eman ta zabal zazu

Universidad del País Vasco Euskal Herriko Unibertsitatea

COULD THE BLOCKCHAIN BE THE FUTURE OF TECHNOLOGY?

Patricia Bernal Villaluenga

Tutor: Francisco Jaime Ibáñez Hernández

UPV/EHU
Grado en Administración y Dirección de Empresas
Facultad de Economía y Empresa. Sección Álava
2022/2023

A mis padres, por quererme como lo hacen y por no cesar nunca en su esfuerzo de darme la mejor educación. A mis abuelos, que han sido una parte importante de mi desarrollo, y siempre se han sentido orgullosos de cada logro. A mi familia por creer en mí a cada paso del camino. A mis compañeros, que han sido mi red de seguridad tanto dentro como fuera de la facultad. A Moha, por estar a mi lado estos cuatro años, dándome ánimos cuando no tenía fuerzas para seguir, alentándome para mejorar y ser la mejor versión de mí misma. Y especialmente a Laida, que tiene muchos años de estudio por delante y mucho por aprender, para enseñarle que el recorrido académico no lo es todo, para que nunca pierda su buen corazón y trate siempre de perseguir su propia felicidad.

INDEX

Table index

Graph index

Figure index

Image index

RESUMEN

Desde la creación de Bitcoin en 2008, la primera moneda virtual, las criptomonedas y el blockchain, tecnología que sostiene todo el sistema que rodea a las mismas, han sido un tema en boca de todos; y a pesar de que las criptomonedas han acaparado toda la atención, lo que realmente pretende ser el foco de atención de este trabajo es la tecnología tras él: el blockchain. Dicha tecnología es lo que hace posible el funcionamiento del sistema de forma descentralizada y permitiendo transacciones entre iguales (P2P) sin necesidad de ninguna autoridad central que regule todos los procesos. Gracias a esta tecnología se han podido desarrollar incontables herramientas que pretenden facilitar y automatizar muchos procesos que sin ella serían más costosos, además de crear nuevos modelos de negocio que sin esta tecnología no serían viables.

El objetivo principal del presente trabajo será analizar la viabilidad de la tecnología blockchain y el potencial de las aplicaciones y diferentes usos que se le están dando a la misma, más allá del "boom" de las monedas virtuales, de las cuales también se analizara su posible recorrido. Para llegar a este análisis también se deberá exponer el concepto de blockchain, analizando su definición, historia y estructura, así como los conceptos más importantes que la rodea. Posteriormente se procederá a analizar las plataformas que se han ido creando gracias a esta tecnología. A continuación, se tratarán las diferentes herramientas que se han desarrollado: criptomonedas, Smart contracts, NTFs…; y, por último, analizar los usos que hasta ahora se les han ido dando a las mencionadas aplicaciones en los diferentes sectores y se tratarán de predecir posibles usos en el futuro más próximo.

ABSTRACT

Since the creation of Bitcoin in 2008, the first virtual currency, cryptocurrencies and blockchain, the technology that supports the entire system surrounding them, have been a hot topic; and despite cryptocurrencies have grabbed all the attention, what is really meant to be the focus of this work is the technology behind it: the blockchain. This technology makes it possible for the system to operate in a decentralized manner and allows peer-to-peer transactions without the need for a central authority to regulate all processes. Thanks to this technology, countless tools have been developed that aim to simplify and automate many processes that would be more expensive without it, and also create new business models that would not be feasible without this technology.

The main objective of this work will be to analyse the viability of the blockchain technology and the potential of the applications and different uses that are being given to it, beyond the "boom" of virtual currencies, of which their possible path will also be analysed. To reach this analysis, the concept of blockchain must also be exposed, analysing its definition, history, and structure, as well as the most important concepts that surround it. Subsequently, the platforms that have been created thanks to this technology will be analysed. Then, the different tools that have been developed: cryptocurrencies, Smart contracts, NFTs... will be treated; and finally, the uses that have been given to the aforementioned applications in different sectors will be analysed and possible uses in the nearest future will be predicted.

KEY WORDS

- **Blockchain:** “Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. (…). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.” (IBM, n. d.)
- **Consensus Algorithm:** Mechanism through which a blockchain network reaches consensus. Decentralized blockchains are distributed systems and, because they do not depend on a central authority, their nodes need to agree on the validity of transactions. They are responsible for maintaining the integrity and security of the systems.
- **Crypto assets:** A crypto asset is a digital asset that relies primarily on cryptography and blockchain or similar technology; that is not issued by a public authority or central bank and that can be used as a means of exchange, for investment purposes or to access a product or service under certain conditions.
- **Cryptocurrency:** “A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.” (*Virtual Currency, Cryptocurrency, and Digital Assets Primer*, n. d.)
- **dApp:** Stands for Decentralized Applications, applications that run distributed, hosted on a blockchain.
- **Distributed ledger technology (DLT):** a type of digital decentralised database that is used to record and manage transactions across a network of computers with greater transparency. Blockchain is a type of DLT.
- **Mining:** Is the process of validating and adding transaction records to a public ledger, called a blockchain, and releasing new units of a particular cryptocurrency. Miners are responsible for verifying transactions and ensuring that they are valid, as well as for adding new transactions to the blockchain.
- **Node:** “A piece of equipment, such as a computer that is attached to a network.” (Oxford Dictionary, n. d.)
- **Peer-to-peer (P2P):** Also known as user-to-user. It refers to systems that work as a collective organization, allowing everyone to interact directly with others.

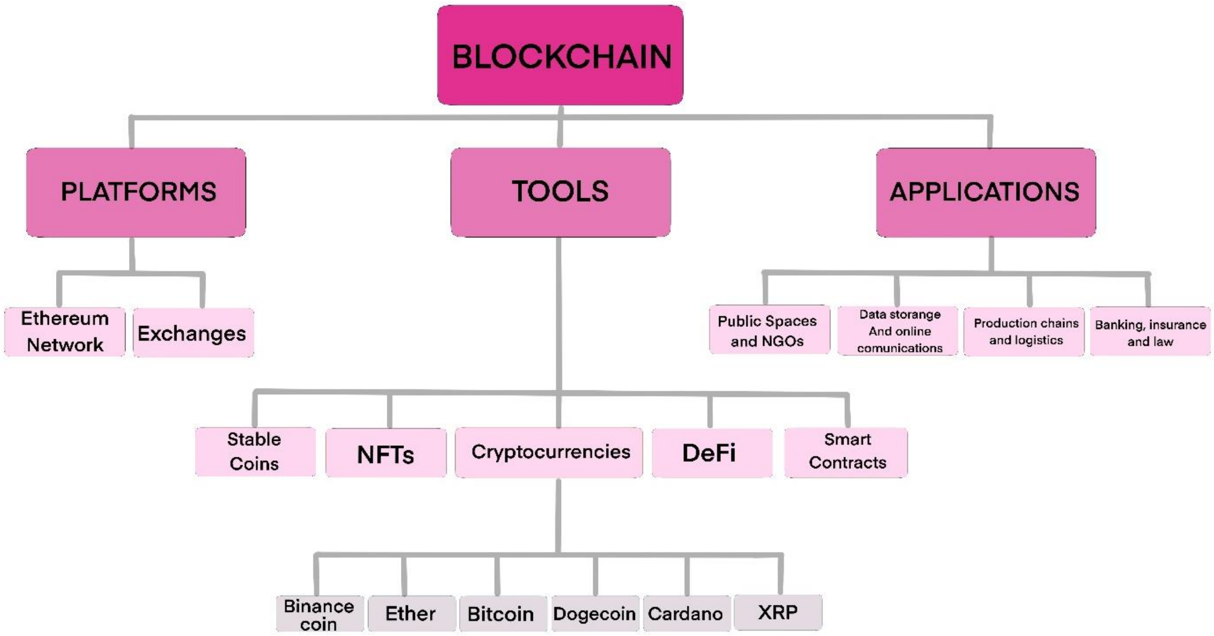
INTRODUCTION

The topic of blockchain technology has been chosen to develop this work because personally In my opinion it has countless benefits to bring to our society, both in personal and business areas, which can bring privacy and transparency to our lives at the same time and speed up many processes through automation. From the first day the topic caught my attention as I started thinking in how many applications it could have and how it could change so many people's lives. That is why I considered it appropriate to evaluate its feasibility and possible development.

The blockchain technology is the key to all the concepts developed in this paper; it is what makes everything possible. The blockchain technology is the system that allows the registration and validation of every operation. It could be used in nearly every situation of daily life, not only regarding cryptocurrencies, but also in smart contracts, logistics… It is based on decentralised networks, so that every participant node could operate and make decisions individually, instead of having a central server or intermediate as we are used to, in order to regulate the flow of transactions. These nets are called peer-to-peer (P2P), which means that they operate as equals, so that are the users the ones that assume the role of "managers" and behave as a collective organisation, allowing each user to interact directly with any user in the network. To comprehend blockchain, it can be compared to an account book, where the registers (the blocks) are coded and weaved together for the security and privacy of the transactions. The requirement is the existence of a number of users (nodes) in charge of verifying and validating those transactions so that the block could be registered in the "account book".

The next figure is intended to show graphically the subjects that are going to be explained in this paper. It can be seen how everything revolves around blockchain technology.

Figure 1: Paper's structure



Source: own elaboration.

The main objective of the work to be conducted will be to analyse the feasibility of blockchain and the potential of possible applications of the same technology. To be able to meet the objective that is presented to us, certain previous steps and concepts will have to be explained. This will develop the interest of some secondary objectives, which also will help giving structure to the work we have in hand.

- To begin, we aim to thoroughly analyse the concept of blockchain, with the goal of extracting the unique characteristics that have the potential to be incredibly useful in the future.
- Next, we will delve into the platforms and chains that support this technology, trying to determine which ones are the most relevant and why, reviewing its evolution and development, commenting also which ones are the most used nowadays and in which platforms or chains can be hosted.
- Then, our goal will be to analyse the tools that have been developed thanks to this technology in the past years.
- Finally, and in an effort to follow the thread of the previous objective, we will evaluate the applications of these tools in different sectors, evaluating the possibilities they offer, with advantages and disadvantages, as well as possible new business models. Along with these applications it will be studied the viability of cryptocurrencies.

Through all the previous sub-objectives, we will try to solve, with the information and knowledge provided, if blockchain truly has a place in our society or if it is just a passing trend or a useless technology without a future.

In order to reach the mentioned objectives, it will be used the bibliographic search, not only online thanks to tools such as Google Scholar but also by consulting physical books, online academies, official web pages or YouTube videos. The numerical values or currency exchange rates will be obtained from platforms such as ProRealTime, Investing.com, Google Finance or Yahoo Finance.

CHAPTER I: BLOCKCHAIN AND DECENTRALISED NETWORKS

1.1 HOW DOES BLOCKCHAIN TECHNOLOGY WORK

Blockchain technology has just been briefly explained in the previous introduction, but in the next paragraphs the subject will be developed thoroughly. The blockchain technology and decentralised networks are the ones responsible of holding a large variety of technologies, tools and platforms, such as smart contracts, NFTs and cryptocurrencies.

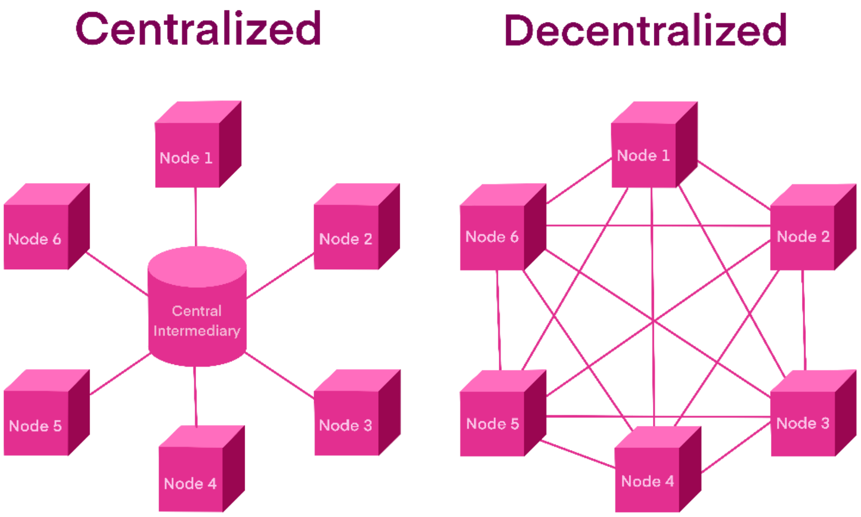
In our daily lives we are used to centralised networks, which are the ones with a central server coordinating all the processing of the network, and every transaction must get through this server, which impulses everything going on. With centralised networks, if there is a problem in the central node, the entire system can fail, as it has been seen on some occasions with social media, when a failure in the central server leaves all the users uncommunicated. In centralised networks there is not only a central figure but also there are intermediaries, who can confirm, censure, or revert transactions and share confidential information. In some cases, especially when talking about financial or banking services, they can decide who has or does not have access to them. (Ethereum.org, n. d.-e)

On the other hand, decentralized networks are not controlled by any single authority or central entity; instead, they are made up of a network of participant nodes, which are run by individual users or organizations and manage all the data processing and supervising as equals, this means that they are connected to each other in a peer-to-peer fashion. Even though nowadays decentralised networks are not as common as ones, decentralised ones were not born with cryptocurrencies and are not new in our daily lives, this is the case of, for example BitTorrent, in which the downloaded file indicates where, in other users' computers it can be found the pieces of the wanted file. At the same time, there are other users connected to your computer to download the parts they need for their own files. In this way the users interact without a central figure to intercede between them who organises all the transactions, they interact as equals, creating a P2P network, which is the basis for blockchain technology and therefore every cryptocurrency. In this way, as a file is uploaded in a lot of different nodes, it is nearly impossible to delete a file from the network or ever trace it.

In the previous paragraphs the concept of node has been mentioned several times; a node "in computer science, is usually a virtual or physical connecting point where all kind of data or information can be created, sent and received. In blockchain technology, nodes are built up of all the computers that are interconnected to a coin's network executing the software in charge of the functioning." (Academy, B., 2022a) A node can be either a personal computer or a supercomputer, but all the nodes must have the same software in order for them to communicate. In these networks, the nodes operate as equals, this is, peer-to-peer (P2P), without a central server managing all the information. When Bitcoin was born, which will be developed in Chapter V, Satoshi Nakamoto created what he named "a peer-to-peer electronic cash system," which was a proposition of a decentralised system that aimed to substitute the whole financial system. In the case of digital currencies, each node stores the information of the transactions that have been made, which are the coin itself. Whenever a transaction is made, the information must be shared with all the participant nodes, which means that when talking about any virtual currency we are really talking about the information about how all the users are transferring from one another, therefore this register is the coin itself.

Decentralized networks have several key advantages over centralized networks. They are more resilient and less susceptible to failure because there is no single point of failure in the network. They are also more secure, because there is no central authority that can be targeted by attackers. Decentralized networks are used in a wide range of applications, including cryptocurrency, peer-to-peer file sharing, and distributed computing. They are based on blockchain technology, which allows for the creation of a decentralized, transparent, and secure ledger of transactions.

Image 1: centralized VS. decentralised networks.



Source: Li, P. & Nelson, S. D (2018)

In 1990 the University of California, Santa Barbara held a *"Conference on the Theory and Application of Cryptography",* and the subjects were gathered in Menezes and Vanstone (1991, p. 437-453). In such conference the cryptographers Stuart Haber and W. Scott Stornetta developed a secure block system for storing documents while looking for a practical solution for "time-stamping digital documents so that they could not be backdated or tampered with." With the addition of Merkle Trees to the project in 1992, they were able to gather multiple documents into one block, also gathering information from the previous block in the next one. Despite the multiple applications that blockchain technology has today, the patent expired in 2004 due to disuse. It was in that same year, when the cryptographer Hal Finney, who also participated in the early stages of Bitcoin, created Reusable Proof-of-Work (RPoW) a system that "worked by receiving a non-exchangeable or a non-fungible Hash cash based proof of work token in return"; this solved the double-spending problem[1]. (Javapoint.com, n. d.)

A blockchain is a decentralized distributed ledger that records transactions on multiple computers. This allows for the creation of a tamper-evident record of transactions that is transparent, secure, and efficient. It is made up of a series of blocks, each of which contains a timestamp and a link to the previous block which creates a chain of blocks, hence the name "blockchain." Each block on the chain contains a record of one or more transactions, and once a block is added to the chain, the data in it cannot be altered or deleted without having to repeat all the following nodes already shared with the other users. From a technical point of view, it is a global network of computers that manages a huge database. Blockchains are typically managed by a peer-to-peer network, which allows for the distributed nature of the technology. Each participant in the network has a copy of the blockchain, and the network must reach consensus on the state of the ledger before a transaction can be added to the chain; this ensures that the ledger is accurate and secure. Blockchains are used in a wide range of applications, in supply chain management, voting systems, and other applications that require a secure and transparent record of transactions; they also are the underlying technology for cryptocurrencies like Bitcoin and Ethereum.

[1] Chapter V

According to Preukschat et al. (2017 p. 15), blockchain technology is "a database that is distributed among different participants, cryptographically protected and organized in blocks of transactions related to each other mathematically." The author argues that given the characteristics of this technology, it has the potential to transform multiple industries. The basis of a decentralised networks is the consensus that allows every participant to trust the information in the chain, along with the fact that each and every participant operates as equals without a central figure in charge of managing and supervising every transaction made.

One of the biggest problems to solve when operating in a decentralised network is the “double spending problem”, if every transaction does not go by the same central figure, and every node does not have the same information at the same time, how can be verified that a user has not spent the same money twice? When a transaction is made, the information needs to pass along the network in order for each node to have its accounting updated, but this takes time, so probably the order of the operations will be different in the different nodes, so how could the transactions be verified? (Dot CSV, 2021) This process is very easily understood using digital currencies as an example. In order to fully understand this process, we will try to explain step by step an operation. When the user makes the transaction, which can be a sale of a good, another currency, an exchange..., that transaction is recorded and entered into a block. It is possible that not all participating nodes have the same operations or that they are not registered in the same order; this is why they must reach a consensus on which is the valid block that will be introduced into the chain. Depending on the network or chain, the consensus mechanism will variate. The different mechanisms for reaching this consensus are explained below.

