



ICADE BUSINESS SCHOOL

# **BITCOIN AND OTHER CRYPTOCURRENCIES AS PAYMENT METHODS**

Author: Antonio Rodríguez Ramos

Director: Luis Garvía Vega

Madrid  
June 2018



Antonio  
Rodríguez  
Ramos

**BITCOIN AND OTHER CRYPTOCURRENCIES**



## **ABSTRACT AND OBJECTIVE**

The motivation of this final work came from the perception that a time has arrived where payment methods and financial instruments can change significantly as we used to understand them.

Although cryptocurrencies and Bitcoin (their maximum expression nowadays) were created some years ago, it was not until 2017 when we experienced their worldwide explosion.

To start from the beginning and then going deeper, we must answer first some question; What is a Bitcoin and how does it work? What is Blockchain the technology in which Bitcoin rely on useful for and how secure are your Bitcoins? Are there any other technologies?

How anonymous are Bitcoin and other alternative coins (“altcoins” from now on) users? How are cryptocurrencies created and distributed, used for and what determines the price of these coins? How many coins exist, what is an ICO and how reliable or confident they are. Do they have any future from now on and if so, what will be the future of regulation? Do all the countries have the same weight on the definition of standards?

Related to this all, will show how it affects the global economic and financial system and why it created a fever among millions of people such as the Gold Rush in California. Is this a millionaire-making machine or, on the other hand, this is a bubble?

After gaining some initial knowledge of what this is, we will move further into more complicated terms and issues, and why initially international banks and Governments did not give any value to this environment and now they are in a hurry trying to regulate them, by technology and firms behind some projects and even banking institutions owning some of these cryptocurrencies. What is the main use, purpose with them or the value (or just fear) they have seen on them.

Keywords: bitcoin, digital money, blockchain, cryptocurrencies, central banking, decentralization, virtual currency, payment method.

## INDEX

1. <u>Methodology .....</u>	<u>7</u>
2. <u>Introduction .....</u>	<u>8</u>
2.1 Money .....	8
2.2 Electronic money .....	9
2.3 Virtual money, pre-Bitcoin .....	11
3. <u>What is Bitcoin. A bit of history .....</u>	<u>13</u>
3.1 Bitcoin .....	14
3.2 Bitcoin uses .....	17
3.3 Other cryptocurrencies .....	18
3.4 Quick start on cryptocurrencies trading .....	20
4. <u>How Bitcoin works .....</u>	<u>24</u>
4.1 Blockchain technology .....	24
4.2 Obtaining Bitcoin. Mining .....	27
4.3 Wallet and transactions .....	32
4.4 Token .....	36
4.5 Security and weaknesses .....	38
5. <u>Alternative technologies -Ethereum network- .....</u>	<u>41</u>
6. <u>Future of virtual currency .....</u>	<u>44</u>
7. <u>Quick glossary and reference guide .....</u>	<u>45</u>
8. <u>References and bibliography .....</u>	<u>47</u>

## CONTENT INDEX

Figure 1.- Keywords and results obtained on academic websites

Figure 2.- The Byzantine Generals' Problem

Figure 3.- Byzantine Generals' Problem simile with Bitcoin

Figure 4.- Example of 24-hour trade volume by exchange

Figure 5.- Bitfinex trading platform. Source: bitfinex.com

Figure 6.- Binance basic platform. Source: binance.com

Figure 7.- Binance advanced platform. Source: binance.com

Figure 8.- Example of transaction interaction on traditional banking systems.  
Source: coindesk.com

Figure 9.- Example of transaction interaction on Blockchain. Source: coindesk.com

Figure 10.- Example of a transaction performed on Blockchain. Source: medium.com

Figure 11.- Hashrate distribution. Market share of the most popular bitcoin mining pools,  
last 24 hours. Source: blockchain.info

Figure 12.- Complete transaction process. Source: blockgeeks.com

Figure 13.- Digital signature transaction. Source: medium.com

Figure 14.- ICO vs. IPO comparison. Source: masterthecrypto.com

# 1. METHODOLOGY

As still the topic has had short lifetime but facing a long way to go, currently establishing the foundation of terms and discussing how regulations should be done, there is not many official repositories or official academic/workpapers.

Methodology will be based on solid research and contrast of available data, investigation on the main projects and technology and official documents available (whitepapers / development teams papers and comments), interviews to people involved on the creation and financial regulators and experiences of people and users inside the industry.

Cryptocurrencies nowadays present a vast potential for research. A summarize and categorization of available literature on the abovementioned topic has been done in order to get an important and realistic overview of the main issues surrounding Bitcoin and Altcoins (*“Alternative coins”*, name that receive other cryptocurrencies that are not Bitcoin).

I made a first attempt of the available literature doing some searches on recognized websites such as Google Scholar, Academia and Refseek (CiteSeerX and arXiv) with different keywords, to be noted; “bitcoin”, “bitcoin blockchain” and “cryptocurrencies”.

	G. Scholar	RefSeek	Academia
Term	# results		
"bitcoin"	36,700	238	5,335
"bitcoin blockchain"	12,000	238	15,20
"cryptocurrencies"	10,300	192	12,43

Just to have an idea, typing on the searching box “digital money” or “payment technology”, we got more than two million results.

Figure 1.- Keywords and results obtained on academic websites

At a first glance we do not have as much literature as we would have imagined, but most of them useful taking into account I did not reduced the timeframe and most of academic papers are dated after year 2008. As the topic is fresh and constantly evolving at a fast-pace, it is helpful for my review that most of literature is quite recent.

From these sources and personal investigation I captured the most relevant ideas and knowledge about the field to review in this paper the cryptocurrency universe, starting from the very beginning and going through more complex conditions, such as the technology in

which cryptocurrencies rely on, problems cryptocurrencies are facing, regulatory framework and possible evolution on coming years.

## 2. INTRODUCTION

First of all, let me explain what is money and what we use it for. All of people know what money is about, but when you ask most of times we receive silence as an answer or referring to any other thing.

As the International Monetary Fund defines it, money is:

- Store of value. People knows it has value and be stored and used over time.
- Unit of account. It represents a common economic cost or value of an item.
- Medium of exchange. It sets the standard for all people to use it.

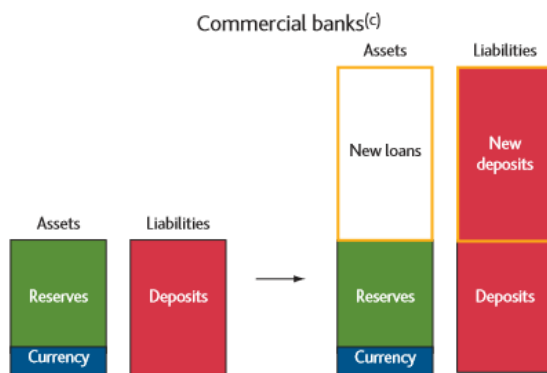
### 2.1 Money

After knowing the theoretical definition, money is overall based on confidence. Not all existing money is physically available to withdraw and storage at home.

On our society the creation of money rely on the confidence we all have on the banking system, as banks only need to keep a fraction part of the deposits they receive in the form of cash (or highly liquid equivalent assets). This is the effect of money multiplier. [ECB, 2011]

Most money takes the form of bank deposits, and lending is the way money is created and transformed into new deposits.





From the perspective of a bank, this is how new money is created. They maintain a small fraction of existing deposits on their balances and lending expands the monetary base.

Figure 2.- Money creation by banking sector. Source: <https://www.monetary.org/wp-content/uploads/2016/03/money-creation-in-the-modern-economy.pdf>

The value of this money is based on the confidence people have in it, and to do so it is needed the support of a trust-worthy third party that support the system (i.e. Central Banks).

Inside their main duties are included banking and regulatory settlement and supervision, money transferring and processing systems and monetary policy rules to follow

## 2.2 Electronic money

People knew already the functioning of banks and money. We saw on how money is created how the system works, and people could not have access to all their funds physically nor even was it convenient to carry on a bag full of banking notes. This search of convenience on payments led to what we call electronic money.

As defined by the ECB: “electronic money (also known as e-money) is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions”.

First electronic money payment method are dated back in 1946, when a banking industry worker at Flatbush National Bank in Brooklyn whose name was John Biggins, launched the Charg-It card.

By using the Charg-It card, payments were transferred to Biggins’ bank, that acted as a

middleman between the buyer and the seller of merchandise. Payments could only be made locally and this simple transaction that was known as “closed-loop” system.

Years after in 1951 first credit card of history was created by New York’s Franklin National Bank. It was needed to own a current account at the bank.

At same time Diners Club card was making its debut. It was mainly used at high-range New York restaurants to pay for meals. In coming years it quickly became widely used for travel and entertainment. It made the step ahead from only local payments to international use, being accepted at stores of more than ten countries apart from US. But Diners club was not what we would properly call a credit card but a charge card. That means that all purchases made with the card where taken into account and collected in full at the end of the month.

Following this trend, some other cards backed by different corporations appeared. This is the case of American Express. American Express was set up in 1850 to compete face to face to the US Postal Service. In its transformation, it managed to do money orders by 1882 and invented the travelers’ checks in 1891. It even made a first attempt of a charge card in 1946 at the time Biggins created its own, but was not until 1959 when they launched the first plastic card ever.

Up to this time, all previous cards offered where made of cardboard. American Express became quickly used, issuing more than a million plastic cards five years later.

Plastic cards lived its glorious days after this decade. American payment services providers such as MasterCard and Visa where founded by 1966 and 1970 respectively, having as their main business the issuance of plastic cards and providing payment services.

Following inventions on plastic money to note are also:

1960, International Business Machines (nowadays IBM) created the mag-stripe. This is the magnetic band on the rear part of plastic cards, providing more security and verification patterns.

On the beginning of XXI Century, RFID technology starts to be implemented of cards. RFID technology allowed short-distance verification when close to a compatible device (i.e. long into ATM machines) or small-amount quick-payments with no PIN code nowadays.

## 2.3 Virtual money, pre-Bitcoin

First attempt talking about virtual money was made in 1983 by American scientist David Chaum.

On his first trial, in 1983 he developed what he called “e-cash” an electronic money transferring application with a focus to preserve the user’s identity.

After this, he founded and improved version in 1989 called DigiCash, which aim was to be a complete electronic money corporation, which first objective was to provide micropayments for consumers’ online transactions. DigiCash was based on Chaum’s previous ideas, and promised every transaction to be anonymous and unique ID, thanks to the implementation of all previous cryptographic protocols developed, so it differentiates from credit cards that it not revealed buyers’ identity.

Small payments managed by DigiCash sunk in coming years due to consumers confidence on using credit cards for the newly created e-commerce activity, and unfortunately DigiCash went bankrupt in 1998 and sold after to eCash Technologies.

Maintaining anonymity was one of the other Chaum’s development focus, and from his scientific background he studied the cryptography field which led to invent multiple cryptographic protocols.

On one of his first research, *Blind Signatures for Untraceable Payments* [Chaum, 1983], he was concerned about the future and the way people used to pay for goods and services will be turned into electronic methods. That final development would have significant impact on personal privacy as banks or payment processing institutions will have all your personal purchasing and money transferring data available. On the other side, this extent or personal privacy could also lead to the elimination of criminal use of money and illegal activities (tax evasion, bribery, black markets...), usually performed with “not-traceable” instruments such as bank notes.

