (https://blog.equinix.com/blog/2017/10/05/blockchain-a-new-type-of-internet/)

Blockchain may allow greater security and decentralization in the storage and transfer of information, seeking to ensure privacy.

Various possibilities have been identified for the application of Blockchain by using decentralized information to make markets more democratic, avoiding over-concentration of market power in a small group of people by shifting control of information from business to consumers.

Although it is a recent use and may take years to have full effect, several companies are already working on the adoption of blockchain technology[13], seeking to simplify and strengthen their value chains, such as JPMorgan Chase & Co, Bank of China Ltd., Toyota Motor Corp., Samsung Electronics Co., BNP Paribas SA, Microsoft Corporation, Allianz SE, Banco Santander or AXA Group.

According to Bansal (2017), the application of the blockchain could allow considerable advances in the following sectors:

[13] List of top 50 companies exploring blockchain technology available at https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/big-blockchain-the-50-largest-public-companies-exploring-blockchain/#79c2bbe12b5b.

- "Financial Services – Faster, cheaper settlements could save billions of dollars in transaction costs, while improving transparency. Blockchain's encryption properties allow insurers to securely capture the ownership of assets to be insured.
- Automotive – Consumers could use the Blockchain to manage fractional ownership in autonomous cars.
- Voting – Using the Blockchain code, constituents could cast their votes by phone/computer, resulting in immediately verifiable results.
- Healthcare – Patients' encrypted health information could be shared with multiple providers, without the risk of a privacy breach.
- Decentralized Notary – Timestamping is an interesting feature of Blockchain. The whole network essentially validates the state of a wrapped piece of data (a "hash") at a certain particular time. As a trustless, decentralized network, it essentially confirms the "existence" of a document or information at a stated time that is further provable in a court of law. Until now, only centralized notary services could serve this purpose.
- Smart Contracts – These are legally binding programmable digitized contracts entered on Blockchain. Developers implement legal contracts as variables and statements that can release funds using the Bitcoin network as a "third party executor," rather than trusting a single central authority."

In addition, Blockchain might become a mean to enable consumers to avoid counterfeiting by proving the identity of the retailer and the consumer, monitoring the movement of products and creating verifiable registrations.

8. Practical use

The use of cryptocurrencies makes it much easier to buy and sell goods and services, allowing transferring money quickly.

Although in some cases cryptocurrencies were created for specific purposes, the main cryptocurrencies (Bitcoin and Ethereum) were created with the aim of having a more general use.

In terms of acceptability, there are currently a limited number of entities that allow its use. Still, the number of possibilities for cryptocurrencies applications is increasing in retail businesses (such as the sale of food or computer products) and in large consultancy companies (such as the "Big 4").

Although the reduced acceptance of cryptocurrencies, Jonker (2017) believes that there is substantial interest among retailers in accepting this type of currency in the future, indicating that their acceptance may increase rapidly. According to the same author, the main factors influencing the adoption of cryptocurrencies are the demand for this form of payment by consumers (one reason for non-adoption has been the low consumer demand), the added value resulting from the use (which can be influenced by the positive experience of other retailers) and non-financial barriers (retailers consider the compatibility between the use of virtual currencies and current business processes to be extremely important).

On the contrary, expectably, recent warnings from European institutions, such as the European Bank Authority and European Central Bank, and nationals such as the Bank of Portugal, cast doubt on the credibility of the cryptocurrencies and could hinder the increase in goods and services that can be paid through those coins (casting doubts on traders as to whether they should accept this form of payment).

Bitcoin is the currency that is most easily usable today, having a greater range of choice with several examples in areas such as:

- Crowd funding – Crowdtilt;
- Donations – Save the Children, The Libertarian Party and Wikipedia;
- Bookstores – MIT Coop Store;
- Newspapers – Bloomberg;
- Music – Grooveshark;
- Movies – Lionsgate Films;
- Tv shows – EZTV;
- Board games – Nestorgames;
- Gaming – Green Man Gaming, Steam and Zynga;
- Commodities – BitcoinCommodities;
- E-commerce – OpenBazaar;
- Electronics – Newegg;
- Second-hand goods – CEX;
- Food – KFC (Canada), PizzaForCoins (USA) and Subway (USA);
- Organic food - Whole Foods;
- Pubs – Old Fitzroy (Australia) and Pembury Tavern (England);

- Real estate – RE/MAX London (UK);
- Financial accounts – Mint;
- Auto repairs – Straub (USA);
- Travel – Bitcoin. Travel, CheapAir, Expedia.com and WebJet;
- Hotels – One Shot Hotels (Spain);
- Pharmacy – The Swiss Pharmacy;
- Medical equipment – mspinc;
- Dating – Badoo, Dream Lover and OkCupid;
- Adult content – Naughty America and Playboy;
- Cloud data file services – Lumfile and Mega;
- VPN provider – PureVPN;
- Software for online stores – Shopify;
- Technology and Software – Microsoft.

Here are some ways to search online and physical stores where cryptocurrencies may be used.

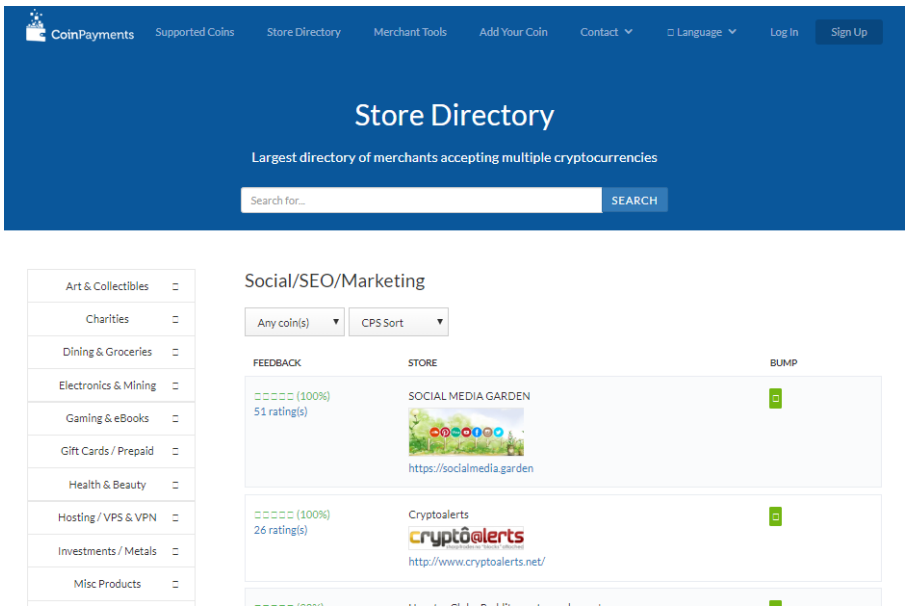
8.1 Buying online

One of the possibilities for using cryptocurrencies is through the purchase of goods and services at online stores. In this sense, here are some websites that allow carrying out this search.

CoinPayments

The website Coin Payments is a directory of online operators that accept transactions in multiple cryptocurrencies.

Image 5 - CoinPayments

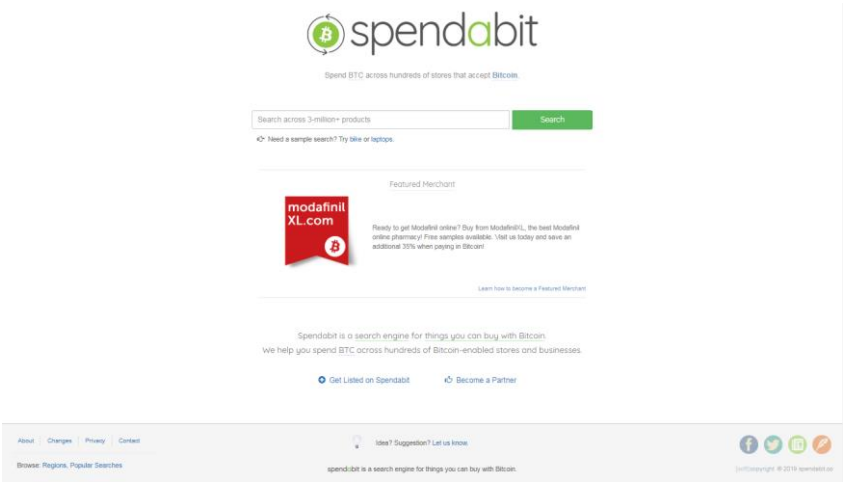


Souce: https://www.coinpayments.net

Spendabit

Spendabit is a search engine that allows searching for products sold in merchants and online platforms that can be purchased with Bitcoins.

