Title: **Bitcoin: An Overview**

Authors: **Eduardo Santos, Hugo Ferreira, João Soares, Pedro Bastos**

Date: **13/04/2021**

Contents

1. Introductory Note

This report consists of a brief analysis of Bitcoin and its protocol, exploring its surge and growth in the cryptocurrency market, as well as the seven pillars of Bitcoin. The main goals is to explain Bitcoin in a way that anyone can understand.

We will start by addressing the topic of cryptocurrencies, explaining what they, how they work, and how they are compared to the money we know, also going through the topic of cryptocurrencies mining. We will also address the topic of blockchain, explaining what it is and how does it work.

To finish, we will explain some of Bitcoin's socio-economical impact.

2. Summary / Abstract

Cryptocurrencies like Bitcoin have been widely spoken over the past few years, majorly because of what they represent: the beginning of the globalization of digital currencies.

They came as a new way if looking at money, and they wouldn't exit without blockchain.

3. Cryptocurrency

3.1. Definition of Cryptocurrency

3.1.1. What is Money

To understand what is a cryptocurrency, we first need to understand the concept of money as a form of currency, as well as a medium of exchange of goods and services. Before money as we know it existed, the payment/trade of goods and services was made with commodity money.

3.1.1.1 Commodity Money

Commodity money is a physical good whose value comes from the resource of which it is made, in other words, that has "intrinsic value" - utilization outside of its use as money. As such its underlying value and use ensures that people trust it because it has value in and of itself and so people can trade it freely with the knowledge that someone will accept it. This type of money is usually durable, divisible, easily exchangeable, and rare.

Some historic examples of commodity money being salt (extremely important to conserve food) and tobacco - after World War II some parts of Europe briefly used this type of money.

Eventually, society evolved into a system of representative money and fiat money.

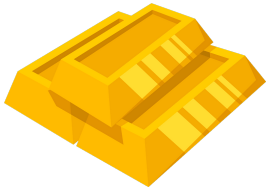

Figure 1: Commodity Money

3.1.1.2 Representative Money

Representative money is a form of currency often printed on paper that represents something of value - a resource/commodity - but has little or no value of its own. Its acceptance requires that the population trusts the certificate as much as the value that it represents. It was usually backed by a physical resource such as precious metals like gold or silver that existed in the United States as silver certificates or gold certificates issued by state banks. Nowadays, financial instruments like checks and credit cards are the most common forms of representative money.

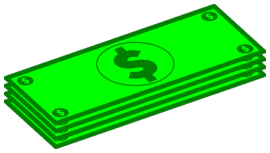

Figure 2: Representative Money

3.1.1.3 Fiat Money

Fiat money is the most common type of currency nowadays, with every other nation operating on some form of fiat money like the Euro or the GBP[1].

> **Fiat money is a currency without an underlying value. Instead, its value is derived by government and the trust people place in its value. In other words, it is a form of currency that only holds value because of government enforcement.**
>
> *Source:BoyceWire's definition of fiat money*

It's a type of money where trust is fundamental because, although its value is given by an official law or order, its true value lies in the trust that people place in it. If consumers and businesses did not trust its enforcement value, then it would not be accepted as a method of payment/trade of goods and services. It is only because people believe others will accept it as a method of payment/trade that it maintains its value, if this did not happened, it would be worthless.

Figure 3: *Fiat money*

[1] Great British Pound

Some advantages of this type of money is that it can technically be unlimited and it's cheaper to produce, central banks can "print" as much money as they want, and the production cost is small if not null. Because much of the transactions are being done online nowadays.

On the other hand, gold, silver, or any other resource/commodity is limited by the extraction process, for instance on a mine, and the limited nature of its existence with an exorbitant cost, because it requires workers to mine it, process it, transport it, and then finally store it in a safe place.

The two previously mentioned advantages create stability because the money supply can react quicker to an increasing/decreasing economic output and enter the market in a short period of time, preventing and decreasing the effects of cases like the Great Depression by creating a greater level of price stability, in other words controlling high inflation and deflation.

3.1.1.4 Inflation and Deflation

Inflation, measured using the consumer price index, is where the price of goods increases over a set period of time, in other words, the price of a good or service is increasing and each unit of currency buys fewer goods and services consequently reflecting a reduction in the purchasing power per unit of money therefore damaging the economy.

Deflation, measured using the consumer price index, is a decrease in the general price level of goods and services, in other words, allows more goods and services to be bought than before with the same amount of currency, being generally associated with a contraction in the money supply. Although it can be positive in the short-term as it can provide a boost to economic growth if consumers believe prices won't continue to fall, in the long-term, if consumers start to expect deflation every year, they start delaying purchasing decisions in the perspective that they will get the goods and services even cheaper next year which can depress the economic output.

The previously referred stability was demonstrated in the 2008 financial crisis where prices remained relatively stable with inflation rising by an average of over 1,5 percent in the following three years, something that most economists favor while in the Great Depression inflation declined by an average of over 8,8 percent in the following three years.

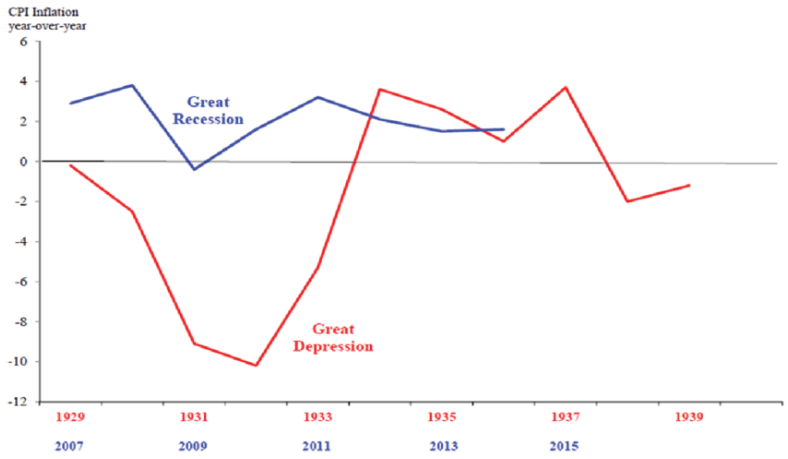

Figure 4: Inflation and deflation rates during the Great Depression and Great Recession

However, stability relies more on the decisions made by the central banks that can have more of an effect than the type of money or even the type of currency used, as demonstrated by the Venezuela currency, the Bolivar Fuerte, replaced the original Bolivar in 2008, but inflation is still very high because among other factors there are no clear restrictions on how much the government can or cannot print money.