Privacy is a point which we should emphasize. Knowledge by a third party of our habits can reveal not only what we buy or like, but also our habits. Every electronic transaction is associated to a unique transaction ID, which also contains additional data such as timing of the operation, place where it was made and so on. This sensitive information, if not well protected, can end in wrong hands or resold to advertising agencies.

Chaum’s new blind signature proposed in 1983 a system to implement electronic payments with following properties:

- Inability of third parties to determine payee, time or amount of payments made.
- Ability of individuals to provide proof of payment, and to identify the payee under exceptional circumstances.
- Ability to stop use of payments media reported stolen.

The basic idea behind the blind signature system is that it allows a person to receive a message signed by another one while not revealing any other information about the message to the other party.

Typical analogy to explain it better that we can find in Chaum's papers about the topic is:

- To enclose a message in a carbon paper lined envelop.
- To write a signature on the outside of the envelop.
- To leave carbon copy of the signature on the paper inside the envelop.
- Signer does not view the message content, but a third party can be able to verify later the signature.

Most common blind signatures schemes are based on RSA signing and elliptic curve cryptography (ECDSA) signing.

Currently both methods present some dangers. In the case of RSA signing, through a RSA blinding attack it can be cheated to decrypt a message by blind-signing another one. In the case of ECDSA, they are more technical concerns and difficulty to correct implementation.

### **3. What is Bitcoin. A bit of history.**

The creation of the first virtual currencies digital or virtual have been pumped by the development of cryptography and common technological progress.

Basically is a transformation in which bits take the shape of money, and so they represent value that can be exchanged between users. No bank notes, no coins, no plastic backed by current account holders.

Bitcoin and the rest of virtual currencies are, as the name says, virtual money. But is virtual money as trustworthy and useful as it is the ordinary and the plastic one? That make us question two important things:

- Is this money authentic and will it have value for me to use it?
- Will any other third-party claim the ownership of that money that I now own? (Known as “double-spending” problem).

First virtual currencies created prior to Bitcoin (BTC) did not properly satisfied the public these questions. Some examples to be noted:

- Flooz: made appearance during the first years of XXI Century. It was published with the same aim as DigiCash was, to be a digital payment method for small merchants in the beginning of the e-commerce era. Flooz was compared to coupons or promotional loyalty points for companies that you could accumulate. It was backed by venture capital. Its inability to create a critical user base and and accusations of criminal activities performed with its currency using stolen credit cards ended up with the company filing for Chapter 11 at the end of year 2011 and closing down after three years or operation.
- Beenz: another digital method aimed to attract users by granting Beenzes through online advertising campaigns (doing polls, clicking on ads, watching commercials and so on). Compared again to some kind of online loyalty points, Beenz did even signed an agreement with MasterCard and raised venture capital money. Unfortunately the tech bubble peaked by that time and punched on Beenz financial structure and led to its bankruptcy at the end of 2011.
- E-cash and DigiCash: not to forget this Bitcoin’s most important forerunner, explained before and whose father was one of the brightest minds in cryptography.

As we see previous digital currencies before Bitcoin presented some problems to the public. Briefly defined, Bitcoin is a mixture of previous concepts and technologies better implemented, and set a new standard of money creation.

### 3.1 Bitcoin

It all began with the paper *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto (2008).

Satoshi Nakamoto is a pseudonym used by the one (or ones) that created the Bitcoin.

A gaming developer called Hal Finney was one of the first persons that heard about Nakamoto's idea and his proposal of the Bitcoin network. To be mentioned, Finney was one of the member at the beginning of the "cypherpunk movement". The "cypherpunk movement" are said to be a group of activist developers that started from David Chaum's initial ideas on cryptography and blind signature. Some other early members of the movement have been pointed at any time claiming to be Satoshi Nakamoto, but all of them have denied any kind of relationship.

Satoshi made public the first Bitcoin software and its related coins in 2009, meanwhile he asked to the online cryptography community to join in and help on the project. No one ever met Satoshi Nakamoto in person and all his communication were made through an online forum and his email address.

Nakamoto relied on previous concepts and technologies to develop its virtual currency, targeting it to be a decentralized electronic cash system that do not depend on a third-party acting as a supervisor or authority. To do so, he implemented new technologies to solve one of the problems we saw before digital currencies had, the double-spending problem, which until this time it was fixed by using a central clearinghouse acting as the trustworthy part of the transaction chain. The implementation was called the "proof-of-work" algorithm (similar to Adam Back's Hashcash) [Back, 2002]. This implementation makes the confirmation work of an accomplished transaction by using the rest of Bitcoin network users as confirmation nodes. Will see in depth in next chapter.

In the Bitcoin's whitepaper [Nakamoto, 2008], he described a peer-to-peer money transferring system that was aimed to be the system that breaks the traditional path a transaction goes through, this is purchase → bank (acting as intermediary) → merchant

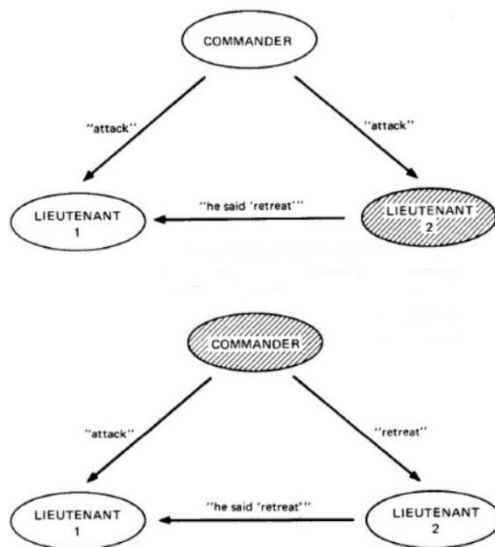
Bitcoin goes one step ahead of traditional monetary systems, and implements an alternative to exchange of goods (transfers), value storage and unit of account without being under the control of a “central clearing authority”.

It is the maximum expression of years of cryptographic developments and distributed electronic systems which contains four key innovations in a powerful combination:

- “A decentralized peer-to-peer network (the Bitcoin protocol)
- A public transaction ledger (the blockchain)
- A decentralized mathematical and deterministic currency issuance (distributed mining)
- A decentralized transaction verification system (transaction script)”

[M. Antonopoulos, 2015]

Nakamoto’s invention also comes to solve an old problem in distributed computing known as “Byzantine Generals’ Problem” (first called “Chinese General Problem”).



An army guided by its General are awaiting to attack the enemy. Communication can only be made via messenger and there is not confirmation if the message ever arrives. The problem presented is trying to agree on a common action in a compromised network (the outlined bubbles acting as traitors). The algorithm “proof-of-work” made its appearance here and allows the network to put in common and confirm, this is, to achieve consensus in the orders coming from every person (the nodes) so it is not compromised. Tasks are managed by the network.

Figure 2.- The Byzantine Generals’ Problem. Source: Microsoft.com

The application of this solution goes way further than being only used for the Bitcoin network.

Lotteries, registries and elections could be the most common areas to start its application on.

Here is a picture comparing the Byzantine Generals' Problem and the Bitcoin




		
Agree on a Strategy	Objective	Agree on Valid Transactions
Separated Camps	Spatial Distribution	Distributed Nodes in the Network
Loyal Troop and Loyal Generals	The Good Ones	Truthful Nodes
Traitors	The Bad Ones	Evil Nodes
Corrupt a Message	The Attack	Add an Invalid Transaction to the Blockchain
How to Know which Message is True	The Problem	How to know which Transaction is Valid
Don't Have	A Solution	Proof of Work
Don't Have	Consensus	Blockchain with More Combined Difficulty

Figure 3.- Byzantine Generals' Problem simile with Bitcoin. Source: weusecoins.com



## 3.2 Bitcoin uses

Bitcoin network is on its soul defined as a system that do not need to rely on trust nor a third party, so it is a combination of various technologies shaped as money to be useful for the people.

Micropayments, as the first' virtual money the we saw before objective. Through Bitcoin software on the merchant's computer, people can go in and transfer Bitcoins directly to him by inputting his address on the client software or using a generated QR code linked to that address.

Every Bitcoin user has a Bitcoin address which is its personal and unique identity, formed by a 27 to 34 alphanumeric characters-long address line, starting from number 1 or 3. Addresses are easily created and managed, and in any desired number. In conclusion, they are similar to email addresses. Will go in depth about Bitcoin mechanisms in section "4.3 Wallet and transactions".

Also used for bigger payments, such as in import/export industries. Acting with the open ledger that Bitcoin's technology provides, we could eliminate the intermediary (bank or exporting agency) as we have the possibility to confirm the payment by every side and avoid higher fees.

Donations and fundraising, easily sent to any place around the globe with access to internet.

In countries with currency exchange problems or extreme high volatility (inflation/deflation) it can be used as a way to storage some value, keep the activity with others accepting Bitcoin as payment or using it outside the troubled country. (Note: Bitcoin currently can only be exchanged for US Dollars (\$). Exchange price to US Dollars is also volatile in case you want to convert to fiat currency in any way).

Mining. Mining rigs made booming appearance after year 2016. Will see in depth in section "4.2 Obtaining Bitcoin. Mining."

Money laundering. An old and well known problem as it happened to first virtual currencies attempts. Bitcoin offers anonymity on ownership and transaction, and it has been used for illegal or criminal activities such as money laundering, evading tax or bribes. See a clear example, money being transferred and exchanged to Bitcoins from a tax heaven or a figurehead. Once on Bitcoin's pipelines, it is not possible to know the beneficiary through anonymous transactions nor the final destination. Closing the circle, that Bitcoins could make appearance on any other country in the world with low taxation and legally recognized framework (different from where it came), exchange it to fiat money and declare it as gains on capital → money introduced on legal circuit after really coming from "unknown" origin.

Fortunately, some Governments are taking some measures at respect (i.e. proofs of activity that granted that Bitcoins, proof of trades etc.)

### 3.3 Other cryptocurrencies

Bitcoin was the first and most well-known, but not the only one. Based on its technology and in some case in any other variations (see section “5. Alternative technologies”) a huge base of coins are on the air.

Some other privacy-focused coins to mention are ZCash (ZEC), Dash (DASH) and Monero (XMR), and not so focused but planning to introduce also some privacy features is Ethereum (ETH/ETC). Regarding Ethereum, will see in depth in section “5. Alternative technologies. – Ethereum Network”.  
LiteCoin (LTC) as another relevant coin to mention.

ZCash, created by the end of year 2016 it is following the path Bitcoin opened but with some different features. Basically, Bitcoin allows anonymity between transactions and parties but as the ledger is publicly open, if you know someone’s address (unique 27 to 34 alphanumeric character address line) is open to public that addresses’ transactions. In ZCash the procedure is the same, all transaction confirmed by consensus of the network but the blockchain is also encrypted and therefore protected against observation, same to with the amount transferred and any other details, adding up higher privacy. ZCash allows also to make public transactions. Total supply will reach 21 million coins (same as Bitcoin).