Image 6 – Spendabito

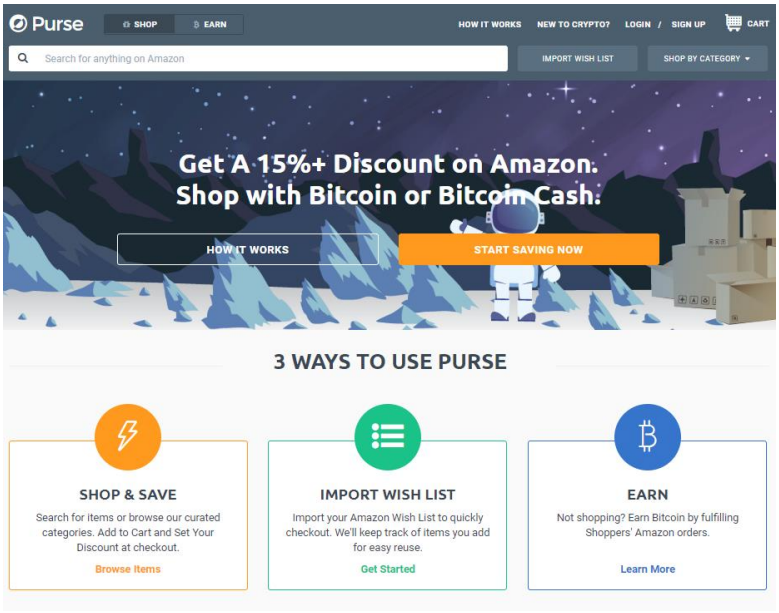


Source: https://spendabit.co/

Purse

The site Purse.io connects buyers and holders of gift cards, allowing purchases at Amazon with bitcoins (and with discount) and allowing the balance to be used to purchase goods from third parties receiving bitcoins in exchange.

Image 7 – Purse



Source: https://purse.io

8.2 Buying at a local merchant

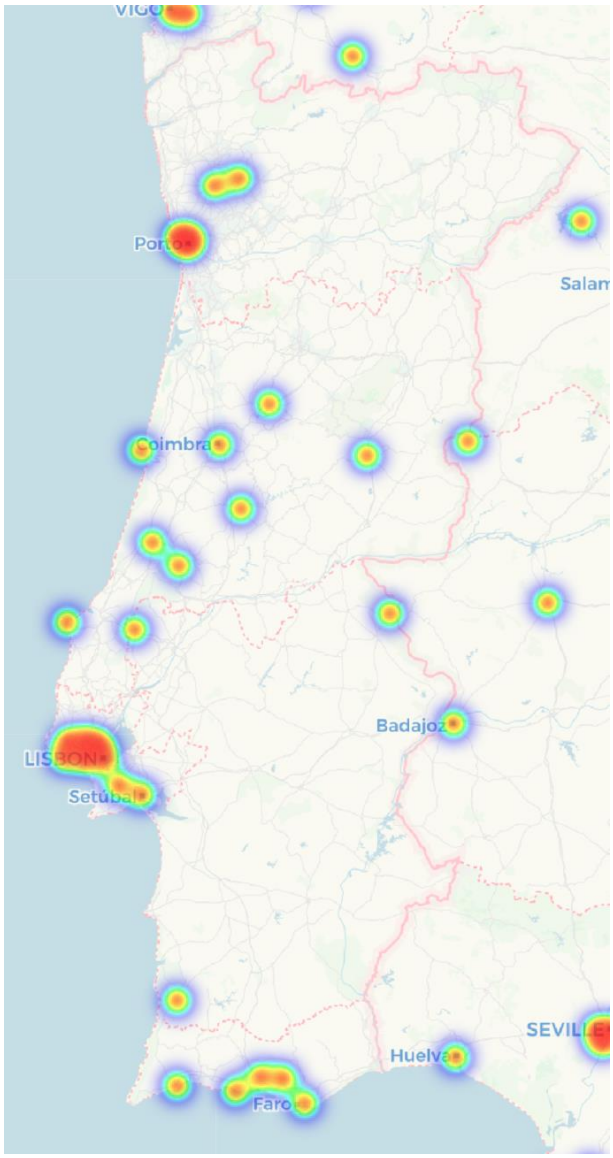
More difficult is finding local merchants that accept bitcoins. There are, however, several sites on which searches can be performed.

Coinmap

The Coinmap website allows you to identify on the map establishments that accept bitcoins as a payment method.

At the geographical level, Portugal still has few options in terms of physical stores.

Map 1 - Coinmap

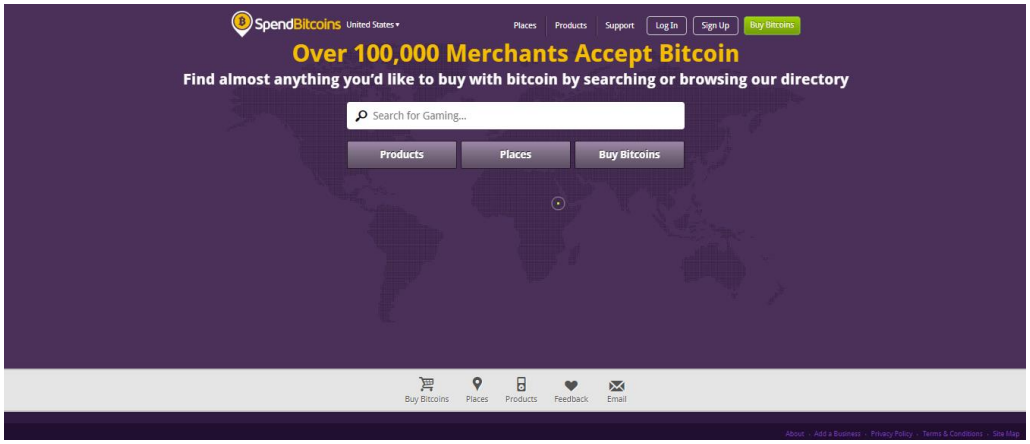


Source: https://coinmap.org/

SpendBitcoins

The SpenBitcoins site allows you to identify physical stores (but also online) where there are merchants that accept bitcoins.

Image 8 - SpendBitcoins



Source: http://spendbitcoins.com/

CoinATMRadar

Although it is not a site for buying goods and services, CoinATMRadar allows you to identify "Coin ATM" in which you can buy and sell various crypto coins (not just bitcoins) in exchange for conventional money.