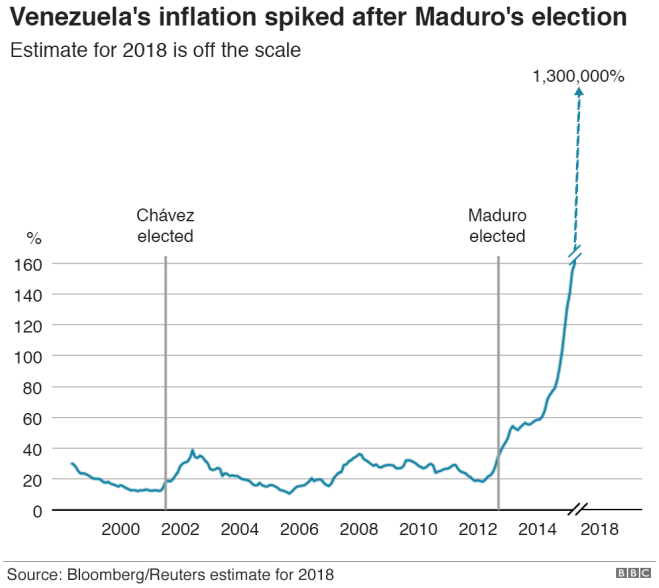

Figure 5: Venezuela's inflation fluctuation between 2000 and 2018

3.1.2. What is Cryptocurrency

A cryptocurrency is a digital currency, in other words, a medium of exchange that is encrypted and decentralized. Unlike the U.S. Dollar or the Euro, there is no central authority that manages and maintains the value of a cryptocurrency. It doesn't rely on banks to verify transactions, instead it's a P2P[2] system that can enable anyone anywhere that has a digital wallet to send and receive payments using a technology called blockchain, which we will talk about later on in this report.

A cryptocurrency wallet doesn't actually hold any currency, it merely provides an address for your funds.

Unlike physical money that is carried around and exchanged, cryptocurrency payments exist purely as digital entries to an online database that describes specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger.

It's possible to buy or sell cryptocurrency in exchange for a fiat currency like the U.S. Dollar using a cryptocurrency exchange. Exchanges, which can hold deposits in both fiat and cryptocurrencies, credit and debit the appropriate balances of buyers and sellers in order to complete cryptocurrency transactions. People can also use cryptocurrency to buy products and services with more and more companies accepting this type of currencies as a payment method.

Cryptocurrency got its name because it uses encryption to provide security and safety in transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers.

[2]peer-to-peer

Figure 6: Types of cryptocurrencies

3.1.3. Comparison between Cryptocurrencies and Fiat Money

Compared to fiat money, cryptocurrencies share some characteristics as both can be used for payments and as a store of value. Both rely on widespread trust of people in order to function as a means of exchange although cryptocurrencies' trust and value is based on the underlying technology blockchain while fiat money's value and trust is derived from a governmental institution or a trustworthy authority such as the ECB[3].

Some key differences are that cryptocurrency is produced and distributed through a process called mining and most have a cap which means there is a set amount of coins that will ever be in supply, making it possible to tell the amount in circulation at any given time, something impossible in fiat money.

Cryptocurrency is not controlled by a centralised authority, transactions can't be reversed, cancelled or charged back and while fiat money can be physical, cryptocurrency is only digital.

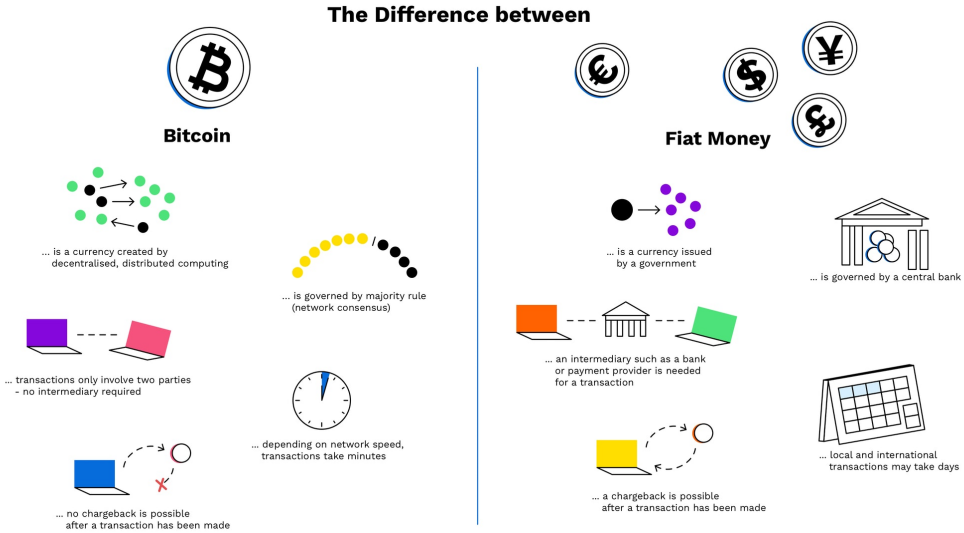

Figure 7: Difference between cryptocurrencies and fiat money

[3]European Central Bank

3.2. How Cryptocurrencies Work

Cryptocurrencies work using a technology called blockchain. Blockchain is a decentralized technology spread across many computers that manages and records transactions in a way that makes it difficult or impossible to change, hack, or cheat the system, a characteristic that constitutes much of the appeal for this technology.

We will talk more about blockchain on the next section.

3.3. Cryptocurrrencies Mining

The process by which new currency is produced and entered into circulation is designated as Mining. Mining is also a critical process of the maintenance and development of the blockchain ledger is performed by high power computers that require either a GPU[4] or an ASIC[5] in order to set up a mining rig, to solve complex computational math problems. When computers solve these complex math problems on the network, they produce new cryptocurrency (similar when a mining operation extracts gold from the ground) and by solving the computational math problems, miners make the blockchain network trustworthy and secure by verifying its transaction information.

Transactions made in-store or online are documented by Banks, point-of-sale systems, and physical receipts and Miners achieve the same by clumping transactions together in blocks and adding them to the blockchain. When Miners add a new block of transactions to the blockchain, they need to make sure that those transactions are accurate. In particular, make sure that the cryptocurrency is not being duplicated, a characteristic of digital currencies designated as “double-spending.”

Miners after completing blocks of verified transactions which are added to the blockchain can then receive a reward if they are the miner who discovers a solution to a complex computational math problem first, and the probability that a Miner will be the one to discover the solution, is related to the portion of the total mining power on the network making mining a very meticulous, costly, and only sporadically rewarding but nevertheless important.

Figure 8: Bitcoin Mining

As previously mentioned, to make transactions in cryptocurrency, you need a wallet for that currency, that in fact doesn’t hold any currency as it merely provides an address for your funds on the blockchain. A cryptocurrency wallet also includes private and public keys that enable you to complete secure transactions.

[4] Graphics Processing Unit
[5] Application-Specific Integrated Circuit

So every time it's made a transaction to payment of goods and services or transfer cryptocurrency, an individual authorizes the movement of a specified amount of the cryptocurrency from his wallet address to the wallet address of the seller. The transaction is encrypted with the individual private key and pushed to the blockchain. The cryptocurrency network's miners access the individual public key to confirm that his private key was used to encrypt the transaction. Once the block that includes the individual transaction is confirmed, the ledger is updated to show the new cryptocurrency balances for both the individual address and the seller's address and the miner may be rewarded with cryptocurrency for confirming the transaction, with this entire process being conducted by software.