Dash, created in the beginning of 2014. Functionality based on Bitcoin, main differences are Dash transaction are confirmed within seconds and it implemented the “two-tiered architecture” to create “master nodes”. The Master Node algorithm had a significant failure mode since the beginning, when it allowed a reduced number of a specific web services provider users to pre-mine an important part of supply. Dash also shares a voting system that allows quick decisions to make important changes. On the anonymity side, it implements PrivateSend. “PrivateSend is a currency mixing technique, used to add additional privacy to transactions. Identical inputs from multiple users are added to a single transaction, with several outputs. Due to the identical transactions in the inputs, the outcome is obfuscated, making it difficult to trace the flow of funds (direct methods will not yield a solution). This is based on the CoinJoin method but

is heavily modified.” [Forensic et al., 2017]  
Total supply is 22 million.

Monero, early 2014. Implemented “Ring Confidential Transactions”. Monero is an open-source, more security focused currency. Ring signatures idea was first described by MIT academics in early 00’s. Basically, it creates ambiguity on transactions. When a transaction is made, the Ring (a group of Monero network users) endorse a specific piece of information and members digitally sign it. The ring is composed by more network members than the blockchain requires to confirm the transaction and achieve consensus, so it is not possible to know which members have signed in order to compile the information altogether (all members have equal probability) and keys are only of one use. Monero sets by default all data in private mode (not accessible from outside) and users can select specifically which data to share. Every Monero account has its own “view key”, which as the names suggests allows anyone in possession of it to take an eye to the transactions linked to the account attached to that “view key”. This coin is usually blacklisted from most of exchanges due to its extreme privacy scheme. Total supply is unknown.

Litecoin, created in 2011 by a former Google employee. If Bitcoin is referred as gold, Litecoin is to silver. It is some kind of spin-off from the Bitcoin client, maintaining its core functions but modified to improve the following. It can handle higher transaction volumes than Bitcoin. It was designed to be more “CPU-friendly” regarding its usage and mining. This leads the network to a more frequent block generation (mean 2.5 minutes) on the ledger and as results faster response confirmation and consensus times. Litecoin has been largely affected by criminal attacks, to mention in 2013 malware was filtered in the network and took control of private wallets and funds. In 2015 a detected malware on computers used them to act as “zombies” controlled to mine Litecoins on the background. This kind of malware have been discovered lately mining some other coins. Total supply is 84 million.

Ethereum, created by Vitalik Buterin in 2013. Not a currency by itself (currency is named Ether), it is an open-source decentralized platform that allows peers on the network to create different kind of contracts (consensus), following the blockchain model. Its ledger is public as Bitcoin’s one, so is accessible to see transactions, contracts and values storage on wallets, and blocks on the blockchain are created faster.

Bitcoin and rest of purely coins aims to unseat online banking, Ethereum believes in the power of blockchain as a network to replace third parties on internet, this is, the ones that storage, control or watch the information that passes by (i.e. centralized data centers, financial quotes, medical histories and so on). The idea was presented from the base that centralized organization is not the best structure (see when hackers stole personal data or Government listening to our conversations). So Ethereum is not just a money transferring or store of value system, the main point is what they called the “smart contract system”.

As defined on their website:

- “Build unstoppable application
- Smart money, smart wallet
- Design and issue your own cryptocurrency
- Create a democratic autonomous organization
- Kickstart a project with a trustless crowdsale
- Build a new kind of decentralized application”

Source: Ethereum.org

Will see in depth about Ethereum in section “5. Alternative technologies. – Ethereum Network”.

### **3.4 Quick start on cryptocurrencies trading**

Transactions to transform conventional fiat money into any other kind of cryptocurrency are carried on places called exchanges. This exchanges are usually based on internet web services where you simply access through your internet browser.

At the time of writing this, most important platform that articulate the exchange network are Coinbase, Kraken, Bittrex and Bitfinex. However, as listed on April 2018 at Bitcoin official website, there are over 500 exchanges, with many of them based on places of dubious reputation or even directly made to scam.

This fragmentation ended up with the first listed sites being the most used due to the confidence of its users on them, and at the same time during 2017 when cryptocurrencies

experienced the boom and now on accomplishing with new regulations that they are required to every day by Governments and regulators.

But these businesses that allow users to trade are always under scrutiny and never free of danger.

Youbit (first known as Yapizon), an important South Korean Bitcoin exchange, declared bankruptcy after hacking attack last year.

Mt. Gox, a Japanese bitcoin exchange and maybe the most important one on the early times of the coin. By 2013 it haned over 70% of all Bitcoin transactions worldwide. During its time it suffered million dollar lawsuits, outages, hacks and even faced the US Government. In 2014, they shut down business operations as they could not face all withdrawals request because an attacker that slowly drained all Mt. Gox’s bitcoins hold on its balance without no one noticing was discovered. When completing the review process, the approved claims accounting for more than \$400 million.

As we may notice, we could list theft, fraud, mismanagement or a combination of these as main reasons of exchanges disappearing and so their most important problems suffered.

At the time Mt. Gox went bankrupt, it affected the whole ecosystem as it was the first player regarding exchanges. Nowadays, with plenty of options to choose from this risk is diversified.



Figure 4.- Example of 24-hour trade volume by exchange. Source: bitcoin.com

The appearance of some unknown names on one daily traded volume podium is because due to higher regulatory requirements and confidence on the big ones the only allow trading on clearly recognized cryptocurrencies/projects. Usual path in depositing fiat money (EUR or USD) into the exchange, convert it into Bitcoin or Ethereum and afterwards use that coins to trade any other options. Backwards conversion should follow the same path to be back into fiat money, this is, there is no direct conversion between the other alternative coins and fiat money (EUR or USD).

Due to this, when fresh projects or alternative coins are created and wanted to go into the market, they are usually only accepted on that small and not well-known exchanges until the market shows its support as a decent alternative and it got accepted on the big ones.

In this lapse hundreds of projects burst and they do not make it to the next step. Sometimes they even create their own initial exchange to only trade that altcoin and offer issue premium or any other kind of rewards to create user base, increase expectancy and traded volume.

At the time of writing this, Binance sits on the top with his more than 6 million users and has gone into a multi-billion dollar business, putting its creator and owner Changpeng “CZ” Zhao into the billion-dollar list according (February 2018, Forbes). Binance now supports about 120 coins, 100+ wallets and 240 trading pairs. (Binance website).

Cryptocurrency exchange most demanded features are its trustworthiness, resumed as their ability and speed to convert fiat-crypto-fiat and trading speed.