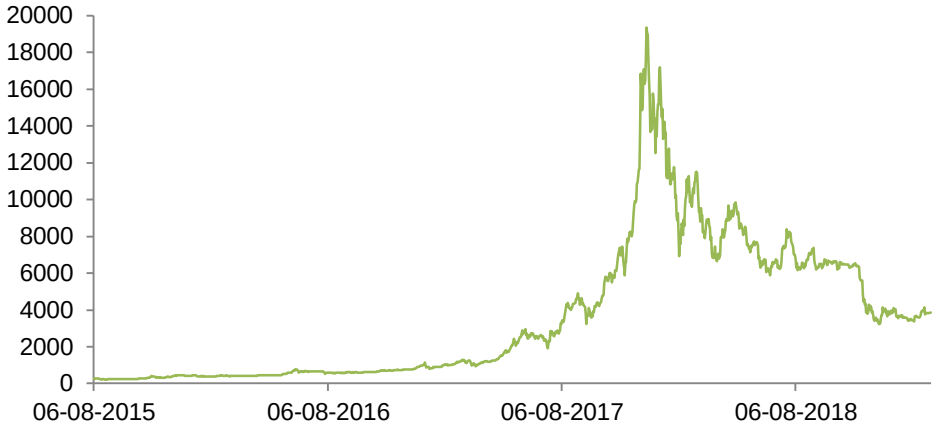
Map 2 – Coin ATM Radar

Source: https://coinatmradar.com/

9. Volatility

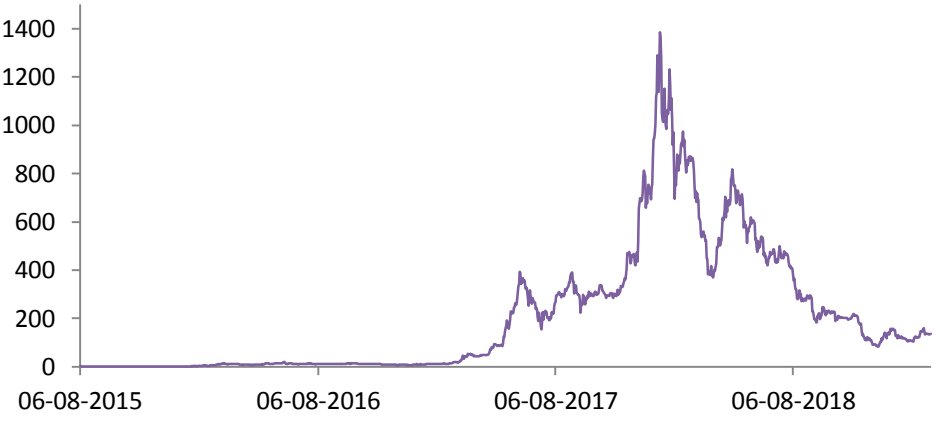
One of the problems associated with cryptocurrencies is their volatility. In fact, they attracted many buyers not only because of the possibility of escaping the traditional means of currency controlled by the financial system but also because they anticipated high gains. However, the Crypto-currencies have been very volatile, for example as compared with other indexes or reference prices - as is the case of the S&P 500 and Gold (information regarding the period between August 6, 2015[14], and March 5, 2019).

Graph 3 – Evolution of the price of the Bitcoin cryptocurrency (Adjusted Close, USD/BTC)



Source: https://finance.yahoo.com/quote/BTC-USD

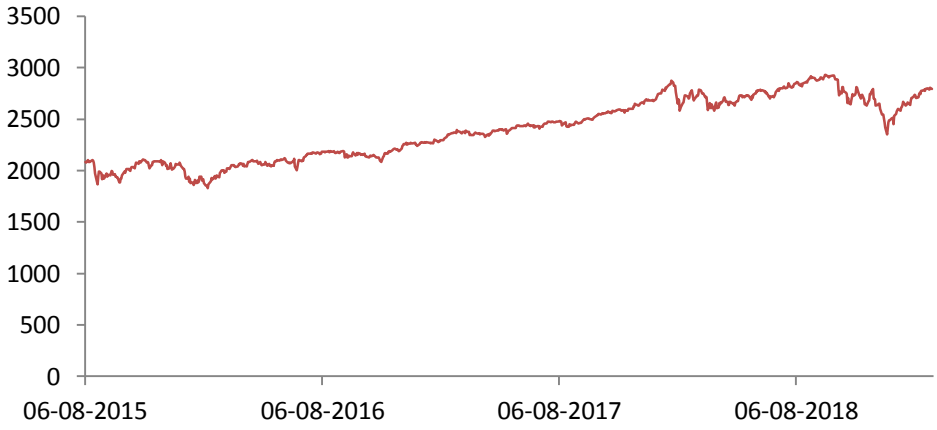
Graph 4 – Evolution of the price of the Ethereum crypto-currency (Adjusted Close, USD/ETH)



Source: https://finance.yahoo.com/quote/ETH-USD

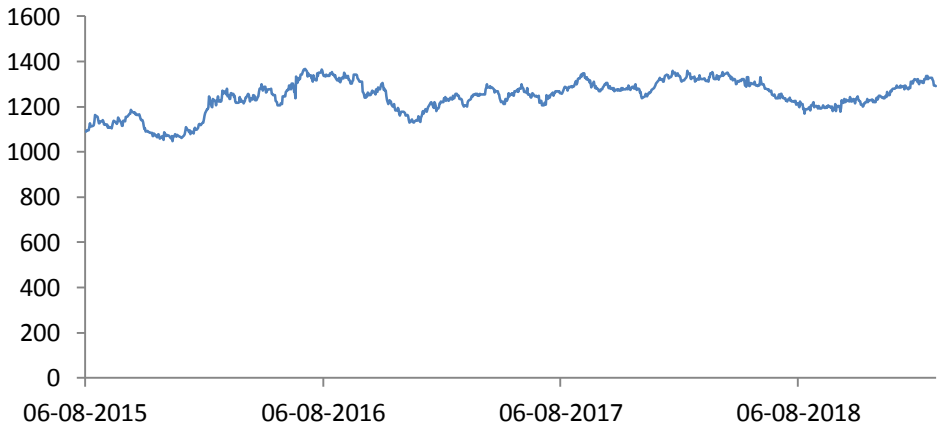
[14] The date on which Ethereum was created.

Graph 5 – Evolution of the S&P 500 (Close, Index)



Source: https://eu.spindices.com

Graph 6 – Evolution of the price of Gold (Closing Price, USD/oz)



Source: https://markets.businessinsider.com

Historical volatility measures the variation over a given period. In the present study were considered the closing values of two of the main crypto-currencies, Bitcoin and Ethereum, and compared them with the evolution of the S&P500 index and the price of Gold in the period between August 6, 2015, and March 5, 2018.

Analyzing the information in previous graphs, there is great instability in the cryptocurrencies, registering what appears to be a "bubble-crash" in Bitcoin and Ethereum in December 2017 and January 2018, respectively.

In this study, we have calculated the volatility of S&P 500, Gold, Bitcoin and Ethereu with the following calculations:

1. Calculation of ln(Pi/Pi-1), where ln is the natural logarithm, Pi is the daily reference price on day i and Pi-1 is the price relative to the previous day;
2. Calculation of the standard deviation of the series calculated in point 1 for the n days considered;
3. Annualization of the value of the volatility obtained in point 2 - since it is based on a daily value - multiplying the standard deviation by the square root of the average number of observations per year.

Table 2 - Volatility in the period between August 6, 2015, and March 5, 2019

	Standard deviation	Volatility
S&P 500	0,009	14%
Gold	0,009	15%
Bitcoin	0,040	76%
Ethereum	0,076	146%

Source: Own calculations

The volatility recorded in the analyzed period was much higher in the case of Ethereum (146%) and Bitcoin (76%) than in the evolution of the price of Gold (15%) or of the S&P 500 index (14%). This confirms the high volatility of the Crypto-currencies in comparison with other assets. While it is true that volatility can lead to high gains in a short period of time, it is also true that it can also lead to high losses.

The price of cryptocurrencies has been directly influenced by several shocks, some of which are related to measures taken by governments. For example, Bitcoin's legalization in Japan had its effect as recovery while China's ban on ICOs led to its devaluation (Navickas et al., 2018).

10.Investment with Cryptocurrencies

10.1 Investment in projects through Initial Coin Offering

Cryptocurrencies (in particular Ethereum) have allowed virtual fundraising for investment in projects, in particular start-ups, and project development through Initial Coin Offering (ICO).