- Proof of Work (PoW)

Proof-of-Work (PoW) is a consensus mechanism used to validate transactions and secure the blockchain. In a PoW system, miners compete to solve complex a computationally intensive puzzle in order to add new blocks to the blockchain and receive a reward for their efforts. This problem is known as a "hash puzzle", is difficult to compute but easy to verify, and the solution to the puzzle is a unique string of characters, known as a "hash," that meets certain requirements. Once the miner finds a solution, they can create a new block and add it to the blockchain. The difficulty of the hash puzzle is adjusted periodically to ensure that blocks are added to the blockchain at a consistent rate. This process helps to ensure the security of the network and makes it more difficult for attackers to manipulate the blockchain. This consensus algorithm is the one used in Bitcoin.

The idea behind Proof-of-Work algorithm is to make it difficult and resource-intensive to add new blocks to the blockchain, which helps to prevent malicious actors from tampering with the network. The difficulty of the mathematical problems that miners need to solve is adjusted over time to ensure that new blocks are added to the blockchain at a steady rate. "The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains." (Nakamoto, 2008)

There is a quite important disadvantage of this algorithm: the high electrical consumption. This is a problem not only for the miners that must face remarkably excessive cost but also environmentally speaking it is very polluting.

To summarize, the proof-of-work algorithm is an important part of many cryptocurrency systems, as it helps to ensure the security and integrity of the network. By requiring miners to perform a certain amount of work to add new blocks to the blockchain, such algorithm helps to prevent attacks and maintain the trust of users in the network.

- Proof of Stake (PoS)

Proof-of-Stake (PoS) is an alternative algorithm to Proof-of-Work (PoW) used as this one to validate transactions and secure the blockchain. Proof-of-stake (PoS) allows users to "stake" their coins by holding them in a wallet and using them to validate transactions. The idea behind PoS is that users who hold a large number of coins are more likely to act in the best interests of the network, as they have a financial incentive to maintain the value of their holdings. This means that the proof-of-stake (PoS), unlike proof-of-work, does not require significant amounts of computational power to secure the blockchain. According Vitalik Buterin[2], "to implement a proof-of-stake system, we require each node to have a weight, proportional to the number of coins it is staking. When a node finds a new block, it must choose the previous block in the chain that it thinks is the most difficult to modify and include a set of transactions in the new block that are difficult to modify without invalidating the new block." (Buterin, V. 2013).

In the mentioned Ethereum whitepaper, Buterin describes how the PoS algorithm works and how it is used to secure the Ethereum network. PoS is an important part of many cryptocurrency systems, as it provides an alternative to PoW that is more energy-efficient and environmentally friendly. By allowing users to stake their coins in order to validate transactions, PoS helps to secure the blockchain and maintain the trust of users in the network. Even though Ethereum was originally created based on a PoW algorithm, it changed to a Proof-of-stake one for climatic reasons in the larger update of the platform till the date.

- Delegated Byzantine Fault Tolerance (dBFT)

The Delegated Byzantine Fault Tolerance (dBFT) is a consensus algorithm, based on Byzantine Fault Tolerance (BFT)[3], used in some blockchain networks to ensure the integrity of the distributed ledger[4]. This algorithm is a variation of the traditional Byzantine Fault Tolerance (BFT) algorithm. In a dBFT system, a group of nodes called "delegates" are elected by the network to validate transactions and create new blocks. These delegates are responsible for reaching consensus on the state of the blockchain and ensuring that the distributed ledger remains accurate and tamper-

[2] Vitalik Buterin is a Russian-Canadian programmer and founder of Ethereum. He co-founded Bitcoin Magazine in 2011 and has been involved in the Bitcoin community since then. He proposed Ethereum in 2013 and the project was launched in 2015. He is a leading figure in the cryptocurrency and blockchain technology space.

[3] Byzantine Fault Tolerance (BFT) is a concept in distributed systems that refers to the ability of a network of nodes to reach consensus despite the presence of malicious nodes that may try to disrupt the process. This is achieved by ensuring that most nodes in the network are honest and that the network can continue to function even if some nodes fail or behave maliciously. In a BFT system, nodes communicate with each other in order to reach consensus on the state of the network. This is done through a series of rounds of communication, during which each node sends messages to other nodes and receives messages in return. If a node receives conflicting messages from different sources, it uses a set of rules to determine which message to trust and which to discard. (L. Lamport et al., 1982) BFT is an important concept in distributed systems, as it provides a way for nodes to reach consensus despite the presence of malicious actors. This allows distributed systems to function securely and reliably, even in the face of attacks or other disruptions. (L. Lamport et al., 1982)

[4] Distributed ledger technology (DLT) refers to the protocols and supporting infrastructure that allow computers in separate locations to propose and validate transactions and update records in a synchronised way across a network. (BIS, 2017b)

proof. "In dBFT, a consensus is reached when two-thirds or more of the delegates reach consensus. If less than two-thirds of the delegates agree, there will be a fork in the chain. However, the fork with the most delegates will be considered the valid one, and the other fork will be discarded." (NEO project, n. d.)

Delegated Byzantine Fault Tolerance (dBFT) is an interesting consensus algorithm, as it helps to ensure the security and integrity of the network by allowing a group of elected delegates to reach consensus on the state of the blockchain. The dBFT consensus algorithm helps to prevent attacks and maintain the trust of users in the network.

Once users have agreed on the validated block, it is added to the chain. The new block would include the information of the one before so that previous transactions cannot be modified without affecting the entire chain and thus ensuring the already completed transactions. If the case were to occur that two blocks are validated at the same time, both would be added to the chain, resulting in two different chains, and the next block of transactions would continue. It will be the validation of the next block that will determine which will be the definitive previous block that will now be shared with the rest of the network, this is, the longest chain.

There is a wide range of types of blockchain, and most of them are derived from two large groups: public blockchains and private blockchains. Those defined as public are accessible to anyone without the requirement of being a user, from these derive the open, decentralized, and pseudo-anonymous ones. Two of the most known public blockchains are Bitcoin and Ethereum. Blockchains that are defined as private are those in which not all data is publicly disseminated and only participants and users can access. From these derive closed, distributed, and anonymous blockchains. It must be highlighted that private blockchains are weaker in terms of security than public ones, but in order to leverage both there also exist hybrid blockchain, that combines the characteristics of both types. (Preukschat et al., 2017)

1.2. BLOCKCHAIN TECHNOLOGY APLICATIONS.

In the previous section, the operation of blockchain technology, the processes it entails, and the different consensus algorithms have been explained. One of the best-known and popular applications of this technology nowadays are cryptocurrencies, in fact, this technology is what makes them possible, without blockchain there would be no Bitcoin or any altcoin[5]. Even so, seeing the consequences of the application of this technology forces us to ask ourselves, what can we apply this technology to and what benefits (not just economic) can be achieved? Knowing, as explained in this chapter, what the main characteristics of blockchain technology are and how it works, in this section we will try, based on these data, to study the uses that can be given to it.

Blockchain operates in a decentralized way, so it can be applied to any type of network to replace the central server with multiple operational nodes and thus avoid a failure that makes the entire network inoperable. This has been demonstrated on platforms such as Telegram, on the occasions when the Meta Platforms server (Facebook) has failed, leaving users of What's App, Facebook, and Instagram disconnected, Telegram has continued to function without problems because it is a decentralized network. The same happens with Ethereum, which has not been inoperable at any time since its launch in 2015. Of course, given the data recording and unchangeability capacity, it can be applied to the banking and insurance system, traditional banks could process their operations leaving

[5] Short for "alternative coin," is any cryptocurrency other than Bitcoin.

them recorded in their own blockchain. So instead of creating a new financial system based on blockchain and decentralised networks as private coins suggest, blockchain could be applied to the existing system and decentralise it.

It has been explained that blockchain technology operates on decentralized networks, which avoids massive failures and complete network crashes. If one of the nodes were to stop operating, nothing would happen. It is also known that the chains are highly secure, once the information is stored in a validated block, it is practically impossible to change it without modifying the rest of the chain, which at the same time continues to grow and be shared with the rest of the network users; therefore, modifying a previous block requires modifying all the following ones (including those that have been validating during these modifications) and sharing the new chain by convincing the rest of the users that the one being shared is actually the correct one. Finally, the chains are transparent but at the same time respect the privacy and anonymity of the users, which means that, any interested person (authorized in the case of private chains) can consult the transactions they or the rest of the users have made since they are stored on the network; however, what can be visualized is the user who has carried out the operation (identified with something similar to a username), but it is not possible to know, unless the user reveals it, who is behind the transactions carried out. A very representative example of this "anonym privacy" is S. Nakamoto: nobody knows who he is, but as his user is public anyone could identify him as he made the first transaction. Anybody could notice if he made a transaction and still not know who is behind the user.

The possibilities grow considerably when network applications such as Smart contracts and NFTs come into play. The first ones have potential to replace any traditional legal contract by increasing their effectiveness and eliminating any possibility of non-compliance given their automatic execution. In the case of NFTs, their benefits are clear in the world of art, for example, where they eliminate intermediaries who keep part of the artist's profits or demonstrating the property and originality of the same file. This subject, along with lots of other alternative applications in different fields will be thoroughly explained in Chapter III.

CHAPTER II: PLATFORMS AND NETWORKS. ETHEREUM

There are many blockchains nowadays, and in most cases, all platforms within this blockchain universe have one or several. If they were analysed based on the value that resides in them, the most important would be the Bitcoin blockchain without a doubt, as it represents 40% of the value of all cryptocurrencies and its market capitalization reached over 300,000$ in November 2022. On the other hand, if the breadth and transactions were taken into account, Ethereum would be considered the most relevant. In 2021, the number of verified transactions on the Ethereum blockchain exceeded that of Bitcoin; and that is because the Ethereum blockchain not only houses Ether, its own virtual currency, but also many other digital currencies and stablecoins, a large number of Smart contracts and most NFTs. (Kriptomat.io, n. d.) Apart from the ones already mentioned, there are hundreds of other blockchains, such as Ripple, Cardano, which despite having its own currency, is a next-generation blockchain based on smart contracts created with the intention of building fast and scalable dApps, or Stellar, which is focused on the financial sector and aims to create fast and secure fintech applications. (Parmar, D. 2022)

If we were to talk about cryptocurrencies exclusively, the concept of "exchange" must be introduced. An exchange is a virtual meeting place where cryptocurrency exchanges are made, either between them or with fiat money (depending on the exchange, it has different currency compatibility); some of them can also perform other operations with stocks or financial securities. (Academy, B. 2023a) The following table shows the main exchanges (ordered from most to least important), with the most relevant information about them to make an informed comparison of them.

Table 1: Most important exchanges

	Trading volume	Weekly visits	Digital currencies	Fiat compatibility
Binance	20,910,130,413$	13,598,160	383	11
Coinbase exchange	2,072,641,453$	527,283	241	3
Kraken	$622,185,447	898,694	220	7
KuCoin	$789,542,126	1,700,020	786	48
Bitfinex	$230,123,933	582,520	187	4

Source: Coinmarketcap.com (n. d.-b) (30/01/2023)

Thanks to the information obtained in the previous table, we know that in terms of volume of operations and weekly visits, data that could be related, Binance is the most relevant. However, if on the other hand, the availability of currency is considered, we would be talking about KuCoin, which handles a noticeably higher volume of both digital and fiat currencies, which could facilitate many operations due to its compatibility.

Given its already mentioned relevance and the fact that gives a lot more possibilities to their users that a simple exchange, this chapter will focus on the Ethereum network, due to its extent and the number of possibilities it offers to its users and the multiple tools hosted on it.

In order to address correctly this chapter about Ethereum it is quite relevant to distinguish between Ethereum and Ether. The Ethereum official page states that: “Ethereum is the communitarian management technology that impulses the Ether (ETH) cryptocurrency and thousands of decentralised applications (…) it is home to digital money, global payments, and applications. The community has created a thriving digital economy, new audacious ways for the creators to earn money online and a lot more”; this is, the term “Ethereum” is referred to the whole network and “Ether” is the official cryptocurrency of such network. It is only needed an Ethereum account and an internet connexion, so that, as they announce, the problems that loads of people can face in to have access to a banking account are avoided; in Ethereum is free and accessible to anybody. (Ethereum.org n. d.-e).

Ethereum has its basis in a decentralised network, which means that there is not a central figure that manages and supervises all the transactions made, instead are the nodes participants, controlled by voluntary users that operate as equals (peer-to-peer), the ones in charge of managing and supervising. As it is already known, the fact that it is a decentralised network makes it nearly impossible to fail, because each and every one of the nodes should have to fail at the same time, unlike in a centralised network that can fall apart just if the central supervising figure fails, in fact, the Ethereum platform has not failed not even once since its creation in 2015. The users in charge of managing the nodes, as in the Bitcoin network, they receive a reward for their job. The algorithm of Ethereum was Proof of Work (PoW) based, which consumes a great deal of computational power and therefore energy, which turns to be awfully problematic. This is why at the beginning of 2022 Ethereum changed its algorithm to a Proof of Stake[6] (PoS) based one, which helps to reduce the environmental impact[7] and to offer a much more secure network for the users. (Ethereum.org n. d.-k).

Thanks to the Ethereum technology the users can create apps, have assets, make transactions… and everything in a decentralised way thanks to the ERC[8]-20 standard[9]. The applications in this platform are open coded, so that the code can be used by other developers in order to create other applications in the platform. In the same way, they highlight their privacy policy, thanks to being a decentralised network, it is easier for the user to maintain the control over their data and assets. One of the apps developed over this Ethereum blockchain is Telegram.

Ethereum is a major blockchain-based platform for smart contracts. It shares a lot of characteristics with Bitcoin, but this is a payment network and Ethereum is more like a service market. Ethereum is also programable, so that other than the transactions that can be made with Ether, as it has been mentioned before, it can be built over its infrastructure.

Thanks to the Ethereum network it can be created a whole lot of different services. Though such network, for example, stable coins where born, which will be thoroughly explained in the following paragraphs. As it has been mentioned in the introduction of this paper, cryptocurrencies, and especially stable coins, have proven to be very useful in the last years in countries like Venezuela or Ukraine in order for their citizens to preserve their wealth. The Ethereum network has been used in order to make exchanges in the videogames hosted in such network or act as support for numerous artist who have been able to make some profit of their creations. All these possibilities and more will be explained in the following paragraphs.

[6] It is actually the largest update in the Ethereum network so far.

[7] The environmental impact has been reduced a 99,988% according to the Ethereum official webpage. (Ethereum.org, n. d.)

[8] Ethereum Request for Comment

[9] ERC-20 is a technical standard for Smart Contracts on the Ethereum blockchain for implementing tokens. The ERC-20 standard specifies a common set of rules that all Ethereum tokens must adhere to, which makes it easier for developers to create and integrate these tokens on the Ethereum network. Some of the key features of ERC-20 tokens include support for transfers, approvals, and the ability to check a token's balance. It was developed by Fabian Vogelsteller in 2015 and has since become the most widely used standard for Ethereum tokens. The ERC-20 standard is not the only one, there also exists the ERC-721, whose tokens are unique and indivisible, which makes them suitable for representing assets that are distinct and cannot be replicated, such as collectible items, digital art, and unique virtual items in games. On the other hand, is ERC-1155 suitable for implementing multi-token smart contracts on the Ethereum blockchain. (Proposals, n. d.)

CHAPTER III: TOOLS DEVELOPED FROM BLOCKCHAIN TECHNOLOGY

In this chapter, various tools developed thanks to blockchain technology will be discussed, as they all must be hosted on a blockchain. Many of these tools, despite existing on their own and being able to be hosted on any blockchain, have been developed thanks to some of the platforms mentioned in the previous chapter; these platforms have also provided users with a secure space for their use and development. As seen in the previous chapter, one of the most important blockchains is Ethereum, which hosts a large number and possibilities of the tools that will be studied below.

Cryptocurrencies are also considered a tool developed thanks to blockchain technology and their relevance is undeniable. That is why a whole chapter has been dedicated to discussing them in detail, giving them the space and importance they deserve in the topic being addressed. In Chapter V, not only will the most relevant virtual currencies be discussed, with the most important information about their history, operation and use, but also public digital currencies such as CBDCs or Stablecoins will be also studied. Additionally, it will be made a comparison of their market capitalization in respect of large companies and the volatility and feasibility of the same will be evaluated.

3.1. SMART CONTRACTS

According to what Nick Szabo, the creator of smart contracts stated in 1994, Smart Contracts are a protocol that executes the terms of a contract. The objectives of such contract are to satisfy common contractual conditions, minimize not only malicious and accidental conditions but also the need for trusted intermediaries. Its structure has a conditional basis, which mean that have an if-then semantics; the specific inputs guarantee predetermined outputs. The creator of the mentioned contracts, Nick Szabo, thought that these processes could be applied to any field of the digital market, thanks to one of its most important characteristics: it does not require any kind of trust between the parties because the smart contract will be executed by itself, as soon as the condition is fulfilled, the result will be executed automatically without the need of intervention nor participation of any of the parties. Furthermore, all the Smart contracts are executed in a precise way, not leaving place for interpretations, the conditions are stipulated in the code of the contract. In this way under the same circumstances the contract will provide the same result.

On one hand, smart contracts can be hosted in any blockchain, and any person can monitor instantly any contract; on the other hand, it needs to be remembered the characteristic anonymity of blockchain, so even though it is public, the data are referred to a cryptographic address (similar to an email address), and despite knowing the username and the transactions it is impossible to link that to the person who actually made them. Thanks to the transparency offered by the blockchain technology it is important to notice that both parties will be able to visualize the smart contract and interact with it before they sign it. To sum up, blockchain can be, at the same time, anonym, public and transparent; this is, the person behind any transaction is unknown even though the user is public, and furthermore, a chain is transparent as anybody[10], participant or not, can see any transaction made at any point.

Smart contracts are the mechanism that allows users to create and develop apps, new coins… and everything in a decentralised way on the blockchain. Once a Smart contract is published nobody can change or delete it, not even its creator; the smart contract will live and be executable as long as the blockchain where it is hosted is operative. Thanks to it, smart contract can be used for apps,

[10] Only applies to public blockchains. If talking about private or hybrid ones, anyone that is authorised to access that information.

videogames, stable coins, loans, insurance companies, crowdfunding… They also have the ability of receiving, storing, sending funds and even calling other smart contracts. (TEDx Talks, 2018)

3.2. NON-FUNGIBLE TOKENS (NFT)

Thanks to the blockchain technology NFTs are created, this term stands for Non-Fungible Token. This concept is easier to understand separately. The "non fungible" refers to an asset that cannot be exchanged for an equal one, as they are unique and irreplaceable goods; according to the Cambridge dictionary, it is defined as "not easy to exchange or mix with other similar goods or assets". A very common example of these assets can be digital art pieces.