4. Blockchain

4.1. What is the blockchain

A blockchain is a chain of blocks that contains information. A blockchain is a distributed ledger that is completely open to anyone, and it relies on a key property: when some data is recorded inside a blockchain, it becomes very difficult to change it. But how does that work?

Each block in the blockchain contains:

- **Data** - this stored data depends on the type of blockchain. In the case of the Bitcoin blockchain, it stores the following details:
  - Sender
  - Receiver
  - Amount of coins to be traded
- **Hash of the block** - it works like a fingerprint, identifying the block and all of its contents and it is always unique.
- **Hash of the previous block** - this creates a chain of blocks, they form the blockchain itself.

Once each block is created, its hash is calculated. Changing something inside the block, will cause the hash to change. In another words, hashes are very useful when we want to detect changes to blocks, if the fingerprint of a block changes, it no longer is the same block.

4.2. How does it work?

Let's take, for instance, the chain of blocks in the image below:

Figure 9: *Example of a blockchain*

As we can see, each block has a hash and the hash of the previous block. So block number 2 points to block number 1, and block number 3 points to block number 2. The first block is called the *Genesis Block*, as it has not got previous blocks.

Now, let's say that someone tampers with the second block, as shown in the image below:

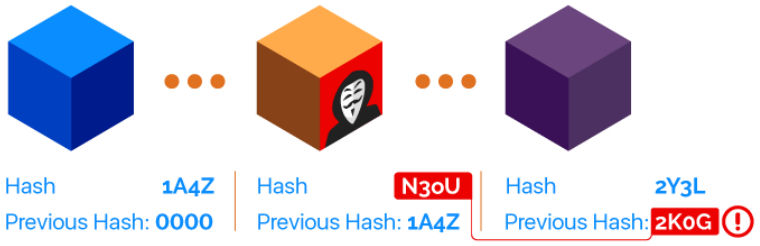

Figure 10: *Example of a tampered blockchain*

This will cause the hash of the block to change as well. This change will make block 3 and all following blocks invalid because they no longer store a valid hash of the previous block. So changing a a single block will make all following blocks invalid.

But using hashes is not enough to prevent tampering. Computers these days are very fast and can calculate hundreds of thousands of hashes per second, this being said, we could tamper with a block, and recalculate all the hashes of the previous blocks to make our blockchain valid again.

To mitigate this, blockchains have something called proof-of-work.

4.2.1. Proof-of-work

Proof-of-work is a mechanism that slows down the creation of new blocks. In Bitcoin's case, it takes about ten minutes to calculate the required proof-of-work and add a new block to the chain. This mechanism makes it very hard to tamper with the blocks, because if we tamper with one block, we will need to recalculate the proof-of-work for all the following blocks.

So, the security of a blockchain comes from its creative use hashing and the proof-of-work mechanism.

But there is one more way that blockchains secure themselves, and that is by being distributed. Instead of using a central entity to manage the chain, blockchains use a P2P network that anyone can join. When someone joins this network, he gets the full copy of the blockchain, the node can use this to verify that everything is still in order.

But what specifically happens when someone creates a new block? That block is sent to everyone on the network, each node then verifies the block, to make sure that it has not been tampered with. If everything checks out, each node adds this block to their own blockchain.

All the nodes in this network create consensus: they agree about what blocks are valid and which are not. Blocks that are tampered with will be rejected by other nodes in the network. This being said, to successfully tamper with a blockchain we would need to tamper with all blocks on the chain, redo the proof-of-work for each block, and take control of more than 50% of the P2P network. Only then our tampered block would be accepted by everyone else. This entire process is almost impossible to do!

4.2.2. Smart contracts

Blockchains are also constantly evolving. One of the most recently developments is the creation of smart contracts.

These contracts are simple programs that are stored on the blockchain and can be used to automatically exchange coins, based on certain conditions.

5. Bitcoin

5.1. What is Bitcoin

As its name suggests, Bitcoin is an electronic currency, but unlike government issued currencies, there is no single entity that issues Bitcoin or is in charge of processing its transactions.

Before Bitcoin, it was not possible to make electronic payments without the help of a third party, like a bank or payment processor. Payments were often slow, expensive, and not available to everyone. To solve those problems, Bitcoin operates without a trusted third party, instead, it works as a P2P electronic currency, meaning that payments are sent directly from one person to another.

That works by simply putting computers all over the world, using mathematical functions to independently verify all Bitcoin transactions, which are then added to a public a blockchain, which we already know it works.

Early on in Bitcoin's history, there are very few transactions being processed by the network, but as time went on, more and more people started using this cryptocurrency, so the number of transactions to be processed went up too. Eventually, the Bitcoin network needed to be updated, to keep transactions fast, cheap, and reliable. But, because there was not consensus on how this update should be performed, or wether it should be implemented at all, Bitcoin ultimately had to split into two separate currencies for that update to happen:

- **Bitcoin Cash (BCH)** - this was the version that implemented the original planned update. Bitcoin Cash can currently process over one hundred transactions per second, with fees reliably less than a 0.01 USD per transaction.
- **Bitcoin (BTC)** - this version made different updates to the network, and kept the original name and symbol. Bitcoin can only process between 3-7 transactions per second, and is now considered by many to be digital gold, instead of digital cash. Its fees have ranged anywhere from several cents to tens of dollars per transaction, depending on the number of people trying to use the network at once.

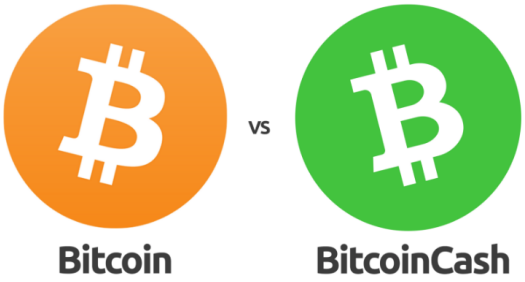

Figure 11: Bitcoin vs Bitcoin Cash

5.2. The Pillars of Bitcoin

The Bitcoin system has seven main pillars that allow the construction of a fair market.

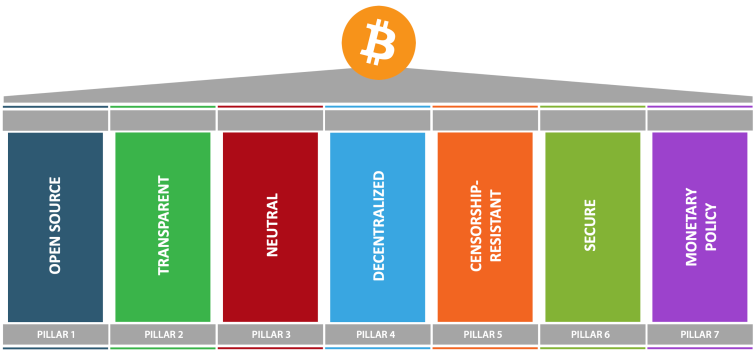

Figure 12: *Pillars of Bitcoin*

5.2.1. Open Source

This will be the first pillar approached. Bitcoin is based on the open source software core. This means that the source code is available to anyone who wants to see how the network works. Not only that, anyone can contribute to it. There is a resemblance with the Linux community. The community that daily keeps improving it is its main strength.