An ICO is an innovative way of obtaining financing in which a company or individual issues digital coins and puts them up for sale in exchange for coins (digital or conventional), goods and services, or a percentage of future profits.

Several projects have come up for this purpose, such as those available on Crypto Potato (https://cryptopotato.com/ico-list/) or ICO Drops (https://icodrops.com/category/active-ico/), and others have already ended (https://icodrops.com/category/ended-ico/).

Although it appears as a way to get funding for start-ups, an activity that could initially bring benefits in economic terms, several entities (such as the European Securities and Markets Authority - ESMA) and countries (such as China - https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html) have been warning for the high risk of ICO.

ESMA (2017a) has pointed out that companies involved in ICO, when developing regulated activities (e.g., when they qualify as financial instruments), are obliged to comply with EU legislation, stating that depending on how they are structured, they may have to comply with the following directives:

- The Prospectus Directive, that aims to ensure that adequate information is provided to investors by companies when raising capital in the EU;
- The Markets in Financial Instruments Directive, which aims to create a single market for investment services and activities and to ensure a high degree of harmonised protection for investors in financial instruments;
- The Alternative Investment Fund Managers Directive, which lays down the rules for the authorisation, ongoing operation and transparency of the managers of alternative investment funds which manage and/or market alternative investment funds in the EU;
- The Anti-Money Laundering Directive, which prohibits money laundering and terrorist financing.

ESMA (2017b) alerts in particular to the following risks associated with ICO:

- ICO is particularly vulnerable to illegal activities and fraud because it is an unregulated space;
- There is a risk of loss of all capital invested, as projects are at an early stage, and the guarantee of earning is very low;
- The possibility of exchange for conventional currency is reduced;
- There is great volatility in the price of virtual currencies;
- The information provided is inadequate, focusing on the potential benefits but without much information about the risks;
- Blockchain technology flaws are still unknown but can be used to hack cryptocurrencies.

In China, new projects for obtaining funding through ICO were banned and the financial sector regulator was asked to inspect ICO's main platforms. However, this measure proved ineffective as ICO activity continued to intensify (https://bravenewcoin.com/insights/china-ico-ban-proving-ineffective). China is currently considering banning crypto-coins (https://www.newsbtc.com/2019/04/09/china-bitcoin-mining-ban-crypto/).

10.2 Investment vs speculation

As previously referred, the cryptocurrencies have very high volatility which makes them unsuitable either as a means of payment or as a reserve of value.

Even so, the increase in the value of cryptocurrencies attracted a large number of users with the aim of investing and getting money quickly.

Associated with the expectation of high income through the cryptocurrencies is the possibility of being a process similar to a Ponzi scheme (Krugman, 2018), that is, where the incomes of the earlier investors are paid with the capital of new investors[15]. In this sense, it is only possible to recover the funds in commercial currency as long as there are interested in buying the cryptocurrencies, that is, as long as there are new users entering the system.

As earlier mentioned, the fact that the cryptocurrencies do not disclose essential information such as the risks to which investors are exposed increases the risk that the latter will suffer financial losses.

Another great risk is that even when investors are aware of this framework, they might still take the risk in the perspective of being able to take out the money in time.

If the decision is to invest in the acquisition of cryptocurrencies, common sense advises a diversification of investment (not only in several cryptocurrencies but also in another type of assets) in order to reduce the risk.

[15] "A Ponzi scheme is an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors. Ponzi scheme organizers often solicit new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk. In many Ponzi schemes, the fraudsters focus on attracting new money to make promised payments to earlier-stage investors and to use for personal expenses, instead of engaging in any legitimate investment activity." US Securities and Exchange Commission (https://www.sec.gov/fast-answers/answersponzihtm.html)

11.Lack of regulation

The cryptocurrencies, by nature, are not subject to any regulation, that is, there is no appropriate legal basis for the operation of digital money. This allows for some independence from public authorities. However, cryptocurrencies face great legal uncertainty and risk of fraud as a consequence of this same lack of regulation.

Additionally, a large amount of money in cryptocurrencies takes away from central banks an important monetary policy instrument, undermining financial stability. Cryptocurrencies, thus, represent a major challenge for central banks, with studies referring the creation of cryptocurrencies by these institutions as a possible way to deal with the problem (EBC, 2019).

On the other hand, there is no clear definition of the rights and obligations of the parties involved. In fact, users are unaware of the reliability of the remaining users and the people with whom they are doing business. The lack of information and regulation can be conducive to criminal activity as seen below. As such, the regulation of cryptocurrencies is a challenge for public authorities, since it is difficult to identify the users and the transactions they perform. For this very reason, and because the information is spread by all users, there is no central point that can be turned off and a government or central bank can hardly prohibit a cryptocurrency, as observed in China.

Krugman (2018) points out that the cryptocurrencies are coated with a certain "technological mysticism" focusing on a "libertarian ideology" which argues the risk that governments control all money but does not take into account the risks of hacking to steal crypto-coins on a large scale.

11.1 Risks for consumers

In addition to investors concerns, entities such as the European Securities and Markets Authority, the European Banking Authority or the European Insurance and Occupational Pensions Authority (European Supervisory Authorities, 2018) have raised concerns about the need to customers who own and use cryptocurrencies as an exchange currency.

These warnings are based on the fact that cryptocurrencies are highly risky, highly speculative, have no tangible assets and are not regulated under EU law, thus not offering consumer protection.

The European Supervisory Authorities (2018) highlights as the main risks the extreme volatility and risk of a bubble, the absence of consumer protection, the absence of exit options since there is a risk of not being able to switch to a conventional currency, the lack of transparency in price formation, operational problems that hinder the functioning of the system, lack of consumer information, and the fact that it is not an appropriate investment application (not only in the short term but also in the long term regarding savings for retirement).

It is also to consider the lack of guarantees and the lack of a compensation policy in case of fraud.

11.2 Income and Taxes

Money circulating outside the financial system is out of the control of the authorities, allowing a tax-exempt parallel economy, since trading with cryptocurrencies may represent a taxable event but is not controlled.

At the income level, there is a risk of evolving into a situation of payments of part of the remuneration (above the minimum wage, for example) in crypto-coins in order to avoid paying taxes and social security.

Regarding social security contributions and tax evasion, this situation puts the collection of revenues at risk, jeopardizing the functioning of states in areas so essential as pension payments, social support, health care, justice, security or defence.

With regard to personal income, we should consider the same risks as mentioned above with regard to consumers and investors, in particular lack of regulation, high volatility, lack of exit options and lack of compensation policy in case of fraud.

11.3 Money laundering and financing of terrorist activities

Converting money into cryptocurrency could also be a form of money laundering and terrorist financing. In fact, unlike conventional currencies, controlled by a central and regulated authority, cryptocurrencies have a high potential for use in illegal activities.

For example, "dirty money" can be exchanged successively for different cryptocurrencies, allowing not only the non-traceability of the origin but also its use in the purchase of goods and services or even in the cash back for conventional money to finance terrorist activities (European Banking Authority, 2016).

12.Energy consumption and environmental impact

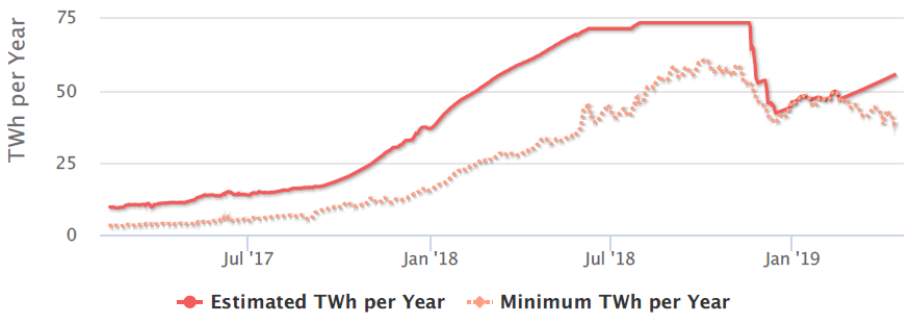
As previously mentioned, in transactions using the Blockchain users do not need to trust each other but only in the code that serves as the basis for the network. This requires that for a transaction to be considered valid the amount must be in the possession of those who use the currency and users must confirm that the transaction complies with this rule. For this control, the Blockchain uses the "proof-of-work" in which the next valid block is the one that is sent by the first miner that produces a valid block and that is rewarded by it. All other users are informed, confirm the validity and discard the blocks they were working on, restarting the process.