In order to dig deeper into his matter, William Mougayar defined in "The business of blockchain" token as a "unit of value that an organisation creates in order to rule their business model and give more power to the users in order to interact with their products and make the benefit sharing easier at the same time." NFTs are digital assets that are unique and indivisible. This means that they cannot be replicated or divided like other cryptocurrencies, such as Bitcoin or Ethereum. Each NFT has a unique digital signature that verifies its authenticity and ownership.

Given this, it can be stated that an NFT is a type of digital asset that represents ownership of a unique digital item, such as a piece of artwork or collectible. NFTs are built on blockchain technology, which allows them to be bought, sold, and traded like other cryptocurrencies. Unlike cryptocurrencies, each NFT is unique and cannot be replaced by another identical token, which makes them useful for verifying the ownership and authenticity of digital items. NFTs have gained popularity in the art world, where they are being used to sell digital art and other collectibles.

Blockchain technology enables them to be traded on digital platforms. The use of blockchain technology provides a tamper-proof way to track the ownership and provenance of an NFT, making it a secure way to buy and sell digital assets. One of the main applications of NFTs is in the art world. Digital artists can use NFTs to sell their artwork and collectibles, giving buyers the ability to own a unique and verifiable piece of digital art. NFTs have also been used to sell other types of digital assets, such as virtual real estate and in-game items. (Ethereum.org, n. d.-g)

The Ethereum official webpage also provides a table comparing the internet with and without NFTs that is quite representative.

Table 2: internet with and without NFTs

An NFT internet	The internet today
NFTs are digitally unique, no two NFTs are the same.	A copy of a file, like an .mp3 or .jpg, is the same as the original.
Every NFT must have an owner, and this is of public record and easy for anyone to verify.	Ownership records of digital items are stored on servers controlled by institutions – you must take their word for it.
NFTs are compatible with anything built using Ethereum. An NFT ticket for an event can be traded on every Ethereum marketplace, for an entirely different NFT. You could trade a piece of art for a ticket!	Companies with digital items must build their own infrastructure. For example, an app that issues digital tickets for events would have to build their own ticket exchange.
Content creators can sell their work anywhere and can access a global market.	Creators rely on the infrastructure and distribution of the platforms they use. These are often subject to terms of use and geographical restrictions.
Creators can retain ownership rights over their own work and claim resale royalties directly.	Platforms, such as music streaming services, retain most profits from sales.
Items can be used in surprising ways. For example, you can use digital artwork as collateral in a decentralised loan.	

(Source: ethereum.org, n. d.-g)

The use of NFTs has gained popularity in recent years, but it has also been the subject of some controversy. Some critics argue that NFTs are not truly ownership of an artwork because the original artwork can still be reproduced and distributed without permission from the NFT owner. Others have raised concerns about the environmental impact of NFTs, as the process of creating and trading the m can require a significant amount of energy. This fact changed when the network changed its consensus algorithm.

Overall, NFTs are a unique type of digital asset that allows for the ownership and verification of unique digital items. While they have gained popularity in recent years, their use and potential impact are still being debated.

3.3. DECENTRALISED FINANCE (DEFI)

This concrete subject has great relevance as it gives the possibility of substituting the current financial system by a decentralised one and it will be of a huge importance to analyse the viability of cryptocurrencies in the future.

Table 3: decentralised VS traditional finance

Decentralised finance	Traditional finance
The user stores its own money.	Companies store the users' money.
The user controls the purpose of its money and the way it is spent.	The user must believe that the companies would not manage badly their funds.
The funds are transferred in a matter of minutes.	Some payments can take days due to the human intervention.
The financial activity is performed under a pseudonym.	The financial activity is highly linked to the identity of the user.
DeFi is accessible for anybody.	The user must request the use of such financial services.
The markets are always opened.	Markets close due to the rest need of the employees.
It is built over transparency: anybody can look up the data of the product and examine how the system works.	Financial institutions are like closed books: a user cannot ask about the loan record, the activity register of its assets…

(Source: ethereum.org, n. d.-c)

Thanks to the creation of Ethereum, the platform allows users to pursue operations like loans, trading, derivatives… DeFi (Decentralised Finances) is the term that comprehends all the product and services available inside a network using virtual currencies. Thanks to smart contracts, which have the capacity to replace the centralised traditional financial institutions, all the operations are carried out automatically and in a much more secure way that the traditional finances.

Thanks to Decentralised Finances (DeFi), not only it exists a decentralised choice for almost every financial product and service, but also have allow for completely new financial services to take place, that would not be possible without the Ethereum network, which is in this case the network that offers more possibilities regarding this subject. Thanks to such network the users can engage transactions as regular money transfer, national and international, in a faster way than it would be with the traditional banking system, using Ether (ETH) or any other stablecoin[11] to avoid volatility. Another quite common transaction in the traditional banking system, that can be carried out in a decentralised way thanks to Decentralised Finances are loans. To lend or borrow money can be quite simple peer-to-peer (P2P): user A lends money to user B, who agrees to return it after a period of time plus interests; but this kind of transactions can get a lot more complicated according to how it is carried out as the fact of being peer-to-peer, gives them the capacity to adapt to the necessities of both participants. Another advantage of this kind of transactions is the fact that none of the parties need to identify themselves, which keeps clear of prejudices, using as guarantee certain assets that the moneylender will receive as payment if the borrower does not fulfil the payment. (Finematics, 2021)

There are some more complex decentralised loan operations such as "flash loans", in which the amount of the transaction is withdrawn and reimbursed in the same transaction (if the money cannot be reimbursed the transaction is simply reverted as if nothing would have happened). Nowadays this kind of loans are only available for a few users that have a wide technology knowledge. From the point of view of the money lender is quite simple to lend its money and receive it back, making a profit of it in a matter of days or even hours. There also exist other kind of products for users to save like PoolTogether, which share some characteristics with the lottery: the users buy tickets but if they do

[11] Chapter V. Section 5.5.

not win the prize the money is reinvested in the tickets for the next week. For the most experienced users there are other kind of transactions that allow them to increase the control over their assets through limited orders, margin trading… There also exist funds such as the DeFi Pulse Index, which includes the most relevant tokens according to their market capitalization. (Ethereum.org, n. d.-c)

In addition to that, there are other kind of services managed by smart contracts (like all the figures mentioned before) that are being already managed in the Ethereum network, like insurances, used to protect the user from the losses of a virus that make them lose their assets; or as they are innovatively doing in Kenia, where some farmers are using these decentralised insurances to protect their crops from flooding.

CHAPTER IV: ALTERNATIVE USES OF BLOCKCHAIN. COULD BLOCKCHAIN BE THE FUTURE

In previous chapters, the topic of blockchain has been presented in depth. In the first chapter, both the operation of blockchain technology and its characteristics have been described in depth. This technology can have multiple applications and different uses in everyday life, many of which are already beginning to be seen. In the previous chapter, it has been shown one of the possible applications of the same technology, the Ethereum platform, which provides users with a wide range of possibilities within its blockchain. In this chapter, the interest will focus on other uses that can be given to this technology, apart from those already mentioned and the cryptocurrencies that will be discussed in the next chapter. According to Preukschat et al. (2017, p. 29) "blockchain allows us to program trust, property, identity, assets and contracts through, payments, transactions, processes, authentication, reconciliation and real-time information and all with full transparency and auditability." The applications that will be presented below are less known, but not less useful; in fact, the current chapter aims to demonstrate how incredibly useful the application of this technology can be and its multiple benefits for users.

4.1. APPLICATIONS IN BANKING, INSURANCE AND LAW

In the banking sector, the application of blockchain can also be of great interest, bringing many benefits for both banks and users. It should be noted that, despite the countless possible applications to existing processes and markets, the application of this technology will open new markets and businesses.

The first application of this technology that will be discussed in relation to banking is global payments. Today, despite the fact that with SWIFT the processes are relatively fast, the unique characteristics of blockchain would save the time that occurs with the settlement between entities, making the payment almost instantaneously. Global payments can be conducted through public and private blockchains. Among private blockchains, the platform Ripple, specialized in international interbank payments and currency conversion, is showing its great usefulness. In the chapter dedicated to cryptocurrencies, we will discuss XRP, the virtual currency of the Ripple platform, but for the moment we will delve into the platform in a generic way to understand the benefits of its application.

The aforementioned network is an open-source protocol to streamline and lower the cost of certain transactions. It is a public blockchain for users, but it requires authorization from the platform for the parties that want to operate as liquidity providers. As already mentioned, Ripple has its own currency, XRP, and also allows users to create their own currencies through RippleNet. It has become "an institutional payment network (...) that uses solutions developed by Ripple to provide a hassle-free experience for sending money worldwide" (Cointelegraph.com, 2021a). "In addition, Ripple has a custom consensus mechanism, unlike networks like Bitcoin and Monero that work with the Proof of Work (PoW) algorithm. The algorithm used by Ripple is known as the Ripple Protocol Consensus Algorithm, abbreviated RPCA, and is the system that makes it possible to verify and validate all transactions that will be recorded in the Ripple ledger (XRPL)." (Criptonoticias.com, 2021). Transactions are conducted through a downward auction process in which liquidity providers compete to process payments. The settlement process between the parties is managed by Ripple in real-time. RippleNet will try to connect users who have something of value to offer and at the same time demand another asset, looking for the cheapest combination to try to meet their needs. The platform is especially useful in currency exchange operations in which users can use the currency, XRP, as a bridge currency, instead of the dollar (USD), making the process cheaper and faster. In fact, the commission is practically zero (0.00001$), it exists to prevent attacks, and the average time per transaction is 4 seconds. This platform is already used by entities such as Santander Bank or UniCredit as infrastructure technology for its payment speed, technology stability and the effectiveness of its currency (XRP) as a bridge currency. The countless benefits of its application in trade finance should also be mentioned, as it allows users not only to accelerate and lower the costs of bureaucratic processes, but also to automate processes and digitize communication, thereby notably reducing circulating cash. There are already several start-ups working on this application, which will allow users to automate the buying and selling of products and certify their origin thanks to the traceability and transparency of the blockchain. (Cointelegraph.com, 2021b)

It has already been discussed in the chapter dedicated to the Ethereum network about peer-to-peer loans. Currently, financial institutions are relied upon for trust, but in the case of loans formalized through blockchain technology, trust is not necessary. Smart contracts would play a role in replacing the lack of trust among users, as they guarantee compliance by both parties, as has been explained several times. This application would also eliminate intermediaries in the operation, leaving only the lender and borrower, reflecting their agreement in a Smart contract stored on a blockchain.

In the insurance sector, the competition has grown considerably in recent years, and the type of customer it is targeting has changed a lot, now being a demanding customer with the ability to compare the services offered and the clauses included. The sector is aware that it needs to increase its profitability margins, for which it is beginning to rely on technology. "Blockchain (...) allows the participating actors in the chain (insurers and customers, agents and brokers, or technicians and experts) to exchange information securely, quickly and constantly through an open, decentralized, reliable and flexible infrastructure." (Preukschat et al., 2017, p. 33)

“The point of insurances is to facilitate the distributing of risk from individuals to a larger community, not centralising risk in a single corporation or even a small handful of companies. And blockchain gives us the technological means of spreading risks and lowering uncertainty. In terms of transactions per second the insurance industry operates in a far smaller scale than traditional banks, so it does not face the same scaling challenges and limitations of blockchain as does the banking community.” (Kim, H. M., and Izhar Mehar, M. 2022) The application of this sector can cut a large portion of the expenses generated in bureaucratic processes by automating most of them. In the case of a travel insurance, the passenger could automatically receive the refund of the money in their bank account in case of any unforeseen event without having to fill out any complaint or form. In addition, combined with the application of the Internet of Things, it will allow insurance companies to offer their customers much more tailored rates to their needs, for example, in the case of a car insurance, they will be able to study the driver's driving style or automatically evaluate the damages after an accident, executing the contract and therefore the coverage automatically. These applications, besides increasing customer satisfaction and trust, and minimizing the company's expenses, help to prevent and practically eradicate fraud.

Some insurance companies are starting to adopt this technology, creating Blockchain Insurance Industry Initiative-B3i, a collaboration of insurers and reinsurers formed to explore the potential of using Distributed Ledger Technologies within the industry for the benefit of all stakeholders in the value chain, was launched in October 2016. It is the resulting cluster after the consortium of: Mapfre, Aegon, Allianz, Munich Re, Swiss Re y Zurich. (Mapfrere.com, 2021)

Another possible application of blockchain technology, which is expected to have a long future, are Smart Contracts, which, as it has been seen, collect the agreement between two parties, who do not need to have any trust or information about them, and which is hosted on a block chain. These contracts are also automatically executed, so once one party fulfils what is established, the second party will execute. This way there is no room for interpretations or contract breaches. This specific application covers practically all areas of legality, as it can replace any contract, from a rental contract, which automatically activates the access key once the rental transfer is received, to a prenuptial contract that is executed in case of non-compliance of any of the parties.

4.2. APPLICATIONS IN PRODUCTION CHAINS AND LOGISTICS

As already explained, blockchain technology allows for data to be stored securely, immutably, but also publicly and freely accessible at the same time. These characteristics are very useful in supply chain and logistics, which can be very long and made up of different companies and intermediaries, as they allow both links in the chain and end consumers to consult any part of the process and track it quickly and reliably. Companies such as Carrefour or Angulas Aguinaga already implement this technology in their processes. This application also has its place in the health sector, as in the case of any type of food contamination or illness that causes a problem for the citizenry, it can be easily traced. In addition, this way, the consumer can be offered information about the food safety and quality of the product. For manufacturers and distributors, it allows them to streamline and automate bureaucratic processes that can be long and tedious with more traditional systems. (Cuadrado, 2022)

The energy industry can also benefit from the advantages of blockchain. Nowadays’ energy demand is managed by a small number of large power plants located far from consumers, but what this new system proposes is to increase the number of energy-producing plants, even if most of them are much smaller, closer to the end consumer, in some cases on their own roof, argues Preukschat et al., (2017) The application of blockchain technology to this sector allows users to produce their own energy and sell their surplus to other users or to the general provider in a decentralized way. If this application were adopted by a large number of people, it would force existing massive production plants to adapt to this new structure, in which electricity can be injected from any point on the network and in any direction. It could also cause the disappearance of large energy providers, as they could allow people to partially avoid the abusive prices of energy that generate those excessive profits. This would create the known as Virtual Power Plants (VPP), "an initiative that aims to group small generators, accumulators (...) in order to operate as a single entity in the market, thereby competing with major power generation centres." (Preukschat et al., 2017, p. 47). According to Next, n. d. "depending on the market environment, VPPs can accomplish an entire range of tasks. In general, the objective is to network distributed energy resources such as wind farms, solar parks, and Combined Heat and Power (CHP) units, to monitor, forecast, optimize and trade their power. This way, fluctuations in the generation of renewables can be balanced by ramping up and down power generation and power consumption of controllable units."

There already exist companies that apply this technology, like Electron, founded on the belief that energy systems of the future would need digitally optimised marketplaces rather than large scale new generation capacity, to deliver Net Zero in a cost efficient and resilient way. (Electron.net) Siemens has also decided to bet on a project applying blockchain technology to distributed energy generation. Siemens, along with other companies worldwide, has formed Lo3 Energy, whose mission, as described on their website is "to accelerate the decarbonization of electric grids worldwide with a software platform that allows our partners to implement innovative compensation mechanisms that best support their customers, DERs, and the networks they operate" (Lo3energy.com)

Another tremendously innovative application in this energy field is Solarcoin. SolarCoin is a cryptocurrency based on blockchain technology, designed to reward solar energy producers. The coin is used as an incentive to encourage the production of renewable energy and reduce carbon emissions. Solar energy producers can claim SolarCoins for each megawatt-hour (MWh) of energy they produce. The coin can also be bought and sold on various cryptocurrency exchanges. SolarCoin is based on the Litecoin cryptocurrency and uses the Scrypt algorithm. (*SolarCoin*, n. d.)

Blockchain can also play a role in terms of user possession certification, as it has been seen with NFTs. This can be applicable to the artistic field by certifying that the work in question belongs to a user who bought it, or that certain music is the work of a specific musician who receives a direct commission when his songs are downloaded, for example, forgetting about copyright problems or control by record labels. It can also be applied to existing brands, certifying the originality of the article by allowing the tracking of the article from the beginning and confirming its authorship; this particular application can be especially useful in luxury brands. Thus avoiding counterfeits, an application to which Nike has already joined with Cryptokicks. This application could protect the user from any type of counterfeiting in any field, from diplomas to identity itself. (Cuadrado, C. 2022)

4.3. APPLICATIONS IN DATA STORAGE AND ONLINE COMUNICATIONS

According to Preukschat et al. (2017, p. 38) "any industry that uses centralized databases that are fed by different sources is susceptible to being affected by blockchain technology disruption". The authors bet on the creation of new business models with the application of this technology in the telecommunications sector. In the mentioned book, "*Blockchain: la revolución industrial de internet*," blockchain is described as a technology for managing authenticity, duplicates and security automation;

and they argue that any automation that speeds up processes will eventually be imposed in a generalized way in the industry. Moreover, thanks to its highly secure design, it is invulnerable to external attacks. This technology, according to the mentioned authors, will generate the usual response to innovation in any industry: some companies, those that are agile and quickly adopt the change and the new model, will survive thanks to the optimization that this provides, those that cannot make the change in time will fade and disappear as time goes by.

One possible application in this area is cloud storage. As we know, blockchain operates in a decentralized way and therefore on different nodes and servers, in this way massive failures in the central server are avoided. Therefore, the application of the technology would make the data be completely resistant to any type of modification or attempt at fraud, given the already known high security of blockchain and the fact that the data stored would be located in different nodes at the same time. This can be applied to any other type of information that needs to be stored, replacing databases. This application also ensures the security of the data, as it is protected by unalterable cryptography.