With that in mind, bitcoin will not be replaced by a more powerful technology. As mentioned earlier, its developers will keep improving it, making it evolving alongside the internet. Besides that, its security is an essential point to keep improving. And again, thanks to its developers, it will keep up, allowing bitcoin to continue its dominance in the cryptocurrencies market.

5.2.2. Transparent

As it was explained in the open source topic, bitcoin blockchain is based on open source code and anyone can check it. Besides that, anyone can enter the network, making bitcoin trustless and permissionless. Anyone can verify any transaction made in the network. This allows people to form their own opinion regarding this market. That is why bitcoin is originally based on a simple quote:

Don't trust, verify.

Bitcoin's motto

This is a very important aspect of bitcoin. All users can verify everything by their own, making their decisions a lot easier and allowing them the opportunity to see the impact of every transaction.

5.2.3. Neutral

As this system, capable of revolutionizing the current financial system, is available to literally anyone, the success of bitcoin its every user's responsibility. And by this we mean that the users are the ones who make the difference. So, there isn't really an owner of bitcoin. Everyone has equally the same influence. With this, your transactions are only made by you and no one can have a say in it.

There are many studies that point bitcoin to the U.S dollar's next replacement as the world's reserve currency. They predict the fall of the U.S dollar and the rise of bitcoin, as it is politically neutral.

5.2.4. Decentralized

The whole bitcoin system is decentralized. This means that it is distributed and resistant to potential attacks. Because of this, its up-time is incredibly high: **99.985%**, making it almost unbreakable.

Bitcoin remains the easiest, fastest and most efficient solution to transfer any amount of money across the world. When compared to other solutions, like banks, its transaction fees and taxes are almost insignificant. In addition, the transaction time is also much faster, completing any transaction in 10 minutes. This is usually 300 times faster than any bank transaction.

As you probably go to this, it is pretty obvious that bitcoin allows you to make transactions without the inter bank system making it difficult.

5.2.5. Censorship-Resistant

As we discussed before, bitcoin has always been a democracy in the sense that there is no leader, all users are equally relevant. Each users possesses their own bitcoins as long as they have their private keys, and no one can take that away.

Not your keys, not your Bitcoins.

Bitcoin's rules

Therefore, you have no fear that your bitcoins will be confiscated by any government. This is a major guarantee that you can have by owning bitcoins.

5.2.6. Secure

Bitcoin miners are responsible for validating blocks of transactions by allowing their own computing power to be used by the network. To ensure that these miners run the operation smoothly, they are rewarded by 2 things:

- **Halving - Bitcoin reward every 210,000 blocks issued**
- **Transaction fees**

Currently, this makes bitcoin the most secure network in the entire world.

5.2.7. Monetary Policy

The bitcoin's policy will prevent bitcoin from its vanishment. Unlike the U.S dollar, bitcoin exists in limited amounts, as there will be no more than 21 million BTC[6] in circulation. This ensures users that they always own the same percentage of the world's bitcoins as time goes by.

In addition, the process of creating new bitcoins is always predictable. No one can change it and everyone can know when new bitcoin will be created, as it is not influenced by any human decision.

This makes bitcoin's policy better than the one practiced by the banks. The banks' policies change the money quantity and this is not a problem with bitcoin.

[6] Bitcoins

5.2.8. Media

This one is not a main pillar, its more of a support one. As in almost everything, the press and social media have a huge impact and can almost ”move mountains” and Bitcoin has not overlooked this phenomenon, having had great success and appreciation thanks to it.

It all started on a small forum (at the time), Bitcoin Talk, where Laszlo Hanyecz posted a potential Bitcoin transaction for two Papa John’s pizzas that were bought for 10,000 Bitcoins, worth millions today. This simple social forum transaction has led to bigger things, and thus began the interest of social media and press in Bitcoin.

In fact Bitcoin can attribute much of its growth to social forum Reddit where crypto-enthusiasts to crypto-analysts and even crypto-journalists got the most updated Bitcoin news and stories and had and still have detailed information on everything about Bitcoin. This started the construction of the Trust that today people have in cryptocurrencies with for instance most of the trending cryptocurrency stories that hit other social media networks having origins in Reddit.

A more recent example of this social media impact was when billionaire Elon Musk changed his Twitter bio to include “bitcoin” which made it climb on the market 15%.

Figure 13: Pizza for Bitcoins

5.3. The Bitcoin Protocol

Being a decentralized digital currency, Bitcoin is not something that we can physically own, which in itself generates a large deviation from the concept of money that we are used to and that we use in our day-to-day. To use this digital asset, there are many steps/rules that need to be followed, they make up the Bitcoin protocol.

Bitcoins are not stored centrally nor locally, they exist in a distributed ledger called blockchain. This ledger runs on a P2P network of computers.

Owning a Bitcoin is, nothing more, nothing less than simply having the power to transfer it to someone else, with the transaction being recorded in the blockchain. But how does this work?

This is made possible with the usage of an private key - public key ECDSA[7] pair.

[7] Elliptic Curve Digital Signature Algorithm

5.3.1. ECDSA

ECDSA is a variant of the DSA[8], this uses elliptic curve cryptography. An elliptic curve is mathematically represented by the following equation:

$$y^2 = ax^3 + bx + c$$

In the case of Bitcoin:

$$a = 1$$
$$b = 0$$
$$c = d \, mod \, p$$
$$d = 7$$
$$p = 1.158 \times 10^{77}$$

Replacing the values, we obtain:

$$y^2 = x^3 + 7 \bmod 1.158 \times 10^{77}$$

Finally, this equation can be translated to the following graphic:

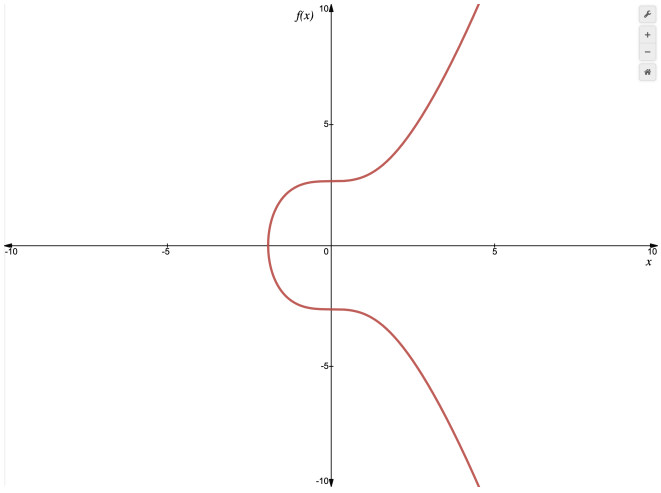

Figure 14: *Kobiltz curve*

The curve on the graph above is called *Kobiltz curve*, and its often referred as *secp256k1*. This curve was created on purpose, and with a very defined objective: to increase efficiency in the generation of public and private keys, making the computation of this key pair 30% faster. But this is not the only thing that differentiates this curve from the rest of the elliptical curves, due to the precision in choosing the values of the constants a, b, c and d, the probability of having an attack in the process in a way that can compromise it is as small as possible.