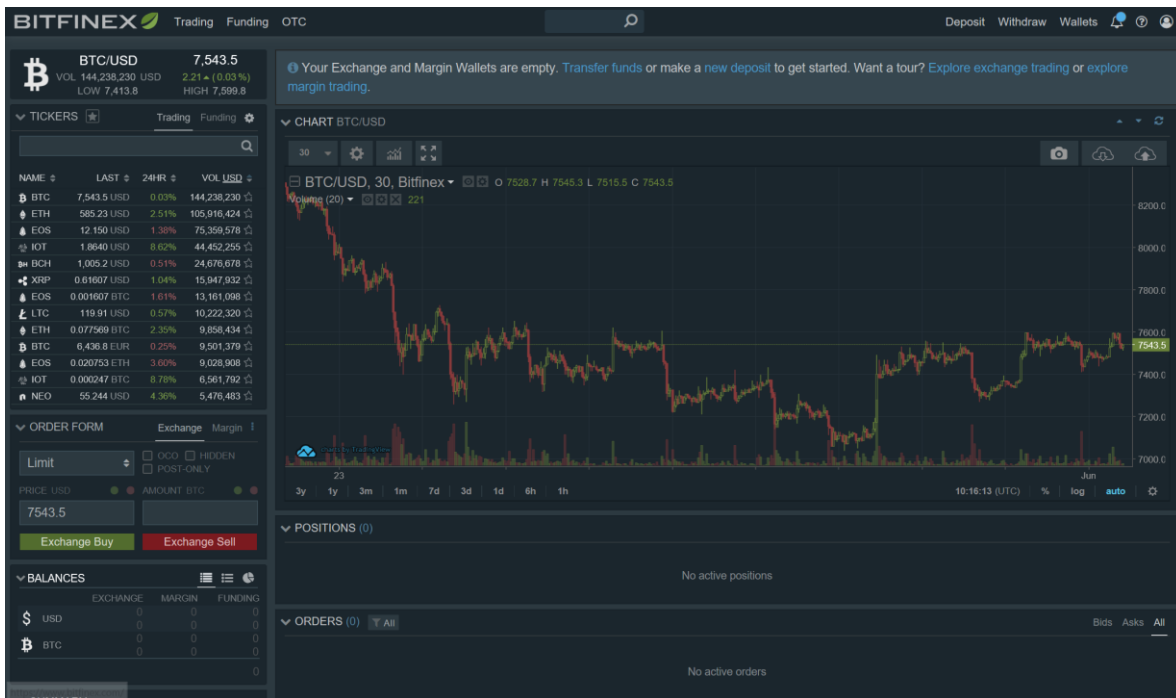


Figure 5.- Bitfinex trading platform. Source: bitfinex.com

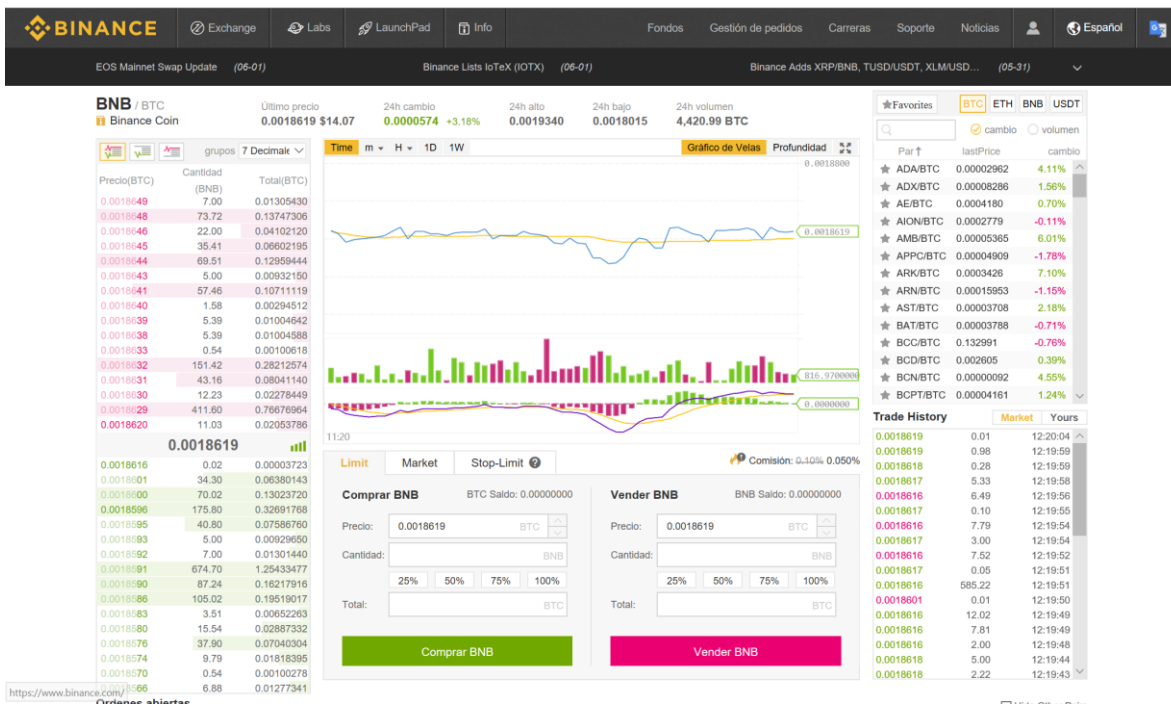


Figure 6.- Binance basic platform. Source: binance.com

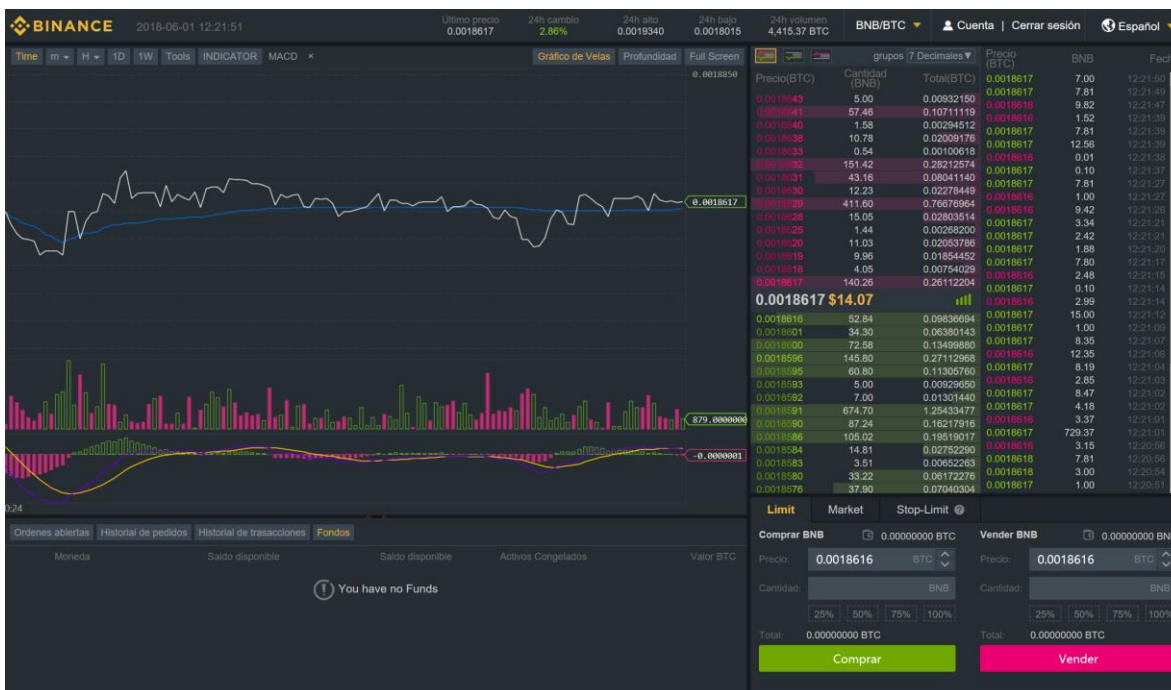


Figure 7.- Binance advanced platform. Source: binance.com

## 4. How Bitcoin works

In this chapter we will see the basics of Bitcoin network perform its operation, how they are stored and more technical issues regarding its security and obtaining methods.

### 4.1 Blockchain technology

"The practical consequence [...] for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate." (Marc Andreessen, Netscape Communication founder and venture capitalist).

Blockchain has become one of the hottest words since the cryptocurrency booming interest in 2017.

What Blockchain technology does is basically allowing two or more people to exchange value without the need of any central authority acting as an intermediary.

Bitcoin system, unlike traditional banking systems, was created on the base of decentralized trust. Transactions do not through an intermediate trusted authority, but benefits from interaction of their users.

We will be talking about the Bitcoin case and its Blockchain application, but must be noted that could be applicable to the vast majority of cryptocurrencies as they use the blockchain to keep track of their transaction. We could say that Blockchain is the origin of all these cryptocurrencies, while the origin of Blockchain was the group led by Satoshi Nakamoto.

We could name the blockchain as a public ledger. In the blockchain many people can write entries completing the record of information, and the user network overwatches and control how this information is recorded, amended and updated. The ledger allows us to know the amount of Bitcoins each of us own. This ledger is represented as a digital file or document where the network quotes the information.

As mentioned, unlike traditional banking where we trust the bank institution and its database to keep our money, and we access their services to trust what they are showing



we own (even though nowadays there are several checks and tools to keep track of it) the fact is that the bank is the one owning our savings and transaction and trust them. On the Blockchain when I start a transaction, useful information regarding what I did (time and date, amount, sender and recipient...) is spread through a bunch of different nodes of the network (the users) that have a copy of the central database (the ledger).

At that time, every node updates the version of the central database they own independently from each other so there are not inferences, and then spread again the notice to compare with the rest of nodes the update they made whether is it same (correct) or not. The most agreed version becomes the new official record of the database (the ledger).

Here we have a graphic comparison between the procedure of transaction on a regular banking institutions (see Figure.- 8) and how the Blockchain performs the operation (see Figure.- 9).

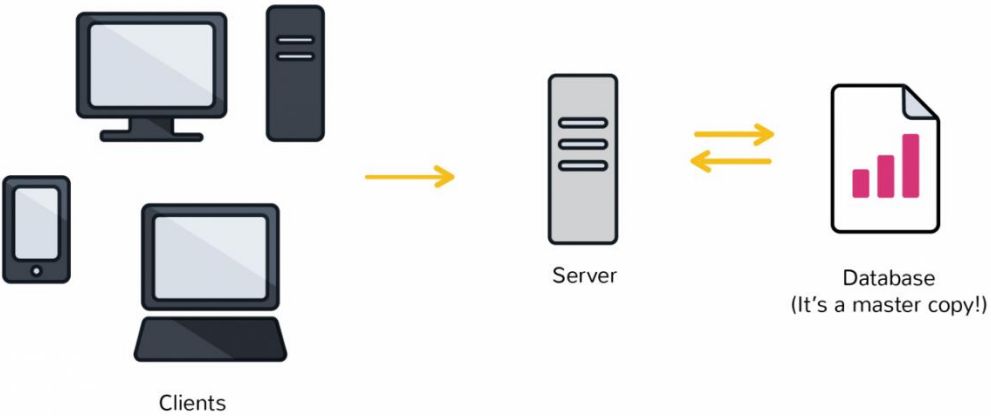


Figure 8.- Example of transaction interaction on traditional banking systems. Source: coindesk.com

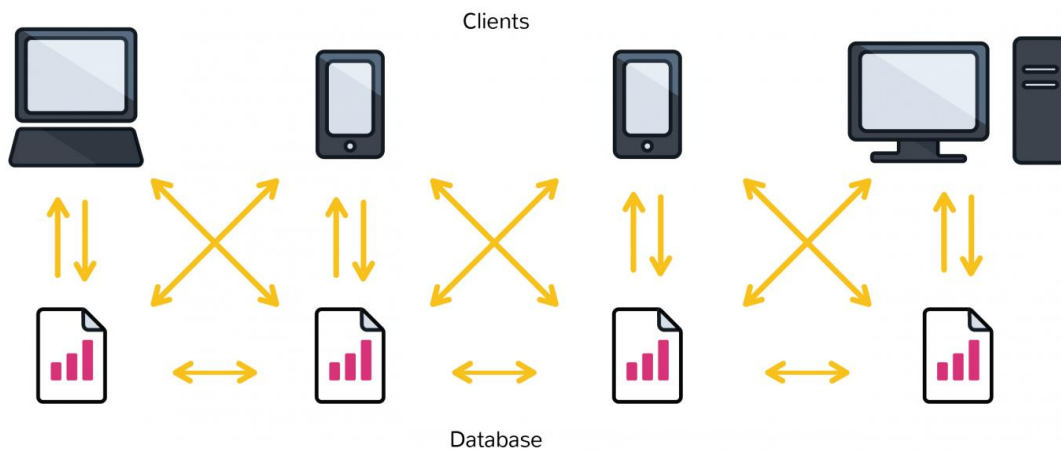


Figure 9.- Example of transaction interaction on Blockchain. Source: coindesk.com

Going back to the ledger, as we see the functioning it is not stored in a central server nor anywhere, it is distributed worldwide across the nodes that conform the private blockchain network that store their own version and then check with the rest of nodes whether to consider legit a transaction and update the database. These nodes are basically the computers of the network users (Each computer is a node and has its own copy of the ledger). Acting this way the ledger cannot be corrupted in any way by its own nature.

The fact of the ledger being maintained by a group of members (the connected nodes) rather than a central institution such as a bank has many implications, as for example:

- In own bank we can see our account balances, positions and transactions while on the blockchain all transactions are publicly available (although only anonym addresses with no names).
- You trust your bank or financial institution, and there a place or person where you can go in case of doubts or complaints, and even a regulated path to complaint. The blockchain network is distributed and therefore there is no one or place you can go to in order to complain in case something goes wrong or not as desired.
- Blockchain system is not fully backed by trust but for special algorithm and mathematical operations that secure and check the network.

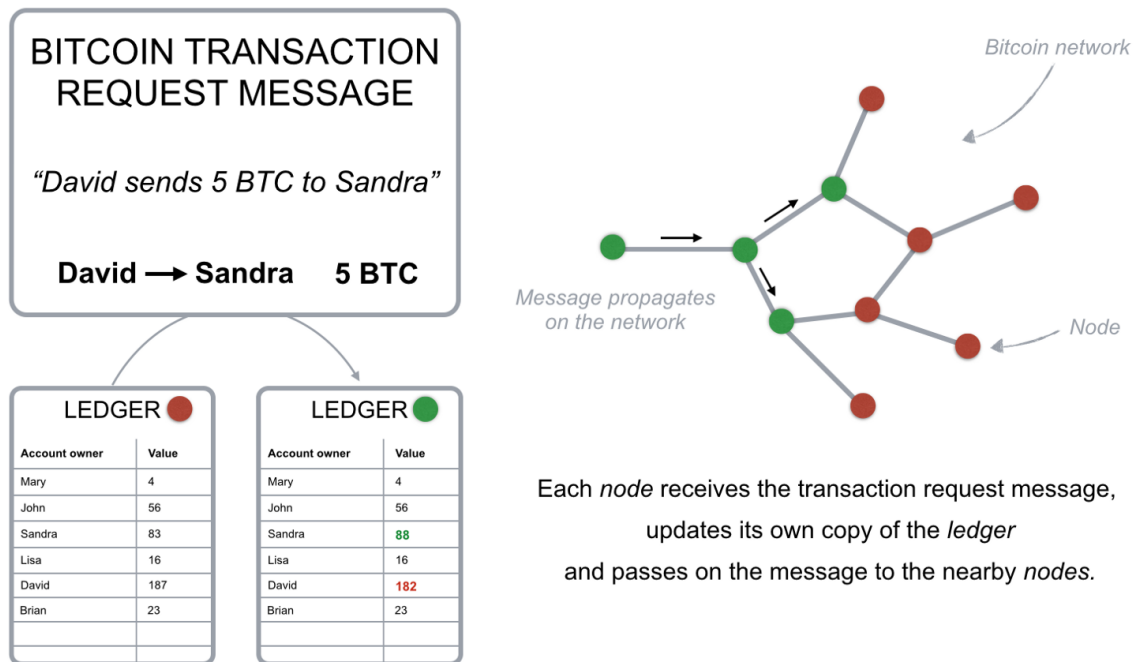


Figure 10.- Example of a transaction performed on Blockchain. Source: medium.com

## 4.2 Obtaining Bitcoin. Mining.

We saw how the Bitcoin network works and the use of Blockchain technology to perform correct transaction. To continue understanding how the network does this operations and checks, next step is mining.