Identities can also be managed by tokenizing them, creating unique profiles using NFTs and verified with a simple photo, replacing usernames and passwords, and limiting the information needed and avoiding the risk of identity fraud. NFTs, which use a method of intelligent encryption and validation, in conjunction with the other technologies already mentioned, are extremely useful for creating a cyber-secure system, offering encrypted and immutable systems, as well as tokenized digital signatures for transactions. This allows for interaction between users through authentication, preventing identity fraud. NFTs are virtually impossible to duplicate, which, combined with their versatility, offers one of the major applications of blockchain technology in the future in the field of cybersecurity, not only for individuals but also for business organizations. (Zafar, T. 2022)

Thanks to the resulting need for tokenization by users and companies, companies like KwikTrust are born. It "not only empowers users to create collaborative workspaces that are safe and secure, but it also makes it easy to work with different organizations and clients." and tries to respond to the necessity of managing and empowering their digital activities. Thanks to this company, their clients can "upload their content to create a tamperproof, timestamped record of creation. Files can be added, validated, signed, and stored at any time and linked to the owner's identity." (Ashley, C. 2023)

For years, social networks have been very present in our lives, from WhatsApp to Instagram or recently BeReal, they capture our attention with their content. These types of systems can also benefit from blockchain technology, a proof of which is Telegram, a social network on a decentralized blockchain (TON[12]) that even has its own currency (Gram), a decentralized social network that demonstrates its usefulness every time there is a failure in the central servers of Meta Platforms, leaving users disconnected, while those who use Telegram continue with their lives as if nothing had happened. At the beginning of 2020, the company made public the details about the blockchain that had been in development since 2017, confirming that its code would be open, public, and that both the management and employees of the network would have the same position as the rest of the users, resulting in a completely decentralized and peer-to-peer network. (Leal, A. 2020)

4.4. APPLICATIONS IN PUBLIC SPACES AND NON-GOVERNMENTAL ORGANIZATIONS

The blockchain system can also be applied to voting at shareholder meetings, for example, being decentralized and having each user a digital identifier. In addition, it would be done in a completely secure and impartial way. The process would be carried out with high transparency that would allow

[12] Telegram Open Network

control of everyone. Given these characteristics, it could even be used to hold national elections in any country. Although some nations already consider blockchain as a new way to approach democracy; obtaining from this application a new framework on which to regulate, for example, the voting system, some cybersecurity experts believe that the blockchain is still not able to ensure the guarantee of electronic voting. In the same way, in the future, the application of DAO[13] could help manage city hall or even governments.

In the same way, it can be applied to non-governmental organization, allowing users to track where their contribution has been allocated or even guarantee the purposes in which they invest thanks to Smart contracts. It could be that through an smart contract, an agreement is drafted in which the organization commits to donating capital for a specific purpose when users have exceeded a specific number of contributions, automatically and without the need for human intervention: at the time the amount aimed is reached, the transfer of funds is made to the specific cause. In this way, the intermediaries cannot make a profit from the donated amount, achieving that all the money donated arrives to its destination. Although no NGO has yet adopted this technology, some such as Save The Children have begun to accept payment in cryptocurrency. (IMNOVATION. n. d.).

As we have already seen, blockchain can be applied to nearly any aspect of our daily lives, and to help companies transition, there are companies like Chainalysis, which provides blockchain analysis tools for businesses and government agencies. According to their own webpage “We are paving the way for a global economy based on blockchain. Companies, banks, and governments use Chainalysis to make critical decisions, foster innovation, and protect customers.” Their products allow customers to track and investigate blockchain transactions, with a focus on identifying and preventing illegal activity such as money laundering, fraud, and terrorist financing. The company's software can be used to analyse transactions on a variety of blockchain platforms and provides businesses and government with the tools to track and comply with regulations, providing insights on identifying suspicious activities. Chainalysis is also known for its participation on providing blockchain analysis and forensic services to law enforcement agencies and regulatory bodies worldwide to help them trace criminal activities and support investigations. Overall, it provides a range of services that allow its customers to better understand and navigate the blockchain ecosystem, with a focus on identifying and mitigating risks associated with illegal activity. (Chainalysis.com, 2022)

So far, we have delved into the countless benefits of the application of this technology, but as with any innovation, not everything is easy for its development and implementation. In 2017, the World Economic Forum (WEF) reported the need for collaboration and legislative coordination by regulatory bodies, as well as the potential risks associated with possible security failures. Additionally, the European Securities and Markets Authority (ESMA) acknowledged that it is pending to establish a regulatory framework that includes this new technology that promises to revolutionize the world of transactions as we know it. (Fabregas & Asoc. 2018)

[13] "A DAO or Decentralized Autonomous Organization (...) is an organization that is controlled by algorithms or smart contracts, is not tied to any particular law (...). That is, it seeks to do away with intermediaries, (...) so that a company or institution can operate without a hierarchical management." (Estrategias de Inversión, n. d.-b)

CHAPTER V: CRIPTOCURRENCIES

5.1. TRADITIONAL CURRENCIES: HISTORY OF MONEY

In order to understand the peak of cryptocurrencies it is necessary to acknowledge the concept of money, its history, first appearances and how it led to money as we know it nowadays, and its characteristics of now and then, together with the purposes of its birth, which is the aim of the following paragraphs.

At first, when money did not exist, people used to barter, this is, exchange the products they had for the ones they needed. This rudimentary system posed some complications, such as the fact that people had to be able to offer what the other person needed in order to have what they were seeking, which became more and more complicated as civilizations began to grow. As a solution to this uneasy system, money was born.

The Cambridge dictionary (2022) defines money as: "1. The coins or bills with their value on them that are used to buy things, or the total amount of these that someone has. 2. The value of what a person or organization owns, keeps in a bank, has in investments, or spends. 3. The coins or paper currency which can be used to buy things." From a more accurate perspective and according to C. Domingo (2018, p. 34) money has had, since its creation, three basic functions: first of all, it needed to be able to store value, be quantifiable; second, it had to be exchangeable, this is, meet the capacity to make transactions; and finally, to be a reference value, and so, to price things. It is extremely important to bear these objectives in mind when analysing any coin, even the virtual ones will need to match these functions if they want to be considered and used as any other fiat currency. On the other hand, according to S. Ammous (2022, p.25-26), "A good that is given the role of a widely accepted means of exchange is called money. Being a means of exchange is the defining function of money; (...) it is not a good that is acquired to be consumed (...) or to be used in the production of other goods (...) but to be exchanged for other goods." The same author, based on the ideas of C. Menger, argues that the essential characteristic for a good to be accepted as currency is its 'sellability', and that this will depend on its capacity for divisibility or fragmentation, its ability to be transported, and its durability over time. Back to C. Domingo's (2018, p. 35) ideas, in order for the correct functioning of any coin, it had to meet also some characteristics, a coin has to be scarce, difficult to copy, durable, easily divisible and desirable. It will be important to bear in mind the mentioned basic functions at the end of this very chapter.

During centuries, the object used as coins changed, being the most popular ones the precious metals, due to the real physical back up of the material by itself, until the notes were popularised. It was an important change because notes had not the backup of the value of the material itself, only the support of the issuing, which is an important idea to bear in mind in the next pages when talking about cryptocurrencies. Another quite important moment in history in order to understand the evolution of money and how it has led to cryptocurrencies, was 1971, when, after years of the gold standard practically ruling the economies of the world, Richard Nixon decided to eliminate it, and every country followed his lead. Since that very moment, the money of each country does not have the support of the physical reserves of gold, just the backup of the trust of each government. It was in that very moment when the fiat money was born. (C. Domingo, 2018, p.38-39)

The concept of fiat money is quite important to understand virtual currencies because of the non-physical support of their value. "Fiat" is a latin origin word that can be traduced as "it shall be" and it is used when referring to government issued money not supported by any physical commodity. The value given to fiat money depends on the stability and credibility of the country issuing the coin and the supply-demand relationship of the currency. Nowadays most paper currencies, such as euros, pounds or dollars are fiat. Fiat money will be accepted as a currency as long as it can meet the three basic functions of money stated in the previous lines: value storing, quantification and exchangeability. Nevertheless, fiat money increases the power invested in central banks, which gain control over the economy; thanks to controlling the supply, since fiat money is not scarce, they have power over credit supply, liquidity, interest rates and money velocity. A currency referenced to a physical commodity is usually more stable, due to the limited amount of, for example gold and silver. Consequently, with fiat money bubble creation is more likely. Fiat money has the value that people want to give them; for example, the pesetas (Spanish currency before the euro) do not have any value nowadays because they cannot longer store value and are not accepted as a payment method, they have lost the government backup. (J. Chen, 2022)

This fact of the gold reserves not supporting any coin and the appearance of fiat money, is very important in order to understand cryptocurrencies. One of the biggest objections that people have with virtual money is that very same fact, without being aware that the fiat money does not have this support either, if people do not trust the nation's currency, it will no longer hold its value.

5.2. VIRTUAL CURRENCIES

Virtual currencies, also known as digital currencies or cryptocurrencies, are digital assets used as a medium of exchange. They are based on and protected by cryptography, which is used to secure and verify transactions, and they use decentralized networks to maintain an open, transparent, and secure ledger of transactions. Virtual currencies are not issued or backed by any central authority, and their value is determined by the law supply and demand on the market. According to the CMPI report on digital currencies (BIS, 2015) there are many digital currency systems based on distributed ledgers, they are being developed, or have been introduced and then disappeared. These digital currencies are similar to commodities like gold because their value is determined by supply and demand, rather than having intrinsic value.

They are traded on various online exchanges[14], and their value can fluctuate significantly. They are valued based on the belief that they can be exchanged for other goods, services, or a certain amount of traditional currency in the future. Some of the most well-known virtual currencies are Bitcoin and Ethereum; usually, to refer to other currencies, different to these two, it is used the term "altcoin," the combination of the words "alternative" and "coin". They are used for a variety of purposes, including as a store of value, a means of payment for goods and services, and a speculative investment.

The creation of new units of these digital currencies is often determined by a computer protocol and the supply is determined by an algorithm, which helps to create scarcity. These digital currencies are not usually tied to or expressed in terms of a specific fiat currency. Another key characteristic of these digital currency systems is the way that value is transferred from one person to another. In the past, peer-to-peer exchanges of physical money could be conducted without the need for trusted intermediaries. However, the use of distributed ledgers now enables electronic value to be exchanged peer-to-peer remotely, without the need for trust between the parties or intermediaries. When a transaction is made, it goes through a confirmation process that verifies it and adds it to a shared ledger, copies of which are distributed across the peer-to-peer network. Lastly, another difference between these digital currency systems and traditional e-money schemes is the way they are structured institutionally. Many digital currencies are not operated by any specific individual or organization, unlike traditional e-money schemes which have one or more issuers who are responsible for the value and whose liabilities are recorded on their balance sheets. Additionally, some digital

[14] Exchanges have been defined along with the mention of the most important ones in Chapter II.

currencies are decentralized, meaning there is no identifiable operator for the scheme. However, there are intermediaries that provide various technical services for these digital currencies, such as "wallet" services that allow users to transfer value or services that facilitate the exchange of digital currencies for traditional currencies, other digital currencies, or other assets. These intermediaries may also store the cryptographic keys that give access to the value for their customers.

As it has been seen, it is true that fiat money and cryptocurrencies have some things in common, but they have some quite major differences; these are shown in the following table.

Table 4: differences between traditional and virtual coins

Traditional money	Cryptocurrencies
It is exchanged in order to purchase something valuable.	Value is exchanged into virtual coins.
They are tangible	They are virtual
They are rooted to one or several concrete countries.	They are global
They are controlled by central banks and federal reserves.	They are he users who control them, supported by the blockchain technology.
The enter the economic system though bonds.	They enter the economic system directly.
Issues by governments.	Issued online.
Very slow and bureaucratized money transfers.	Payments between individuals are immediate and without intermediaries.
Costs for commissions	Costs due to software maintenance
Not all people in the world can have a bank account	All society can use them, included those who have not access to financial resources.

Source: Daviescoin.io (2019)

However, at this point of the paper, it is necessary to clarify the difference between value and price. Nowadays cryptocurrencies have a higher price than fiat money but lower value. According to the definition of value, this is understood as the benefit or satisfaction for the individual provided by the asset, in this case the cryptocurrency. It can be a very abstract concept, since it depends on the opinion of the user and it is not linked in any way to market facts, as supply, demand, or volatility. At the same time, the concept of price can be understood as the amount of money that the individual is willing to exchange for an asset in the market. This now is, unlike value, a quantifiable concept, and it will rely on facts that the value will not. Furthermore, a price can be altered by governments and institutions, which make the price not a reliable indicator in terms of how the consumer values the asset at issue. (Morales, F. C., 2020)

Therefore, and taking into consideration the nowadays cryptocurrency context, it can be considered a future where virtual currencies could replace fiat money? Could this be nothing more than mere speculation, originated from the higher prices that nowadays cryptocurrencies have in markets? However, this days, traditional coins provide to society a higher value, being prevailing in the exchange of assets. So, if virtual currencies start to be used in a wider stage, could they really replace fiat money due to their higher accessibility and connexion to the internet sphere and what would it take?

To understand how cryptocurrencies work, it will be necessary to have some context about their creation and some of the concepts that surround them and are necessary to understand the functioning of the whole system.

Cryptocurrencies are based on both decentralized networks and blockchain, which are concepts that have been explained before, thanks to which we know that in decentralised systems users operate among equals, without a central figure that supervises them, which in a centralized network would be a bank, for example. Users interact with each other buying and selling products or services or the currencies themselves; and all of this on an equal footing (P2P). Among these users are the miners, who, to simplify, are responsible for validating the transactions made and receive a reward for it. This reward is made up of an amount offered by the platform for which they work, such as Bitcoin or Ethereum, for example, and the commission that users pay for miners to verify their transaction. Nevertheless, their rate, along with rewards and fees will be explained in depth later.

Blockchain, as mentioned, is the technology that acts as a ledger for all the made transactions. Its functioning is mostly simple, although there are some facts that may complicate it. When a transaction is made, a miner, which is also user of the network, gathers it along with other transactions of their choice to form a block. These transactions must be validated in some way in order to know that no user is cheating, and the validation method depends on what the platform states; it can be: proof-of-work (PoW), proof-of-stake (PoS), delegated byzantine fault tolerance (dBFT)… The functioning of all these consensus algorithms has been previously explained and whether which one is chosen depends on the platform. As it has been said, for example, Bitcoin uses a proof-of-work (PoW) algorithm whereas Ethereum is now based on a proof-of-stake (PoS) one.

5.2.1. Tokens

Token according to Academy B. (2022c) is defined as " objects similar to coins but they lack legal tender value. This is because tokens are issued by a private entity for a specific use and are normally made using low-value materials. They are created in the private sphere and have little value. However, the value of tokens can be extremely high within the community that uses them, where everyone agrees on their use." With this definition in mind, we know that Bitcoin or Ether are tokens. It is worth noting that newly created tokens reside on the blockchain of a third party, such as Bitcoin[15] or Ethereum.

According to the characteristics of each token, they can be classified[16] as:

1. Security token: A type of digital asset that represents ownership of a real-world asset, such as a company's stock or a property. These tokens are typically issued through a process called security token offering (STO), like an initial public offering (IPO) in the traditional financial world. They are built on blockchain technology so they can potentially offer faster and cheaper transactions, increased liquidity, and enhanced accessibility to a wider range of investors. (Academy B., 2023b)
2. Utility token: A digital asset that represents access to a product or service. They are often issued through initial coin offerings (ICO). Utility tokens are used to purchase goods or services within a particular ecosystem or platform. They are not intended to be investments, but rather a means of exchange within the platform.
3. Equity token: A digital asset that represents ownership in a company, similar to traditional equity such as stock or shares. Equity tokens can be used to represent ownership in a variety of several types of businesses, including startups, established companies, and even real estate or other physical assets. They may give token holders the right to vote on company decisions, receive dividends or other distributions, and participate in the company's growth and success.

It is important to note that the line between equity tokens and other types of tokens, such as security tokens and utility tokens, can be blurry. The determination of whether a token is an equity

[15] Tokens that reside on the Bitcoin blockchain are known as Coloured Coins.

[16] Classification obtained from Academy B., 2022c.

token depends on a variety of factors, including the nature of the token, the purpose of the token sale, and the rights and privileges granted to token holders.

5.2.2. Doble spending problem.

"The doble spending problems is a potential flaw in a cryptocurrency or other digital cash scheme whereby the same single digital token can be spent more than once, and this is possible because a digital token consists of a digital file that can be duplicated or falsified"; this "would constitute a form of cheating and that would collapse any workable system" (Chohan, 2015) In a traditional financial system, double-spending is prevented through the use of intermediaries, such as banks, which keep track of transactions and ensure that the same money is not spent twice. In a digital currency system, however, there is no central authority to keep track of transactions and prevent double-spending. Although it remains a risk, a way to prevent, or at least minimize the double-spending problem, is to use a blockchain, which allows multiple parties to reach consensus (through the mentioned methods) on the state of the ledger without the need for a central authority. Each block contains a record of multiple transactions, and once a block is added to the chain, it cannot be altered or deleted which makes it difficult for a digital token to be spent more than once, because any attempt to do so would require altering the entire chain, which is not practical. The possibilities of a secret block being introduced into the blockchain is small as it would have to be accepted and verified by the network of miners. Another way to prevent the doble spending problem are the proof-of-work (PoW) and proof-of-stake (PoS) algorithms, as transactions are verified by miners, and they would notice such problem. (Chohan, 2015)

5.2.3. Initial Coin Offering (ICO)

An ICO, which stands for Initial Coin Offering, is a new funding method based on cryptocurrencies. A most traditional, even rudimentary, external financing method would be for a company to look for funding via the sale of their stocks, indebting themselves or thanks to subsidy. These systems require a long bureaucratic process, besides not everybody could have access to them. A few years ago, crowdfunding[17] was born as a more modern funding method, even though it also presented its cons. Every person could have access to financing but there is anything that guarantees the investor that the fund will be destined to the development of the project. Besides, given the bureaucratic process they are treated as donatives with the hope of receiving some kind of discount or recognition. As an answer this funding necessity, and thanks to the blockchain technology, the ICO were born despite they also have their pros and cons as it will be explained later. (Academy B. 2022e)

According to P. Momtaz (2020) "ICOs are smart contracts based on blockchain technology that are designed for entrepreneurs to raise external finance by issuing tokens without an intermediary." To simplify, an ICO is the obtention of external finance by selling a newly issued amount of a virtual currency. It is a much faster method that any of the previously mentioned, therefore anybody can get funding easier and faster than with the previous options, knowing that anybody could obtain funding their ideas from any part of the world in seconds.

In the period between 2009-2014 the most common thing was that the new cryptocurrencies were based on an emission linked to an algorithm like Proof of Work (PoW) or Proof of Stake (PoS) and there does not exist any central figure that issues them, but they are mined. In 2013 the first pre-mined coins started to appear, such coins were mined by the developers in private before the software was published, which gave them some leverage over the other miners and allowed them to obtain external financing after. In 2014 Ether was born, during its creation, they mined the virtual coin in advance, and

[17] The person applying for funds will present their project to investors, who will contribute their money to it. After a previously established period of time, investors recover the capital.

they sold it to obtain external funding to develop the Ethereum project that would see the light over a year later. This became the one of the first ICO, which collected 19 million dollars in Bitcoins.