Elliptic curves have some properties, in this case, for example:

[8]Digital Signature Algorithm

- A non-vertical line that intersects two non-tangent points on the curve will always intersect a third point on the same curve.
- A non-vertical line tangent to the curve at one point will intersect only one other point on the curve.

This properties allow us to define two operations: point addition and point doubling.

5.3.1.1 Point addition

Point addition consists of following this steps:

- Take two points of the elliptic curve, P and Q.
- Pass a line through the previous points.
- Mark the point $(-R)$ from the intersection of the previous line with the curve.
- Mirror $-R$ through the x-axis, obtaining R.

This algorithm can be put into the following expression:

$$P + Q = R$$

With R being the result of the sum of the original points.

Finally, this equation can be translated to the following graphic:

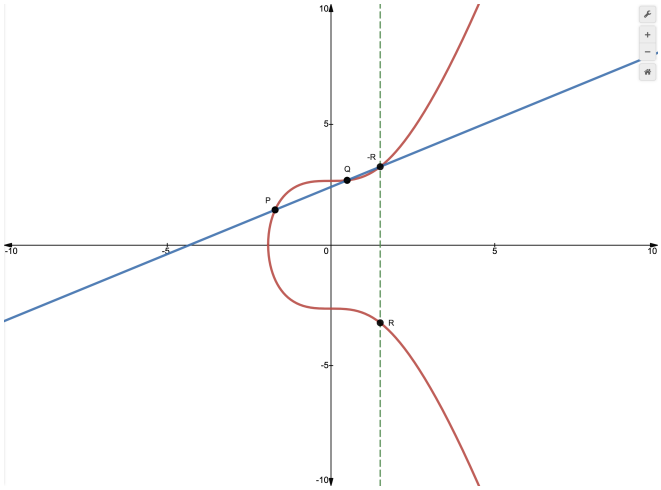

Figure 15: *Point addition*

5.3.1.2 Point doubling

Point doubling consists of following this steps:

- Take a point of the elliptic curve, P.
- Pass a tangent line tangent to P.
- Mark the point $(-R)$ from the intersection of the previous line with the curve.

- Mirror $-R$ through the x-axis, obtaining R.

  This algorithm can be put into the following expression:

$$P + P = 2P = R$$

  With R being the result of the sum of R with itself.

  Finally, this equation can be translated to the following graphic:

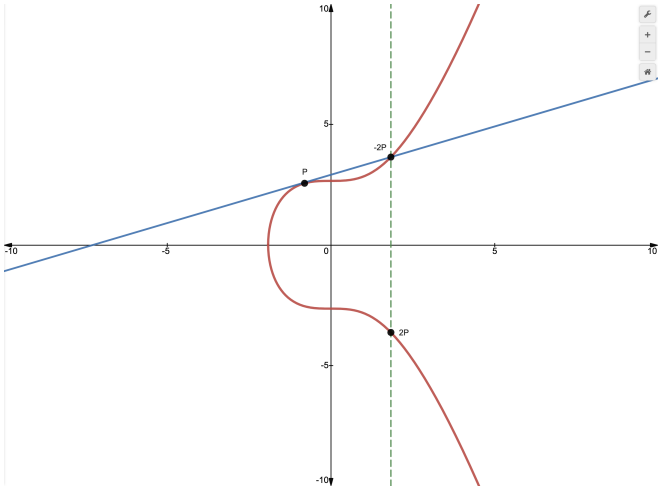

Figure 16: *Point doubling*

5.3.1.3 Scalar multiplication

Point addition and point doubling combined are used for scalar multiplication, this means adding a point to itself n times:

$$R = nP$$

To explain it better, we will use the following example:

$$R = 11P$$

$$R = P + (P + (P + (P + (P + (P + (P + (P + (P + P)))))))))$$

This can be simplified using the previous operations:

$$R = 11P$$

$$R = P + 10P$$

$$R = P + 2(5P)$$

$$R = P + 2(P + 4P)$$

$$R = P + 2(P + 2(2P))$$

As we can see, we just decomposed $11P$ into two point additions and three point doubling. This can be very useful when n is a large number.

One of the uses of scalar multiplication is to calculate the private-public key pair, we will take a look on how it works and where it is placed in the Bitcoin protocol in the section bellow.

5.3.2. Private-Public key pair generation

The private-public key pair is used on Bitcoin transactions between users. This keys can be represented as:

- **Public key** - represents a public Bitcoin address
- **Private key** - personal key, secret and unique to each user.

For generating this pair, we first need a initial point, usually referred as generator point. This point multiplied by the private key will give us the public key:

$$public\ key = generator\ point \times private\ key$$

This is the same as saying that we will add the point to itself as many times as the private key value.

Graphically is easier to understand this. For instance, if we take a point P of the *secp256k1* curve, and we say that the private key is 4, we will add P to itself 4 times, obtaining $4P$, this would be the value of the public key associated with the given private one. The process would result in this graph:

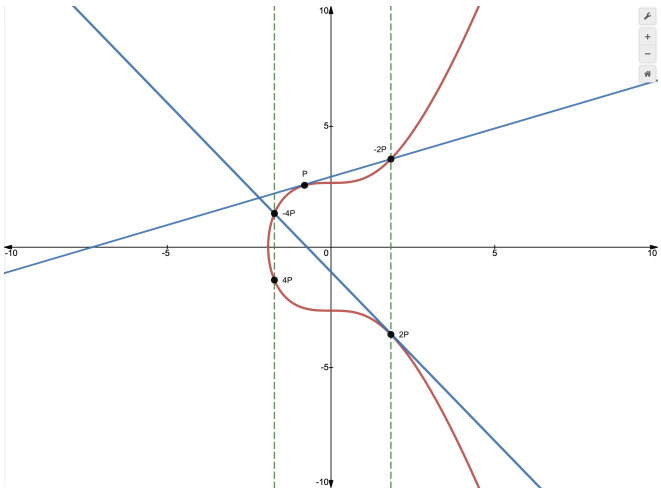

Figure 17: *Process of obtaining $4P$ from the point P, using scalar multiplication*

And this is only for a private key of 4, if the private key is a larger number, there are many more calculations to be made, and many other points created during this process.

As we previously discussed, the curve used for public-private key generation in the case of Bitcoin has a parameter p, that is the prime order. This number, being a large prime number, prevents the points taking decimal numbers, during the scalar multiplication process, making the curve a collection of dots.