Mining became also a hot word in 2017 since many news talked about it related to Bitcoin as a way to earn money and accessible to everyone as the only requirement was to have a computer and internet connection.

Indeed, mining is an important part of the cryptocurrency ecosystem. The term “mining” is slang for the use of computational power to solve the complex algorithms and mathematical operations that allows confirming of transactions and grant security to the system.

Information is always encrypted and the Blockchain is permanent and immutable to any other thing no related to this process.

The computational power is to process transactions on a cryptocurrency blockchain and receive a reward (a piece of that cryptocurrency) for that effort.

Computational process is the output produced out of the CPU power (computer's main processor) or GPU power (computer's graphic card processor). These rewards that miners receive for the process in form of cryptocurrency assets or tokens comes from the fees collected to the ones that initiated the transaction, so they receive a fee in the form a surplus of Bitcoin. Today fees represent less 1% of miners total earnings, as the majority on this income comes from the fresh mined Bitcoin. Before confirming a transaction they enter into a "block", which is a batch of data pending to be introduced on the Blockchain. Rewards for completing a Bitcoin or any other coin block depends on the active miners at that moment or number of transactions. After that the information is entered in the Blockchain and the verification among nodes mentioned before takes place. These rewards decrease over time and number of transaction per every block increase at the same time. Although mining is rewarded with these fees and successful miners granted with portions of the coin, it is not only the process new Bitcoin are created. Mining is the skeleton of the decentralized network, which allow transaction validation and clearing and in a perfect and harmonized view of the system, the creator aligned the miners objectives while making stronger the network at the same time.

Bitcoin is mined at a fixed and diminishing rate, on the creation of each block of the Blockchain. Every block is created on an average of 9 minutes (source: bitinfocharts.com) and contains new Bitcoin created. After all Bitcoin had been issued (21 million), no new Bitcoin will be created. Every 210,000 blocks the currency issuance rate decrease by 50%. 210,000 blocks were planned to last for at least 4 years of operation, but current developments and high processing power have broken this timelapse to move in some months frame. After total issuance set at 13.44 million blocks all Bitcoin will have been mined and miner will only be rewarded transaction fees. Having a look at the difficulty level (it reflects how difficult the proof of work is in respect of the difficulty value set at inception, which was 1). In Jun' 17 difficulty was 678,760,110,082 meanwhile Jun' 18 the number was set at 4,306,949,573,981 million (source: blockchain.info). In regards on this vast increase in difficulty, the huge processing power installed and improvements made to mine had been the key to maintain the average time of block creation at 9 minutes.

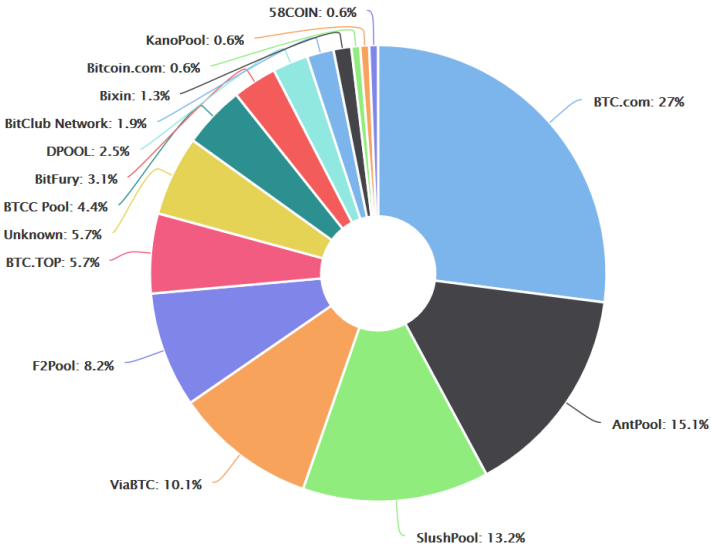
The way of establishing a mining machine varies from: Solo Mining or Pool Mining.

- Solo Mining: miner use the resources (CPU or GPU power) of their own domestic computer. Pros of the method is that the miner will receive full rewards given to the block he completes, and Cons are that there are few chances to repeatedly completing blocks with the limited processing power of one domestic machine. This method then present advantages for fresh new cryptocurrencies introduced (few users, limited network) and losses its place when the network becomes bigger (solid coins as Bitcoin).  
Should be noted that some advantaged developers found a way to benefit from which is called “pre-mine”. As the name indicates, they mine by themselves on a blockchain of a fork developed by them hoping to introduce later one the project and earn a good sum with the selling onto the public (main idea is to sell their pre-mined coins once they make it to an exchange and get a profit from a “pump and dump” scheme). Due to the public nature of the Blockchain, it is completely transparent to the people with knowledge to detect this behaviour and once discovered the tactic exchanges can become reluctant to list them on their services.
- Pool Mining or Mining Rig: when professionalising the mining, next step is constructing “mining pools”. It consists on the share of processing power of a network and split the reward in the amount of power they provided to help fill the block. The miners configurate the pool using a software hosted on a server or VPN (private network) to authenticate all machines running together and split their shares.

Mining lived its own golden era alongside the cyrptocurrency euphoria.

The use of this computer hardware and time has been demonstrated to be also a high consumption process. While CPU processing was originally used to mine at its origing Bitcoin and Litecoin, difficulty rates increased and became not profitable enough and miners then changed to GPU power, being now the most common method used when constructing mining rigs. Increased network of users and therefore miners leads to an increasy in difficulty to earn every reward. Usual “modus operandi” of miners were to storage the rewards earned and only use small

parts of it to keep the installation running and updating component (not cheap) with the thought that more difficulty to process and due to the limited supply of coins, prices will keep rising and then benefit from selling in the long future. At the date of writing this, Bitcoin is down more than 50% from its peak price achieved in December 2017 (CoinDesk Bitcoin Price Index's all-time high of \$19,783.21 on Dec. 17).



Here we have an estimation of hashrate distribution amongst the largest mining pools.

It should only be used as a rough estimate and for various reasons it will not be 100% accurate as expected. Dynamic data for the last 24 hours.

Figure 11.- Hashrate distribution. Market share of the most popular bitcoin mining pools, last 24 hours. Source: blockchain.info

A quick reference for Malware Mining and the use of Botnets. Botnets (also known as zombie computers) are a group or network of computers infected with malware that allows the malware creator to use them on his wish, most of time with tasks running on the background of the computer meanwhile the owner does not even realize.

These botnets have been lately found to be using the infected computer’s processing power illicitly to mine in their behalf any kind of cryptocurrency possible.

“Interestingly, many mining pools that have discovered evidence of mining botnets participating in their efforts have noted that many such botnets are ‘good actors’ from the perspective of the pool. Alperium (a Swiss mining pool) received a portion of botnet hashing power in April of 2017, largely from devices that had individual contributions of less than 5MH/s . Mobile phones, home PC’s and other hardware were all directed to mine Ethereum in this manner, as the electricity costs of doing so are not of importance to the

botnet operator. The botnet does not seek to overload the target network, though this example caused issues by registering many individual addresses to the pool, causing database load problems. These problems led to the discovery of the substantial number of low-rate miners, and the subsequent purge of those miners from the pool. Technical staff commented that the botnet appeared, in all other respects, to act like any other miner and accrue funds, without inconveniencing the pool.

Bondnet is an example of a diversified mining malware: it mines multiple coins but appears to favour Monero. In May 2017, it was reported as mining \$1,000 a day in cryptocurrencies, the majority of which was derived from Monero proceeds. Infecting over 15,000 windows servers, this malware has been active since December 2016. The primary impact on the victims is increased power costs, with quotes of \$1,000-2,000 in additional electricity costs. It is strongly suggested that as well as frequent patching, companies monitor their energy and resource usage to spot any anomalous behaviour, such as intensive out-of-hours processing.

Mirai has been reported as mining Bitcoin in early 2017, but only for a few days. IBM X-Force reported that an unknown group (or individual) was experimenting with the computational power represented by the many IoT devices under the control of the botnet . However, the mining difficulty of Bitcoin, long dominated by ASIC hardware optimised for low power and high return on investment, is so high that the return provided by such a Botnet is exceptionally low. This does have implications for less hard currencies, however, and those that favour CPU mining over ASIC mining.” (Forensic *et al.*, 2017)

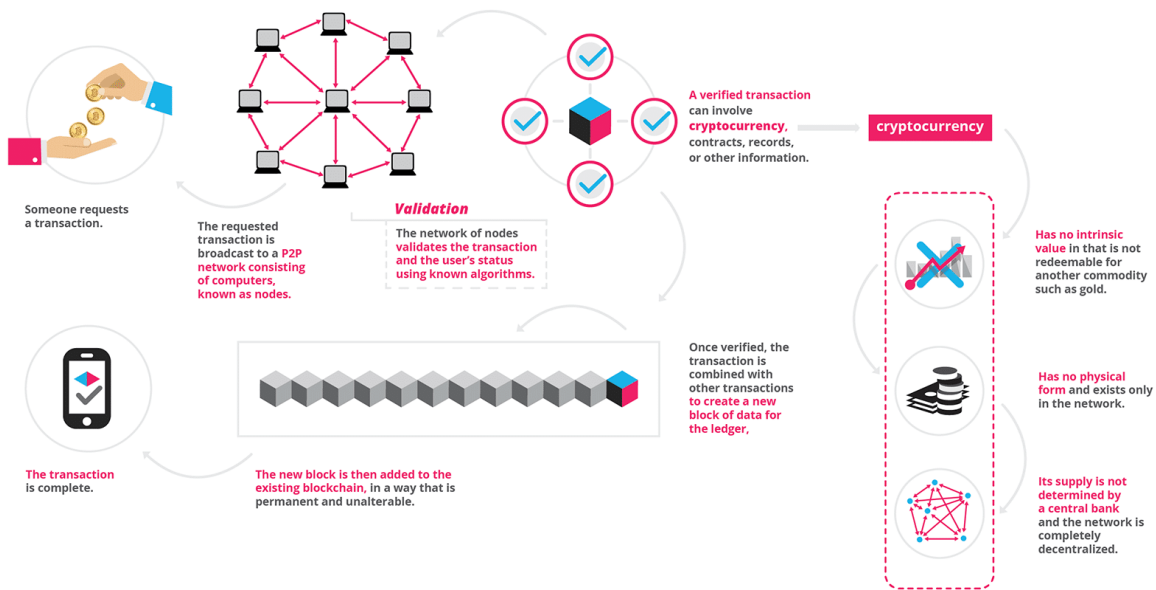


Figure 12.- Complete transaction process. Source: blockgeeks.com

### 4.3 Wallet and transactions.

To carry on operations with your Bitcoins or alternatives coins and storage them safely, you need a wallet. This wallet is basically a client software that allows you to storage your Bitcoins. Every wallet belongs to one user, and this wallet is protected by cryptographic methods that holds two type of keys (public and private), different but connected between them.

The wallet works as follows: if a message is encrypted with a specific public key on the owner of the connected private key will be able to decrypt it back and read the message. It also works on the other way around when encrypting a message with your private key only the paired public key could decrypt it.