With special emphasis on the largest cryptocurrencies, the so-called "proof-of-work algorithm" aimed at ensuring system reliability consumes a large amount of resources - computing capacity, electrical energy and computer waste.

In this section, the analysis will be based on data from Digiconomist, "a platform that is dedicated to exposing the unintended consequences of digital trends, typically from an economic perspective". This platform estimates impacts for the two main cryptocurrencies: Bitcoin[16] and Ethereum.

In terms of electricity consumption, Bitcoin, the most commonly used cryptocurrency, currently uses more than 55 TWh per year, a figure very close to that consumed by Israel and above the consumption of many other countries, resulting in an annual carbon footprint of 26,327 kt of CO2 per year.

Graph 7 – Bitcoin Energy Consumption Index Chart



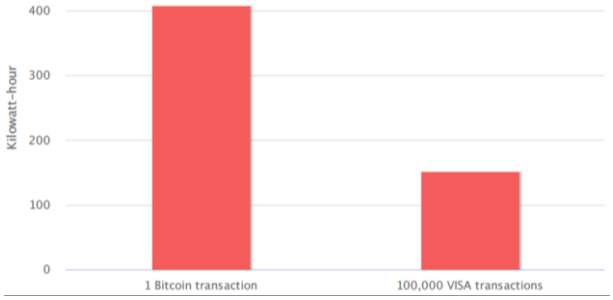
Source: www.bitcoinenergyconsumption.com

This value will increase as the number of cryptocurrency transactions increases and could jeopardize overall efforts to reduce CO2 emissions.

When comparing Bitcoin with another payment system, Visa, it is observable that one single Bitcoin transaction consumes much more energy than 100,000 VISA transactions.

[16] In this section, whenever Bitcoin is mentioned, it refers only to the sum of the information relating to Bitcoin and Bitcoin Cash.

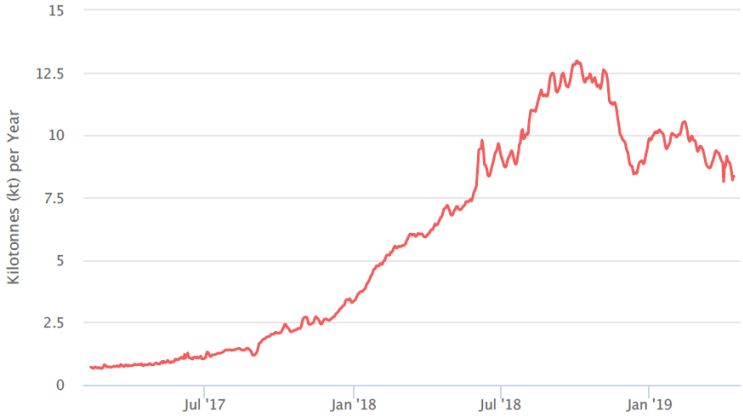
Graph 8 – Bitcoin network versus VISA network average consumption



Source: www.bitcoinenergyconsumption.com

This pressure on computers leads to the rapid devaluation of less efficient equipment, causing electronic waste to reach more than 8,000 kt a year in Bitcoin alone.

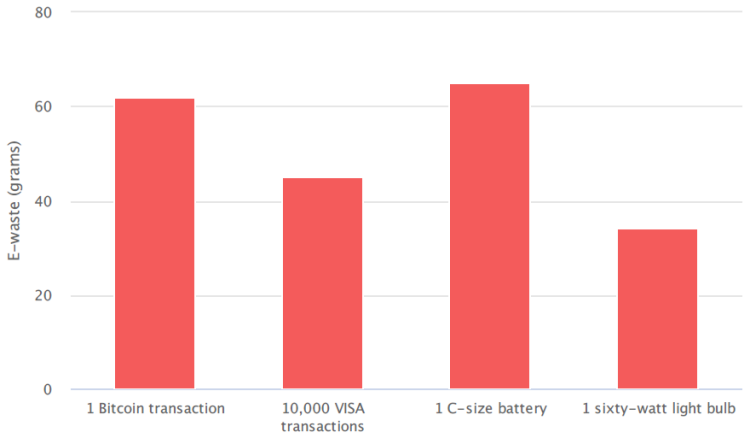
Graph 9 – Bitcoin Electronic Waste Generation



Source: www.bitcoinelectronicwaste.com

Again, Bitcoin's high electronic waste footprint reaches 60 grams per transaction, similar to the e-waste value of a c-size battery (65 grams) and much higher than the e-waste of 10,000 VISA transactions (45 grams) or of a sixty-watt light bulb (34 grams).

Graph 10 – Bitcoin Electronic Waste Footprint per Transaction



Source: www.bitcoinelectronicwaste.com

Considering annualized information for Bitcoin, the estimated global mining costs represent almost 75% of the global mining revenues.

The second largest cryptocurrency, Ethereum, due to its size has a much lower consumption than Bitcoin. Still, in annualized terms, estimated global mining costs represent more than 77% of global mining revenues.

As mentioned before, one of the main immediate consequences of cryptocurrencies is the consumption of computational resources, both in the consumption of electricity and in the degradation of the performance of computers. According to Microsoft (2019), continuous crypto-coin mining can lead to performance problems on computers and excessive CPU utilization can even damage computers. The European Banking Authority (2019) also warns for the energy consumption of cryptocurrencies and for the need for a cost-benefit analysis that takes into account the environmental protection and the sustainable development of the energy sector. On this regard, the technological revolution also entails environmental and social costs.

13. Attacks

The history of cryptocurrencies has not been exempt from attacks that seek to exploit the pseudonymity of users in current networks, trying to influence the behaviour of the network for malicious purposes. Although the proof-of-work makes the mining process more resilient to some of these threats, it is not impossible that attacks like the ones referred below take place.

13.1 Double Spend Attack or 51% Attack

In centralized systems, the banks guarantee the validity of operations. In the case of cryptocurrencies based on Blockchain, the decision results from the votes of the peers and the protocol becomes a kind of governance that seeks to replace the existence of a bank system.

To add new blocks to the blockchain users vote and reach a consensus. The proof-of-work associates voting with hashing power and its correct functioning presupposes that the majority of computational power is associated with honest users and that this majority will be able to mine faster than a malicious users.

However, if a malicious entity can control more than 50% of computational power, it can double spend the same crypto-coins in the blockchain. Sometimes the goal is not to spend twice but to destabilize and discredit a cryptocurrency by affecting its integrity.

Nevertheless, it is important to note that this type of attack is extremely difficult to execute and the probability of success of an attack is smaller the larger the network, as this would require an exorbitant expenditure with hardware, storage space and electricity to compete with the rest of the network. In fact, although this type of attack has already occurred in the past in smaller blockchains (eg: Krypton, 2016, Verge, 2018, MonaCoin, 2018), it has never occurred with Bitcoin blockchain (although not impossible).

13.2 Distributed Denial-of-Service

A distributed denial-of-service (DDoS) attack is the most common network attack and aims to stop normal traffic from a server or network flooding the target with excessive internet traffic. By compromising multiple computers, servers or networks, it turns them into sources of traffic to carry out the attack. These attacks can be carried out at no cost to attackers

In the specific case of cryptocurrencies, this attack seeks to deny service or drive honest users, increasing the hash rate of malicious miners. For example, if an honest miner receives a high number of transactions from a large number of customers, he will start discarding new orders, even from honest customers. In this way, the attackers seek to obtain most of the hash power.