On the graph bellow, we can see a ”curve” of finite field with $b = 7$ and $p = 37$:

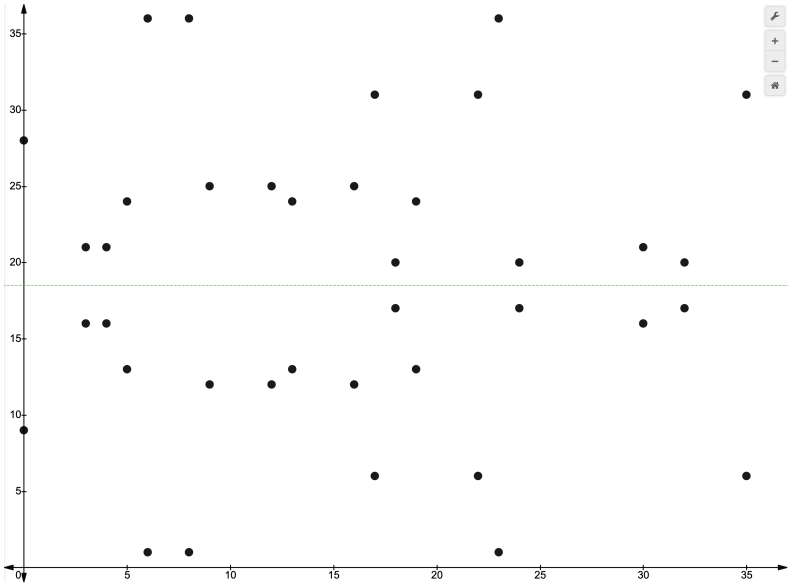

Figure 18: *”Curve” of finite field with prime order 37*

Doing this calculation on today’s computers is rather fast and efficient, but reversing the same operation is very complex. Although deducing the private key from the public key is possible, it would take a huge time to do so, this process would take 2^{128} attempts, meaning that, even with a million CPU[9]s, it would take approximately 260 billion times the age of the universe to break Bitcoin’s elliptic curve cryptography.

Generated the pair, this is now used to encrypt data used on Bitcoin transactions.

6. Socio-Economic Impact of Bitcoin

6.1. Price increases and lack of hardware stock related to “Mining”

GPUs are one of the most important components in a mining Machine as they provide a lot of computational power. GPUs are widely used in many other industries such as the Movie industry, the growing Gaming industry and in the Artificial Intelligence industry. For the mining process to be profitable most miners use more than one GPU on their system (with Warehouses full of them at times) and try to get the more recent versions quickly.

This among other factors creates stock problems in the GPU market as a growing number of miner companies and individual miners take the majority of the stock available and manufacturers can’t keep up with the demand and retailers take advantage and raise the prices as much as three times more than the recommended. (Source: VideoCardz)

A side effect of this stock problem is the big impact on the second hand GPU market. With no stock available miners turn to this market and buy everything they can as a Second GPU, performance is pretty much the same as a brand new one and their slightly reduced life span is not a problem because the goal is

[9]Central Processing Unit

always getting the more recent GPU with better performance. Noticing this behavior, second hand sellers took advantage and started to increase prices to a point where some depending on the GPU model that they were selling would put prices above the retail price.

This made it almost impossible for a normal consumer to get a brand new or used GPU.

In an attempt to correct the situation Manufacturers took some actions. NVIDIA, one of the biggest manufacturers of GPUs, decided to create a dedicated line of GPUs optimized for Professional Mining, the NVIDIA CMP HX. Another critical action taken by NVIDIA to make miners go with the new line optimized for mining was reducing the mining performance of new GPUs produced on the Geforce line, (a line dedicated to Gaming but very appreciated by miners), by reducing the hash rate.

The effects of these actions in the market is yet to be felt at the time of writing, but many have already criticized NVIDIA because the manufacturer will focus more resources on the professional Mining line of GPUs taking advantage of the growth of mining investors leaving aside the remaining lines and because this new line of GPUs will have basically no resale value, the GPUs are going to be very disposable and with very little to recycle in this product the environmental impact will increase.

6.2. Monetary System

For the time being the impact of Bitcoin on the Monetary systems is close to none as the market capitalisation (814.7 billion U.S. dollars around May 2021) is still small compared with the Market capitalisation of the banking market worldwide (8.9 trillion dollars around the first Q1 of 2021).

To put in another perspective some Central Banks are experimenting with a type of cryptocurrency, but none of the Central Banks plan to use a blockchain based version in their projects, because it was deemed still not mature and stable enough for the infrastructure of national currency to rely on. As Bitcoin relies on blockchain this makes it not suitable and so it does not have a direct impact on the future plans of the Monetary system, because although it does have some big advantages like controlling fraud and maintaining privacy, there are still many cracks that create highways to commit tax evasion or criminal activities.

6.3. Energy Expenditure

The mining process of Bitcoin requires machines with a lot of processor power so, consequently, a large energy expenditure is necessary to support the hardware involved in the process like GPUs, which despite major advances in its electrical efficiency still have a significant energy expenditure. Besides energy consumed by more and more machines, individuals and companies with many mining systems or even entire warehouses full of mining systems are investing heavily in refrigeration systems to improve performances and keep the machines constantly working. The energy dispensed in the Mining Process of Bitcoin is commonly known as Bitcoin Energy Consumption and with the growth of the Bitcoin Network this value will consequently increase with time, even with more efficient mining hardware in the future.

If Bitcoin was a country, it would be in the Top 30 energy users worldwide in 2019, according to an analysis made by University of Cambridge. Bitcoin Energy Consumption in 2019 was around 144.28 TWh[10], a value above many developed countries like, Sweden with 131.798 TWh, Netherlands with 110.682 TWh or Portugal with 48.0351 TWh.

[10] Terawatt-hour

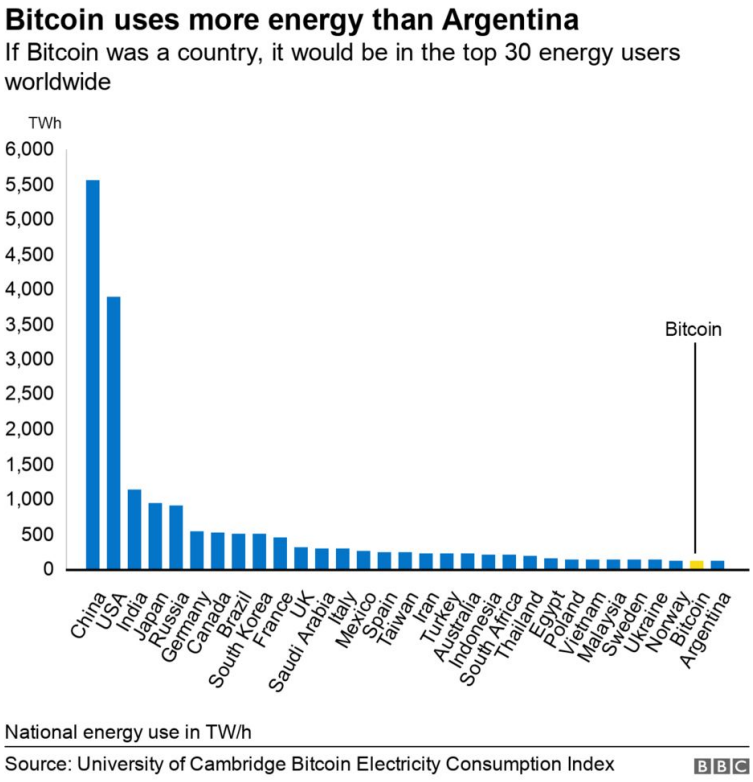

Figure 19: Bitcoin's electricity consumption

In order to get the following results University of Cambridge used a Best-Guess estimate of Bitcoin's electricity consumption. The method assumes that all miners use an equally-weighted group of hardware types that are profitable in electricity terms, assuming the PUE[11] of 1.10. So the Best Guess Power Consumption is calculated by multiplying the average energy efficiency of profitable hardware, with the hashrate, with the PUE with the electricity cost per joule (Pel):

$$E_{estimated}(P_{el}) = \frac{\sum_{i=1}^{N} \vartheta i}{N} * H * PUE * 3.16 * 10^{7}$$

with

$E_{estimated}$ – best guess power consumption (W)