Following previous examples, if I want to send a Bitcoin to anyone, the transaction is spread on the network encrypted with my private key (I am the only one that can access my Bitcoins with my private key to unlock my wallet). Then the nodes check that I am the owner of the transaction by using my public key to decrypt the request.

This is because when encrypting a transaction with my private key I generate a digital signature which is what the network uses to cross check the source, request and



authenticity of transaction. This digital signature is a combination of my transaction request and private key, so it is unique for every transaction and cannot be used for anything else.

Let's see in the following chart a graphic example of this, which is quite clear and extracted from medium.com

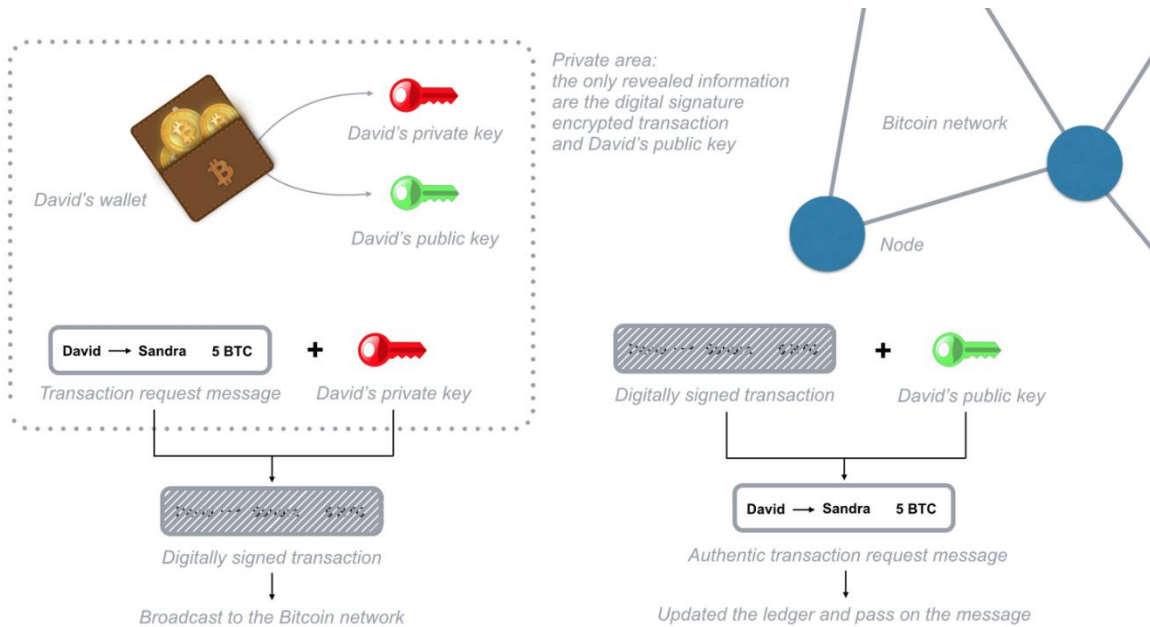


Figure 13.- Digital signature transaction. Source: medium.com

It is important to understand that the wallet does not actually contain your Bitcoin as you could have imagined. The blockchain system doesn't keep track of account balances at all, it only records every transaction that is requested. The ledger in fact does not keep track of balances, it only keeps track of every transaction that is broadcasted within the Bitcoin network. To know your wallet balance, you need to analyze and verify all the transactions that ever took place on the whole network connected to your wallet. With the keys of your own wallet you are granted permission to access and spend your Bitcoin. Therefore if you lose access to your wallet, you will lose the Bitcoin stored on it.

So as a resume, you do not really get to own Bitcoin and store it in a place. There are transactions on the ledger that point out to your wallet (anonymous address) and are available to use.

Regarding the type of wallets and its specifications, the older ones are usually full node wallets. This means that you download the full blockchain and act as a relayer or

transmitter, you receive transactions from network and spread them onto other nodes, and help contributing to the update of the blockchain. This is why it was mainly done on the older and first versions, because you have to download and update all time the whole blockchain (currently sized 170 GB at the end of May 2018, source: blockchain.info)

More recent wallets are called “thin wallets” or SPV (Simplified Payment Verification). Widely used now on desktop computer and mobile phones as this SPV wallets only download the block headers (low consumption).

The total number of possible Bitcoin addresses is  $2^{160}$  or 1461501637330902918203684832716283019655932542976. This large number protects the network from possible attacks while allowing anyone to own a wallet.

“Wallet technology is evolving rapidly in terms of efficiency and functionality, so this overview does not hope to cover all wallet types, but the basic principle is the same for most: wallets hold your keys, not your bitcoins, although the distinction is actually not that relevant for the average user. Bitcoin wallets are a fundamental piece in the path to increase bitcoin use beyond geeks and techies, as it is the only face of bitcoin that most will ever see. Wallet ease of use and security will increase confidence in transactions, while at the same time encourage more use cases. With more users comes even more innovation, and the entire sector – from front-end wallets to back-end miners and including the many applications in between – benefits.” (Noelle Acheson, CFA, Editorial Producer at CoinDesk).

Reaching this point, we should mention which are the different types of wallets available to users, they vary from client software installed on your personal computer or hosted in cloud services. Client software is a common proprietary software you install to manage your wallet/s and the ones hosted in cloud services have technically the same functioning but you are relying your confidence on a 3<sup>rd</sup> party (the cloud company or hosting servicer) to storage online your keys. This could have different problems in sense that you are not protected to a malware or hacking attacks that affects the servicer and steals your data (as we have seen many times happening on other kind of services).

- Software wallet: installing the client software on you PC and the certainty that you are the only one maintaining and accessing to your private keys. They are free (most of times) and easy to install. You should carefully configure backup files and have a second copy on an external drive, so in case the computer breaks down or infected through corrupted file you do not lose your Bitcoin. The first and original software was the Bitcoin Core Protocol. As a disadvantage, you

will have to download and manage backups containing the full Bitcoin transaction database (the full ledger of Blockchain), and as mentioned before currently sized 170 GB at the end of May 2018, source: [blockchain.info](http://blockchain.info). However, and for the sake of convenience the most common software wallets in use nowadays are light ones or SPV (you do not have to deal with the full downloaded ledger).

Examples of SPV wallets mentioned are “Jaxx”, which offers the possibility to have various profiles to store a bunch of different cryptocurrencies. “Electrum”, Bitcoin wallet with cold storage specs (understanding “cold storage” as an option to work with it offline). And “Copay”, which main characteristic is the possibility to create shared accounts with other users.

- Cloud wallet: or online-only wallet. Main advantage is it does not depend on the software installed on your computer nor to have physical access to it, you can access to your Bitcoin or cryptocurrencies from anywhere in the world with your passwords. Disadvantage is, as mentioned, that you give your trust to a 3<sup>rd</sup> party to store and manage the access to your account and therefore your Bitcoin. They are usually free to use and offers desktop and mobile access and also light software to install (APK for mobile phones). Cloud wallets are usually linked to exchanges (CoinBase and Kraken as the most famous ones). Actually they sometimes offer offline storage, and increase security methods you can set up your account with (2-Step verification at access, notifications at your email/mobile phone when accessing, use of 3<sup>rd</sup> party security measures as Google Authenticator, delayed withdrawal transactions and so on). They are the easiest way to store and manage your keys and use of coins, as these internet services offers nice ease-of-use user interfaces.
- Mobile wallet: for smartphone use only, in the form of a general APP (APK installation). Widely used for mobile transactions through users (send/receive) and as a payment method in stores with contactless payment capabilities (making use of our Bitcoin account and the NFC chip included on latest smartphones). Most wallets (both desktop client and cloud ones) as their respective mobile versions.
- Hardware wallet: small devices (usually with the shape of a commonly known USB flash drive) to use as a secure place to store your keys, which is only connected to approve transactions. One of the most secure methods of storage, as they are not accessible through internet to be hacked or infected. Disadvantage is, however, if you lose it you will lose your private keys (and therefore your Bitcoin). Hardware wallets are the preferred storage method of important investors with

large sums invested. An example of this could be the Trezor, supporting 500+ coins which even offers the possibility to create an offline backup along with a personal recovery seed that will allow you to recover access in case you lose or get it stolen. Price of these devices are in the range of \$100 to \$200.

- Paper wallet: simple method and also one of the most secure. It consists on a paper where the private keys and addresses are printed. No one could access it from internet and protected from hacking attacks as they are not storage anywhere but in your paper. Obvious disadvantage in case you lose the paper. Famous service to create a new wallet address in [bitcoinpaperwallet.com](http://bitcoinpaperwallet.com).

People investing serious amounts of money usually develop a mixed strategy. They have the majority of their assets hold in an offline hardware wallet which they even keep in safe-deposit boxes, and maintain a current amount to spend on cloud services for easy and quick access.

#### **4.4 Token**

Tokens represent any assets (in this case, any cryptocurrency) that is fungible and tradeable. This definition includes digital coins, commodities or even store loyalty points.

Issuing token is much easier than creating a new project of digital cryptocurrency. It is not needed to code a particular protocol nor modify a previous one, not even create from zero a Blockchain to work with.

There are some services or platforms that allow you to create your own tokens, a standardized path on the blockchain easier to create for example on the Ethereum network. The possibility to create our own token and mention Ethereum is because it is made through “smart contracts” (one of the main uses of this network out of being a digital altcoin or platform).

Smart contracts computer codes that can be modified to fit a particular need, self-executing and not needing a centralized or third-party entity to operate (following the principles of decentralization).

Creation and distribution of tokens are made through and ICO (Initial Coin Offering) which is something similar to an IPO (Initial Public Offering) for regular stocks, but with differences.

ICO is only referred to digital assets and it is some kind of crowdfunding which includes the launch of a new cryptocurrency or token and need funding for that new project.

ICO's have been under scrutiny as they experienced a booming growth in 2017. People saw them as an attractive opportunity to be first ones owning that new cryptocurrencies at a discount and really cheap price so that they will be able to sell them later in short/medium time making a hefty profit. Some projects did not have even any development base nor future use and followed a "pump and dump" scam structure, in which the people that held the assets since the IPO sold them quickly after some days heating the market and transferring that worthless right to a fooled investor.