Because of the decentralized nature of networks based on Blockchain technology and proof-of-work, such an attack will have a very limited effect unless a large-scale attack is launched.

13.3 Sybil Attack

Similarly, the Sybil Attack floods the network with zero-power nodes. In a system where users are not identifiable (even in Bitcoin where there is no strong anonymity) and in which there is no central authority that confers the identity of the participants it is possible to create many false entities to which multiple votes correspond.

In this way, the attackers give the idea that there are a lot of different participants when in fact they are pseudo-identities controlled by the attackers.

This operation will allow the attacker, for example, to perform "double spend" (as previously seen).

13.4 Forking

Forking occurs when different miners create different blocks to place at the same point in the blockchain, creating several versions of the transaction history. The solution resulting from the protocol implies that the miners agree which valid chain will be the one on which they will continue to build blocks.

Forking may happen unintentionally but may also occur intentionally with the purpose of making changes to the protocol in order to validate transactions that were previously considered invalid or to attack specific addresses by preventing them from transacting which may constitute a form of blackmail in which the attacker will fork all transactions of a particular user, invalidating them until he pays a certain amount.

13.5 Malicious cryptocurrency miners

According to Microsoft (2019), the mining of crypto-coins can be very profitable but it takes a huge computing power that implies a great expense of resources. For this reason, attackers have increasingly turned to malware[17] in order to gain access to victims' computers that they use to increase computing power. In this situation, the victims do not realize that they are being used because mining occurs in the background. The only effect being eventually visible is the reduction in the performance of computers. For this reason, these attacks can last for a long time without being detected or fought.

Microsoft (2019) also notes that many of the malicious mining processes do not need to be installed and are based only on JavaScript-enabled browsers (through, for example, introducing the mining code into supposedly credible sites), allowing attackers to mine crypto-coins without the consent of the users. Again, the user is not aware that the computer is being used and computer degradation may occur.

[17] On this regard, Barros (2018b) refers that Portugal has one of the highest rates of malware incidence among EU28 countries (9th position). According to Microsoft (2017), in March 2017 malware was found in 8.3% of computers in Portugal, compared to a worldwide incidence rate of 7.8%.

14.Final Remarks

Cryptocurrencies have gained great visibility and adhesion in a short time but they are not exempt from risks. This study identified the main advantages and risks associated with this new form of digital money.

Among the main advantages are the ease and speed of transaction, the privacy (pseudonimity, for example in the case of Bitcoin, which does not correspond to total anonymization), the system is available 24 hours a day, the costs associated with transactions are low and the crypto-coins in circulation are limited (which avoids inflationary processes arising from the issuance of currency).

However, several risks associated with cryptocurrencies have been identified: they are highly volatile (which makes them highly speculative), privacy attracts criminal activity, lack of central and supervisory authority (namely undermining monetary policy), difficulty in identifying users (which makes them vulnerable to hacking, terrorism and money laundering), there is no system to resolve the dispute between the parties (which is not possible because there is no central authority) and there is no deposit guarantee system. Cryptocurrencies are only accepted by a small number of traders, which makes their use more difficult and in some countries it is even illegal to trade, for example, in Bitcoin. It is also highlighted that the cryptocoins are lost if the owner loses their private keys.

This study also emphasizes the externalities associated with Blockchain. It seems possible that Blockchain will revolutionize financial and economic infrastructure - moving from the idea of decentralized crypto-concept to the idea of a decentralized world. However, Blockchain is a technology in development and the success of the application to other sectors is still ongoing. Its use is still at an early stage and there is some scepticism about the results it will provide.

In the future, several challenges arise, not only in relation to Blockchain but in particular in relation to cryptocurrencies, that require technological evolution. With regard to the mentioned attacks, there are studies that seek to improve the safety of the cryptocurrencies, so that the existing Blockchain system can be improved in the future.

Cryptocurrencies may be passing through a period of some turbulence but it is impossible to predict their future. This future will depend, of course, on the capacity to respond to the challenges identified in this study.

References

Abrams, R., Goldstein, M., and Tabuchi, H. (2014). Erosion of Faith Was Death Knell for Mt. Gox.

Aggarwal, D., Brennen, G., Lee, T., Santha, M., and Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them.

Back, A. (2002). Hashcash - A Denial of Service Counter - Measure.

Baldi, M., and Franco, C. (2017). A trusted cryptocurrency scheme for secure and verifiable digital transactions. First Monday, Volume 22, Number 11.

Bansal, L. (2017). Blockchain: A New Type of Internet - How Interconnection is powering global cryptocurrency.

Barros, G. O. (2018a). A Economia da Cibersegurança. Tema Económico n.º 54, Gabinete de Estratégia e Estudos do Ministério da Economia.

Barros, G. O. (2018b). A Cibersegurança em Portugal. Tema Económico n.º 56, Gabinete de Estratégia e Estudos do Ministério da Economia.

Ben-sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. 459-474.

BerkeleyX/edX (2018). Bitcoin and Cryptocurrencies. Blockchain Fundamentals program.

Biais, B., Bisière, C., Bouvard, M., and Casamatta, C. (2018). The blockchain folk theorem. Toulouse School of Economics (TSE), Working Papers Nº 17-817.

Böhme, R., Christin, N., Edelman, B., and Moore, T (2015). Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives, 29 (2): 213-38.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., and Felten, E. W. (2014). Mixcoin - Anonymity for Bitcoin with accountable mixes. Part of the Lecture Notes in Computer Science book series (LNCS, volume 8437).

Bonneau, Joseph & Miller, Andrew & Clark, Jeremy & Narayanan, Arvind & A. Kroll, Joshua & W. Felten, Edward. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. IEEE Symposium on Security and Privacy, 104-121.

Bouoiyour, J., and Selmi, R. (2017a). Are Trump and Bitcoin Good Partners?.

Bouoiyour, J., and Selmi, R. (2017b). Ether: Bitcoin's competitor or ally?. Working Papers hal-01567277, HAL.

Buterin, V. (2014). Ethereum White Paper.

Caporale, G. M., Gil-Alana, L., and Plastun, A. (2017). Persistence in the Cryptocurrency Market. DIW Berlin Discussion Paper No. 1703.

Chatzopoulos, D., Ahmadi, M., Kosta, S., and Hui, P. (2017). FlopCoin: A Cryptocurrency for Computation Offloading. IEEE Transactions on Mobile Computing.

Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. Comm. ACM 28, 10.

Chaum, D. (1988). Privacy Protected Payments: Unconditional Payer And/or Payee Untraceability. In D. Chaum and I. Schaumuller-Bichl (eds.), Smartcard 2000: 69-93. Amsterdam, North Holland.

Chaum, D., Fiat, A., and Naor, M. (1990). Untraceable Electronic Cash. In: Goldwasser S. (eds) Advances in Cryptology - CRYPTO' 88. CRYPTO 1988. Lecture Notes in Computer Science, vol 403. Springer, New York, NY.

Conley, J. P. (2017). Blockchain Cryptocurrency Backed with Full Faith and Credit. Vanderbilt University Department of Economics Working Papers 17-00007, Vanderbilt University Department of Economics.

Conti, M., Kumar, E., Lal, C., and Ruj, S. (2017).A Survey on Security and Privacy Issues of Bitcoin. Published in IEEE Communications Surveys & Tutorials, Volume 20, Issue 4.

Dagher, G. G., Bünz, B., Bonneau, J., Clark, J., and Boneh, D. (2015). Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges. In CCS 2015 - Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Vol. 2015-October, pp. 720-731, Association for Computing Machinery.

Dai, W. (1998). B-Money, an anonymous, distributed electronic cash system.

Davradakis, E., and Santos, R. (2019). Blockchain, FinTechs and their relevance for international financial institutions. EIB Working Papers, No. 2019/01, European Investment Bank (EIB).