$\frac{\sum_{i=1}^{N} \vartheta i}{N}$ – average energy efficiency of profitable hardware (J/h)

H – hashrate (h/s)

PUE – power usage effectiveness

P_{el} – electricity cost per joule (USD/J)

[11] power usage effectiveness

The Energy Efficiency of Profitable Hardware, in other words, the Profitability Threshold is calculated by dividing the electricity cost per joule by the mining revenue per hash:

$$\theta = \frac{SRev}{P_{el}}$$

with

θ – profitability threshold (J/h)

$SRev$ – mining revenue per hash (USD/h)

P_{el} – electricity cost per joule (USD/J)

This high value of energy consumption comes with many side effects. A Bitcoin Mining Map from September 2019 to April 2020 created by the University of Cambridge based on geolocation data (i.e. IP addresses) of "hashers" connecting to the Bitcoin mining pools BTC.com, Poolin, and ViaBTC, indicates that from September 2019 to April 2020 roughly 71,70% of Bitcoin mining was done in China.

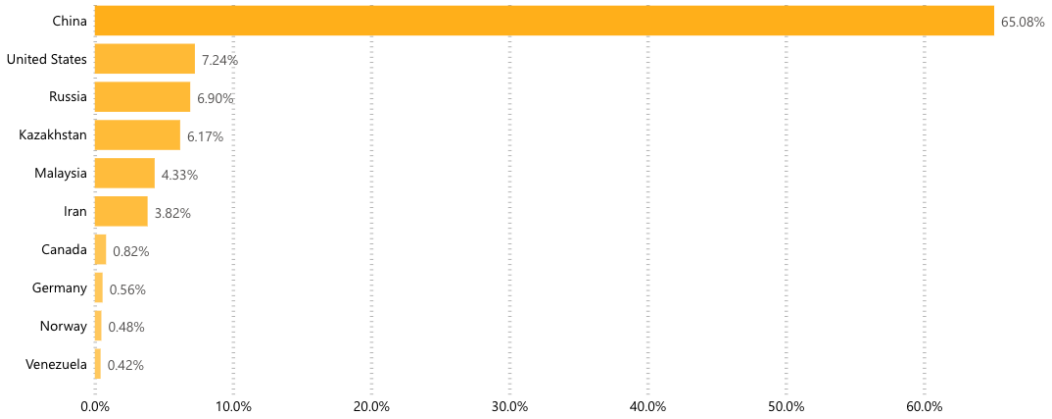

Figure 20: Average monthly share of total hashrate

This fact is important, because it means that the Bitcoin Network depends heavily on coal-based power that produces some of the worst emissions, which increases Bitcoin's carbon footprint. Many studies have approached this situation with one study indicating that growth in bitcoin mining alone could result in a 2 degree Celsius increase in global temperatures, although many say such estimates are inflated as miners increasingly go to sources of cheap renewable energy, like hydropower and another study says that bitcoin's mining carbon footprint in China can threaten its climate change targets.

These discoveries and studies recently made a big negative impact on Bitcoin's reputation as people increasingly understand the effects of climate change and prefer solutions based mostly in green energy to those who don't. This also led to a statement, on 12 of may, from Tesla's CEO Elon Musk informing that Tesla has suspended vehicle purchases using Bitcoin because of the concerns regarding the rapidly increasing use of fossil fuels for Bitcoin mining and transactions, especially coal. Although believing and trusting the Bitcoin concept, investing in it would go against Tesla's mission to accelerate the world's transition to sustainable energy. (Source: https://twitter.com/elonmusk/status/1392602041025843203)

This means that controlling the energy expenditure and transitioning to sustainable energy are some of the challenges for Bitcoin in the next few years.

6.4. Political implications

Virtually everything can be used politically and Bitcoin is no exception. Some governments consider Bitcoin a menace because it doesn't have a central authority and that can destabilize or undermine the authority or control of central banks or even from the government itself. Bitcoin anonymity can be used to circumvent capital controls, for money laundering or illegal purchases, and Bitcoin it's still too risky for many investors, with for example Bitcoin being recently connected to the US Capitol attack where a Large bitcoin payment was made to far-right individuals before the attack.

For that many politicians point out many of the problems surrounding Bitcoin like its energy expenditure, to disrupt people's trust in the cryptocurrency. Other politicians take a different route and prefer to elaborate taxes surrounding Bitcoin gains and transfers to discourage some investors and at same time gain money on taxes, Portugal for example can still be considered a fiscal paradise regarding Bitcoin gains, but many are already proposing taxes and regulation.

Despite this government distrust of Bitcoin and in general from cryptocurrencies, many consider that different cryptocurrencies have different supports with many indicating that Bitcoin is supported by more right-wing and extremist right-wing individuals as explored in the book "The Politics of Bitcoin: Software as Right-wing Extremism", by David Golumbia, while the rival Ethereum is supported by more left wing and extremist left-wing individuals as shown in a survey conducted by CoinDesk with 1200 cryptocurrency users in 2018, found out that 55% of "Ethereans" tended left ideologies, while 55% of "Bitcoiners" tended Right ideologies.

7. Conclusion

From the analysis and discussion of cryptocurrencies, more specifically Bitcoin, we can infer that, thanks to the advanced technologies and processes that it uses as Blockchain, that allows Bitcoin and most cryptocurrencies to have characteristics very appreciated and valued nowadays, that shows potential to compete with the current monetary system, and in this way, the same already manages to have a sufficient level of support and trust from people in a way that we can't ignore it anymore and proof of that are the socio-economic effects caused by Bitcoin that are reflected by the whole population regardless of whether or not persons have a direct connection with Bitcoin or with any cryptocurrency.

Despite these levels of trust and support Bitcoin still needs to solve many of its problems, some derived from its special characteristics to have a real, effective, and strong impact on the current monetary system.

References

[1] Zeenat Ali. *Explaining the Math Behind Blockchain Algorithms*. [Accessed 29/04/2021]. URL: https://medium.com/dataseries/explaining-the-math-behind-blockchain-algorithms-98d06e06c2e3.