*"It's like penny stocks but with less regulation" (Jeff Garzik)*

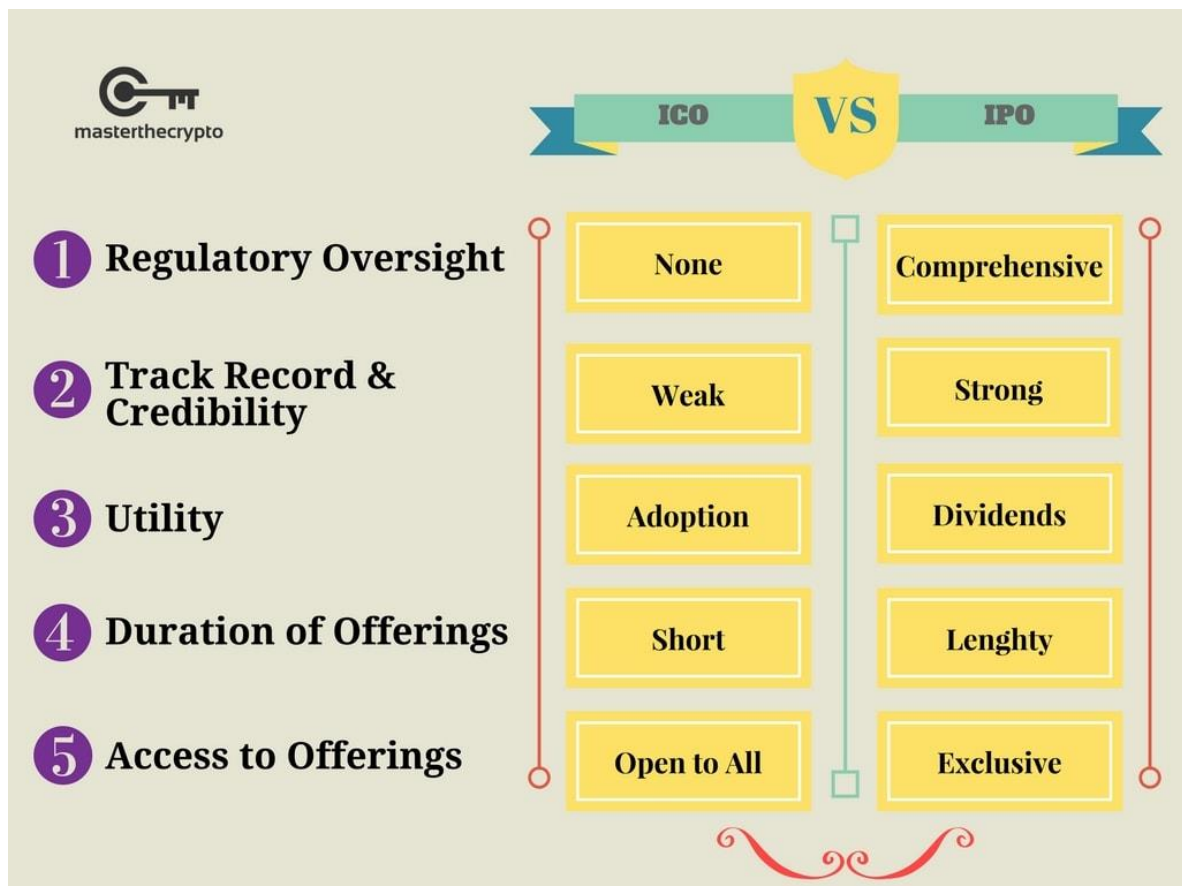


Figure 14.- ICO vs. IPO comparison. Source: masterthecrypto.com

## 4.5 Security and weaknesses

Bitcoin is the most famous and dominant technology, it is on the peak of cryptocurrency market capitalization and in utilization in cybercrime. The nature of the Bitcoin network as decentralized and unregulated makes it ideal for illegal activities, although it is not resistant to tracking techniques. These digital assets implement cryptography as a central part of the protocol, in order to establish high privacy and decentralized currencies. Bitcoin uses SHA-256 encryption for both its Proof-of-Work (PoW) system and transaction verification. The Bitcoin Blockchain is a public ledger, and although we cannot know the real identity of a person behind a Bitcoin public address it is possible to follow and track transactions from and to a particular address, so transactions are traced. This is why increased interest in altcoins with improved anonymity features has surged lately.

It is possible to access the network (in this case, the Bitcoin one) through TOR or VPN services (granting anonymity to the connection established), so then the only information that could be traced would be the public address (public key). The user is granted full privacy, but the problem remains on the public address, where everyone can trace transactions coming to and from. However, on the Bitcoin network we are able to generate multiple wallets (as many as we want to own), every one of them with their own collection of public and private keys. By acting this way, we could have multiple wallets in use so it would be harder for anyone following our steps to track all transactions to different wallets not related.

As said on previous pages, main vulnerabilities are related to the way we store Bitcoin and hackers and cyberattacks. According to a report made by researchers belonging to Edinburgh University, weak spots on highly encrypted hardware wallets were found in order to be exploited by malware (a loophole). By using malware the researchers were able to catch the communication on the bus between the PC and the hardware wallet, so the security of the transaction was compromised and they could take control of the destiny of funds. Also problems related to online Bitcoin wallets are not exempt from security breaches. The protocol could be safe enough, but not so the environment and services related to it.

To recall;

- Bitcoin wallet service [inputs.io](https://inputs.io) was hacked twice in a year (year 2013). More than 4,000 Bitcoin were stolen through a backdoor attack to its hosting service provider.

It all started with a compromised email account belonging to the site's founder that he had used years ago, before creating the website.

- Mt. Gox, the old leading bitcoin exchange provider that went bankrupt. Mentioned on chapter 3.4, by 2013 it handed over 70% of all Bitcoin transactions worldwide. During its time it suffered million dollar lawsuits, outages, hacks and even faced the US Government. In 2014, they shut down business operations as they could not face all withdrawals request because an attacker that slowly drained all Mt. Gox's bitcoins hold on its balance without no one noticing was discovered. When completing the review process, the approved claims accounting for more than \$400 million.
- Silk Road 2.0, almost \$3 million worth of Bitcoin were stolen from Silk Road's escrow account (Escrow account is referred to a temporary pass through account held by a third party during the process of a transaction being performed between two parties). Hackers attacked the Bitcoin's transaction malleability (valid transactions that can be modified through a process that make them appear as unrealized, when they really were performed).

Other attack suffered by the Bitcoin network was the Pony Botnet one. By the end of 2013, the attackers used a botnet named Pony to steal more than \$200,000 worth of digital coins. This same botnet was reportedly found to have also stolen more than two million user's passwords of Bitcoin wallet from installed client software on infected computers.

There are also some technical witnesses affecting the Bitcoin protocol, to mentioned as the main ones: 51% attack, Double Spending, Selfish Mining.

- 51% attack: also called "Over 50%". It is a security concern for users that does not have a simple solution and is catalogue as one of the most serious dangers. As the difficulty of mining Bitcoin increase over time, more miners have come together to conform more powerful mining rigs. This opens the doors to the possibility of a group owning more than 50% of the network processing power appearing the possibility of a 51% attack. They could threat the network by manipulating transactions mining invalid block or double-spending. This could seem further away, but was nearly to happen in the beginning of year 2018 when in the middle of the panic lived in January led Ghash.io (a powerful

mining pool) to reach almost 50% of network processing power. Antpool, one of the most powerful mining rigs (from China, owned by Bitman Tech.) controls around ¼ of total computational installed power. Combined with any other 2 or 3 mining pool, they could achieve the 50% mark. Mining pools have shown conscious and prudent with this issue, managing the situation to avoid reaching high portions of power by stopping acceptance of new members or leaving to smaller pools. Mining power distribution has become more diversified lately.

- Double spending: related to transactional risk, it is related to the possibility to fool the system and spend twice the same Bitcoin. Double spending can be done in a variety of ways. One is transactional, say I send one Bitcoin to my cousin and after that I execute the same movement to other wallet of my property. During the process of confirming, there are two conflictive transactions on the network and I can end up with the Bitcoin credited on my other wallet while my cousin does not receive anything. No recourse can be made by my cousin as no central authority to intervene exists. Another way is pre-mine a transaction into a new block and spend it before releasing that block to the Blockchain. This is a less typical trick as it requires much more processing power than legitimate mining of Bitcoin.
- Selfish mining: or Block Withholding. Can make appearance when powerful mining pools gain significant mining ratio. The pool uses their computational power to hide a mined block to other miners from outside the pool instead of engaging the new completed block into the Blockchain. The gaining pool then tries to find a second block in a row while the rest of pools are still behind on the chain. If the selfish miners get the second block and and share it, the resulting two blocks makes their chain the longest addition to the Blockchain with the consequent reward earned. On a large scale Block Withholding can grant the power to invalidate transactions on the Blockchain.



## 5. Alternative technologies –Ethereum network-

Mentioned on chapter 3.3, and repeating a small and brief introduction to Ethereum here.

Created by Vitalik Buterin in 2013. Not a currency by itself (currency is named Ether), it is an open-source decentralized platform that allows peers on the network to create different kind of contracts (consensus), following the blockchain model. Its ledger is public as Bitcoin's one, so is accessible to see transactions, contracts and values storage on wallets, and blocks on the blockchain are created faster. Bitcoin and rest of purely coins aims to unseat online banking, Ethereum believes in the power of blockchain as a network to replace third parties on internet, this is, the ones that storage, control or watch the information that passes by (i.e. centralized data centers, financial quotes, medical histories and so on). The idea was presented from the base that centralized organization is not the best structure (see when hackers stole personal data or Government listening to our conversations). So Ethereum is not just a money transferring or store of value system, the main point is what they called the "smart contract system".

As defined on their website:

- "Build unstoppable application
- Smart money, smart wallet
- Design and issue your own cryptocurrency
- Create a democratic autonomous organization
- Kickstart a project with a trustless crowdsale
- Build a new kind of decentralized application"

Source: Ethereum.org

Ethereum is currently second on market capitalization, right after Bitcoin, and it was conceived as an improved version of Bitcoin. Major differentiation point is related to the smart contract system. Smart contact applications run on the Ethereum network, so it is not only a cryptocurrency or store of value by itself. This system supports Intelligent Contracts, DAO's and Dapp's and use Ether as its raw material. Ether is the name that Ethereum network cryptocurrency receives.

It is the currency used by the user's network to execute payments to any other user or machines that perform the requested operation (smart contracts).

Some data about Ethereum:

- 60 million Ether were created to the contributors in pre-ICO.
- 12 million were created to the development fund, first contributors, developers and Ethereum Foundation.
- 5 Ether are created on each block (every 15 second in average) as rewards for miners.
- 2 Ether are sometimes sent to other miners if they were able to find a solution but their block was not included on the Blockchain (called Uncle Reward).
- Ether creation is limited to 18 Million units per year (accounting for 25% of the initial offering)

With the aim to eliminate accidentally infinite loops, hostile or any other depuration when coding, every transaction is forced to establish a limited number of executing computational lines to go through. The main computational unit is named "gas". As a general rule, every computational step consume 1 gas, having some operations charging more than 1 gas because they are computationally heavier to carry, or because they dramatically increase the amount of data required to be storage. There is also a fixed fee of 5 gas for every byte included in a transaction data.

The purpose behind this commission scheme is to force a hypothetical attacker to pay proportionally as the resources consumed (processing power, bandwidth and storage).

## **HOW DOES ETHEREUM WORK**

Ethereum follows Bitcoin's principles of a decentralized network. The nodes are the different actors that joint conform the global Ethereum network. This nodes dedicate their resources to keep the network running properly, interconnected between them and making use of the Blockchain. Ethereum is open source, so anyone can access to the font code to see its depuration, modify or propose improvements, alongside with the creation of EVM based applications.

EVM (Ethereum Virtual Machine) is a software executed on the Ethereum network that allows anyone to execute any program, not related to the programming language used. This helps to make the creation of applications based on the Blockchain much easier as you can build whatever application you can adapt in a same platform instead of having to create a new original Blockchain for every application.

Main purpose of this project, as stated on its white paper, is to decentralize and anonymize the internet. To stop giving the power to treat and manage our personal information to big internet corporations and be the users their solely owners and allow full privacy on internet.