Dwork, C. and Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. In: Brickell E.F. (eds) Advances in Cryptology — CRYPTO' 92. CRYPTO 1992. Lecture Notes in Computer Science, vol 740. Springer, Berlin, Heidelberg.

Elbahrawy, A., Alessandretti, L., Kandler, A., Pastor-Satorras, R., and Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. Royal Society Open Science. 4.

European Banking Authority (2014). EBA Opinion on 'virtual currencies'. EBA/Op/2014/08.

European Banking Authority (2016). Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD). EBA-Op-2016-07.

European Banking Authority (2019). Report with advice for the European Commission on crypto-assets.

European Central Bank (2012). Virtual currency schemes.

European Central Bank (2015). Virtual currency schemes - a further analysis.

European Central Bank (2018). What is bitcoin?.

European Central Bank (2019). Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures. ECB Occasional Paper Series No 223, ECB Crypto-Assets Task Force.

European Securities and Markets Authority (2017a). ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements. ESMA50-157-828.

European Securities and Markets Authority (2017b). ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs). ESMA50-157-829.

European Supervisory Authorities (2018). ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies.

Eyal, I, and Sirer, E. G. (2014). Majority is not Enough: Bitcoin Mining is Vulnerable. Conference Paper, Chapter from book Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados.

Fahmy, S. F. (2018). Blockchain and its uses.

Frunza, M. (2015). Solving Modern Crime in Financial Markets: Analytics and Case Studies.

Gainsbury, S., and Blaszczynski, A. (2017). How Blockchain and Cryptocurrency Technology Could Revolutionize Online Gambling. Gaming Law Review, 21, 482-492.

Gandal, N., Hamrick, J. T., Moore, T., and Oberman, T. (2017). Price manipulation in the Bitcoin ecosystem. Journal of Monetary Economics.

Gerlach, J. C., Demos, G., and Sornette, D. (2018). Dissection of Bitcoin's Multiscale Bubble History from January 2012 to February 2018. SSRN Electronic Journal.

Greenberg, A. (2012). Black Market Drug Site 'Silk Road' Booming: $22 Million In Annual Sales. Forbes.

Guo, L., and Li, X. J. (2017). Risk Analysis of Cryptocurrency as an Alternative Asset Class. W.K. Härdle et al. (eds.), Applied Quantitative Finance, Statistics and Computing, 309-329.

Harvey, C. R., Tymoigne, E. (2015). Do Cryptocurrencies Such as Bitcoin Have a Future?. Wall Street Journal.

Hegadekatti, K., and S G, Y. (2016a). Examining Taxation of Fiat Money and Bitcoins Vis-A-Vis Regulated Cryptocurrencies. Published in International Finance eJournal, Vol. 8, No. 117.

Hegadekatti, K., and S G, Y. (2016b). Banking Systems in an Economy Dominated by Cryptocurrencies. Published in: Monetary Economics: Central Banks - Policies & Impacts eJournal , Vol. 01, No. 81: pp. 1-16.

Hotz-Behofsits, C., Huber, F., and Zörner, T. O. (2018). Predicting crypto-currencies using sparse non-Gaussian state space models. Journal of Forecasting. 2018;37:627–640.

Jonker, N. (2017). What drives virtual currency adoption by retailers?. Payments Conference 2017 Academic Paper, Joint ECB/BdI "Digital transformation of the retail payments ecosystem".

Kampl, A. (2014). Analysis of Large-Scale Bitcoin Mining Operations. White Paper, Applied Control.

Krogt, D. van der (2018). GARCH Modeling of Bitcoin, S&P-500 and the Dollar. Bachelor Thesis Financial Economics, Erasmus University.

Kroll, J. A., Davey, I. C., and Felten, E. W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In Proceedings of The Twelfth Workshop on the Economics of Information Security (WEIS).

Krugman, P. (2018). Bitcoin is basically a Ponzi scheme. The Seattle Times, 30 January.

Lee, D. K. C., Guo, L., and Wang, Y. (2018). Cryptocurrency: A new investment opportunity?. Journal of Alternative Investments. 20, (3), 16-40, Research Collection Lee Kong Chian School Of Business.

Lin, Q., Yan, H., Huang, Z., Chen, W., Shen, J., and Tang, Y. (2018). An ID-Based Linearly Homomorphic Signature Scheme and Its Application in Blockchain. In IEEE Access, vol. 6, pp. 20632-20640.

Li, X., and Wang, C. A. (2017), The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin. Decision Support Systems, 2017, 95, 49-60.

Mersch, Y. (2018). Virtual currencies ante portas. Speech by Yves Mersch, Member of the Executive Board of the ECB, at the 39th meeting of the Governor's Club Bodrum, Turkey,14 May 2018.

Microsoft (2019). Microsoft Security Intelligence Report. Volume 24, January – Dezember 2018.

Mochizuki, T., and Stech, K. (2014). Mt. Gox Files for Liquidation - Defunct Bitcoin Exchange Gives Up On Plan to Rebuild.

Moore, T., and Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In Financial Cryptography and Data Security, vol. 7859 of Lecture Notes in Computer Science, pp. 25–33. Springer.

Möser, M., Böhme, R., and Breuker, D.(2013). An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. In: eCrime Researchers Summit (eCRS).

Möser, M., Böhme, R. (2015). Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. 2nd Workshop on Bitcoin Research, affiliated with the19th International Conference on Financial Cryptography and Data Security, Puerto Rico.

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

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

Navickas, M., Bagdonas, I., and Ngoc Viet Nguyen, V. (2018).Predicting Bitcoin Price using Machine Learning.

Pagliery, J. (2013). FBI shuts down online drug market Silk Road. CNN Money.

Rosenfeld, M. (2011). Analysis of Bitcoin Pooled Mining Reward Systems. arxiv:1112.4980v1.

Sharma, A. (2018). Digital Money- Bitcoin. In Digitalization, Chapter-30, pp. 122-124.

Schwartz, D., Youngs, N., and Britto, A. (2018). The Ripple Protocol Consensus Algorithm.

Shaw, C. (2018). Conditional heteroskedasticity in crypto-asset returns. Munich Personal RePEc Archive, Paper No. 90437.

Smalley, C. W. (2017). Cryptocurrency and taxes. The Tax adviser, Tax Insider, pp. 1-3.

Staley, H. (2018). Blockchain technology as a disruptor in Finance. The Business and Management Review, Volume 9, Number 3.

Stavroyiannis, S. (2017). Value–at-Risk and Expected Shortfall for the major digital currencies. Article in SSRN Electronic Journal.

Taylor, M. B. (2013). Bitcoin and The Age of Bespoke Silicon. International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES).

Vasek, M., Thornton, M., and Moore, T. (2014). "Empirical analysis of denialof-service attacks in the bitcoin ecosystem". Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC, Springer Berlin Heidelberg, pp. 57–71.

Vasek, M., and Moore, T. (2015). There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. Financial Cryptography and Data Security. FC 2015.

Velankar, S., Valecha, S., and Maji, S. (2018). Bitcoin Price Prediction using Machine Learning. 20th International Conference on Advanced Communications Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), pp. 144-147.

Vora, G. (2015). Cryptocurrencies: Are Disruptive Financial Innovations Here?. Modern Economy, 6, pp.816-832.

Walter, T., and Klein, T. (2018). Exogenous drivers of cryptocurrency volatility - A mixed data sampling approach to forecasting. University of St. Gallen, School of Finance Research Paper No. 2018/19.

World Economic Forum (2019). Globalization 4.0 - Shaping a New Global Architecture in the Age of the Fourth Industrial Revolution. White Paper.