[2] Richard G. Anderson. "Money and Velocity During Financial Crises: From the Great Depression to the Great Recession". In: (2014). DOI: https://www.frbsf.org/economic-research/files/S04_P1_JohnVDuca.pdf.

[3] Tara Annison. *The Maths Behind the Bitcoin Blockchain*. [Accessed 30/04/2021]. URL: https://www.linkedin.com/pulse/maths-behind-bitcoin-blockchain-tara-annison/.

[4] BBC. *Guide: What is Bitcoin and how does it work?* [Accessed 29/04/2021]. URL: https://www.bbc.co.uk/newsround/25622442.

[5] BitDegree. *What is Cryptocurrency: Your Complete Crypto ABC*. [Accessed 16/05/2021]. URL: https://www.bitdegree.org/crypto/tutorials/what-is-cryptocurrency.

[6] BoyceWire. *Deflation Definition*. [Accessed 16/05/2021]. URL: https://boycewire.com/deflation-definition-causes-and-effects/.

[7] BoyceWire. *Fiat Money Definition*. [Accessed 16/05/2021]. URL: https://boycewire.com/fiat-money-definition/.

[8] BoyceWire. *Fiat Money Definition*. [Accessed 16/05/2021]. URL: https://boycewire.com/fiat-money-definition/.

[9] BoyceWire. *What is Inflation*. [Accessed 16/05/2021]. URL: https://boycewire.com/what-is-inflation/.

[10] Toby Chitty. *The Mathematics of Bitcoin — The Blockchain*. [Accessed 29/04/2021]. URL: https://medium.com/swlh/the-mathematics-of-bitcoin-89e7ab59edc.

[11] CryptoCompare. *Explaining the Math Behind Blockchain Algorithms*. [Accessed 30/04/2021]. URL: https://www.cryptocompare.com/wallets/guides/what-is-elliptic-curve-cryptography/.

[12] Ricardo Perez-Marco Cyril Grunspan. *The Mathematics Behind Bitcoin*. [Accessed 28/04/2021]. URL: https://webusers.imj-prg.fr/~ricardo.perez-marco/blockchain/BitcoinP7.pdf.

[13] DIVERSYFUND. *Types of Money: from Commodities to Cryptocurrencies*. [Accessed 16/05/2021]. URL: https://diversyfund.com/blog/types-of-money-from-commodities-to-cryptocurrencies/?utm_source=www.google.com%5C%2F.

[14] Higher Rock Education. *Representative Money*. [Accessed 16/05/2021]. URL: https://www.higherrockeducation.org/glossary-of-terms/representative-money.

[15] Euromoney. *What is blockchain?* [Accessed 16/05/2021]. URL: https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain.

[16] The Motley Fool. *Cryptocurrencies Explained, in Plain English*. [Accessed 16/05/2021]. URL: https://www.fool.com/investing/2018/01/02/cryptocurrencies-explained-in-plain-english.aspx.

[17] The Motley Fool. *What Is Cryptocurrency?* [Accessed 16/05/2021]. URL: https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/guide-to-cryptocurrencies/.

[18] Forbes. *What Is Cryptocurrency?* [Accessed 16/05/2021]. URL: https://www.forbes.com/advisor/investing/what-is-cryptocurrency/.

[19] IBM. *What is blockchain technology?* [Accessed 16/05/2021]. URL: https://www.ibm.com/topics/what-is-blockchain.

[20] IBM. *What is blockchain technology?* [Accessed 16/05/2021]. URL: https://www.ibm.com/topics/what-is-blockchain.

[21] Investopedia. *Bitcoin*. [Accessed 29/04/2021]. URL: https://www.investopedia.com/terms/b/bitcoin.asp.

[22] Investopedia. *Bitcoin*. [Accessed 29/04/2021]. URL: https://www.investopedia.com/terms/b/bitcoin.asp.

[23] Investopedia. *Bitcoin Mining*. [Accessed 16/05/2021]. URL: https://www.investopedia.com/terms/b/bitcoin-mining.asp.
[24] Investopedia. *Blockchain Explained*. [Accessed 16/05/2021]. URL: https://www.investopedia.com/terms/b/blockchain.asp.
[25] Investopedia. *Cryptocurrency*. [Accessed 16/05/2021]. URL: https://www.investopedia.com/terms/c/cryptocurrency.asp.
[26] Investopedia. *Fiat vs. Representative Money: What's the Difference?* [Accessed 16/05/2021]. URL: https://www.investopedia.com/ask/answers/041615/what-difference-between-fiat-money-and-representative-money.asp.
[27] Investopedia. *How Does Bitcoin Mining Work?* [Accessed 16/05/2021]. URL: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/.
[28] Investopedia. *Money*. [Accessed 16/05/2021]. URL: https://www.investopedia.com/terms/m/money.asp.
[29] Kaspersky. *What is Cryptocurrency? Cryptocurrency Security: 4 Tips to Safely Invest in Cryptocurrency*. [Accessed 16/05/2021]. URL: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency.
[30] Hans Knutson. *What is the math behind elliptic curve cryptography?* [Accessed 29/04/2021]. URL: https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3.
[31] James McCumiskey. *WHAT IS MONEY*. [Accessed 16/05/2021]. URL: https://positivemoney.org/2011/05/what-is-money/.
[32] CNN Money. *What is bitcoin?* [Accessed 29/04/2021]. URL: https://money.cnn.com/infographic/technology/what-is-bitcoin/index.html.
[33] Positive Money. *WHAT IS MONEY*. [Accessed 16/05/2021]. URL: https://positivemoney.org/2011/05/what-is-money/.
[34] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: (2008). DOI: https://bitcoin.org/bitcoin.pdf.
[35] nerdwallet. *Bitcoin, Explained for Beginners*. [Accessed 29/04/2021]. URL: https://www.nerdwallet.com/article/investing/what-is-bitcoin.
[36] nerdwallet. *What Is Cryptocurrency? Here's What You Should Know*. [Accessed 16/05/2021]. URL: https://www.nerdwallet.com/article/investing/cryptocurrency-7-things-to-know.
[37] Alberto Pace. *Mathematics, Cryptography, Blockchains, and Cryptocurrencies: Myths and Realities*. [Accessed 28/04/2021]. URL: https://indico.cern.ch/event/848910/attachments/1918060/3183443/2019-10-10-KT-Seminar-Crypto-Blockchain-V09-Publishing.pdf.
[38] Eric Rykwalder. *The Mathematics of Bitcoin — The Blockchain*. [Accessed 29/04/2021]. URL: https://www.coindesk.com/math-behind-bitcoin.
[39] Sylvain Saurel. *The Seven Pillars of Bitcoin*. [Accessed 01/05/2021]. URL: https://www.inbitcoinwetrust.net/the-seven-pillars-of-bitcoin-d12056280c54.
[40] Kevin Werbach. *The History of Bitcoin in One Chart (And it Says Nothing About Prices!)* [Accessed 29/04/2021]. URL: https://medium.com/@kwerb/the-history-of-bitcoin-in-one-chart-and-it-says-nothing-about-prices-33575c337f37.