## APPLICATIONS

Constantly improving and finding new applications, the main ones could be listed as follows:

- Cryptocurrency and payment method. As any other digital currency, Ether is the name that Ethereum network cryptocurrency receives. Ether is also the fuel that keeps the network running as we saw to grant rewards to the actors involved of the correct functioning of Ethereum. Ether payments follow same path as Bitcoin, they are validated by different nodes and registered on the Blockchain.
- Smart Contracts. Code developments over Ethereum network that allow a secure exchange of value, money, properties, shares, contents or any other adaptable and valuable thing. After registered in the Blockchain, a Smart Contract is a software that executes automatically when default conditions are met. The registration on the Blockchain allows to comply with the contract with no inference or fraud from any other side. They are developed on a programming language called Solidity and make use of gas to encourage depuration on coding.
- Dapp's. To allow developers to create and implement decentralized applications ( a Dapp), applications similar to the ones we already know not controlled by any central authority or 3<sup>rd</sup> party entity but for their users. Pros are increased safety and transparency while eliminating the intermediate connection point. They interact with Smart Contracts and make use of the Blockchain.
- DAO's. Also kown as Decentralized Autonomous Organizations. Could be something as an organization with no head, with default rules executed through program code. Defined as an array of Smart Contract written on the Blockchain. A DAO belong to the ones owning the tokens, and instead of being shares or a property piece these token as rights of vote.

Extrapolating from these past applications, we could also add some other as: Connector to IoT, Crowdfunding, Voting System, Market Watch, Online Gaming Fairness and so on.

## 6. FUTURE OF VIRTUAL CURRENCY

After having some knowledge about what the Blockchain technology brings in and what it is behind them, some appreciation should be made.

Especially after the falling and scamming of some exchange servicers, there is a claim for appropriate and independent auditing and safety measures that protect the investor from misappropriation and deliberate scam schemes. If Bitcoin and the rest of altcoins want to survive and adapt to be used by a wide range of people, some measures as this have to be taken into consideration. Not to forget that this forms of control are explicitly in front of what Bitcoin represents and nothing to do with its initial purpose, but for sure in the middle point is the virtue. it has mainly to do with the fact that fiat money (traditional money) is issued and control, with planned money supply and monetary policy politics that influence on it, made by Governments what provide it trustworthiness among its users whereas Bitcoin with its self-regulation, limited supply and independent network with no authority but its users to regulate it rely its power and confidence on its user base.

Blockchain technology has several Pros:

- Open to the public ledger, timestamped and everyone can access and monitore transactions.
- Transaction completed in few minutes time and confirmed as valid in hours.
- You are the one responsible and full owning your value in the form or any cryptocurrency you hold.
- Cost effectiveness, as fees are the same for local and international transactions.
- Blockchain network allows developers to build new applications using the basics of the Blockchain for other purposes, not online transactions.

Whereas it also has some Cons or points to improve:

- Anonymity of transactions and misuse of the project for illegal activities, although the flow can be monitored.

- Huge fragmentation on exchanges and payment methods.
- Extreme high volatility. Cryptocurrencies and especially Bitcoin price is highly affected by news or announcements.

The Blockchain technology is one of the greatest inventions lately and has the power to introduce a new revolution not only in the Finance industry. Usage is not only dedicated to transactions, also the possibility to create a decentralized network with no supervision to develop Smart Contracts.

## 7. QUICK GLOSSARY AND REFERENCE GUIDE

- Bitcoin: name of the network, the software client and the unit of value (the coin itself)
- Wallet: client software used to manage private address keys and the place to send, receive and store our virtual currencies. It can be soft (software based, on internet) or hard (hardware based, only accessible by having the physical device and password to access to its storage).
- Address: personal and unique identifier (similar to a current account number), formed by a 27 to 34 characters-long line, starting from number 1 or 3. Addresses are easily created and managed.
- Blockchain: technology behind Bitcoin. Is a transaction database, when a transaction is requested the chain (nodes or network members) has to confirm the movement and write it on the correct block of the book. This is what a bank does when we transfer money to other person, acting as the trustworthy party. In the blockchain, decentralization takes the power and members achieve consensus on the transaction (no third party).
- Mining: act of adding transaction records to the Bitcoin's database (the blockchain).
- Hashrate / hashing power / mining effort / hashpower: computational power of the computer machine appointed to mine. Measured in hash per second. One hash is one iteration of the cryptographic algorithm (hash function). [Hayes, 2016]

- Block: group of transactions that conform a part of the chain (Blockchain). Marked with a timestamp and a fingerprint to assure legitimacy over the previous block.
- Confirmation: when a transaction is included in a block, it has one confirmation. When another block is mined in the chain, it has now two confirmations and so on. Six or more confirmations are considered enough proof of transaction legitimacy.
- Difficulty: how much computational processing power is needed to produce a proof-of-work.
- Fee: small payment applicable to the sender of a transaction in order to process every transaction by the network.
- Poof-of-Work: piece of data that requires important computational processing power to find. In the Bitcoin case, miners have to find a solution to the SHA256 algorithm that meets a network-wide target, the difficulty.

## 8. REFERENCES AND BIBLIOGRAPHY

Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System," [Www.Bitcoin.Org](http://www.Bitcoin.Org), p. 9. doi: 10.1007/s10838-008-9062-0.

Lamport, L., Shostak, R. and Pease, M. (1982) "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, 4(3), pp. 382–401. doi: 10.1145/357172.357176.

Krombholz, K. et al. (2017) "The other side of the coin: User experiences with bitcoin security and privacy," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9603 LNCS, pp. 555–580. doi: 10.1007/978-3-662-54970-4\_33.

Huhtinen, T.-P. (2014) "Bitcoin as a monetary system: Examining Attention and Attendance," p. 110.

European Central Bank (2011) "The Supply of Money - Bank Behaviour and its Implications for Monetary Policy," *Monthly Bulletin*, October(October), pp. 63–79.

Bonneau, J. et al. (2015) "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," *IEEE Symposium on Security and Privacy*, pp. 104–121. doi: 10.1109/SP.2015.14.

Polasik, M., Piotrowska, A. and Wisniewski, T. P. (2015) "Price Fluctuations and the Use of Bitcoin : An Empirical Inquiry \* Price Fluctuations and the Use of Bitcoin : An Empirical Inquiry," pp. 1–43.

Biggins, B. J. et al. (2004) "History of the Card Payments System," (03), pp. 2004–2005.

Back, A. (2002) "Hashcash - A Denial of Service Counter-Measure," [Http://Www.Hashcash.Org/Papers/Hashcash.Pdf](http://www.Hashcash.Org/Papers/Hashcash.Pdf), (August), pp. 1–10.

Hileman, G. and Rauchs, M. (2017) "2017 Global Cryptocurrency Benchmarking Study," *SSRN Electronic Journal*. doi: 10.2139/ssrn.2965436.

Chaum, D. (1983) "Blind Signatures for Untraceable Payments," *Advances in Cryptology*, pp. 199–203. doi: 10.1007/978-1-4757-0602-4\_18.

Forensic, I. et al. (2017) "D6 . 2 Altcoins : Alternatives to Bitcoin and their increasing presence in Malware-related Cybercrime Lead Authors ;," pp. 1–36.

Morisse, M. (2015) "Cryptocurrencies and Bitcoin: Charting the Research Landscape," Americas Conference on Information Systems, pp. 1–16.

Jason Mick (12 June 2011). "Cracking the Bitcoin: Digging Into a \$131M USD Virtual Currency". Daily Tech.

Empson, Rip (28 March 2013). "Bitcoin: How an Unregulated, Decentralized Virtual Currency Just Became a Billion Dollar Market". TechCrunch. AOL inc.

S., L. (2 November 2015). "Who is Satoshi Nakamoto?". The Economist. The Economist Newspaper Limited.

Lee, Tim (December 12, 2017). "A brief history of Bitcoin hacks and frauds". Ars Technica.

"Bitcoins Virtual Currency: Unique Features Present Challenges for Deterring Illicit Activity" (PDF). Cyber Intelligence Section and Criminal Intelligence Section. FBI.

Kaushik Basu (July 2014). "Ponzis: The Science and Mystique of a Class of Financial Frauds" (PDF). World Bank Group

Gaby G. Dagher; Benedikt Bünz; Joseph Bonneau; Jeremy Clark; Dan Boneh (26 October 2015). "Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges" (PDF). International Association for Cryptologic Research.

Gervais, Arthur; Karame, Ghassan O.; Capkun, Vedran; Capkun, Srdjan. "Is Bitcoin a Decentralized Currency?". InfoQ. InfoQ & IEEE Computer Society

Tschorsch, Florian; Scheuermann, Björn (2016). "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies". IEEE Communications Surveys & Tutorials.

Antonopoulos, Andreas M. (2015) "Mastering Bitcoin". O'Reilly Media, Inc.

White Paper · ethereum/wiki Wiki · GitHub (no date). Available at: <https://github.com/ethereum/wiki/wiki/White-Paper>

Crypto ICO vs. Stock IPO: What's the Difference? - Master The Crypto (no date). Available at: <https://masterthecrypto.com/crypto-ico-vs-stock-ipo/>

Security Concerns and Risks Related To Bitcoin (no date). Available at: <https://www.tripwire.com/state-of-security/security-awareness/security-concerns-risks-related-bitcoin/>

What is a Cryptocurrency Token? - CryptoCurrency Facts (no date). Available at: <https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-token/>



Differences Between Cryptocurrency Coins and Tokens (no date). Available at: <https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/>

The Mystery Behind Block Time – FACILELOGIN (no date). Available at: <https://medium.facilelogin.com/the-mystery-behind-block-time-63351e35603a>

How does a bitcoin wallet work? (no date). Available at: <http://www.fintechblue.com/2016/02/how-does-a-bitcoin-wallet-work/>

How Does the Blockchain Work? – Michele D’Aliessi – Medium (no date). Available at: <https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae>

The Number of Cryptocurrency Exchanges Has Exploded - Bitcoin News (no date). Available at: <https://news.bitcoin.com/the-number-of-cryptocurrency-exchanges-has-exploded/>

Comparison of cryptocurrencies - Bitcoin Wiki (no date). Available at: [https://en.bitcoin.it/wiki/Comparison\\_of\\_cryptocurrencies](https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies)

CoinDesk - Leader in blockchain news. (no date). Available at: <https://www.coindesk.com/>

Bitcoin Wiki (no date). Available at: [https://en.bitcoin.it/wiki/Main\\_Page](https://en.bitcoin.it/wiki/Main_Page)

Bitcoin and the Byzantine Generals Problem (no date). Available at: <https://www.weusecoins.com/bitcoin-byzantine-generals-problem/>

Lamport, L., Shostak, R. and Pease, M. (2016) “The Byzantine Generals Problem,” ACM Transactions on Programming Languages and Systems, 4/3.

Mastercard - Global Leading Company in Payment Solutions Offering Credit, Debit, Prepaid Cards & More (no date). Available at: <https://www.mastercard.us/en-us.html>

Education | Why do we need a central bank like the Fed when the laws of supply and demand will keep everything working perfectly? (no date). Available at: <https://www.frbsf.org/education/publications/doctor-econ/2004/december/supply-demand-central-bank-established/>

Back to Basics: What Is Money? - Finance & Development, September 2012 (no date). Available at: <http://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm>

Proper Bitcoin Price Analysis Part 1: Methodology (no date). Available at: <https://99bitcoins.com/bitcoin-price-analysis-part1-methodology/>