Temas Económicos

1: Relacionamento económico com Angola
Walter Anatole Marques

2: Relacionamento económico com Moçambique
Walter Anatole Marques

3: Relacionamento económico com a Federação Russa
Walter Anatole Marques

4: Evolução da taxa de crescimento das saídas de mercadorias portuguesas face à receptividade dos mercados - Janeiro a Setembro de 2007 e 2008
Walter Anatole Marques

5: Comércio Internacional de Mercadorias - Séries Anuais 2008-2017
Walter Anatole Marques

6: Exportações portuguesas de veículos automóveis e suas partes e acessórios
Walter Anatole Marques

7: Trocas comerciais entre Portugal e a União Europeia na óptica de Portugal e na dos países comunitários 2005-2008 (mirror statistics)
Walter Anatole Marques

8: Expedições portuguesas de Têxteis e de Vestuário para a União Europeia
Walter Anatole Marques

9: Portugal no mundo do calçado
Walter Anatole Marques

10: Entrepreneurship performance indicators for active employer enterprises in Portugal
Elsa de Morais Sarmento | Alcina Nunes

11: Business creation in Portugal: comparison between the World Bank data and Quadros de Pessoal
Elsa de Morais Sarmento| Alcina Nunes

12: Criação de empresas em Portugal e Espanha: Análise comparativa com base nos dados do Banco Mundial
Elsa de Morais Sarmento| Alcina Nunes

13: Comércio Internacional no âmbito da Comunidade dos Países de Língua Portuguesa (CPLP)
Walter Anatole Marques

14: Evolução das exportações de mercadorias para Angola entre 2007 e 2009: Portugal face aos principais fornecedores
Walter Anatole Marques

15: Análise comparada dos procedimentos, custos e demora burocrática em Portugal, com base no "Doing Business 2011" do Banco Mundial
Elsa de Morais Sarmento| Joaquim Reis

16: Exportações portuguesas para Angola face aos principais competidores
Walter Anatole Marques

17: Internacionalização no Sector da Construção
Catarina Nunes | Eduardo Guimarães | Ana Martins

18: Mercado de Trabalho em Portugal desde 2000
Paulo Júlio | Ricardo Pinheiro Alves

19: Comércio Internacional de mercadorias no âmbito da CPLP
Walter Anatole Marques

20: Exportações nacionais – principais mercados e produtos (1990-2011)
Eduardo Guimarães

21: Formação Contínua nas empresas em 2010 e 2011
Anabela Antunes | Paulo Dias | Elisabete Nobre Pereira | Ricardo Pinheiro Alves | Cristina Saraiva

22: Portugal: Uma síntese estatística regional até ao nível de município
Elsa Oliveira

23: Comércio internacional de mercadorias com Espanha em 2013
Walter Anatole Marques

24: Comércio Internacional de Mercadorias Séries Anuais 2008-2013
Walter Anatole Marques

25: Comércio Internacional de Mercadorias - Importações da China - Janeiro-Dezembro de 2011 a 2013
Walter Anatole Marques

26: Evolução das quotas de mercado de Portugal nas importações de mercadorias na UE-27 - Janeiro-Dezembro de 2007 a 2013
Walter Anatole Marques

27: Comércio Internacional de Mercadorias da Guiné-Equatorial face ao mundo e no contexto da CPLP (2009 a 2013)
Walter Anatole Marques

28: Comércio Internacional de mercadorias da Índia face ao mundo e a Portugal
Walter Anatole Marques

29: Comércio Internacional de Mercadorias no contexto da União Europeia 2009 a 2013
Walter Anatole Marques

30: Comércio bilateral entre os membros do Fórum Macau de 2003 a 2013
Ana Rita Fortunato

31: Exportações portuguesas de produtos industriais transformados por nível de intensidade tecnológica - Mercados de destino (2009 a 2013 e Jan-Out 2014)
Walter Anatole Marques

32: Evolução do comércio internacional de mercadorias com Angola - 2010 a 2014
Walter Anatole Marques

33: Exportações nacionais – principais mercados extracomunitários e produtos (1990-2013)
Eduardo Guimarães

34: Evolução do comércio internacional português da pesca - 2013 e 2014
Walter Anatole Marques

35: Comércio Internacional de Mercadorias - Séries Anuais 2008-2014
Walter Anatole Marques

36: Evolução do Comércio Internacional português da pesca e outros produtos do mar (1º Semestre de 2014 e 2015)
Walter Anatole Marques

37: Desafios e oportunidades para a Ilha Terceira. Estudo sobre o impacto da redução de efetivos na Base das Lajes
GEE

38: Análise Comparativa de Indicadores da Dinâmica Regional na Região do Algarve e Continente
Ana Pego

39: Comércio internacional de mercadorias - Taxas de variação anual homóloga em valor, volume e preço por grupos e subgrupos de produtos
Walter Anatole Marques

40: Análise Descritiva das Remunerações dos Trabalhadores por Conta de Outrem: 2010-2012
Elsa Oliveira

41: Comércio Internacional de Mercadorias - Séries Anuais (2008 a 2015)
Walter Anatole Marques

42: A indexação da idade normal de acesso à pensão de velhice à esperança média de vida: análise da medida à luz do modelo das etapas
Gabriel Osório de Barros

43: Balança Comercial de Bens e Serviços - Componentes dos Serviços - 2012 a 2015 e Janeiro-Abril de 2014 a 2016
Walter Anatole Marques

44: Comércio internacional de mercadorias entre Portugal e o Reino Unido
Walter Anatole Marques

45: Comércio Internacional de mercadorias Contributos para o 'crescimento' das exportações por grupos de produtos e destinos (Janeiro a Agosto de 2016)
Walter Anatole Marques

46: A atividade de Shipping em Portugal
Ricardo Pinheiro Alves | Vanda Dores

47: Comércio Internacional de mercadorias no âmbito da CPLP - 2008 a 2015
Walter Anatole Marques

48: Digitalização da Economia e da Sociedade Portuguesa - Diagnóstico Indústria 4.0
Céu Andrade | Vanda Dores |Miguel Matos

49: A participação Portuguesa nas cadeias de valor globais
Guida Nogueira | Paulo Inácio

50: Contributos dos grupos de produtos e principais mercados de destino para a evolução das exportações de mercadorias - Janeiro a Março de 2017
Walter Anatole Marques

51: Comércio internacional de mercadorias: Portugal no âmbito da CPLP - 2012 a 2016
Walter Anatole Marques

52: Administração Portuária – Empresas e sistemas tarifários
Francisco Pereira | Luís Monteiro

53: Comércio Internacional de Mercadorias - Séries Anuais 2008-2017
Walter Anatole Marques

54: A Economia da Cibersegurança
Gabriel Osório de Barros

55: Contributo de produtos e mercados para o 'crescimento' das exportações de bens
Walter Anatole Marques

56: A Cibersegurança em Portugal
Gabriel Osório de Barros

57: Comércio internacional de mercadorias Portugal - China
Walter Anatole Marques

58: Comércio internacional de mercadorias de Portugal com a Venezuela - 2013 a 2017 e 1º Semestre de 2018
Walter Anatole Marques

59: Balança Comercial de Bens e Serviços Componentes dos Serviços (2015-2017 e 1º Semestre 2015-2018)
Walter Anatole Marques

60: O Comércio a Retalho em Portugal e uma Perspetiva do Comércio Local e de Proximidade
Paulo Machado | Vanda Dores

61: A Indústria Automóvel na Economia Portuguesa
Sílvia Santos | Vanda Dores

62: Impacto Económico da Web Summit 2016-2028
João Cerejeira

63: Comércio Internacional de Mercadorias - Séries Anuais (2008-2018)
Walter Anatole Marques

64: A Tarifa Social de Energia
Gabriel Osório de Barros | Dora Leitão | João Vasco Lopes

65: Evolução recente do comércio internacional no 'Ramo automóvel' (2017-2018)
Walter Anatole Marques

66: Comércio internacional de mercadorias com Moçambique (2014-2018)
Walter Anatole Marques

67: Cryptocurrencies: Advantages and Risks of Digital Money
Gabriel Osório de Barros

Gabinete de Estratégia e Estudos