Over Ethereum there exist the smart contracts in base of which new digital currencies can be created, in the case of Bitcoin this tool is coloured coins, and they allow the creation of virtual coins over existing ones, this is, the infrastructure, security, transparency, speed and privacy of the new cryptocurrencies is delegated over Ethereum's or Bitcoin's blockchain, which actually makes their creation easier and faster. In this way new tokens are generated that can only be fully comprehended by adapted nodes and wallets, although they share most of their characteristics with Bitcoin or Ethereum and work over an existing blockchain From that moment on, the ICO revolution started and any idea could use this method in order to obtain external financing and the more demanded it was the linked service or better characteristics had the coin, the higher would it price be given the demand. Thanks to smart contracts or coloured coins, anybody can create a cryptocurrency ICO, and the process is quite simple. The first thing to do is the creation of a whitepaper, a document that explains the idea that needs funding, stablish the number of tokens on sale, the earning minimum and maximum and the rest of requirements. This whitepaper should be attractive and convincing. The next stage would be to gather a team to develop the idea and create an explanatory web page. It will be necessary to promote the idea and the ICO to call investors' attention. Finally, the smart contract will be programmed to create the tokens and sell them according to the terms stablished in the initial whitepaper. (Academy B., 2022d)

5.3. CRYPTOCURRENCY MINING

The mining of cryptocurrencies consists of the validation of the transactions made by users; and are the miners who are responsible for choosing the transactions to include in each block and validate it. As seen before, there are different ways to validate a block and it will depend on the chain in which it is operating. In the case of Bitcoin, for example, the algorithm used is Proof of Work (PoW) miners must solve a cryptographic puzzle, for which a certain amount of computational power is needed, which is increasing, as the difficulty of the puzzle is adapted to the capacity of the users; whereas in Ethereum, despite having started with the same mechanism, it was changed to a Proof of Stake algorithm.

The blocks in Bitcoin are protected by what is known as a secure hash algorithm. As users of the network carry out transactions, the work of the miners is to select them to form a block[18] and verify the transactions in it. The blocks of the different miners do not have to be the same since they have chosen other transactions or have them in a different order, but they need to reach consensus[19] on the block that will be added to the chain. This is where the mentioned algorithm, known as SHA-256, comes in, which when it receives a file provides a set of alphanumeric characters that will always be identical as long as the input is exactly the same file. The input to be entered will be the block formed by the transactions plus a numerical value that the user will modify. The goal is to modify the number until the result of the output begins with a certain number of zeros. (Dot CSV, 2021)

When the hash is found, the block is added to the general chain. And the miners receive a reward, which is intended to "motivate" them to continue with their duty and to cover the high computational expenses of mining. On one hand, the miner receives in the case of Bitcoin, a number of coins, that

[18] Users pay a voluntary commission for the transactions, so the ones that will generate the most benefit for the miner are usually chosen first.

[19] Proof-of-work

nowadays is 6,25BTC (16.868,60USD/BTC[20]), but it reduces in half every 210.000 blocks (Halving effect[21]). On the other hand, the miner also gets the commission paid by the users in the transaction. As it has been explained, this fee is completely voluntary, and the users can decide if they want to pay it and how much they want to pay. The thing is, that, in times when the network is swamped, the miners, logically, decide which transactions they prefer to validate based on the commission.

Again, when talking about Bitcoin, the commission paid by users, as mentioned before, is voluntary. In addition, it does not depend on the amount being transferred, but rather on the weight of the file and the user's need. The transaction will take more or less time to be verified depending on the commission and the load on the network. Theoretically, and according to Fornell (2023), for a transaction with one or two outputs of about 250 bytes, the commission should be around 150 satoshis[22]. However, as mentioned before, it will depend on the load on the network and the size of the file. Likewise, the most popular exchanges already include calculators so that the user knows what the commission corresponds to their transaction according to its specific characteristics at that time.

In the case of Ethereum, it is completely different after the switch to a proof-of-stake consensus algorithm. Users will need to have at least 32ETH in their wallets for the platform to consider them as validators, and they will be randomly chosen to validate blocks that they have not themselves formed. The reward they will receive has not yet been published but will be received annually. (Ethereum.org, n. d.-b)

5.4. MAIN CRIPTOCURRENCIES

As it has been mentioned before, even though the first cryptocurrency, the Bitcoin, was created in august 18th 2008, the first transaction was not made until 2009 and had its boom since 2017. During that period virtual currencies became increasingly popular, contributing to the creation of a wide variety of new cryptocurrencies. In 2011 Litecoin is born, which in a couple of years, the 6th of December 2013 leads to the coin known as Dogecoin (DOGE). Months before, in April 2013 was born XRP from the Ripple protocol. Afterwards mid-2015 Ethereum (ETH) was born; and finally, on of September 23rd, 2017, Cardano (ADA) was created. (OSI, n. d.)

The coins mentioned in the previous paragraph are considered some of the most relevant in the "crypto universe." Currently, at the beginning of 2022, there are around 10,000 different cryptocurrencies. (Santaella, J. 2022)

Virtual currencies, as fiat currencies, have their own value and therefore their exchange rate with other coins. In the following table there are shown some of them in comparison to American dollars and euros.

[20] 21/12/2022 11.14

[21] The rewards are newly minted coins, so the amount of these as well as the Halving effect is part of the Bitcoin emission policy and will be discussed later in the chapter dedicated virtual currencies, in the Bitcoin section, where the pros and cons of this policy and its effectiveness will also be debated.

[22] 1 Satoshi = 0,00000001BTC

Table 5: Exchange rate between the main virtual currencies and the main traditional currencies

	USD	EUR
BTC	16.787,80 USD/BTC	16.127,78 EUR/BTC
ETH	1.262,41 USD/ETH	1.210,03 EUR/ETH
ADA	0,3393 USD/ADA	0,33 EUR/ADA
DOGE	0,0872 USD/DOGE	0,084 EUR/DOGE
BNB	276,1638 USD/BNB	264,83 EUR/BNB
XRP	0,3810 USD/XRP	0,37 EUR/XRP

Source: Own preparation based on Google finance (15/11/2022)

5.4.1. Bitcoin (BTC)

On October 31st, 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System" was published, giving birth in this moment to Bitcoin. The article was written by Satoshi Nakamoto, around whose figure has been a lot of mystery and speculations. The 9-page paper develops a system of electronic money transactions based on peer-to-peer (P2P) networks. These networks have been explained thoroughly in previous chapters, but is important to bear in mind their basis, the possibility for all the members to communicate among them and to operate as equals, without intermediaries or central figures. Therefore, Bitcoin put the all the financial system as we know it in check, as it had created a cash system that could manage without any central figure, allowing users to avoid banks or even central banks by operating between them as equals.

A few months later, in January of 2009, it was distributed the Bitcoin software, necessary in order to create a node; this was how the first Bitcoins where born. This software has been since the beginning open coded so anyone could download it without costs and have access to Bitcoin's source code. The first Bitcoin block, known as Genesis[23], contained 50 BTC and were assigned to S. Nakamoto; since this moment it is known that Nakamoto has not sold nor transfer his 50 Bitcoins. As it has been explained when talking about the characteristic anonymity and privacy protection of blockchain, the system preserves de anonymity of the users but every transaction is public, so the number attributable to Satoshi Nakamoto is known by all users even though we still do not know who he really is. In the Genesis block, encrypted, it was discovered to be the front page of The Times from January 3rd, in which it can be read "Chancellor on brink of second bailout for banks". This message not only portrayed the difficult situation of crisis that the whole world was living, but also added mystery to Nakamoto's enigmatic figure. (C. Domingo, 2022, p. 52)

The Bitcoin whitepaper was released in October 2008, shortly after the collapse of Lehman Brothers on September 15 of that year. This event led to the so-called Great Recession, in which numerous banks had to be rescued with newly issued money. These events affected the working lower and middle classes, thit is, it impoverished the already impoverished. All these events created a climate of discontent and protests that even reached Wall Street. How was it possible to create money to rescue the financial entities that had caused the crisis, allowing executives to leave their positions unpunished and with millionaire severance packages while hunger, evictions, and suicides increased? It is at this moment, in the midst of this climate of confusion and outrage, when Nakamoto publishes the Bitcoin whitepaper, providing society with a monetary system that would allow users to operate

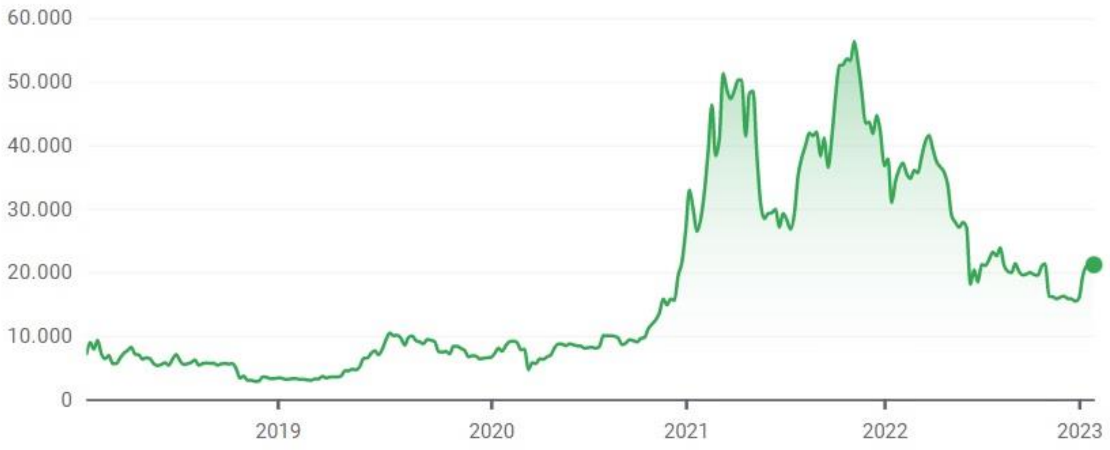
[23] The name Genesis refers to the first book of the Old Testament in the Christian Bible and therefore the first book of the Jewish Tora.

without the need for central entities that had caused so much confusion. The creator of the first virtual currency made his revolutionary ideology and position on the subject truly clear when he launched the Bitcoin project in January 2009 and published the already mentioned headline in the source code of the software, thus confirming the eminently political character of his invention. (S. Ammous, 2022)

The next year, on December 12th, 2010, Nakamoto published his last post, disappearing forever. Bitcoin circulation that year in the hands of investors is estimated at 2,630,000 BTC. In September 2012, the Bitcoin Foundation was born, an entity that can standardize, protect, inform, and promote the open-source protocol that makes up Bitcoin as a mechanism for accelerating global currency growth. The launch of the mentioned foundation provided support for the currency. The following years passed normally with small advances for the platform, such as the acceptance of virtual currency as a form of payment by Microsoft in 2013, or the announcement in 2016 by the Japanese Government through its Economic Cabinet, recognizing Bitcoin as a virtual currency and that it has a similar function to real money; In addition, that same year, the conclusions of several investigations were published, which showed that, since November 2013, through the improvement of the Blockchain-based trade chain, Bitcoin trade was no longer driven by illegal activities, but by legal companies, mainly payment platforms. In 2017, Russia announced the legalization and acceptance of cryptocurrencies as a means of payment and investment, and in June of that same year, the Bitcoin quotation exceeded the price of an ounce of gold for the first time in its history, breaking its historical maximum and reaching a quotation of 1,402.03 USD/BTC at the beginning of the year. The currency manages to close that same year reaching values of up to 19,000 USD/BTC. (Álvarez, L. J. 2019)

According to Cortés (2020), Bitcoin had risen more than 290% and had been breaking records almost every week, leading to 2020 being dubbed the year of Bitcoin. What no one expected was that these increases would continue throughout the following year, with its all-time high in November, approaching $70,000/BTC. These data clearly contrast with what happened during 2022, when Bitcoin has begun to suffer falls below $20,000/BTC, losing 70% of its value. (C. Castillo, 2022) At the moment, as of January 28, 2023, a slight upward trend is observed since the beginning of the year.

Graph 1: Bitcoin's evolution



Source: Own preparation based on Google finance 28/01/2023

S. Nakamoto's whitepaper stablishes that, thanks to the decentralised network, each user will store the information about all the money exchanges made among the Bitcoin users. It has been explained in the previous pages, but it is quite important to remind it, that any cryptocurrency, as it is

Bitcoin, Ether or any other, it is made up by the transaction register, distributed through all the network. The blocks at first may not be the same for each node, as they may have not received the same transactions or in the same order. So, in order for the register to be updated and equal for all the members in the network, bearing in mind that lack of a central figure makes it quite complicated, it appears the Proof of Work (PoW), together with blockchain.

It has been explained in the mining section how transactions are arranged into blocks so that they can be shared with the rest of the users of the network. The nodes will have to solve a "cryptographic puzzle" to decide which is de definitive and correct block, for which it will be used a secure hash algorithm (SHA), which having a series of data as an input (in this case will be the block that is trying to be validated), provides as an output an alphanumeric sequence. In the mentioned puzzle, the proof of work will consist in introducing together with the block of the transactions a number that will be modified until the resulting hash code starts with a sequence of 10 zeros. The first miner that resolves the puzzle receives a reward[24]. In the case that two blocks are validated at the same time, the block accepted will be the one of the miners that solves first the next block, this is, the longest chain. This method is secure and hard to manipulate, as in each block it is included the hash of the previous one, and if anybody would try to manipulate it, they would have to modify all the next blocks, this would delay the work, which would make the chain in question shorter than others' hence the blocks would not be accepted by the rest of the users. (Dot CSV, 2021)

Another of the tremendously revolutionary aspects of Bitcoin lies in its predetermined and unchangeable monetary rules and policy. In this way, we know that at no time will there be more than 21 million Bitcoins, as their issuance will be halted at this point. This can make the popular virtual currency the first strictly scarce good and the best store of value in history according to Smith (2021). The effects of this monetary policy are yet to be seen, but it will be explored in more detail in subsequent sections.

Everything around Satoshi Nakamoto, the creator of Bitcoin, is filled with mystery. This name is a pseudonym, under which it is not known if there is a single person or a group of people. Despite being numerous names under the possibility of being Nakamoto, but it is still a mystery nowadays; numerous hypotheses have been raised about who the person or people behind the figure of Nakamoto could be, but they have not been found yet. It is known that it must be a person or several people with extensive knowledge in cryptography, mathematics, computer science and economics, so known and reputable cryptographers have been pointed out as possible Nakamotos, but without success. Some people have claimed to be Satoshi Nakamoto, but none of these claims have been proven. Satoshi's identity is still unknown and have been topic of many discussions and investigations, but so far, all evidence seem to be inconclusive. The last thing known about Satoshi Nakamoto was in 2011, when he handed over the source code repository and network alert key to Gavin Andresen, a prominent developer, who later became lead developer at the Bitcoin Foundation and wrote to him that he had "moved on to other things"; and since then, there are no more signs of the cryptographer, since he stopped participating in online forums and debates that he was once very active. (C. Domingo, 2018 p. 53-56)

Unfortunately, little is known about Satoshi Nakamoto's background, beliefs, or motivations. Some of the information we do know about Satoshi comes from their activity on online forums and email exchanges with other members of the Bitcoin community. From their early posts and conversations, it seems that Satoshi was primarily interested in developing a decentralized digital currency that could be used as a medium of exchange without the need for a centralized intermediary, such as a

[24] The reward will be a number of Bitcoins stablished in Nakamoto's whitepaper plus the fee paid by the users to the miners to validate the transaction.

government or financial institution. Nakamoto was also focused on creating a system that would protect the privacy and security of its users and is said to have been concerned about the potential negative effects that centralization could have on the monetary system. Satoshi Nakamoto's political or social views are not clearly known. There is no clear evidence as to what political or philosophical ideology Satoshi is affiliated with. Some people have analysed his writings and his posts on forums and have come to some conclusions but is not fully confirmed. (Smith, G. S., 2021, p. 80-81)

It is known that S.N. has not sold the 50 BTC that composed the Genesis block and considering that being one of the principal nodes it has been issuing increased Bitcoins, and therefore receiving the corresponding fee of the validation of nodes, Nakamoto is today one of the richest people on Earth. He is estimated to have mined around one million Bitcoins in the early days of the network.

5.4.1.1." A Peer-to-Peer Electronic Cash System"

"A Peer-to-Peer Electronic Cash System" is the Bitcoin (BTC) whitepaper published by Satoshi Nakamoto in late October 2008. In this whitepaper, all the foundations and rules are established in order to launch Bitcoin and for its correct operation. Nakamoto's proposal was made public through an email sent to a list of renowned cryptographers. The author explains in the twelve sections of this document everything necessary to start the cryptocurrency. And distributes the information as follows:

1. *Introduction:* The whitepaper begins by discussing the limitations of traditional electronic payment systems and how they rely on central authorities to verify and process transactions.
2. *The Problem of Double-Spending:* The whitepaper explains that in a digital currency system, it is possible for a single unit of currency to be spent multiple times, a problem known as "double-spending." The paper discusses various solutions that have been proposed to address this issue, but notes that they all have their own limitations.
3. *A Peer-to-Peer Electronic Cash System:* The paper proposes a decentralized digital currency system called "bitcoin" that uses a peer-to-peer network to verify and record transactions. This approach allows for the transfer of value between individuals without the need for a central authority.
4. *The Blockchain:* The paper introduces the concept of the "blockchain," a public ledger that is a record of all bitcoin transactions. It explains how this ledger is used to verify and record transactions on the network.
5. *Proof-of-Work:* The paper explains how the Bitcoin network uses a proof-of-work system to verify and record transactions on the blockchain. This involves miners, who use specialized computers to solve complex mathematical problems in order to validate transactions and add them to the blockchain.
6. *Network:* The paper discusses the technical details of how the Bitcoin network operates, including how new transactions are broadcast to the network, how nodes verify transactions, and how they add new transactions to the blockchain.
7. *Incentive:* The paper explains how miners are incentivized to participate in the network by being rewarded with newly minted bitcoins for their efforts.
8. *Reclaiming Disk Space:* The paper discusses how the Bitcoin network can periodically discard older transaction data to reclaim disk space, while still maintaining the integrity of the blockchain.
9. *Simplified Payment Verification:* The paper introduces the concept of "simplified payment verification," which allows for lightweight nodes to verify transactions without downloading the entire blockchain.
10. *Combining and Splitting Value:* The paper discusses how bitcoin transactions can be structured to allow for the combining and splitting of value, enabling a wide range of financial transactions to be conducted on the network.

11. *Privacy:* The paper discusses the use of cryptographic techniques to ensure the privacy and security of transactions on the network.
12. *Conclusion:* The paper concludes by summarizing the key features and benefits of the Bitcoin system, including its decentralized nature, low transaction fees, and ability to transfer value without the need for a central authority.

5.4.1.2. The Halving effect.

A major difference between Bitcoin and fiat money is its monetary emission policy. In the case of fiat money, it is common for the corresponding monetary authorities to issue currency as part of their monetary policy in order to reach other objectives. In the case of Bitcoin, the emission policy was established in 2008 with the publication of the whitepaper and cannot be modified, so regardless of the needs of the market, the emission will be the same, thus avoiding inflation according to Nakamoto. It is known that, at the time of stopping emission, there will be 21 million BTC in circulation. The issuance of these and the time it takes to reach that figure will depend on the work of the miners. The reward that miners receive, as already explained, consists of user fees and new coin emissions. This "new coins" reward, which initially was 50BTCs, is reduced by half every 210,000 validated blocks. To date, there have been three halvings: November 20th, 2012, July 9th, 2016, and May 11th, 2020. According to studies, at the current validation rate, 21 million BTC would be reached in 2144. (Jiménez, 2021)

There are various theories about the long-term consequences of this policy. On the one hand, some believe that this event would not trigger a change in the price since speculation has already introduced the effect of this event into the price. On the other hand, being this the theory that weighs more, as it is also supported by the historical evolution of the value of the currency, experts argue that in the face of contractions in supply, an increase in price will occur given the consistency of demand.

5.4.2. Ether (ETH)

Is important to bear in mind before this subject is studied that Ethereum and Ether are not the same thing, therefore they must not be confused. Ethereum is the blockchain and Ether (ETH) is Ethereum's main asset, used to pay for transaction fees, as well as other services on the network.

Ether (ETH) was created along with the Ethereum network in 2015 by the programmer Vitalik Buterin. Ether shares a lot of characteristics with Bitcoin, and as Nakamoto's digital currency the user does not rely on a central figure in order to control the transactions. Ether is protected by cryptography which makes the money and all the transactions highly secure. It is a peer-to-peer system, so the transactions are made among equals. It is accessible for any user with an internet connexion and the units are divisible, so users do not have to buy a hole Ether if they do not want to.

The virtual currency is an important part of the Ethereum network because it is used to pay for the computing power required to run these applications. When developers want to build and run applications on the Ethereum network, they must pay for the computational resources required to do so using Ether. The supply of Ether is not controlled by any central authority, and it is generated through a process called mining. Miners use their computing power to verify transactions on the Ethereum network and are rewarded with Ether for their efforts. Such coin is also used as a digital currency, and it can be bought and sold on cryptocurrency exchanges just like any other cryptocurrency. It is one of the most widely traded cryptocurrencies, with a market capitalization that is second only to Bitcoin. The Ethereum network automatically adjusts the rate at which new Ether is created in response to changes in demand. This means that the amount of Ether that is issued each year will vary depending on a number of factors, including the overall level of activity on the network and the amount of computing power being used to process transactions. (Ethereum.org, n. d.-j)

Unlike Bitcoin (BTC), Ethereum does not wave a fixed issuance policy, to understand how it has been, it is shown the historical evolution of the block rewards:

- Block 0 to Block 4,369,999: 5 Ether
- Block 4,370,000 to 7,280,000: 3 Ether (changed via EIP-649)
- Block 7,280,000 to now: 2 Ether (changed via EIP-1234)

Ethereum's monetary policy is best described as "minimum issuance to secure the network". The network has never increased the issuance, always decreased it; in fact, the algorithm change, form proof-of-work to proof-of-stake had as one of the objectives to reduce the issuance. Ethereum's current yearly network issuance is approximately 4.5%. Overall, the Ethereum issuance policy is designed to strike a balance between ensuring that there are enough ether tokens in circulation to support the network's growing user base and maintaining the stability and value of the ether cryptocurrency. (Ethereum’s Monetary Policy, n. d.)

5.4.3. Cardano (ADA)

Cardano is a decentralized, open source blockchain platform and cryptocurrency focused on providing a more secure and scalable environment for the development and execution of smart contracts and dApps. (*Cardano*, n. d.) Cardano is built on a unique proof-of-stake (PoS) consensus algorithm called Ouroboros, which is designed to be more energy-efficient and secure than other PoS algorithms. It also has a multi-layer architecture that separates the settlement layer, where transactions are recorded and verified, from the computation layer, where smart contracts and dApps are executed. This allows for more flexibility and scalability on the platform. Cardano is being developed by a global team of researchers, engineers, and developers led by Charles Hoskinson, one of the co-founders of Ethereum. The project is being built on a solid foundation of academic research, and it is being designed to address some of the scalability and sustainability challenges faced by other blockchain platforms. (Estrategias de Inversión, n. d.-a)

The native cryptocurrency of the Cardano network is called Ada, and it is used to pay for transaction fees and other services on the platform. Ada can be bought and sold on cryptocurrency exchanges, and it is ranked among the top ten digital currencies by market capitalization.

5.4.4. Dogecoin (DOGE)

Dogecoin is a decentralized, open-source cryptocurrency that was created as a joke in 2013. It was named after the "Doge" meme, which features a Shiba Inu dog, and its logo is a stylized version of the dog from the meme. Despite its origins as a joke, Dogecoin has gained a large and enthusiastic community of supporters and has become a legitimate cryptocurrency with a market capitalization that is ranked among the top fifty cryptocurrencies. (Dogecoin n. d.)

Such coin is based on the same technology as Bitcoin, with a few key differences. It has a faster block time (the time it takes for a transaction to be verified and added to the blockchain) and a higher supply of coins. It also uses a different mining algorithm, called Scrypt, which is designed to be more accessible to a wider range of users. (Fernández, 2022)

Dogecoin was initially used as a means of tipping content creators and other users on social media platforms, as a way to show appreciation for their work. It has since gained wider adoption and is now used for a variety of purposes, including charitable donations and online transactions.

4.4.5. Binance Coin (BNB)

Binance Coin (BNB) is the native cryptocurrency of the Binance platform, which is one of the largest and most popular exchanges in the world. Binance is a decentralized exchange that allows users to trade cryptocurrencies in a secure and decentralized environment.

Binance Coin was initially created as an ERC-20 token on the Ethereum blockchain, but it has since migrated to its own blockchain, called Binance Chain. BNB is used as a utility token on the Binance platform, and it provides several benefits to users, including reduced trading fees and access to unique features on the platform. It is ranked among the top twenty cryptocurrencies by market capitalization. It is also used as a means of payment for various goods and services, and it can be stored in a wide range of cryptocurrency wallets. (Binance n. d.)

5.4.6. XRP

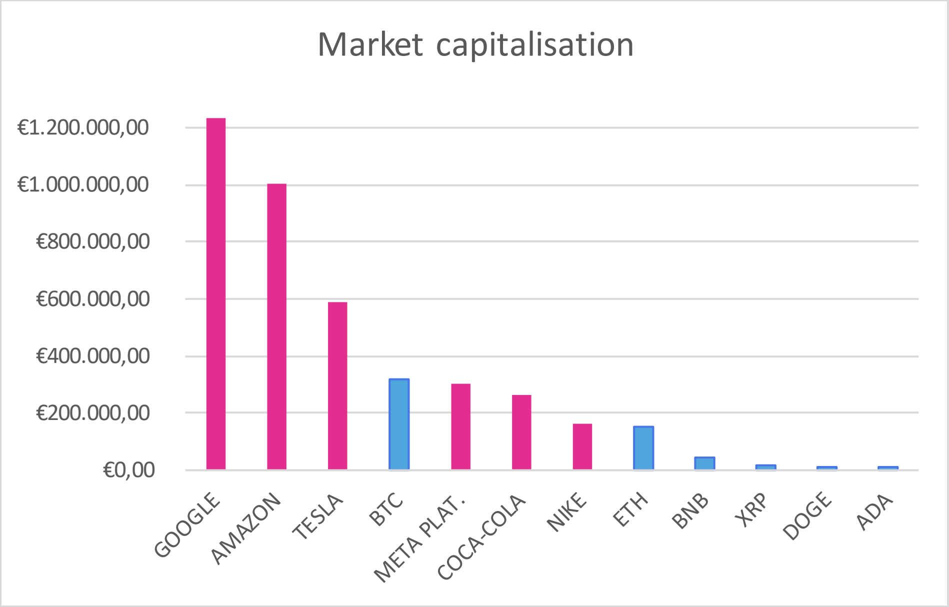
XRP is a digital asset and a cryptocurrency that is native to the Ripple payment protocol. It is used to facilitate transactions on the Ripple network, which is a decentralized, real-time gross settlement system (RTGS) that allows for the instant and secure transfer of money around the world. The Ripple network is designed to be faster and more efficient than existing payment systems, and it is used by a growing number of banks, financial institutions, and other organizations. XRP acts as a bridge currency on the Ripple network, allowing for the seamless and efficient exchange of different currencies. XRP is also used as a digital currency, and it can be bought and sold on cryptocurrency exchanges. It is the third-largest cryptocurrency by market capitalization, after Bitcoin and Ether. (CriptoNoticias, 2021)

As mentioned, the Ripple protocol allows for instant and secure transfer of money around the world. It was developed by the company Ripple Labs, and it uses a distributed consensus ledger to enable efficient and low-cost transactions between different currencies. Such protocol uses a network of nodes, which are run by a consortium of participating financial institutions, to validate and process transactions on the network. It uses a unique consensus algorithm that allows transactions to be processed quickly and securely, without the need for mining or other energy-intensive processes.

It is already known the relevance that virtual currencies have acquired in the last years, and in order to analyse objectively the importance of those currencies they will be compared their market capitalization with some of the most relevant companies of all around the globe. "Market Capitalization (Market Cap) is the most recent market value of a company's outstanding shares. The Market Cap is equal to the current share price multiplied by the number of shares outstanding." (Corporate Finance Institute, 2022) Given the market capitalization definition for a listed company and according to the Ethereum official webpage, the market capitalization of a cryptocurrency is the total number of tokens multiplied by the value of each token. In the graph below, there are shown some of the world's most important companies' market capitalization and the ones of the most relevant cryptocurrencies.

After this comparison, we can appreciate Bitcoins' value, just after Tesla and presenting values similar to Meta Platforms (Facebook). Ether (ETH) does not lag behind, following close-up Nike, with a capitalization over 150 billion USD. The other virtual currencies shown in the graph even though they might appear to fall a little behind in terms of capitalization, they are incredibly relevant in the world of cryptocurrencies; in fact, their capitalization is similar to companies such as LG electronics or Acciona.

Graph 2: Market capitalisation



Source: Own elaboration based on CoinMarketCap (n. d.-a)

5.5. STABLECOINS

It is a new kind of cryptocurrency, that instead of fluctuating by itself, it is indexed to another more stable asset, which usually is the dollar (USD). There is a whole lot of virtual currencies built over the Ethereum network, due to the simplicity mentioned before with smart contracts. Furthermore, it is faster and cheaper than fiat money. But the fact of indexed to a fiat currency makes it no decentralised at all, as it relies on a centralised value. (Ethereum.org, n. d.-f)

Although stablecoins share tons of characteristics with other virtual currencies, its value is considerably more stable and as do not suffer from volatility; this means that they are global and do not need more than an internet connexion to send or receive them from any part of the world instantly. They can be used to make transactions or exchange for other tokens and are protected by cryptography[25]; all of it with the advantage of its stability.

There are thousands of Stablecoins, but in terms of market capitalization this are the most important ones:

- Tether (65,386,972,536$) "Tether tokens are assets that move across the blockchain just as easily as other digital currencies but that are pegged to real-world currencies on a 1-to-1 basis." (tether.to)
- USD Coin (44,178,602,373$) "USD Coin (USDC) is a type of cryptocurrency that is referred to as a stable coin. You can always redeem 1 USD Coin for US$1.00, giving it a stable price." (coinbase.com/usdc)
- Binance USD (22,410,679,339$) "BUSD is fully regulated by a primary prudential regulator - the New York State Department of Financial Services (NYDFS), offering the highest level of consumer protection. All reserves are held 100% in cash and cash equivalents; hence customer funds are always available for 1:1 redemption." (Binance.com)

[25] Procedure that, using a key algorithm, transforms a message without paying attention to its linguistic structure or meaning. It provided an infallible mechanism for encoding the rules of the protocol that govern the system. (Preukschat et al., 2017)

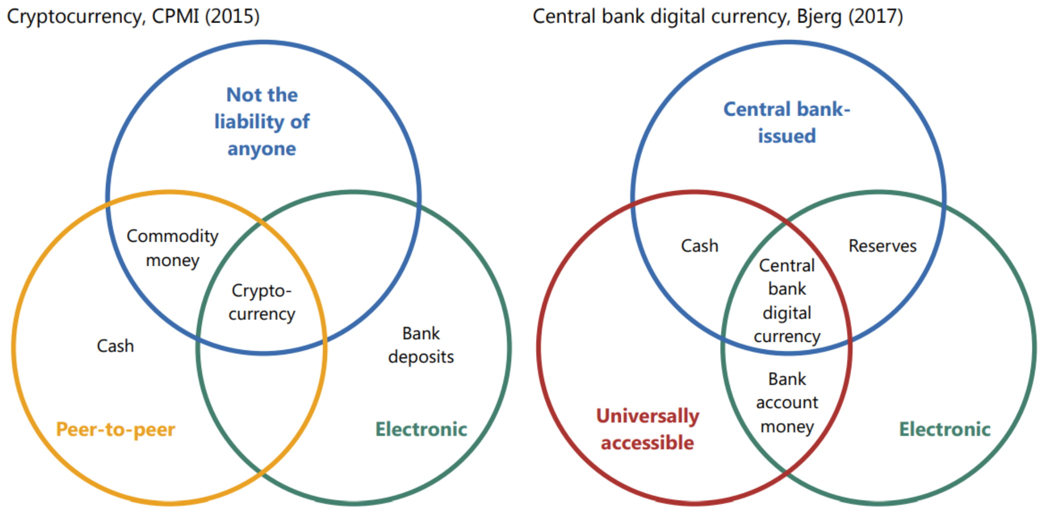
- Dai (5,262,827,342$) Is the first decentralised stablecoin with a 1:1 value with respect to the USD. Is one of the biggest and most important projects in the "crypto-universe" and in the DeFi (Decentralised Finance). (Gastón Í., 2022)
- Frax (1,178,048,588$) "The Frax Protocol introduced the world to the concept of a cryptocurrency being partially backed by collateral and partially stabilized algorithmically. With the vision to create highly scalable, decentralized money in place of fixed-supply digital assets like BTC." (Frax.finance)

5.6. CENTRAL BANK CRYPTOCURRECIES (CBCC)

Central bank cryptocurrencies (CBCCs) are digital versions of fiat currencies issued and backed by central banks. They are designed to function as a form of electronic money that can be used for a variety of purposes, including making payments, transferring funds, and storing value. This kind of currency it is known as public currency, and Bitcoin and Ether are private digital currencies. One of the main differences between CBCCs and other cryptocurrencies, such as Bitcoin and Ethereum, is that CBCCs are issued and backed by central banks, which are trusted and stable institutions that serve as the backbone of the traditional financial system. This means that CBCCs are likely to be more stable and less volatile than other cryptocurrencies, which can be subject to large price swings due to market speculation and other factors.

The following chart shows the distinctive characteristics of cryptocurrencies according to the CPMI report of 2015 and central bank digital currencies so that their similarities and differences can be properly appreciated. In addition, other forms of money and their key features are also shown.

Graph 3: Two taxonomies of new forms of currency



(Source: BIS.org, 2017a)

According to the taxonomy provided by the BIS (2017a), Central Bank Cryptocurrencies (CBCCs) are electronic money and operate peer-to-peer, just like regular digital currencies, with the difference that the former is issued by a central bank rather than by an algorithm. It is necessary to differentiate between wholesale and retail CBCCs, with the difference between them, according to this classification offered by the BIS, being access to them, as retail CBCCs can be accessed by any user, unlike wholesale CBCCs, that would be only for very high-volume transactions, like those between banks.

As mentioned in the BIS article (2017a), it proposes two different types of CBCCs: a retail CBCC, easily accessible to all users, designed as a payment instrument for transactions between users; and on the other hand, a restricted access digital settlement token for wholesale payment applications, which are high-value and priority transactions such as interbank transfers. At the time of publication of the article in question, although there were various versions and projects for retail use currencies, none had been successfully launched; although Fedcoin had been the most advanced and widely debated. In the case of this specific currency, only the Federal Reserve could generate Fedcoins, whose convertibility with cash and reserves would be one-to-one. Fedcoins would only be created (or destroyed) if an equivalent amount of cash or reserves were also destroyed (or created). It is particularly important to note that although transactions with this currency would be decentralized, the issuance would be completely centralized. Fedcoin has the potential to eliminate the high volatility that characterizes digital currencies. On the other hand, as far as wholesale payment currencies are concerned, there are already banks such as Canada's Jasper or Singapore's Ubin that have conducted tests for their launch. Both projects propose an individual and immediate payment processing system. Access to these wholesale systems requires authorization.

5.7. VOLATILITY

It has been mentioned in numerous occasions in the previous pages the concept of volatility, which according to Oxford Dictionaries is “the quality in a situation of being likely to change suddenly.” Volatility is usually measured with assets’ prices’ standard deviation. It is quite important to highlight that it is an historical measure, not a prediction about the future, although volatile assets tend to continue being volatile. One of the most known volatility indexes of markets is VIX, which measures volatility through weighted wallet of call and put options on S&P 500.

Volatility is one of the most notorious characteristics of virtual currencies, which can traduce in an elevated risk for investors. To compare the volatility of these products the Australian firm T3Index has created BitVol and EthVol, which measure the volatility of Bitcoin and Ethereum respectively, with a design similar to VIX, which allows the comparison of the volatility of both values. Thanks to those indicators’ values, it can be appreciated that in most cases the volatility of Bitcoin is three or four times the American Index. (T3 Index, 2022)

In 2019 BitVol reached its annual minimum at 45.4, being the Vix’s minimum the same year 11.54. A similar situation occurred in 2020, when due to the pandemic all the stock markets collapsed, Vix beat records with 82.69, but that was nothing compared to the 190.28 points of the BitVol. In the last months it was registered a notorious upturn the 12th of May 2022, where BitVol’s value was 109.82, being Vix’s 31.77 points. This happened in a time where there were high tensions between Russia and Ukraine and an increasing inflation. In fact, these where some of the most relevant headlines of the 11th and the 12th: “The Bank of Mexico increases the interest rate to 7% in order to restrain a skyrocket inflation”, ”Russia will cut of the delivery of gas to Europe through Poland” (Suárez, K. 2022), ”The OTAN promises Finland a “fast and fluid” adhesion and offers protection since the formal request to the official entrance”, ”Petrol’s and diesel’s prices escalate to a new record” (Gómez M. V. 2022), ”The EBA’s president about the regulation of cryptocurrencies “the objective is not to kill innovation but to use it in an appropriate way”” (Sánchez, A. 2022), ”The CEB sets the stage for an increase of interest rates in July due to the accelerating inflation”. (Pellicer, L. 2022)

5.8. COULD CRYPTOCURRENCIES REPLACE FIAT MONEY?

In this section, we will develop one of the objectives set out for this work: the analysis of the viability of virtual currencies compared to fiat money as part of the study of the possible future of the tools developed from blockchain technology; for this purpose, the opinions of different authors both in favour and against will be used, as well as some of the arguments of those who oppose them.

As mentioned in previous sections, according to C. Domingo's ideas, money, since its creation and its most rudimentary uses, has fulfilled three basic functions for its proper functioning. The currency in question must have the ability to store value, that is, it can be useful in the future; it must also be interchangeable, which implies the ability to make transactions; and finally, it must be able to be used as a reference value in order to establish prices. With these characteristics in mind, they will be applied to cryptocurrencies to evaluate their viability and whether they can be considered money or not. First of all, we know that virtual currencies have the ability to store value, it is not an abstract issue, but rather a user will have a certain amount of Bitcoin, Ether or the cryptocurrency in question reflected in their wallet; the user will continue to hold it over time and the number of coins they own will not change, but their equivalence will. Although this also happens with fiat money, its consequences are more noticeable in the case of digital currencies, given their high volatility, as already mentioned in previous sections, so even though the user in question still sees 2BTC in their wallet, the value of them can vary by thousands of USD in a matter of weeks, or even days. Second, since the inception of Bitcoin (BTC), transactions of greater or lesser value have been carried out successfully, in fact, one of the first transactions made with Bitcoin was the purchase of a pizza by the American computer programmer for 10,000BTC, which at the time was equivalent to 25USD. Although the above example deals with Bitcoin individually, payments can also be made with other currencies as seen in previous paragraphs, in the case of the Ethereum platform with Ether for example. Third, regarding the ability to be a reference value and put prices on items that are intended to be traded, given the aforementioned volatility, this is complicated with cryptocurrencies as the value can vary significantly from one day to the next. To support this idea, we will use the case of Tesla, which was widely reported when the company began to accept Bitcoin as a payment method for the purchase of its cars, although this possibility only lasted 50 days, according to Elon Musk on his Twitter account, due to the environmental impact of mining the well-known virtual currency. Today (January 2023) a Tesla Model S costs $96,590, which is equivalent to 5.6BTC, but in early May 2021, when Musk announced accepting the digital currency as a payment method, the value of a Tesla was less than 1.5BTC. So, in this case, Bitcoin could not be used as a reference value, which applies to other digital currencies as they share the high volatility

On the other hand, if we were to support the ideas of S. Ammous and C. Menger, what characterizes money is its "sellability", which will depend on its ability to be divided, to be transported, and its duration over time. When applying these characteristics to cryptocurrencies, we obtain that divisibility depends on what is stipulated in the code of each of them; in the case of Bitcoin, the smallest unit it can be divided into is a Satoshi, which is equivalent to 0.000000001 BTC, and in the case of Ether it is a Wei, equivalent to 0.0000000000000000001 ETH. As for the ability to be transported, it is not complicated, users can store their coins in wallets or on hard drives, and neither option poses an obstacle for its transportation. Finally, we must evaluate its durability over time, once the coin is stored, it does not deteriorate or lose value or qualities, as long as the user does not lose access to them, as it is estimated that a large part of the Bitcoins issued are currently inaccessible as users have lost the units in which they stored them or have forgotten the access passwords.

Therefore, if we were to evaluate whether cryptocurrencies meet the necessary requirements to replace fiat money in the future based on the necessary characteristics of it according to the mentioned authors, it can be concluded that based on C. Domingo's ideas, cryptocurrencies could not replace traditional money because they do not meet the requirements of it given their extremely high volatility, a factor that may change in the future if values stabilize. On the other hand, if we took into account S. Ammous' ideology, the innovative virtual currencies would meet the necessary conditions to replace fiat money, so it all depends on the users.

Another aspect that concerns the general public regarding the adoption of cryptocurrencies in the economy is the large environmental impact generated by mining techniques such as Proof-of-Work (PoW) explained in the first pages of this work. The creation of huge computer farms consumes a lot of computational power and consequently a lot of energy, which generates a strong environmental impact that already has its detractors such as Elon Musk. On the other hand, and as mentioned in the section dedicated to this same network, platforms such as Ethereum decided to change their algorithm to one based on Proof-of-Stake (PoS) to reduce its environmental impact. The difference between both platforms is that Ethereum is constantly evolving and updating, offering constant improvements to users, while Bitcoin is clinging to its whitepaper, created in 2008, without the possibility of change and without knowing who or where its creator is, hidden under the pseudonym of Satoshi Nakamoto who has not been heard from in more than 10 years.

Finally, another argument of the detractors of virtual currencies is the high rate of crime that they hide given the opaqueness they provide to users, since although all the transactions that are carried out in the blockchain in question are public and freely accessible to anyone who wants it, the user names under which the transactions are carried out give the user total anonymity to operate under.

For months now, major figures in the global economy have warned of the dangers of Bitcoin and speculation with it. In an interview with the BBC World Service's Business Daily program, Nobel Prize in Economics winner Joseph Stiglitz discouraged investment in Bitcoin, justifying it thus: "Why do people want bitcoins? Why do people want an alternative currency? The real reason people want an alternative currency is to participate in vile activities: money laundering, tax evasion. What we really should do is require the same transparency in financial transactions with bitcoins that we have with banks." If this were done, he believes, the Bitcoin market "would simply collapse."

The Europol published a report on cryptocurrencies and criminal finances which notes that while cryptocurrencies have the potential to bring benefits to the financial sector and economy, they also present opportunities for criminal organizations to launder money and finance illegal activities. According to this report in recent years, the use of cryptocurrencies in criminal activities has increased significantly, with some estimates suggesting that around 4-6% of all Bitcoin transactions are related to illegal activity and most criminal cases involving cryptocurrencies involve drug trafficking, followed by fraud and cybercrime. The report also notes that the use of cryptocurrencies in extortion, ransomware attacks, and other forms of cybercrime is on the rise. Additionally, the report highlights the challenges that law enforcement agencies face in tracking and investigating crimes involving cryptocurrencies, including the lack of regulation and the anonymity of transactions. The report emphasizes the need for a coordinated approach to addressing the criminal use of cryptocurrencies, including increased cooperation between law enforcement agencies and the private sector, as well as the implementation of regulatory measures to increase transparency and mitigate the risk of abuse. The report notes that while the use of cryptocurrencies in criminal activity is a concern, it is important to also recognize the potential benefits of cryptocurrencies and the importance of striking a balance between regulation and innovation. (Europol spotlight 2021)

In the CMPI[26] (BIS, 2015) there are stated some ideas about the issue being discussed in the previous paragraphs. It is defended that virtual currencies have the potential to significantly impact financial markets and the wider economy. These currencies can disrupt current business models and systems and create new economic interactions. In particular, they can facilitate certain retail payment transactions (such as e-commerce, cross-border transactions, and person-to-person payments) and make them faster and cheaper for consumers and merchants. However, their implications for payment system efficiency and potential risks are yet to be determined. These digital currencies can also raise policy issues for central banks and other authorities. Despite that, the use of distributed ledgers for peer-to-peer value transfers without a trusted third party has been proven possible in recent years by some digital currency schemes, it suggests that the use of distributed ledger technology may improve the efficiency of payment services and financial market infrastructures in situations where intermediation through a central party is not cost-effective.

[26] Committee on Payments and Market Infrastructure

CHAPTER VI: CONCLUSIONS

Throughout this work, the concept of blockchain has been explored as it was the main objective of it. In the first section, the mentioned main objective of this work was explained, which was to analyse the feasibility of this technology in our society and its possibilities. That is why the final chapter is reserved for reflecting on the topic, briefly commenting on the information obtained and trying to answer the questions raised and draw relevant conclusions. As reflected in the introduction of this work, raising the question of whether blockchain has the capacity to transform our technological relationships as we know them, forces us to raise other objectives, which can help us understand many questions to later focus on the main objective.

In the first chapter, where the objective was to analyse the characteristics of the technology, attention was focused on the definition of blockchain and the concepts surrounding it. Therefore, it is known that blockchain is a data storage technology managed by a decentralized network where nodes operate equally, transparently, anonymously, and very securely. The fact of being so secure is based on decentralized networks helps to avoid major failures and network crashes. If a node fails, it does not affect the network. The chains are secure and once information is stored, it cannot be changed without changing the entire chain. The chains are transparent but respect user privacy, allowing anyone to view the transactions but not knowing the identity of the user unless revealed.

The following objective has been to study different blockchain platforms, which leaves us with the most important blockchains, including Ethereum, and on the other hand, exchanges, which although some of them are not supported by the technology used in this work, deserve special attention since they make a very important part of digital currencies possible: their buying and selling. Despite the brief mention of exchanges and other chains of great relevance, the chapter has focused on Ethereum and its possibilities for development. In addition to hosting Ether (ETH), the most relevant virtual currency after Bitcoin, it is the chain that supports the most NFTs, as well as having brought together many users and allowed the creation of, for example, insurance for farmers in Kenya or provided funds for users who wanted to launch a project. As far as is known, Ethereum is a very wide network with a large number of users who drive it and benefit from it. Its incredible development since 2015 can be surprising, and by not focusing solely on the exchange of private currencies, it has much more room to grow, as it is demonstrating today.

As has been read in Chapter III, dedicated to the tools derived from blockchain, these have arisen to meet the needs of users over time. This chapter initially aims to explain the tools born after blockchain technology and based on it, and then to evaluate its current and future development. Furthermore, starting from the base of blockchain technology, the derived tools are the ones that give meaning to this work and allow the multiple applications that will be seen later, as despite the usefulness of blockchain itself, it is these tools, such as smart contracts or virtual currencies, that have the ability to replace elements of daily life and transform processes.

The last sub-objective in this work has been the analysis of the application of the tools developed in the previous chapter, which subsequently leads to the main objective of studying the feasibility of blockchain technology in our society as a substitute for many processes. As has been seen in the chapter dedicated to this topic, today there are many applications for both smart contracts, NFTs, and cryptocurrencies, some with more trajectory than others. It has already been seen in the development of the topic how many companies and platforms already apply these tools in their daily processes, with long trajectories in areas of logistics, banking, insurance, legality... and that new business models can be opened based on the mentioned tools to meet the new needs of users that without these tools could not be met.

However, it is possible that the blockchain technology has the ability to change the world; as private currencies disappear, a transition could be made towards decentralized public currencies, such as CBDCs. The capabilities demonstrated by the Ethereum platform could be replicated in other organizations, for example, the social security system, where contributions from entrepreneurs and workers would be managed in an automated and decentralized manner, thereby avoiding many delays in pension and unemployment benefits payments. In insurance agencies, it is already possible to use blockchain technology thanks to smart contracts; if they have been adapted to secure user wallets on Ethereum, what prevents us from drafting intelligent contracts to insure the house or car, so that user A (insurer) commits to insuring user B (insured) in a list of predetermined cases. In this way, it operates between equals, the contract is recorded on the blockchain and disputes over the nuances of the contract are avoided. If the conditions are met, it is automatically executed without the intervention of either the insurer or the insured. This, combined with the internet of things, which can impartially inform about the state of the insured object and notify of the failure, so that it is infallibly known if it falls within the coverage of the insurance.

Throughout this work, the generalized feeling regarding the topic is that it is a promising technology, which perhaps, in the case of private currencies, may not have as much trajectory as has been seen in recent months and reminds us slightly of the "dot com" bubble, while the base technology, which in this case is blockchain, remains while some of the currencies such as Bitcoin may eventually disappear. What is clear is that there is still much to develop on this issue, there are thousands of possibilities to explore, but that prior to, the first applications of this technology have been satisfactory.

BIBLIOGRAPHY

Academy, B. (2022a, May 6th). *¿Qué es un nodo?* Bit2Me Academy. Recovered on June 6th, 2022, from https://academy.bit2me.com/que-es-un-nodo/

Academy, B. (2022a, August 26th). *¿Qué es Ethereum (ETH)?* Bit2Me Academy. https://academy.bit2me.com/que-es-ethereum-eth-criptomoneda/

Academy, B. (2022b, August 26th). *¿Qué es un token?* Bit2Me Academy. https://academy.bit2me.com/que-es-un-token/

Academy, B. (2022c, August 26th). *¿Qué es una Colored Coin?* Bit2Me Academy. https://academy.bit2me.com/que-es-una-colored-coin/

Academy, B. (2022d, September 28th). *¿Qué son las ICO de criptomonedas?* Bit2Me Academy. https://academy.bit2me.com/que-son-las-ico-criptomonedas/

Academy, B. (2023a, January 16th). *¿Qué es un exchange de criptomonedas?* Bit2Me Academy. Recovered on January 29th, 2023, from https://academy.bit2me.com/que-es-exchange-criptomonedas/

Academy, B. (2023b, January 17th). *¿Qué es un Security Token?* Bit2Me Academy. Recovered on January 23rd, 2023, from https://academy.bit2me.com/que-es-un-security-token/

ADIAT. (n. d.). *17 APLICACIONES DE LA TECNOLOGÍA BLOCKCHAIN*. Recovered on December 19th, 2022, from https://adiat.org/17-aplicaciones-de-la-tecnologia-blockchain

Alphabet Inc Class A (GOOGL) Stock Price & News. (n. d.). Google Finance. https://www.google.com/finance/quote/GOOGL:NASDAQ?sa=X&ucbcb=1

Álvarez, L. J. (2019). *Cryptocurrencies: Evolution, growth and perspectives of Bitcoin.* Universidad Nacional de Asunción.

Ammous, S. (2022). *El patrón Bitcoin* (Rev. ed.). Deusto.

Antiporovich, N. (2022, October 14th). *El Merge llegó a Ethereum: no más minería.* CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas. Recovered on December 21st, 2022, from https://www.criptonoticias.com/tecnologia/el-merge-llego-ethereum-no-mas-mineria/

Apd, R. (2020, May 28th). *7 aplicaciones de la tecnología blockchain.* APD España. Recovered on December 19th, 2022, from https://www.apd.es/aplicaciones-blockchain/

Apple Inc (AAPL) Stock Price & News. (n. d.). Google Finance. https://www.google.com/finance/quote/AAPL:NASDAQ?sa=X&ucbcb=1

Aranda, J. L. (2022, May 12th). *Los precios de la gasolina y el diésel escalan hasta un nuevo récord.* El País. Recovered on June 5th 2022, from https://elpais.com/economia/2022-05-12/los-precios-de-la-gasolina-y-el-diesel-escalan-hasta-un-nuevo-record.html

Ashley, C. (2023, January 24th). *KwikTrust - Create, Validate, and Protect Your Digital Assets - KwikTrust. KwikTrust - Sign, Send and Store Your Documents.* Recovered on January 29th, 2023, from https://kwiktrust.com/

Barría, C. (2017, 18th). *Cuáles fueron las 5 peores burbujas de la historia que estremecieron la economía mundial (y por qué nos siguen dando terror)*. BBC News Mundo. Recovered on September 16th, 2022, from https://www.bbc.com/mundo/noticias-42374461

BBC News Mundo. (2017, December 1st). *Por qué el Premio Nobel de Economía Joseph Stiglitz cree que se deben prohibir los bitcoins.* BBC News Mundo. https://www.bbc.com/mundo/noticias-42196322

Binance - Cryptocurrency Exchange. (n. d.). *Binance | Cryptocurrency ciExchange.* Binance. Recovered on November 30th, 2022, from https://www.binance.com/en/busd

Binance. (n. d.). *¿Qué es BNB y para qué se usa?* Binance. https://www.binance.com/es/bnb

BIS. (2015). *Digital currencies*. In BIS (ISBN 978-92-9197-385-9). Recovered on November 6th, 2022, from https://www.bis.org/cpmi/publ/d137.pdf

BIS. (2017a) Central bank cryptocurrencies. Recovered on September 3rd, 2022, from https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf

BIS. (2017b). Quarterly Review. In BIS. Recovered on February 14th, 2023, from https://www.bis.org/publ/qtrpdf/r_qt1709y.htm

B., G. (2022, July 20th). *Oasis.app Knowledge Base.* Oasis.app. Recovered on November 29th, 2022, from https://kb.oasis.app/help/what-is-dai

Blockchain definition - Google Zoeken. (n. d.). Recovered on November 10th, 2022, from https://www.google.com/search?q=blockchain+definition

Buterin, V. (2013). *Ethereum white paper.* GitHub repository, 1, 22-23.

Chainalysis. (2022, December 13th). *La plataforma de datos Blockchain.* Chainalysis. Recovered on December 29th, 2022, from https://www.chainalysis.com/es/

Chen, J. (2022, April 19th). *What Is Fiat Money?* Investopedia. Recovered on August 12th, 2022, from https://www.investopedia.com/terms/f/fiatmoney.asp

Chohan, U. (2015). *The double spending problem and cryptocurrencies* [Discussion Paper]. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174

Cambridge Business English Dictionary. (2022). *Money.* In Cambridge Dictionary. https://dictionary.cambridge.org/es/diccionario/ingles/money

Cambridge Dictionary. (2022). *Nonfungible definition.* Cambridge Dictionary. Recovered on December 19th, 2022, from https://dictionary.cambridge.org/dictionary/english/nonfungible

Cardano. (n. d.). *Cardano*. https://cardano.org/

Coinbase - USDC. (n. d.). *Coinbase.* Recovered on November 27th, 2022, from https://www.coinbase.com/usdc

CoinMarketCap. (n. d.-a). *Precios, gráficos y capitalizaciones de mercado de criptomonedas.* https://coinmarketcap.com/es/

CoinMarketCap (n. d.-b). *Principales exchanges de criptomonedas clasificados por volumen*. Recovered on January 30th, 2023, from https://coinmarketcap.com/es/rankings/exchanges/

Cointelegraph. (2021a, July 10th). *¿Qué es Ripple? Todo lo que necesitas saber.* Recovered on January 23rd, 2023, from https://es.cointelegraph.com/ripple-101/what-is-ripple

Cointelegraph. (2021b, August 5th). *Qué es Ripple - Últimas noticias sobre Ripple.* Recovered on January 26th, 2023, from https://es.cointelegraph.com/tags/ripple

Companies ranked by Market Cap - CompaniesMarketCap.com. (n. d.). https://companiesmarketcap.com/

Corporate Finance Institute. (2022, November 13th). *Market Capitalization*. https://corporatefinanceinstitute.com/resources/valuation/what-is-market-capitalization/

Cortés, L. A. (2020, December 30th). *El bitcoin sube más de un 290% en 2020: cerrará su mejor ejercicio en tres años.* elEconomista.es. Recovered on January 28th 2022, from https://www.eleconomista.es/divisas/noticias/10968636/12/20/El-bitcoin-sube-un-287-en-2020-cierra-su-mejor-ejercicio-en-tres-anos.html

CriptoNoticias. (2021, March 25th). *¿Qué es Ripple (XRP)? CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas*. Recovered on January 25th, 2023, from https://www.criptonoticias.com/que-es-ripple-xrp/

Cryptocurrency definition - Google Zoeken. (n. d.). Recovered on December 10th, 2022, from https://www.google.com/search?q=cryptocurrency+definition

Cuadrado, C. (2022, April 22nd). *Aplicaciones de blockchain – 11 usos de blockchain que no conocías.* Armadillo Amarillo. Recovered on December 20th 2022, from https://www.armadilloamarillo.com/blog/aplicaciones-de-blockchain-11-usos-de-blockchain-que-no-conocias/

Cuesta, J. G., & Sevillano, E. G. (2022, May 12th). *Rusia cortará el envío de gas a Europa a través de Polonia.* El País. Recovered on June 5th 2022, from https://elpais.com/internacional/2022-05-12/rusia-cortara-el-envio-de-gas-a-europa-a-traves-de-polonia.html

Del Amo, M. (2022, October 26th). *'Blockchain': la gran promesa tecnológica para Internet y los negocios.* Retina. Recovered on January 14th 2023, from https://retinatendencias.com/tecno-para-mortales/blockchain-la-gran-promesa-tecnologica-para-internet-y-los-negocios/

Del Castillo, C. (2022, June 21st). *El Bitcoin retrocede a 2020 y profundiza el criptopánico: «Muchos proyectos van a caer»*. elDiario.es. Recovered on January 28th 2023, from https://www.eldiario.es/tecnologia/bitcoin-retrocede-profundiza-criptopanico-proyectos-caer_1_9100621.html

Dogecoin. (n. d.). Dogecoin. https://dogecoin.com/

Domingo, C. (2018). *Todo lo que querías saber sobre bitcoin, criptomonedas y blockchain: y no te atrevías a preguntar* (3rd ed.). Ediciones Martínez Roca.

Dot CSV. (2021, May 23rd). *HOY SÍ vas a entender QUÉ es el BLOCKCHAIN - (Bitcoin, Cryptos, NFTs y más)* [Vídeo]. YouTube. https://www.youtube.com/watch?v=V9Kr2SujqHw&list=WL&index=65&t=725s

Electron. (2022, September 16th). *About Us - Electron*. Electron -. Recovered on January 16th, 2023, from https://electron.net/about-us/

Estrategias de Inversión. (n. d.-a). ¿Qué es Cardano y cómo funciona? https://www.estrategiasdeinversion.com/herramientas/diccionario/criptomonedas/cardano-t-1825

Estrategias de Inversión. (n. d.-b). *¿Qué es una DAO y cómo funciona?* Recovered on February 11th 2023,
from https://www.estrategiasdeinversion.com/herramientas/diccionario/criptomonedas/dao-t-1833

Ethereum. (n. d.). *Ethereum Energy Consumption.* ethereum.org. https://ethereum.org/en/energy-consumption/

Ethereum. (n. d.-a). *Ethereum Whitepaper*. ethereum.org Recovered on November 27th, 2022, from https://ethereum.org/en/whitepaper/

Ethereum. (n. d.-b). *Exploradores de bloques*. ethereum.org. Recovered on December 21st, 2022, from https://ethereum.org/es/developers/docs/data-and-analytics/block-explorers/

Ethereum. (n. d.-c). *Finanzas descentralizadas (DeFi)*. ethereum.org. https://ethereum.org/es/defi/

Ethereum. (n. d.-d). *Gobernanza de Ethereum.* ethereum.org. https://ethereum.org/es/governance/

Ethereum. (n. d.-e). *Inicio.* ethereum.org. https://ethereum.org/es/

Ethereum. (n. d.-f). *Monedas estables*. ethereum.org. https://ethereum.org/es/stablecoins/

Ethereum. (n. d.-g). *Non-fungible tokens (NFT).* ethereum.org. Recovered on December 13th, 2022, from https://ethereum.org/en/nft/

Ethereum. (n. d.-h). *Organizaciones Autónomas Descentralizadas (DAO).* ethereum.org. https://ethereum.org/es/dao/

Ethereum. (n. d.-i). *Prueba de participación (PoS).* ethereum.org. Recovered on December 13th, 2022, from https://ethereum.org/es/developers/docs/consensus-mechanisms/pos/

Ethereum. (n. d.-j). *¿Qué es el ether (ETH)?* ethereum.org. https://ethereum.org/es/eth/

Ethereum. (n. d.-k). *¿Qué es Ethereum?* ethereum.org. https://ethereum.org/es/what-is-ethereum/

Ethereum's Monetary Policy - EthHub. (n. d.). https://docs.ethhub.io/ethereum-basics/monetary-policy/

Europol spotlight. (2021). *Cryptocurrencies: tracing the evolution of criminal finances.* Europol (ISBN 978-92-95220-37-9). Recovered on November 3rd 2022, from https://europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Fábregas & Asoc. ¿Qué es el blockchain y por qué debería importarte? (2018, October 23rd). Fabregas & Asoc. Recovered on January 19th, 2023, from https://www.fabregasassociats.com/que-es-blockchain/

Fang, F. (2022, February 7th). *Cryptocurrency trading: a comprehensive survey - Financial Innovation.* SpringerOpen. https://jfin-swufe.springeropen.com/articles/10.1186/s40854-021-00321-6

Fernández, Y. (2022, April 22nd). *Qué es el Dogecoin, cómo funciona y por qué se ha hecho tan popular.* Xataka. https://www.xataka.com/basics/que-dogecoin-como-funciona-que-se-ha-hecho-popular

Finematics. (2020, June 13th). *CODE IS LAW? Smart Contracts Explained (Ethereum, DeFi)* [Video]. YouTube. https://www.youtube.com/watch?v=pWGLtjG-F5c

Finematics. (2021, January 4th). *DEFI - From Inception To 2021 And Beyond (History of Decentralized Finance Explained)* [Video]. YouTube. Recovered on November 30th, 2022, from https://www.youtube.com/watch?v=qFBYB4W2tqU

Fisher, T. (2021, September 27th). *What Is a Node in a Computer Network?* Lifewire. Tech for humans. Recovered on October 16th, 2022, from https://www.lifewire.com/what-is-a-node-4155598

Fornell, J. (2023, January 17th). *Cómo saber la comisión de una transacción Bitcoin.* Bit2Me Academy. Recovered on January 30th, 2023, from https://academy.bit2me.com/como-saber-la-comision-de-una-transaccion-bitcoin/

Frax Cryptocurrency - The first fractional-reserve stablecoin. (n. d.). Frax. Recovered on November 13th, 2022, from https://frax.finance/

Fresno, B. G. del. (2018, May 3rd). *What is the difference between DLT and blockchain? NEWS BBVA.* Recovered on December 20th, 2022, from https://www.bbva.com/en/difference-dlt-blockchain/

Gastón, Í. (2022, August 26th). *¿Qué es DAI?* Bit2Me Academy. Recovered on December 12th, 2022, from https://academy.bit2me.com/que-es-dai/

Gómez, M. V. (2022, May 12th). *La OTAN promete a Finlandia una adhesión «fluida y rápida» y le ofrece protección desde la solicitud formal hasta la entrada.* El País. Recovered on June 5th 2022, from https://elpais.com/internacional/2022-05-12/la-otan-promete-a-finlandia-una-adhesion-fluida-y-rapida.html

History of Blockchain. (n. d.). Javapoint.com. Recovered on January 24th, 2023, from https://www.javatpoint.com/history-of-blockchain

IBM. (n. d.). *What is Blockchain Technology - IBM Blockchain | IBM.* Recovered on February 14th, 2023, from https://www.ibm.com/topics/what-is-blockchain

IMNOVATION. (n. d.). Aplicaciones del blockchain: lo que está por venir. IMNOVATION. Recovered on December 20th 2022, from https://www.imnovation-hub.com/es/transformacion-digital/aplicaciones-del-blockchain/?_adin=02021864894

Jiménez, I. D. (2021, June). *Análisis financiero y bursátil del Bitcoin y otras criptomonedas.* https://zaguan.unizar.es/record/100929/files/TAZ-TFG-2021-249.pdf?version=1

Kim, H. M., and Izhar Mehar, M. (2022, May 15th). *Blockchain In Commercial Insurance.* Blockchain Research Institute. Recovered on January 8th, 2023, from https://www.blockchainresearchinstitute.org/project/commercial-insurance/

Kriptomat. (n. d.). *¿Cuáles son las redes de blockchain más populares?* Recovered on January 28th, 2023, from https://kriptomat.io/es/blockchain/las-redes-de-blockchain-mas-populares/

Lamport, L., Shostak, R. & Pease, M. (1982, July 3rd). *The Byzantine Generals Problem*. Recovered November 17th, 2022, from https://lamport.azurewebsites.net/pubs/byz.pdf

Leal, A. (2020, January 8th). *Telegram asegura que su blockchain será totalmente descentralizada.* CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas. https://www.criptonoticias.com/tecnologia/telegram-asgura-blockchain-descentralizada/

Li, P. & Nelson, S. D. (2018, December). *Network structures of centralized system (left) and decentralized system (right).* https://www.researchgate.net/figure/Network-structures-of-centralized-system-left-and-decentralized-system-right_fig1_330139613

Magas, J. (2020, June 17th). *Ethereum 2.0: La elección entre un nodo propio y un servicio de staking.* Cointelegraph. Recovered on December 20th 2022, from https://es.cointelegraph.com/news/ethereum-20-the-choice-between-ones-own-node-and-a-staking-service

MAPFRE RE joins B3i (Blockchain Insurance Industry Initiative). (2021, September 24th). Mapfre RE. Recovered on January 23rd 2022, from https://www.mapfrere.com/en/news/joins-blockchain-insurance-industry-initiative/

Menezes, A. J., & Vanstone, S. A. (1991). *Advances in Cryptology - CRYPTO '90: Proceedings*. Springer Publishing.

Meta Platforms, Inc. (n. d.). Yahoo finance. Recovered on November 11th, 2022, from https://es.finance.yahoo.com/quote/META/?guccounter=1

Model S. (n. d.). Tesla Recovered January 19th, 2022, from https://www.tesla.com/models

Momtaz, P. P. (2020). *Initial Coin Offerings*. PLOS ONE, 15(5), e0233018. https://doi.org/10.1371/journal.pone.0233018

Morales, F. C. (2020, November 24th). *Diferencia entre valor y precio.* Economipedia. Recovered on December 15th, 2022, from https://economipedia.com/definiciones/diferencia-entre-valor-y-precio.html

Mougayar, W. (2016). *La tecnología de Blockchain en los negocios.* Ediciones Anaya Multimedia.

Nakamoto, S. (2008). A peer-to-peer electronic cash system. In Bitcoin.org. Recovered on August 21st, 2022, from https://bitcoin.org/bitcoin.pdf

NEO project. (n. d.). *NEO Documentation*. neo.org. Recovered on November 26th, 2022, from https://docs.neo.org/v2/docs/en-us/basic/whitepaper.html

Next. (n. d.). Technology of our Virtual Power Plant (VPP). Recovered on January 14th, 2023, from https://www.next-kraftwerke.com/vpp/virtual-power-plant

Node definition - Google Zoeken. (n. d.). Recovered on December 18th, 2022, from https://www.google.com/search?q=node+definition

OSI (Oficina de Seguridad del Internauta). (n. d.). *Historia de las criptomonedas en un clic.* Oficina de Seguridad del Internauta. Recovered on November 8th, 2022, from https://www.osi.es/es/campanas/criptomonedas/historia-criptomonedas

Oxford Dictionary. (n. d.). *Node noun - Definition.* Oxford Advanced Learner's Dictionary. Recovered on February 14th, 2023, from https://www.oxfordlearnersdictionaries.com/definition/english/node

Oxford Learner's Dictionaries. (2022). *Speculation*. In Oxford Dictionary. https://www.oxfordlearnersdictionaries.com/definition/english/speculation?q=speculation

Parmar, D. (2022, December 8th). *Las 8 mejores plataformas de blockchain para crear aplicaciones financieras modernas.* Geekflare. Recovered on January 27th, 2023, from https://geekflare.com/es/blockchain-platforms-for-finance-applications/

Pellicer, L. (2022, May 11th). *El BCE prepara el terreno para una subida de los tipos de interés en julio ante la galopante inflación*. El País. Recovered on June 5th 2022, from https://elpais.com/economia/2022-05-11/el-bce-prepara-el-terreno-para-una-subida-de-los-tipos-de-interes-en-julio-ante-la-galopante-inflacion.html

Preukschat, A., Kuchkovsky, C., Gómez Lardies, G., Díez García, D., & Molero, I. (2017). *Blockchain: la revolución industrial de internet* (1.a ed.) [EPub]. Gestión 2000.

Proposals, E. I. (n. d.). ERC. Ethereum Improvement Proposals. https://eips.ethereum.org/erc

Puig, A. (2022, July 18th). *Diferencia entre criptomonedas y tokens*. cronuts.digital. https://cronuts.digital/es/diferencia-entre-criptomonedas-y-tokens/

Sánchez, Á. (2021, May 13th). *Tesla deja de aceptar bitcoins para comprar sus coches y la criptomoneda se desploma.* El País. Recovered on January 19th 2023, from https://elpais.com/economia/2021-05-13/tesla-deja-de-aceptar-bitcoins-para-comprar-sus-coches-y-la-criptomoneda-se-desploma.html?event=go

Sánchez, A. (2022, May 11th). *El presidente de la EBA, sobre la regulación de las criptomonedas: «El objetivo no es matar la innovación, sino que se use de forma adecuada»*. El País. Recovered on June 5th 2022, from https://elpais.com/economia/2022-05-11/campa-sobre-regular-las-criptomonedas-el-objetivo-no-es-matar-la-innovacion-sino-que-se-use-de-forma-adecuada.html

Santaella, J. (2022, September 12th). *¿Cuáles son los tipos de criptomonedas más importantes?* Economia3. https://economia3.com/tipos-de-criptomonedas-mas-importantes/

Smith, G. S. (2021). *Bitcoin lo cambia todo: implicaciones sociales y económicas de la invención más importante del siglo XXI.* Ediciones Pirámide.

SolarCoin. (n. d.). SolarCoin.org. Recovered on January 16th, 2023, from https://solarcoin.org/

Suárez, K. (2022, May 12th). *El Banco de México eleva la tasa de interés al 7% para contener una inflación desbocada.* El País. Recovered on June 5th 2022, from https://elpais.com/mexico/economia/2022-05-12/el-banco-de-mexico-eleva-la-tasa-de-interes-al-7-para-contener-una-inflacion-desbocada.html

Szabo, N. (1994). *Smart Contracts*. Recovered on November 30th 2022, from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets.* Recovered on November 30th 2022, from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Talin, B. (2021, Decemeber 24th). *28 casos de uso de Blockchain – Posibles aplicaciones de la tecnología de libro mayor distribuido (DLT)*. MoreThanDigital. Recovered on December 20th 2022, from https://morethandigital.info/es/blockchain-posibilidades-y-aplicaciones-de-la-tecnologia/

TEDx Talks. (2018, November 6th). *How Smart Contracts Will Change the World* | Olga Mack | TEDxSanFrancisco [Video]. YouTube. Recovered on December 15th, 2022, from https://www.youtube.com/watch?v=pA6CGuXEKtQ

Tether. (n. d.). Recovered on December 30th, 2022, from https://tether.to/es/

The Future of Energy | Pando | LO3 Energy | Partners. (n. d.). LO3 Energy. Recovered on November 10th, 2022, from https://lo3energy.com/partners/

The Investopedia team. (2021, February 25th). *Mint Definition*. Investopedia. Recovered on August 10th, 2022, from https://www.investopedia.com/terms/m/mint.asp

Tikhomirov, S. (2018). *Ethereum: State of Knowledge and Research Perspectives*. SpringerLink. https://link.springer.com/chapter/10.1007/978-3-319-75650-9_14?error=cookies_not_supported&code=559fc531-175c-46a2-948d-73ed56995e26

Trecet, J. (2022, November 8th). *Cómo invertir en criptomonedas y cuáles son las más rentables en 2022*. Finect. https://www.finect.com/usuario/Josetrecet/articulos/invertir-criptodivisas

T3 Index. (2022, April 13th). *BitVol*. Recovered on June 14th, 2022, from https://t3index.com/indices/bit-vol/

Virtual Currency, Cryptocurrency, and Digital Assets Primer. (n. d.). Washington State Department of Financial Institutions. Recovered on February 14th, 2023, from https://dfi.wa.gov/consumers/virtual-currency/primer

VIX Price, Real-time Quote & News. (n. d.). Google Finance. Recovered on June 4th 2022, from https://www.google.com/finance/quote/VIX:INDEXCBOE?sa=X&ved=2ahUKEwjmiMbd-pX4AhVG-aQKHXWVATkQ3ecFegQIAxAg&window=1M

What Is a Node in a Computer Network? (2021, September 28th). Lifewire. https://www.lifewire.com/what-is-a-node-4155598

Zafar, T. (2022, January 4th). *Blockchain, NFT y el nuevo estándar de identidad y seguridad. Entrepreneur.* Recovered on November 29th 2022, from https://www.entrepreneur.com/es/finanzas/blockchain-nft-y-el-nuevo-estandar-de-identidad-y/409924

¿En qué se diferencian las criptomonedas de las monedas tradicionales? (2019). Davies. https://daviescoin.io/es/blog/en-que-se-diferencian-las-criptomonedas-de-las-monedas-tradicionales

¿Qué es la capitalización de mercado? (n. d.). Coinbase. Recovered on November 10th, 2022, from https://www.coinbase.com/es-LA/learn/crypto-basics/what-is-market-cap